Kropog László

A prímszámok különös világa

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tartalomjegyzék

1. Előszó

„A matematika a tudományok királynője, és a számelmélet a korona a királynő fején.”

Gauss

Az általános iskolában, amikor először hallottam a prímszámokról, teljesen lenyűgöztek. Kételkedtem abban, hogy végtelen sokan vannak. Középiskolában nem értettem, hogy miért nincs még válasz sok egyszerűnek tűnő kérdésre. Soha nem felejtem el ezeket az érdekes matematika órákat. Már akkoriban elhatároztam, ha majd többet tudok a számokról és azok természetéről, akkor szerkesztek egy számelmélettel foglalkozó könyvet.

Most végre megvalósíthatom ezt a régi tervemet! A borítón az első prímkereső algoritmust kitaláló Eratoszthenész szitájának részlete látható.

Végtelen sok prímszám van. Ennek a tételnek napjainkig a legszebb indirekt bizonyítását Eukleidész adta több mint 2300 éve. Tiszteletemet kifejezve, erre a tételre még 11 különböző bizonyítási eljárást mutatok be.

A könyvet három logikai egységre osztottam:

1. A számelmélet története.

2. Amit már tudunk, és amit még nem tudunk a prímekről.

3. Prímszámokkal kapcsolatos feladatok, és azok megoldásai.

Az első részt igyekeztem röviden és érthetően bemutatni. A második egységben vannak olyan tételek és bizonyítások, amelyek meghaladják a gimnáziumi tananyag szintjét. A hatodik fejezetben található feladatok többségének megoldásához nincs szükség az egyetemi tananyag ismeretére, tehát fiatalabb diákoknak is ajánlom a gyűjteményt.

Ha egy bizonyos témakört alaposabban szeretne megismerni, akkor arra biztatom, hogy számelmélettel foglalkozó könyvekben, honlapokon nézzen utána bővebben!

Minden matematikát, és az érdekes feladatokat kedvelő Olvasónak kívánok hasznos szórakozást, jó tanulást!

Nyíregyháza, 2021.07.02. Kropog László

2. A számelmélet története

A számelmélet csak a 17.-18. században vált önálló kutatási területté, de mégis mondhatjuk, hogy ez a matematika legrégebbi ága. Az eredete szinte minden nép esetében a számmisztikára vezethető vissza. Püthagorasz és tanítványai is az Istenekhez való felemelkedés eszközét látták benne. Őket tekinthetjük a számelmélet megalapozóinak. Olyan fogalmakat alkottak meg, mint a páros, páratlan, baráti, tökéletes, figurális számok. Ők vezették be a prímszám és az összetett szám fogalmát. Eukleidész művében találjuk a mai napig az egyik legszebb bizonyítást a prímszámok végtelenségére. Eratoszthenész zseniális algoritmust adott a prímszámok kiválogatására. Tudjuk, hogy a püthagoreusoknál csak a természetes számokat tekintették számnak. Ezeket az eredményeket akkor tudjuk igazán értékelni, ha a **2.3.** fejezetben meglátjuk, hogy milyen számírás és milyen eszközök álltak a rendelkezésükre.

A számelmélet sok szempontból különbözik a matematika többi területétől. Itt található a legtöbb megoldatlan probléma, melyeknek a vonzerejét csak növeli, hogy egyszerűen megfogalmazható és megérthető. A matematikának ez az egyetlen ága, melyben közel 1800 éven keresztül nagyon kevés fejlődés történt, Diophantosztól egészen Fermatig.

2.1. A számfogalom kialakulása és fejlődése

A természetes számokat Isten teremtette, minden egyéb az ember műve.

Kronecker

Már az ókorban jelen voltak a természetes számok mellett a törtek is. A törtekhez viszont nem kapcsolták az osztás fogalmát. Ugyanakkor ie. 2000 körül Babilonban már helyi értékes hatvanas számrendszerben írták a számokat, és bevezették a hatvanados törteket.

Ők nagyon jó közelítést adtak $\sqrt{2}$-nek, ilyen törtekkel. Nem okozott problémát, hogy a négyzet átlója nem fejezhető ki sem egész, sem tört számmal. Ez viszont már a görögöknél az irracionális szám felfedezéséhez vezetett. Ezt ők a geometria nyelvén összemérhetetlen szakaszok formájában fogalmazták meg.

A negatív számok csak nagyon későn kerültek elfogadásra a matematikában. Erre viszont az egyenletek megoldásánál szükség volt. Diophantosz még úgy ügyeskedett, hogy elkerülje a negatív számokat. Ezeket a gyököket nem fogadta el megoldásnak.

Chuquet már jelet is talált ki a negatív számoknak, de Cardano csak fiktív számoknak nevezte azokat, pedig már számolt velük. Ebben az időben Stifel a negatív számokat abszurd számoknak nevezte. Viéte sem tekintette az az egyenlet megoldásának a negatív számokat, viszont Descartes már fenntartások nélkül számolt velük. Még ekkor sem tekintették a törteket és a negatív számokat a természetes számokkal egyenjogúnak, de azért használták őket.

Még nem tisztázták a negatív számok szerepét sem, már jelentkeztek a harmadfokú egyenletek megoldásánál a képzetes számok, illetve komplex számok. Először Bombelli próbálta megalapozni a komplex számok elméletét, kevés sikerrel. Ez Argandnak és Wesselnek sikerült. Véglegesen Gauss 1831-ben tisztázta, amikor a komplex számoknak a derékszögű koordináta rendszerben való ábrázolásával minden komplex számot, mint rendezett számpárt definiált. Ezzel egy időben hasonlóan oldotta meg Hamilton és Bolyai János is, de ők tisztán aritmetikai alapon. Hamilton megpróbálta kidolgozni a számhármasok és számnégyesek algebráját is. A komplex számok $a + bi$ alakja nyomán megalkotta az $a + bi + cj + dk$ alakú kvaterniókat, ahol *a, b, c, d* valós számok, az *i, j, k* pedig egységek.

Ez az elmélet nagy vitákat szült a matematikusok körében. Azonban Charles Pierce, Georg Frobenius és Joseph Cartan kidolgozták a kettőnél több egységet tartalmazó számok elméletét, az ún. hiperkomplex számokat. Ekkor a kvaterniók is elfogadottá váltak az asszociatív számrendszerek világában. Ha az $a + bi + cj + dk$ kvaternióban $a = 0$, akkor tiszta kvaterniónak nevezzük. Minden tiszta kvaterniónak megfelel egy háromdimenziós vektor. Hamilton azért vezette be a kvaterniókat, hogy elvégezhető legyen az osztás a vektorok között. Ezzel egy időben Grassmann megalapozta a vektorelméletet, így ő már eljutott az n-dimenziós vektor fogalmához. Ezt követően William Clifford ezt továbbfejlesztve megalkotta a bikvaterniókat. Ezek $a + b\varepsilon$ alakú számok, ahol a és b komplex számok, ε^2 pedig $+1, -1, vagy\ 0$ lehet. Ezzel alkalmas számokat talált a nemeuklideszi geometriában a mozgások leírásához.

A számfogalom fejlődése az algebra területén történt. Ezt igazolja a következő általánosítás: A racionális számokat az $ax + b = 0$ egész együtthatós elsőfokú egyenlet megoldásainak is tekinthetjük. Ebből ered az algebrai szám fogalma is.

Fermat foglalkozott olyan számokkal, amelyek egész együtthatójú algebrai egyenlet gyökei lehetnek. Definíciója szerint: Algebrai számoknak nevezzük azokat a számokat, amelyek gyökei lehetnek az alábbi *n*-edfokú egész együtthatójú algebrai egyenletnek:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Ezt a gondolatot egészítette ki Lejeune Dirichlet a következővel: Egésznek nevezzük azokat az algebrai számokat, melyek gyökei lehetnek az alábbi *n*-edfokú egész együtthatójú algebrai egyenletnek:

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Ezek szerint a racionális számok azok, melyek az $a_1 x + a_0 = 0$ egész együtthatójú elsőfokú egyenletnek gyökei lehetnek.

Kummer dolgozta ki 1842-ben az algebrai számok elméletét. Georg Cantor bizonyította be, hogy léteznek nem algebrai komplex számok is. Igazolta ugyanis, hogy az algebrai számok halmaza megszámlálható számosságú. Mivel a komplex számok halmaza kontinuum számosságú, ezért kell lennie olyan komplex számnak, amelyik nem algebrai szám. Az ilyen számokat Euler után transzcendens számnak nevezzük. Kissé meglepő, de a valós számok között is vannak transzcendens számok, sőt végtelen sok. Először a π-ről és az e számról derült ki, hogy transzcendens szám. Heinrich Lambert 1766-ban igazolta, hogy a π és az *e* irracionális számok. Charles Hermite 1873-ban a π-ről, Ferdinand Lindemann 1882-ben az *e* számról mutatta ki, hogy transzcendens. Cantor bizonyítása igazolja, hogy végtelen sok transzcendens szám létezik a komplex és a valós számok között is, de nem adott módszert ezek megkeresésére. Ezt tette lehetővé még a Cantor bizonyítása előtt megszületett Liouville tétel (1851).

Ahhoz, hogy a tételt pontosan meg tudjuk fogalmazni, nézzük meg az algebrai szám fokának a meghatározását. Definíció: Ha egy *z* algebrai szám kielégít egy *n*-edfokú ($n \geq 1$) egész együtthatós algebrai egyenletet, de nem elégít ki egyetlen alacsonyabb fokú ilyen egyenletet sem, azt mondjuk, hogy a *z* *n*-edfokú algebrai szám.

Például a $\sqrt{5}$ másodfokú algebrai szám, mert kielégíti az $x^2 - 5 = 0$ egyenletet, de nem lehet gyöke egyetlen $ax + b = 0$ alakú egyenletnek sem. A fejezet elején már volt arról szó, hogy egy irracionális algebrai számot lehet közelíteni racionális számok sorozatával, például ($\sqrt{2}$).

Ha z n-edfokú valós algebrai szám (ahol $n > 1$, valamint p és q relatív prímek), akkor elég nagy q esetén:

$$\left|z - \frac{p}{q}\right| > \frac{1}{q^{n+1}}$$

Vagyis a q nevezőjű törtekkel elég nagy q esetén a z-t $\frac{1}{q^{n+1}}$-nél nagyobb pontossággal nem lehet megközelíteni. Ezzel a feltétellel sikeresen tudott transzcendens valós számokat keresni. Az alábbi z transzcendens szám, ha $q > 1$:

$$z = 1 + \frac{1}{q} + \frac{1}{q^{1\cdot 2}} + \frac{1}{q^{1\cdot 2\cdot 3}} + \cdots + \frac{1}{q^{1\cdot 2\cdot 3\cdot \cdots \cdot n}} + \cdots$$

Az algebrai számoknak a racionális számokkal való megközelítésével többen is foglalkoztak. Axel Thue tovább élesítette Liouville egyenlőtlenségét úgy, hogy $(n + 1)$ helyére $\left(\frac{n+2}{2} + \varepsilon\right)$-t írt, ahol ε tetszőlegesen kicsi valós szám. Carl Ludwig Siegel pedig bebizonyította, hogy $(n + 1)$ felcserélhető $2\sqrt{n}$-re Végül Klaus Fridrich Roth az $(n + 1)$ kifejezést $(2 + \varepsilon)$-ra cserélte, ahol $\varepsilon > 0$.

Az egyik legnehezebbnek tűnő problémát 1900-ban a párizsi matematikai kongresszuson Hilbert vetette fel: A $2^{\sqrt{2}}$ transzcendens szám-e?

Közel harminc évig azt sem tudták belátni, hogy irracionális szám. Új módszereket kidolgozva (a matematikában fontos szerepet játszó számok transzcendens voltának bizonyítására) egymástól függetlenül igazolta Siegel és Gelfond, hogy transzcendens szám. Tételükben kimondták, hogy minden α^{β} alakú szám, (ahol α a 0-tól és 1-től különböző algebrai szám és β legalább másodfokú algebrai szám) transzcendens.

A komplex számokat oszthatóság szempontjából először Gauss kezdte vizsgálni. Rájött, hogy az $a + bi$ komplex számok körében, ahol a és b irracionális szám, az oszthatóság alaptulajdonságai megmaradnak. Ezeket Gauss-egészeknek nevezzük. Meglepő, hogy minden Gauss-féle egész egyben egész algebrai szám is, de fordítva nem igaz.

A számfogalmat sokféle szempontból lehet általánosítani. Nagyon különös általánosítást talált ki Kürschák József. Bevezette a p-adikus számokat az alábbi módon:

Legyen p egy rögzített prímszám, és legyenek $a_0, a_1, a_2, \cdots, a_n, \cdots$ a p-nél kisebb nem negatív egész számok.

Az $a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_n p^n + \cdots$, végtelen összeget (ha létezik) p-adikus egész számnak nevezzük. Ez a számfogalom, amely nagyon mesterkéltnek tűnik, jelentős alkalmazásra talált a hatványsorok elméletében.

Egy másik érdekesség, a negatív alapú számrendszer. A negatív alapú számrendszerek helyi értékes számjelölési rendszerek, ahol az alapszám negatív. Általában felteszik, hogy az alapszám -1-nél kisebb. Ezekben a számrendszerekben is ábrázolható minden valós szám. A negatív számok előjel nélkül is ábrázolhatók, viszont a számok összehasonlítása és a műveletek bonyolultabbak lesznek. Az előjelről szóló információt a szám hossza tárolja, a negatív számok egy jeggyel hosszabbak az ellentettjüknél. Hogy pozitív alapú megfelelőjüktől megkülönböztessék ezeket a számrendszereket, annak neve elé teszik a *nega*- előtagot. Például a -2 alapú számrendszer negabináris, a -3 alapú negaternáris, a -10 alapú negadecimális, és így tovább.

Tekintsük a 12 243 ábrázolás jelentését, ahol az alap -10:

b^4 többszörösei	b^3 többszörösei	b^2 többszörösei	b^1 többszörösei	b^0 többszörösei
(10000)	(-1000)	(100)	(-10)	(1)
1	2	2	4	3

Mivel 10 000 + (−2000) + 200 + (−40) + 3 = 8163, a negadecimális 12 243 jelentése 8163 a tízes számrendszerben.

Elsőként Vittorio Grünwald foglalkozott negatív számrendszerekkel a *Giornale di Matematiche di Battaglini* című művében, ami 1885-ben jelent meg. Grünwald algoritmusokat adott az összeadásra, kivonásra, szorzásra, osztásra, gyökvonásra, oszthatóság megállapítására és a más számrendszerre való áttérésre. Később egymástól függetlenül újra felfedezte A. J. Kempner 1936-ban és Zdzisław Pawlak és A. Wakulicz 1959-ben.

Z. Pawlak és A. Lazarkiewicz elképzelései alapján a lengyel Matematikai Intézet Varsóban 1957 és 1959 között megépítette a BINEG nevű számítógépet, amely implementálta a negabináris számrendszert. Azóta a megvalósítások ritkák.

Használata:

Jelölje az alapot -r. Ekkor minden egész szám egyértelműen felírható, mint:

$$a = \sum_{i=0}^{n} d_i \cdot (-r)^i$$

Ahol minden d_k egy 0 $és$ $r - 1$ közötti egész, és az első jegy pozitív, ha az n is pozitív. Ekkor az a egész -r alapú számrendszerben $d_n d_{n-1} \cdots d_1 d_0$ alakú.

A negatív alapú számrendszerek összehasonlíthatók az előjeles jegyeket használó számrendszerekkel, köztük a kiegyensúlyozott hármas alapú számrendszerrel. Az előjeles jegyek lehetnek pozitívak vagy negatívak is, amit nyomokban, több nyelvben is fellelhetünk. A kiegyensúlyozott hármas számrendszerben a számjegyek 0, 1 és -1, ezekkel a jegyekkel minden valós szám felírható.

Vannak számok, amelyek a -r alapú számrendszerben ugyanúgy néznek ki, mint az r alapú számrendszerben. Erre triviális példák a nem negatív egy jegyű számok. Kevésbé triviális a 107 a tízes és a negadecimális számrendszerben. Hasonlóan, a

$$17 = 2^4 + 2^0 = (-2)^4 + (-2)^0$$

Így 10001 a kettes számrendszerben, és 10001 a negabináris számrendszerben. Negatív alapú számrendszerben a negatív számok páros, a pozitív számok páratlan hosszúak.

Néhány szám pozitív és a megfelelő negatív alapú számrendszerben:

Decimális	**Negadecimális**	**Bináris**	**Negabináris**	**Ternáris**	**Negaternáris**
-5	15	-101	1111	-12	21
-4	16	-100	1100	-11	22
-3	17	-11	1101	-10	10
-2	18	-10	10	-2	11
-1	19	-1	11	-1	12
0	0	0	0	0	0
1	1	1	1	1	1
2	2	10	110	2	2
3	3	11	111	10	120
4	4	100	100	11	121
5	5	101	101	12	122
6	6	110	11010	20	110
7	7	111	11011	21	111
8	8	1000	11000	22	112
9	9	1001	11001	100	100
10	190	1010	11110	101	101
11	191	1011	11111	102	102
12	192	1100	11100	110	220
13	193	1101	11101	111	221
14	194	1110	10010	112	222
15	195	1111	10011	120	210
16	196	10000	10000	121	211
17	197	10001	10001	122	212

2.2. Egyiptom és Babilon matematikája

Az i.e. IV. évezredben, ezekben a kultúrákban fejlődött ki az írás és a számírás.

Egyiptom:

Az Ó birodalom (i.e. 3000-i.e. 2000) idején alakult ki a képírás és a számírás. Ekkor épültek a nagy piramisok is. Ezt az írást hieroglifikusnak nevezzük. A hieroglifa görögül szent bevésést jelent. A hieroglif számírás jegyei a papiruszon tollal való írásra történő áttéréskor hieratikus (papi) számjegyekké módosultak. Az i.e. 700 körüli időben újabb változat alakult ki, a démotikus (népi).

Az ókori Egyiptom matematikáját két nagy és néhány kisebb töredék papirusz alapján ismertük meg. Az egyik a Rhind-papirusz, amit Henry Rhind skót régész vásárolt 1858-ban és a British Múzeumnak ajándékozott. Ezt egy Ahmesz nevű írnok másolta i.e. 1650 körül egy korábbi eredetiről. Ez a papirusz 5,5 méter hosszú, 32 cm széles és 84 gyakorlati feladat megoldását tartalmazza. Nem található rajta matematikai indoklás, illetve bizonyítás sem. A másik a moszkvai papirusz, amit az orosz kereskedő, Golenyisov vásárolt meg 1893-ban. Ez 5 méter hosszú, de csak 8 cm széles és 25 feladat megoldása található rajta.

Az egyiptomi hieratikus írást a kutatók sokáig nem tudták megfejteni. Ez a francia Champollionnak sikerült a rosette-i kő alapján, amelyet Napóleon zsákmányolt a hadjárata során 1799-ben. Ezen a kőtáblán, három nyelven ugyanaz a szöveg olvasható. Görög, hieroglifikus, és démotikus írással. Mivel ismerték a görög írást, így le tudták fordítani a papiruszok szövegét is. A matematikai elemzéseket Neugebauer német matematikus végezte el.

Ezekből a papiruszokból kiderült, hogy az egyiptomiaknak 10-es számrendszerük volt, de a számírásuk nem helyi értékes. Ennek következtében minden tízes egységnek külön jelölése volt. A helyi érték hiánya miatt a matematikájuk additív jellegű.

A törtek ismerete és használata az egyiptomi matematika egyik legkülönösebb vonása. A Rhind-papirusz egy táblázattal kezdődik, amely tartalmazza a $\frac{2}{n}$ alakú törtek törzstörtek (az 1 számlálójú törtek) összegére bontását minden páratlan *n*- re 5-től 101-ig. Az $\frac{1}{2}$ mellett az $\frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}$ törteket tekintették természetes törteknek. Később kialakultak a tetszőleges törzstörtek, vagyis az egység tetszőleges részekre való osztásának fogalma.

A többi törtet – a szorzás fogalmának hiánya miatt – nem egy törzstört többszöröseként fogták fel, hanem törzstörtek összegeként. Például a $\frac{2}{97}$ nem $2 \cdot \frac{1}{97}$, hanem $\frac{2}{97} = \frac{1}{56} + \frac{1}{679} + \frac{1}{776}$. Érdekes, hogy a $\frac{2}{n} = \frac{1}{n} + \frac{1}{n}$ felbontást nem használták. Például:

$$\frac{2}{5} = \frac{1}{3} + \frac{1}{15} \quad vagy \quad \frac{2}{13} = \frac{1}{8} + \frac{1}{52} + \frac{1}{104}$$

Több feladatban is a szorzás és osztás összeadásra (kétszerezésre) történő visszavezetését láthatjuk. A 32. feladat a $13 \cdot 12$ szorzást az alábbi módon oldja meg:

$*$ 1	12
2	24
$*$ 4	48
$*$ 8	96
13	156

Tehát mindig kétszereztek és a $*$-gal megjelölt részösszegeket összeadták.

Még érdekesebb az osztás visszavezetése összeadásra. A kérdést nem úgy tették fel, hogy mennyi 45 osztva 5- tel, hanem: Számolj ötösével egészen 45-ig!

1	5 $*$
2	10
4	20
8	40 $*$
9	45

Ha nem egész szám volt az eredmény, akkor a törttáblázattal oldották meg. Például: Számolj ötösével egészen 43-ig!

1	5
2	10
4	20
8	40 ∗
8	40

A maradék 3-ra újabb feladat jött: Számolj ötösével, míg 1-et kapsz!

∗ 1	$\frac{1}{5}$
∗ 2	$\frac{2}{5} = \frac{1}{3} + \frac{1}{15}$
3	$\frac{1}{5} + \frac{2}{5} = \frac{1}{5} + \frac{1}{3} + \frac{1}{15}$

Tehát:

$$\frac{43}{5} = 8 + \frac{1}{3} + \frac{1}{5} + \frac{1}{15}$$

Ezzel a módszerrel tudtak szorozni törtet törttel, illetve egészet törttel osztani. A papiruszokon található feladatok nagy része konkrét gyakorlati jellegű, de a megoldásokból látszik, hogy egyszerű egy ismeretlenes egyenleteket is meg tudtak oldani. Ezeket nem algebrai úton oldották meg, hanem a hamis feltevés módszerével, aritmetikai eszközökkel. Ilyen a Rhind-papirusz 26. feladata: Egy sokaság és negyede összesen 15. Mennyi a sokaság? Legyen a sokaság 4, ennek a negyede 1, ez összesen 5. Az 5-öt 3-szor kell venni, hogy 15 legyen, ezért a 4-et is 3-szor kell venni. Tehát a sokaság 12.

$$4 + \frac{1}{4} = 5 \;\; \Rightarrow x + \frac{x}{4} = 15$$

Babilónia:

Babilóniában az egyiptominál lényegesen magasabb színvonalat ért el a matematika. Az ismereteik rögzítésére égetett agyagtáblákat használtak, melyekből mintegy 400000 darabot találtak meg régészek. Ezek közül 50 matematikai szöveget tartalmazó és kb. 200 szövegnélküli számolás.

Az ékírás megfejtésében szintén egy háromnyelvű kőtábla segített, a behisztuni kő. A tábla óperzsa, elámi és babilóniai (akkád) szövegéből a német Grotefend és az angol Rawlinson értelmezte az írásjeleket. A matematikai táblák elemzését Neugebauer és Van Der Waerden végezte el.

Ezekből kiderül, hogy a 60-as helyi értékes számrendszert használták. A számok írását két jelre építették fel: az ▼ álló ék, amely értéke 1, és a ◄ fekvő ék jelére, amely értéke 10 volt. Hiányzott viszont az egyértelmű számolvasáshoz a hatvanados vessző (törteknél), illetve a helypótló (nulla) jel. A nullára később bevezettek egy jelet, de a végén nem jelölték, így a pontos értékre csak a szöveg alapján lehetett következtetni. A helyi érték elvét alkalmazták a törtekre is, ami kivételes dolognak tekinthető.

A babilóniaiak a számításokat táblázatok segítségével végezték. Volt reciprok, szorzás, négyzet, négyzetgyök, köb, köbgyök táblázatuk is. Ezek mellett az algebrájukban fontos szerepet játszó $n^3 + n^2$ táblázat. Tudtak szorozni, az osztást a reciprok táblázattal visszavezették szorzásra. Csak olyan számok reciprokait képezték, amelyek véges hatvanados törteket adtak, vagyis a számok prímtényezős felbontásában csak a 60 prímtényezői fordultak elő. Az ilyen számokat szabályosnak nevezték. Például:

$$\frac{1}{600} = \frac{1}{2^3 \cdot 3 \cdot 5^2} = \frac{2 \cdot 3}{2^4 \cdot 3^2 \cdot 5^2} = \frac{6}{60^2}$$

Egy osztást ezek után így végeztek el:

$$\frac{91}{600} = 91 \cdot \frac{1}{600} = 91 \cdot \frac{6}{60^2} = \frac{9 \cdot 60 + 6}{60^2} = \frac{9}{60} + \frac{6}{60^2}$$

A szorzásnak ez a módja megmutatja, hogy az egyiptomiaknál fejlettebb volt a törtfogalmuk. Egy tetszőleges számlálójú törtet nem törzstörtek összegeként, hanem egy törzstört többszöröseként fogták fel. Azonban két szám hányadosaként még nem értelmezték.

Az algebrájuk is fejlettebb volt. Meg tudtak oldani másodfokú egyenleteket és egyenletrendszereket. Ismerték az $(a \pm b)^2$ és az $a^2 - b^2$ azonosságokat. A negatív szám fogalma még nem alakult ki. Talán a legnagyobb eredményük a $\sqrt{2}$ pontos megközelítése az iteráció elvével. Ez az öt tizedes jegyre pontos eredmény az amerikai Yale Egyetemen őrzött 7289-es agyagtáblán olvasható. Ez az iteráció Newton módszeréhez hasonló.

Az egyiptomiak csak a 3, 4, 5 Pitagoraszi számhármast ismerték, míg Babilóniában a képzésük szabályát is.

$$a = p^2 - q^2, \qquad b = 2pq, \quad c = p^2 + q^2, \quad ahol \;\; p > q$$

Ezt az amerikai Columbia Egyetem *Plimpton 322* jelű táblája igazolja.

2.3. A Görög matematika

Az egyiptomi és babilóniai kultúra hanyatlásával egy időben egy új nép indult fejlődésnek, a görög. Az ismeretanyag nagy részét átvették az előző két nagy birodalomból, de azt minőségileg egy új szintre emelték. A konkrét gyakorlati példák helyett, az általános eljárásra, állítások megfogalmazására és bizonyítására törekedtek. Ezzel elkezdődött a matematika egy új korszaka: a deduktív elemi matematika. Két korszakot különböztetünk meg:

A. Eukleidész előtti kor (i.e. VI.- III. sz.)

B. Hellenisztikus kor (i.e. 334.- i.e. 30.)

A.

Az első számírásos emlékek a mükénéi kultúra idejéből származnak az i.e. 1500-as évekből. A számjegyek tízes számrendszerre utalnak. A számok képzése hasonló az egyiptomihoz, vagyis egymás mellé írták a számjegyeket, balról kezdve a legnagyobbal. A jegyek értékét össze kell adni.

Az első igazi görög számírás az attikai volt. Ez is hieroglifikus volt, de más számjegyekkel. Ez az ötös és tízes rendszer keveréke. A legrégebbi leletek i.e. VIII. századból valók és ez időszámításunk kezdetéig használatos volt. Kevés számjegyet használtak, de a számok felírása így hosszú volt.

Az ábécé kifejlődése után alakult ki az un. alfabetikus számírás, amely betűkkel jelölte a számokat. (például $\alpha = 1;\ \beta = 2; 1000 =, \alpha; 2000 =, \beta$) A tudományban i.e. 500-tól ezt a számírást használták. Hogy a számokat megkülönböztessék a szövegtől, egy vonalat húztak fölé. Például, a következő szám: $\overline{,\varepsilon\delta\lambda\alpha} = 5231$. A számok felírása rövidebb lett, de a műveletek elvégzése nagyon bonyolult volt. A hétköznapi életben a számoló tábla (abakusz) segítségével számoltak, attikai számjegyekkel és az egyiptomi szorzás módszerével. Az abakuszon történő számábrázolás tulajdonképpen a helyi érték szerinti elrendezést jelenti. A görög matematikusok feltehetően azért nem jöttek rá a helyi érték elvére, mert nem volt rá szükségük. Geometriai szemléletük miatt a számokat is szakaszoknak tekintették. Ilyen eszközök használatával nagyszerű eredményeket értek el a számelméletben is, melyekre a mai napig csodálattal nézünk fel.

A görög matematika első nagy alakjai a milétoszi Thalész és a számoszi Püthagorasz.

Munkájukat csak későbbi kommentárokból és utalásokból ismerjük. Thalész főleg filozófus volt. A matematikán belül csak geometriával foglalkozott. Püthagorasz egy filozófiai iskolát alapított, ahol nagyon sok geometriai problémával foglalkoztak. Többek között:

1. A kör négyszögesítése (π).

2. A kocka kettőzése ($\sqrt[3]{2}$).

3. Egy szög harmadolása.

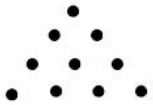
4. Szabályos sokszögek szerkesztése.

Sokkal jelentősebb a munkásságuk az aritmetika területén, hiszen őket tekintjük a számelmélet megalapozóinak. Filozófiájuk alapgondolata ugyanis az volt, hogy a világ lényege a szám. Ezeket önállóan létező szubsztanciáknak tekintették. Felfogásuk szerint a világ lényegének vizsgálata a számok vizsgálatát jelenti. Náluk az őselem az egység, amelyből minden szám, azaz minden dolog ered. Minden létezőnek száma van, minden viszony számviszonyokkal fejezhető ki. felfedezték, hogy a zenei harmónia kifejezhető számviszonyokkal, és ezt kiterjesztették az egész világra.

Pitagorasz nevezte el a világegyetemet kozmosznak (szép rend). Több számelméleti problémájuk is e számmisztikához kötődik. Az egyes számoknak különleges jelentést tulajdonítottak. Az egy nem igazi szám, hanem az egység, amelyből a többi szám származik. Az egy a lényeg száma. A kettő az első női szám, az ellentét száma.

A három az első férfi szám és a harmónia jelképe, mert az egység és a különbözőség összege. A négy az igazság száma, mert a különbözőség önmagával való szorzata. Az öt a házasság jelképe, mert az első női és férfi szám összege. A hat a teremtés száma, mert Isten ennyi nap alatt teremtette a világot. A legszentebb szám a tíz volt. Összege volt a világ gyökereinek tekintett 1, 2, 3, 4 számoknak, így a világ teljességét jelképezte.

A szent *tetraktüsz:*



A pitagoreusok ismerték a prímszám, összetett szám, páros és páratlan szám fogalmát. A számokat különböző formákban rakták ki kavicsokkal. Így jutottak el a figurális számokhoz. Fehér és fekete kavicsokkal felváltva rakták ki két sorban a férfi és női számokat, így jutottak el a páratlan és páros számok fogalmához. Azokat, amelyek kirakhatók két ugyanannyi kavicsot tartalmazó sorba, felezhetőknek (páros számnak) nevezték. A többi szám pedig nem felezhető (páratlan szám). Ezt a módszert folytatva adódnak a vonalszámok és a síkszámok. Az előzőek nem bonthatók tényezőikre, ezért csak egy sorban rakhatók ki (prímszámok). A síkszámok két tényezőre bonthatók, ezért kirakható téglalap alakban (összetett számok). A téglalap számok közül azokat, amelyek két egyenlő tényező szorzatára is bonthatók (vagyis kirakható négyzet alakban), azok a négyzetszámok. Hasonlóan adódik a köbszám is. Ezeket az elnevezéseket a mai napig használjuk. Figurális módszerrel kerestek püthagoraszi számhármasokat is. Írjuk egymás alá a négyzetszámokat és a páratlan számokat:

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**
1	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**	**19**

Az alsó sor minden négyzetszáma a fölötte lévő kettővel együtt Pitagoraszi számhármas.

Ők vezették be a tökéletes számok és a barátságos számpárok fogalmát is. Tökéletes az a szám, ami előáll az osztóinak összegeként, a számot nem beleértve.

A legkisebb ilyen szám a hat. ($6 = 1 + 2 + 3$). A tökéletes elnevezés azért van, mert Isten hat nap alatt teremtette a világot. (Megjegyzés: Eukleidész bebizonyította, hogy ha $2^n - 1$ prímszám, akkor $2^{n-1} \cdot (2^n - 1)$ tökéletes. Később Euler megmutatta, hogy minden páros tökéletes szám ilyen alakú. Ma sem tudjuk, hogy létezik-e páratlan tökéletes szám. Jelenleg összesen 27 darab tökéletes számot ismerünk, a legnagyobb 13395 számjegyből áll.)

Barátságos az a számpár, ha az egyik előáll a másik részeinek összegeként és viszont. Az első ilyen számpár a 220 és 284. (Megjegyzés: A következő számpárt- 17296 és 18416- Fermat találta. Euler újabb hatvan számpárt talált. Érdekes, hogy növekvő sorrendben a második számpárt – 1184 és 1210- egy tizenhat éves olasz diák találta meg 1866-ban. Ma már minden 10^9-nél kisebb barátságos számpárt ismerünk.)

Vizsgálták a számok oszthatóságának kérdését is. A pitagoreusok a zene és arányok tanulmányozása után a következő közepeket és aránypárokat használták:

1. Számtani közép:

$$A = \frac{m+n}{2}$$

2. Mértani közép:

$$G = \sqrt{m \cdot n}$$

3. Harmonikus közép:

$$H = \frac{2 \cdot m \cdot n}{m+n}$$

4. Zenei aránypár:

$$\frac{m}{A} = \frac{H}{n}$$

5. Tökéletes aránypár:

$$\frac{A}{G} = \frac{G}{H}$$

6. Aranymetszés:

$$\frac{n}{m} = \frac{m}{n+m}$$

A pitagoreusok filozófiájára döntő csapást hozott, amikor felfedezték, hogy két szakasz nem minden esetben összemérhető. Erre két probléma kapcsán jöttek rá:

1. Milyen arány van egy négyzet oldala és átlója között? ($\sqrt{2}$)

2. Milyen arány van egy kör kerülete és átmérője között? (π)

Az első kérdés megoldhatatlanságára éppen Pitagorasz tétele vezette rá őket. Az összemérhetetlen szakaszok létezése azt is jelenti, hogy a szakaszok halmaza bővebb a számok halmazánál. Jelentőségét ők is azonnal felismerték, de hosszú időn keresztül titokban tartották. Amikor Hippaszosz (i.e. 450 körül) elárulta a titkot, kizárták a pitagoreusok szövetségéből és megölték. A pitagoreusok számainak „mindenhatósága" véget ér, ha összemérhetetlen szakaszok arányát kell meghatározni. (Megjegyzés: Az irracionális szám definíciója oldotta meg a kérdést több mint kétezer évvel később.) Ez a tény vezetett az aritmetika és a geometria szétválásához, mégpedig úgy, hogy a görög matematikában a geometria került vezető szerepkörbe.

B.

A hellenizmus kora a makedóniai Nagy Sándor hódításaival kezdődött és Egyiptom római uralom alá kerülésével végződött. A kor tudományos központja az I. Ptolemaiosz egyiptomi király által alapított alexandriai Műszóéin lett. Ezt az intézményt (egyetemet) anyagi eszközökkel is támogatta. Óriási könyvtára volt, melyet Eratoszthenész vezetett. A matematikai részleget pedig Eukleidész irányította. A görög matematika aranykorának négy legnagyobb alakja:

1. Eukleidész (Alexandria)

2. Arkhimédész (Szirakuza)

3. Apollóniosz (Perga)

4. Eratoszthenész (Küréne)

1. Eukleidész (ie. 365?-300?)

Alexandriában I. Ptolemaiosz által alapított Muszeion nevű intézmény (egyetem) matematika részlegének a vezetője. A híres könyvtárban mintegy 700.000 kéziratot őriztek, a kor legnagyobb művészei és tudósai itt találkoztak egymással. A törvény szerint, aki a városba érkezett, annak le kellett adnia a nála lévő kéziratot. Azt a könyvtárban helyezték el és a másolatát adták vissza.

Eukleidész életéről szinte semmit sem tudunk. Két anekdota maradt fenn róla. Proklosz szerint, amikor Ptolemaiosz megkérdezte tőle, hogyan lehetne a geometriát egyszerűen elsajátítani, Eukleidész azt felelte: „ A geometriához nem vezet királyi út.” A másik elbeszélés szerint, amikor az egyik tanítványa megkérdezte, hogy mi haszna van a geometria tanulásának, a mester szólt az egyik szolgának, hogy adjon a diáknak három oboloszt, mert hasznot akar a tanulmányaiból.

A munkáiról lényegesen többet tudunk. Fő munkája az Elemek (Sztoikheia). Ez egy összefoglaló mű, amely a kor matematikai ismereteit szedi rendszerbe. Csak geometria és az aritmetika témáit tartalmazza. Nem lehet megkülönböztetni a saját eredményeit a felhasznált forrásoktól. Ezt tekinthetjük az első egyetemi matematika jegyzetnek. E könyvtől több példányszámban, kiadásban csak a Biblia jelent meg! Közel 2000 évig alapműnek tekintették. A szigorúan logikai alapon, deduktív felépítése tette a művet halhatatlanná.

Az első latin nyelvű fordítását 1126-ban Abelard készítette arab nyelvről. Nyomtatásban először Velencében jelent meg 1482-ben. Magyarul két fordítás létezik: Brassai Sámuel (1865) és Mayer Gyula munkája 1983-ból. A 13 könyvből álló anyagot 5 axiómára és 5 posztulátumra építette fel Eukleidész. Ezek alapján bizonyította a 465 tételt. A prímszámok végtelenségére a mai napig ő adta a legegyszerűbb és legelegánsabb indirekt bizonyítást! A rendszer néhány hiányosságát (Rendezési tulajdonságok) Hilbert a 20. század végén javította ki.

Az első könyvben találhatók azok az alapfogalmak és axiómák, amelyekre a deduktív rendszer épül. Ennek a láncolatnak a végpontjai az axiómák, amelyeket az Elemek posztulátumoknak nevez, axiómák alatt logikai alapelveket ért.

Az öt axióma:

1. Egy és ugyanazzal egyenlők egymással is egyenlők.

2. Egyenlőkhöz egyenlőket adva, az összegek is egyenlők lesznek.

3. Egyenlőkből egyenlőket kivonva, a maradékok is egyenlők lesznek.

4. Az egymással egybevágók egyenlők egymással.

5. Az egész nagyobb a résznél.

Az öt posztulátum:

1. Két ponton át egyenes húzható.

2. Az egyenes szakasz korlátlanul meghosszabbítható.

3. Bármely középpontból bármely sugárral kör írható.

4. A derékszögek mind egyenlők egymással.

5. Ha két azonos síkban fekvő egyenest egy harmadik metsz, akkor a két egyenes a harmadiknak azon az oldalán metszi egymást, amelyiken a keletkező belső szögek összege két derékszögnél kisebb.

2. Arkhimédész (i.e. 287-212)

Az ókor legnagyobb matematikusa és fizikusa volt. Tanulmányai több könyvben is fennmaradtak. Három geometriai munkája: 1. A körmérésről. 2. A parabola kvadratúrájáról.

3. A spirálisokról. További két műve térgeometriával foglalkozik. Két fizikai könyve ismert:

1. A síkidomok egyensúlyáról. 2. Az úszó testekről. Nagyszerű aritmetikai munkája: A homok megszámlálásáról.

Mint már említettük, az alfabetikus számírásban – a helyi érték és a nulla hiányában – nagyon nehéz volt számításokat végezni. Ezért a görögök szinte át sem lépték a tízezres számkört. Arkhimédész kidolgozott egy módszert, amely lehetőséget adott a természetes számok korlátlan folytatására. Olyan számrendszert épített ki, amely a tízes alapra épül.

Csoportosítási módszerének kulcsszáma 10^8 (oktád=nyolc) volt:

$$\left.\begin{array}{c} 1 - 10^8 \ első\ oktád \\ 10^8 - 10^{8\cdot 2}\ második\ oktád \\ \dots \\ 10^{8\cdot(10^8-1)} - \ 10^{8\cdot 10^8}\ oktádadik\ oktád \end{array}\right\} Első\ periódus$$

$$\left.\begin{array}{c} 10^{8\cdot 10^8} - 10^{8\cdot 10^8+8}\ első\ oktád \\ 10^{8\cdot 10^8+8} - 10^{8\cdot 10^8+8\cdot 2}\ második\ oktád \\ \dots \\ 10^{8\cdot 10^8+8\cdot(10^8-1)} - \ 10^{2\cdot 8\cdot 10^8}\ oktádadik\ oktád \end{array}\right\} Második\ periódus$$

$$\dots$$

$$\left.\begin{array}{c} 10^{8\cdot 10^8\cdot(10^8-1)} - 10^{8\cdot 10^8\cdot(10^8-1)+8}\ első\ oktád \\ 10^{8\cdot 10^8\cdot(10^8-1)+8} - 10^{8\cdot 10^8\cdot(10^8-1)+8\cdot 2}\ második\ oktád \\ \dots \\ 10^{8\cdot 10^8\cdot(10^8-1)+8\cdot(10^8-1)} - \ 10^{10^8\cdot 8\cdot 10^8}\ oktádadik\ oktád \end{array}\right\} Oktádadik\ periódus$$

Ezek után rátért a világegyetemben lévő homokszemek megszámolására. Arisztarkhosz a világegyetem középpontjának a Napot, sugarának a Nap és az állócsillagok távolságát tekintette. Arkhimédész szerint ez a sugár annyiszor nagyobb Nap-Föld távolságnál, mint ahányszor az utóbbi nagyobb a Föld sugaránál. A világegyetem sugarára így 10^{10} stadiont kapott. Megbecsülte egy homokszem nagyságát és kiszámította, hogy a világegyetemben 10^{63} homokszem fér el. A munka legnagyobb érdeme, a végtelen nagy szám gondolata. Ezek után érthetetlen, hogy nem alkotta meg a helyi értékes számrendszert.

Ezt a munkáját Apollóniosz bírálta, mire Arkhimédész egy feladattal válaszolt neki. Mint már említettük, a pitagoreusok használták a figurális számokat (háromszög szám, négyzetszám). A feladat a következő:

„ Ha ilyen jól ismered a nagy számokat, akkor számold össze a marhákat! Mennyi szarvasmarha legelt valaha Szicília mezein? A marhák színük szerint csoportosulva négy gulyában legeltek, úgymint egy fehér, egy fekete, egy sárga és egy foltos gulya. Mindegyik gulyában pedig a bikák voltak többségben, mégpedig ilyen eloszlásban:

1. A fehér bikák száma egyenlő a sárga bikák száma plusz a fekete bikák $\frac{1}{2}$ $és$ $\frac{1}{3}$ része.

2. A fekete bikák száma egyenlő a sárga bikák száma plusz a foltos bikák $\frac{1}{4}$ $és$ $\frac{1}{5}$ része.

3. A foltos bikák száma egyenlő a sárga bikák száma plusz a fehér bikák $\frac{1}{6}$ $és$ $\frac{1}{7}$ része.

4. A fehér tehenek száma a teljes fekete gulyának $\frac{1}{3}$ $és$ $\frac{1}{4}$ része.

5. A fekete tehenek száma a teljes foltos gulyának $\frac{1}{4}$ $és$ $\frac{1}{5}$ része.

6. A foltos tehenek száma a teljes sárga gulyának $\frac{1}{5}$ $és$ $\frac{1}{6}$ része.

7. A sárga tehenek száma a teljes fehér gulyának $\frac{1}{6}$ $és$ $\frac{1}{7}$ része.

Ha ebből kiszámolnád, hogy mennyi bikát és tehenet számlál egy-egy gulya, meglehet, hogy nem vagy járatlan a számok tudományában, de még semmiképp nem sorolhatod magad a bölcs emberek közé. Forgasd tovább elmédet és vedd észbe a következőket is:

8. A fehér bikák plusz a fekete bikák száma együtt négyzetes szám.

9. A foltos bikák plusz a sárga bikák száma együtt háromszög szám.

Az ókori matematikusok már kiszámolták, hogy az első hét feltételnek eleget tevő legkisebb szám 50 389 082. A nyolcadik és a kilencedik feltétel azonban nagyon megnehezíti a feladatot. Kétezer éven keresztül nem is történt komoly lépés a megoldás felé, egészen 1880-ig. Ekkor egy német matematikus kiderítette és bizonyította, hogy a legkisebb megoldás egy 206545 számjegyből álló tízes számrendszerbeli szám, melynek első négy számjegye:7766. (Ez kb. 30 oldalt tenne ki ilyen karakterméret esetén ebben a könyvben!)

A pontos megoldást 1976-ban találta meg Harry Nelson a Lawrence Livermore Laboratórium munkatársa egy Cray-1 típusú szuperszámítógéppel. Ilyen feladatot, amelyet kétezer év után sikerül megoldani, csak egy matematikai zseni képes kitalálni.

Matematikai szempontból Arkhimédész legfontosabb eredménye, hogy az Eudoxosz által kitalált kimerítési módszert olyan pontosan kidolgozta, ami az integrálszámítás korai felfedezésének tekinthető.

Arkhimédész kiemelkedő számolási készsége megmutatkozik abban is, hogy az irracionális számokat nagy pontossággal meg tudta becsülni. Például $\sqrt{3}$-ra a következő becslést adta:

$$1{,}73202\cdots = \frac{265}{153} < \sqrt{3} < \frac{1351}{780} = 1{,}73205\cdots$$

Ez négy tizedesre pontos becslést jelent.

Arkhimédész tudta, hogy a π értékét nem lehet pontosan kiszámítani. Beírt és köré írt szabályos 96 oldalú sokszög segítségével a π-re az alábbi becslést adta:

$$3 + \frac{10}{71} < \pi < 3 + \frac{1}{7}$$

Sírkövére azt a tételt vésték, amelyre a legbüszkébb volt. Egy henger térfogatának és a beírt gömb térfogatának és a beírt kúp térfogatának aránya:

$$V_H : V_G : V_K = 3 : 2 : 1$$

3. Apollóniosz (ie. 262-190)

Több témában is írt tudományos műveket. A legjelentősebb a kúpszeletekről szóló 8 kötetes *Kónika*. Ezek mellett főleg síkbeli geometriával foglalkozott. Algebrai munkái nem maradtak fenn, ezért munkásságával bővebben nem foglalkozunk.

4. Eratoszthenész (ie. 276?-196?)

Tegyünk említést Eratoszthenészről is, akit Bétának becéztek, mivel minden tudományágban a második legbölcsebbnek tartottak. Ő volt az Alexandriai Könyvtár vezetője. Talán a legjelentősebb eredménye, hogy a Föld kerületét (Egyenlítő hossza) ki tudta számolni (40 000 km) szögméréssel és hasonlóság felhasználásával. Ez az adat a mai ismereteink szerint is nagyon jó közelítés. Ezt felhasználva pontosan meg tudta határozni a Nap és a Hold sugarait, továbbá az égitestek távolságát is.

A matematikában a prímszámok meghatározására szolgáló szitája révén maradt fenn a neve. A szita működése:

Felírjuk a számokat egymás után. A 2 prímszám, tehát az összes többszörösét kihúzhatjuk a felsorolásból. A 3 prímszám, tehát az összes többszörösét kihúzhatjuk a felsorolásból. Az 5 prímszám, tehát az összes többszörösét kihúzhatjuk a felsorolásból. Ezt a módszert tovább folytatva, a végén már csak prímszámok maradnak. Eratoszthenész a számtáblázatát egy pergamen lapra írta fel, majd egy keretre szerelte és a prímszámokat átszúrta. A laikus nézelődők azt hitték, hogy egy furcsa szitát készít, ezért nevezték el Eratoszthenész szitájának. Ettől hatékonyabb prímszámkereső algoritmust csak a huszadik század második felében sikerült találni.

(Megjegyzés: Egy 10x10-es szita látható a könyv borítóján.)

2.4. Matematika a Római korban (i.e. 30.- i.sz. 641.)

Az antik társadalom utolsó korszaka a Római birodalom kora. Ekkor már Egyiptom és Görögország is gyarmati sorba került. A kort a matematika hanyatlásának szokták nevezni. Ez igaz az elméleti geometriára, de a matematikának a gyakorlathoz közelebb eső ágaiban születtek új eredmények.

Előrelépés főleg a trigonometriában és az algebrában történt, ugyanis feladták az irracionalitás problémájának a megoldását. A római kor jellegzetes alakjai a kommentátorok lettek. Ők összefoglaló könyveikben közzétették és magyarázták a klasszikus eredményeket, egyszerűsítették a gondolatmeneteket. A tudomány fejlesztése helyett annak terjesztése, tanítása lett fontosabb.

Jelentőségük abban is megmutatkozik, hogy nagyon sok korábbi munkát csak az ő műveikből ismerjük. A tovább lepéshez szükség lett volna egy algebrai jelölésrendszer és egy könnyen kezelhető számírás kidolgozására.

A római korban a görög matematika központja továbbra is Alexandria maradt. Emellett működött az athéni akadémia is, de csak másodlagos szerepben. Az ekkor született matematikai eredmények főleg három személyhez és három témakörhöz köthetők:

1. Ptolemaiosz (II. század): Trigonometriai táblázata, amely a csillagászathoz kapcsolódott.

2. Diophantosz (III. század): Megteremtette a geometriától független algebrát.

3. Papposz (IV. század): A projektív geometria megalkotása mellett nagyon jelentős a kommentátori munkássága.

1. Ptolemaiosz:

Főleg csillagász volt, ezért számára nélkülözhetetlen volt a trigonometria. Fő műve a tizenhárom kötetes Matematikai Gyűjtemény. Arab fordításban maradt fenn Almageszt címmel. Legérdekesebb része az első kötetben található szinusz- táblázat, amit a csillagászok több mint ezer évig használtak. A babilóniaiak után ő is 360 részre osztotta a teljes kört és hatvanados törtekkel számolt. Saját tétele alapján ki tudta számolni két szög összegének, illetve különbségének húrját a szögek húrjából. Mai jelölésekkel:

$$\sin(\alpha \pm \beta) = \sin\alpha \cdot \cos\beta \pm \sin\beta \cdot \cos\alpha$$

Ezt követően a Püthagorasz tétel felhasználásával kitalálta az alábbi felezési szabályt is:

$$2 \cdot \left(\sin\frac{\alpha}{2}\right)^2 = 1 - \cos\alpha$$

Ezek felhasználásával táblázata $0{,}5°$-tól kezdve fél fokonként tartalmazta $180°$-ig a szögek húrjait, vagyis közelítőleg a szinuszait.

2. Diophantosz:

A kor legnagyobb matematikusa volt, akit az algebra megalapozójának tekintünk. határozatlan egyenletek megoldásával foglalkozott. Számelméleti eredményei mellett megkezdte az algebrai jelölésrendszer kidolgozását is. Fő műve a tizenhárom kötetes Aritmetika, amelyből csak az első hat kötet maradt fenn. Ezek 189 egyenlet megoldását tartalmazzák. Diophantosz megengedett pozitív racionális megoldásokat, ma azonban csak az egész számok körében keressük az ilyen típusú egyenletek gyökeit.

Könyvében használ szórövidítéseket, amelyek révén megtette az első lépést a pusztán szavakat használó retorikus algebrától a mai szimbolikus algebra felé. Őt nevezhetjük a törtvonal feltalálójának is. A törteket a maihoz hasonlóan jelölte, csak a nevező volt felül és a számláló alul. (A sorrendet később a hinduk fordították meg.)

Diophantosz jelölései:

Jelölés	**Jelentése**
ι	egyenlő
δ	ismeretlen
$\overset{\circ}{M}\ vagy\ \overset{\circ}{\mu}$	egység
Δ^γ	az ismeretlen négyzete
K^γ	az ismeretlen köbe
$\Delta^\gamma\Delta$	az ismeretlen a negyediken
ΔK^γ	az ismeretlen az ötödiken
$K^\gamma K$	az ismeretlen a hatodikon
ϯ	kivonás

Volt még jele az ismeretlen reciprokára és annak hatványaira is. Az összeadásnak nincs jele, mert azt az egymás után írás fejezte ki. Ő a $4x^3 + 3x^2 - 2x + 12 = 5$ egyenletet az alábbi módon írta volna le:

$$K^\gamma\bar{\delta}\Delta^\gamma\bar{\gamma}\text{ϯ}\delta\bar{\beta}\ \overset{\circ}{M}\ \bar{\iota}\beta\iota\bar{\varepsilon}$$

3. Papposz:

Ő volt a görög matematika utolsó jelentős alakja. Fő műve a nyolc kötetes Gyűjtemény, amely átfogó képet ad az egész görög matematikáról és önálló eredményeket is tartalmaz. Négy új közepet definiált, majd megmutatta, hogy a 10 lehetséges közép a mértani középből levezethető. Mivel főleg geometriával foglalkozott, ezért a bővebb ismertetéstől most eltekintünk.

Az első két századból még említsük meg Menelaosz és Héron nevét. Menelaosz fő műve a Szphairika a gömbháromszögtannal foglalkozik. Több sík-és gömbháromszögre vonatkozó tételt fogalmazott meg.

Héron matematikus, fizikus és feltaláló is volt. Két matematikai könyve maradt ránk: a Geometria és a Metrika. Az elsőben szerepel a háromszög területét meghatározó képlete bizonyítással együtt:

$$T = \sqrt{s(s-a)(s-b)(s-c)}\,, ahol\ s = \frac{K}{2}\ \text{és a háromszög oldalai: } a, b, c$$

Nála a szakasz bármilyen számot jelenthet, az irracionális számot pedig a gyakorlatban közelíti meg. Nézzük a következő példát: Egy háromszög oldalai 7, 8, 9 egység. Mekkora a területe? A képlet szerint $T = \sqrt{720}$. Mivel ez nem irracionális szám, ezért azt mondja, hogy számítsuk ki a legkisebb hibával. Ezt egy iterációval oldja meg. Ha a megoldás törtekhez vezet, akkor nem a hatvanados törteket használja, hanem az egyiptomi törzstörteket:

$$\sqrt{720} \approx 26 + \frac{1}{2} + \frac{1}{3}$$

A **római számírás** az ókori Rómából származó számjelölési rendszer. A rendszer elve szerint néhány kiválasztott betűnek számértéket adnak, és ezek kombinációival írják le a számokat. A római számrendszer additív számrendszer, amely azt jelenti, hogy egy szám értékét a számrendszer jeleinek összevonásából lehet létrehozni. A felhasznált betűk a latin ábécéből származnak:

1	**5**	**10**	**50**	**100**	**500**	**1000**
I	**V**	**X**	**L**	**C**	**D**	**M**

Nagyobb számok helyes leírása a következő módon történik: először az ezresek, aztán a százasok, aztán a tízesek, végül az egyesek. Például:

1988 = M + CM + LXXX + VIII = MCMLXXXVIII

A rövidítés nagy számoknál nem megengedett, mégis használatos:

1998 = M + CM + XC + VIII = MCMXCVIII, de e helyett használatos az MIIM és az IIMM forma is.

Az I csak V illetve X előtt állhat!

A római számírásban a következő (nem mindig betartott) szabályokat alkalmazzák:

- egymás mellé maximum 3 egyforma szimbólum írható;
- ha kisebb értékű szimbólum a nagyobbat követi, az összeadást jelent;
- ha pedig a kisebb a nagyobbat megelőzi, az kivonást.

Ily módon minden szám ábrázolható I-től MMMDDDCCCLLLXXXVVVIII-ig (4998). Nagyobb számok írásához azonban új csomószámokat és alapjeleket ("számjegyek") kell bevezetni.

A korai időszakban a fenti betűket használták, de a többszörözésre 4 ezer felett az I és egy fordított C szimbólumot „Ↄ” használtak. Később ezt megváltoztatták: egy vízszintes vonal a betű felett ezerszerest jelölt, a betű mindkét oldalán szereplő függőleges vonal pedig százszorost jelölt.

Példák:

$$\overline{\mathrm{I}} = 1000, \qquad \overline{\mathrm{V}} = 5000, \qquad \overline{|\mathrm{I}|} = 100\,000, \qquad \overline{|\mathrm{V}|} = 500\,000$$

Ugyanezt a felülvonást más értelemben is használták, ezzel jelezték, hogy az adott betű számként értelmezendő.

Az idők folyamán egyes számértékek jelölése eltérő lehetett. Így találhatunk 4 értékben IIII-t és IV-t is, hasonlóan 8 értékben VIII-t és IIX-et is. Még furcsább a 99 jelölésére az XCIX helyett az IC. Előfordult, hogy ugyanabban a dokumentumban ugyanazokat a számértékeket más-más formában jegyezték le.

Rekonstruált római kori abakusz:

A római számokat a 14. században elkezdték kiszorítani az arab számok. Napjainkban leginkább sorszámozásra, fejezetszámozásra, valamint dinasztiák neveiben használatosak a római számok. Ezen kívül általában régi épületeken az építés évét jelzik, illetve órák számlapján használjuk.

A reneszánsz idején általános volt, hogy a könyvek első oldalára egy latin szöveget helyeztek el, amelyben összeadva az I, V, X, L, C, D, M betűket, az eredmény a könyvkiadás dátuma lett.

Templomok és más épületek bejárata fölött is hasonlóan olvasható az építés évszáma. Az ilyen számot tartalmazó feliratokat kronogrammának nevezik.

A legismertebb magyar vonatkozású kronogramma a Siculicidium, a madéfalvi vérengzés évszáma:

2.5. Kínai számírás

A kínai matematika fejlődésének történetét LI JANG hat korszakra osztotta:

1. A „boldog” őskor (i.e.2700-i.e.210): HUANG TI-dinasztiától a HAN-dinasztia kezdetéig.

2. Az ókor (i.e.210-i.sz.600): HAN-dinasztia kora.

3. A késői ókor (600-1368): A TANG-, a SZUNG- és a JUAN-dinasztiák ideje.

4. Az újkor (1368-1750): A MING- és a CSING-dinasztia időszaka.

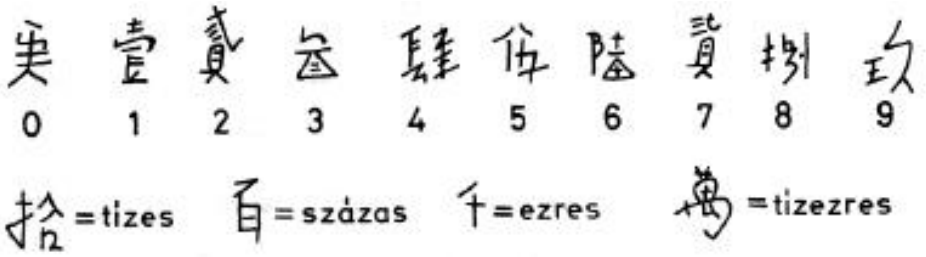
5. Az újabb kor (1750-1949):

6. A jelenkor (1949-):

Ezek közül a legnagyobb fejlődés a 3. szakaszban történt. Ezt CSIN CSIU-SAO, CSU SI-CSIE és LI JE neve fémjelezi. Ebben a korszakban a kereskedelem és a kulturális élet széles körű kapcsolatot alakított ki Indiával, Mezopotámiával, a közép-keleti országokkal, Koreával, Japánnal. Ehhez képest a 4. szakasz hanyatlást hozott, nem születtek új eredmények. Ekkor jelentek meg a nyugati híttérítők, akik elhozták Euklidész tanait. Az 5. szakaszban a matematikusok egy része még mindig a régi „receptszerű” számítási szabályokkal foglalkozott. Azonban már volt egy csoport, amelyik a nyugati matematikát befogadta. Az ő munkájukat dicséri, hogy 1859-ben LI SAN-LAN és VAILI megírták az első kínai nyelvű differenciál- és integrálszámítás könyvet. Ezek után nézzük meg részletesebben a kínai matematika történetét.

Az Első Császár könyörtelenül szembefordult a hagyományokkal. Elégettette az összes korábbi feljegyzéseket i.e. 213-ban. A könyvrejtegető tudósok közül több, mint 400-t élve eltemettek, több ezret pedig a Nagy Fal építésére vittek el. Az ő uralkodásától kezdve lehet egységes Kínai Birodalomról beszélni. A birodalomra kiterjedő egységes törvényeket, naptárt, pénzt, mértékegység-rendszert és írást vezettek be. SI HUANG nagy könyvégetésének esett áldozatul Kína első igazi matematika könyve, a *Csiu csang szuan su* (Matematika kilenc fejezetben). Ez egy i.e. 250-körül keletkezett összefoglaló mű volt. A későbbi korokban ezeket igyekeztek felkutatni, majd LIU HUJ kiegészítette egy tizedik könyvvel. Így lett a címe: *Szuan csing*. (Tíz Klasszikus).

Kínai számírás:



Ezek után nézzük meg néhány kiemelkedő matematikus munkásságát:

1. CSANG CSIU-CSIEN (5. század)

A *Szuan csing* 246 feladata közül 92 az ő műve. Foglalkozott számelméleti kérdésekkel, sorozatokkal és magasabb fokú egyenletekkel. Nála találkozunk először a számtani sorozat összegképletével. Négyzetgyökvonásnál a következő közelítő képletet használta:

$$\sqrt{a^2+b} \approx a + \frac{b}{2a+1}$$

2. CSIN CSIU-SAO (1202?-1261?)

Ránk maradt munkáiban szerepelnek olyan számelméleti feladatok, amelyeket ma kongruencia-rendszerekkel oldunk meg. Foglalkozott magasabb fokú egyenletekkel, sorozatokkal és geometriai problémákkal is. A számolótáblán végzendő gyökvonásra olyan módszert használt (ezt indokolta is), melyet ma Horner-elrendezésnek nevezünk. Horner előtt 500 évvel írta le az eljárást!

3. LI JE (1178-1265)

Kortársa volt CSIN CSIU-SAO-nak, de egymástól függetlenül dolgoztak az algebra ugyanazon területén. Írásaik jól kiegészítik egymást. Két művét ismerjük. Az elsőt 1248-ban írta, *A körmérés tengeri tükre* címmel. Ebben részletes geometriai elmélet és 170 szerkesztési feladat található. Másik könyve 1259-ből származik, amelynek címe: *Új lépések a matematikában*. Ez algebrával foglalkozik. A magasabb fokú egyenletek megoldásánál ő is használta az „égi elemek módszerét”, vagyis a Horner-elrendezést. Használta a negatív számokat. Az utolsó számjegyét egy ferde vonallal húzta át, hogy meg lehessen különböztetni. Kubiláj kán 1260-ban kormányzói állást ajánlott fel neki, de nem fogadta el.

4. CSU SI-CSIE (1280?-1303?)

A *Szung-dinasztia* utolsó nagy matematikusa. Életéből 20 évet „vándormatematikusként” töltött el. Két műve maradt ránk. Az elsőt 1299-ben írta: *Bevezetés a matematikába*. A másik 1303-ból való, *A négy elem jáspis tükre* címmel. Ez a négyismeretlenes egyenletrendszer ismeretleneit jelöli. Ügyesen oldott meg a Horner-elrendezéssel magasabb fokú egyenleteket. Nem csak az egész megoldásokat kereste, hanem a racionális gyököket is meghatározta. Sokat foglalkozott sorozatokkal is. Ismerte a négyzetszámok összegét:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

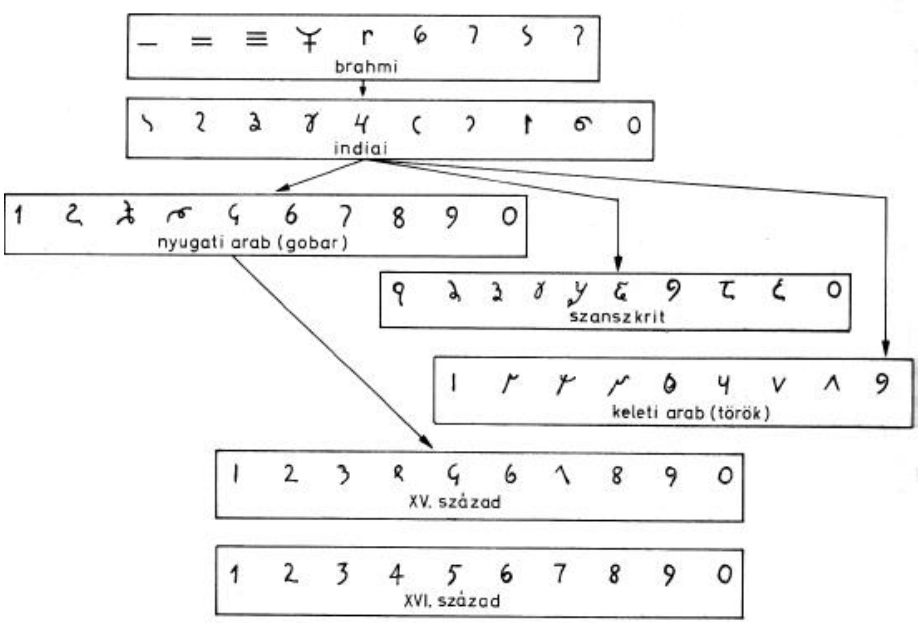
Második könyvében szerepel a következő egyenlőség:

$$1 + 8 + 30 + 80 + \cdots + \frac{n^2(n+1)(n+2)}{1 \cdot 2 \cdot 3} = \frac{n(n+1)(n+2)(n+3)(4n+1)}{5!}$$

Kombinatorikai munkáiból kiderül, hogy ismerte a binomiális-tételt és a Pascal-háromszöget is!

Kínai szuan-pan abakusz, a 15. században terjedt el:

2.6. Hindu matematika



A hindu matematika kevésbé épült a görög örökségre, mint pl. az arab. A legnagyobb eredményének talán a tízes alapú helyiértékes számírást tekinthetjük. A számírás i.e. 300 körül jelent meg kétféle alakban (*brahmi* és a *kharoszti*). Mindkettő 10-es alapú alfabetikus volt (nem helyiértékes). A *brahmi* számírás jegyeiből alakult ki a ma is használt számjegyek.

A következő fontos lépés a helyiérték és a nulla megjelenése volt a *Sziddhánták* verses szinusz-táblázataiban. A nullát jelentő *szunja* (üresség) szó már a negyedik században megjelent, de az ezt jelölő kis kör első írásos emléke 595-ből származik. Egyszerűsége és használatának előnyei ellenére Európában csak a 16. század végére fogadták el teljesen. Tehát 1000 év kellett hozzá! Az új számírás lehetővé tette az aritmetika és az algebra további fejlődését. Ezt a hinduk, majd később az arabok el is végezték.

Az első hindu matematikai írások, a „Zsinórszabályok”, a vallás szent könyveivel (Védák) egyidőben keletkeztek. Ismerték a különböző síkidomok szerkesztését, öt Pitagoraszi-számhármast, a Pitagorasz-tételt és egyéb tételeket. A $\sqrt{2}$ értékét öt tizedesjegy pontossággal határozták meg:

$$\sqrt{2} = 1 + \frac{1}{3} + \frac{1}{3 \cdot 4} - \frac{1}{3 \cdot 4 \cdot 34} = 1{,}4142157$$

A hindu matematika fejlődésében a következő lépcsőt a csillagászati *Sziddhánták* jelentették. Ismerték a szinusz és a koszinusz fogalmát. Három kiemelkedő matematikust meg kell említeni.

1. Arjabhatta (476-550?)

A hindu matematika és csillagászat eredményeit 499-ben összegezte. Nézzünk két példát a számítási műveletek elvégzésére. Ezek sokkal egyszerűbbek, mint a római számokkal.

1. Összeadás. Pl. $345 + 488$

egyesek összege:	$5 + 8 = .13$
tízesek összege:	$4 + 8 = \ 12.$
százasok összege:	$3 + 4 = 7..$
összegek összege:	833

2. Rácsos szorzás.

A szorzási műveletet megkönnyítő „gelosia” algoritmus Európában a XIV. század elején vált ismertté. Nevét a korai olasz építészet geometrikus, osztott rácsos ablakkereteiről kapta. Az eszköz már az arab számok használatára épül. A számolás menete:
Első lépésként egy négyzetrácsos hálót kell készíteni, amelynek – a legfelső sorát, és jobb szélső oszlopát kivéve – átlósan felosztjuk a kis négyzeteit úgy, ahogy az ábrán is látható.
Második lépésként az tényezőket helyezzük el benne. Az egyiket a legfelső sorba, a másikat pedig a jobb szélső oszlopba írjuk, ahová fentről lefele kezdjük el írni a számot.
Harmadik lépésként az átlósan felosztott négyzetekbe az adott négyzethez tartozó oszlop tetején és az adott négyzethez tartozó sor jobb végén lévő számjegy szorzatát írjuk, úgy hogy a tízeseket az átló fölé, az egyeseket az átló alá írjuk, ha nincs tízes vagy egyes, akkor nullát írunk a helyére.
Negyedik lépésként megkapjuk a két szám szorzatát, úgy hogy a ferde sávok mentén összeadjuk a számjegyeket. A jobb alsó sávtól indulunk el – ez adja az eredmény legkisebb helyértékű számjegyét – és haladunk bal sáv felé, ami pedig a legnagyobb helyértéket adja. Ha egy sávban az összeg két számjegyű, akkor az első számjegyet a felette és tőle balra lévő sáv összegéhez adjuk.

1	8	1	6	
0 / 7	5 / 6	0 / 7	4 / 2	7
0 / 2	1 / 6	0 / 2	1 / 2	2
0 / 5	4 / 0	0 / 5	3 / 0	5

7·1 az 7, az átló alá 7-t felé pedig 0-t írunk. 7·8 az 56, az átló alá 6-t felé pedig 5-t írunk. 7·1 az 7, az átló alá 7-t felé pedig 0-t írunk. 7·6 az 42, az átló alá 2-t felé pedig 4-t írunk. 2·1 az 2, az átló alá 2-t felé pedig 0-t írunk. 2·8 az 16, az átló alá 6-t felé pedig 1-t írunk. 2·1 az 2, az átló alá 2-t felé pedig 0-t írunk. 2·6 az 12, az átló alá 2-t felé pedig 1-t írunk. 5·1 az 5, az átló alá 5-t felé pedig 0-t írunk. 5·8 az 40, az átló alá 0-t felé pedig 4-t írunk. 5·1 az 5, az átló alá 5-t felé pedig 0-t írunk. 5·6 az 30, az átló alá 0-t felé pedig 3-t írunk.
Leírjuk a **0**-t. 5+3+2=10 leírjuk a **0**-t az előző számjegytől balra, majd a következő sávhoz adjuk az 1-t. 1+0+0+2+1+2=6. Leírjuk a **6**-t. 5+4+6+0+7+4=26 leírjuk a **6**-t az előző számjegytől balra majd a következő sávhoz adjuk a 2-t. 2+0+2+1+6+0=11. Leírjuk az **1**-t, az előző számjegytől balra majd a következő sávhoz adunk 1-t. 1+0+7+5=13 leírjuk a **3**-t, az előző számjegytől balra majd a következő sávhoz adunk 1-t. 1+0=1 leírjuk az **1**-t.
A szorzat: 1316600.

2. Brahmagupta (598-660)

Fő műve, a verses formában írt 12 kötetes matematikai és 8 kötetes csillagászati ismereteket foglalta össze. Számításaiban gyakran használta az aránypárokat. Nála találkozhatunk először a negatív szám fogalmával (pozitív-vagyon, negatív-adósság). Az általános iskolában ma is így magyarázzák el a tanulóknak! A másodfokú egyenletek általános tárgyalását is ő végezte el először a matematika történetében. Módszere a teljes négyzetté alakítás volt, amit ezért hindu módszernek is neveznek. Ő volt az első, aki határozatlan (Diophantoszi-egyenletek) egyenletek megoldhatóságának kritériumait és általános megoldását meghatározta.

3. Bhászkara (1114-1185?)

A hindu matematika utolsó és egyben a legnagyobb alakja. Fő műve a négy részből álló *Sziddhánta- sironámi* (A tudományok koszorúja). Ebből az első kettő foglalkozik matematikával, a többi csillagászattal. Sikeresen foglalkozott első- és másodfokú határozott és határozatlan egyenletek megoldásával, illetve lineáris egyenletrendszerekkel is. Kiemelkedő eredményeket ért el az úgynevezett Pell-féle egyenletek vizsgálatában. Pell előtt 500 évvel!

A hindu matematikusok tisztában voltak a számtani sorozat összegével, az első *n* természetes szám négyzetösszegével, ismerték a Pascal-háromszöget is. A legnagyobb érdemük az, hogy összeolvasztották a 10-es számrendszer és a helyiérték fogalmát a nulla használatával. Ezzel hozzájárultak a későbbi korok matematikai fejlődéséhez.

2.7. Az arab matematika

Az arabok igyekeztek átvenni a meghódított népek magasabb kultúráját. Elsősorban a görög filozófia, matematika, csillagászati munkák után érdeklődtek, de a hindu matematikát is ismerték. Sok mű az ő fordításuknak köszönhetően maradt fenn. Euklidész *Elemek* című művét 50 arab matematikus fordította le. Így maradtak ránk a hindu *Brahmaguppa Sziddhanták* írásai is. HARUN AL-RASID kalifa nagy könyvtárat (egyetemet) alapított, melynek csillagvizsgálója is volt. Említsünk meg néhány kiemelkedő matematikust.

1. AL-HVARIZMI (780?-850?)

Az ő műveiből vette át Európa az algebrát és a helyiértékes számírást. Több matematikai és csillagászati írását ismerjük. A 825-ben megjelent könyvéből az „al-dzsabr” (helyrerakás) szót a nyugati arabok „al-gebr”-nek ejtették, ebből alakult ki a latin fordítások után az algebra szavunk. Szerinte az aritmetikában közönséges számokkal van dolgunk, míg az algebrában (egyenletek megoldásában) három féle „szám” van: 1. gyök 2. négyzetszám 3. közönséges pozitív szám. Első-és másodfokú egyenleteket vizsgálva hat típust különböztetett meg. Erre a negatív számok hiánya miatt volt szükség. Mai jelölésekkel:

$$1.\, x = b \quad 2.\, x^2 = b \quad 3.\, x^2 = bx \quad 4.\, ax^2 + bx = c \quad 5.\, x^2 + c = bx \quad 6.\, bx + c = x^2$$

Amiben felülmúlja a hindukat, az a megoldások indoklása és minden lépés logikus alátámasztása volt. Nem csak egyedi eljárásokat ír le, hanem általános megoldási módokat dolgoz ki és minden mozzanatot magyaráz is. Ez volt az oka a könyv több évszázadig tartó népszerűségének.

2. ABUL-VAFA (940-998)

Korának neves matematikusa és csillagásza volt Bagdadban. Lefordította és magyarázta Euklidész és Diophantosz műveit. Két önálló munkája maradt fenn. Nála található az első bizonyítása a kétszeres és a félszögekre vonatkozó Addíciós-tételnek. Bevezette a tangens szögfüggvényt és bizonyította a gömbháromszögtan szinusz-tételét. Új szinusz táblázatot készített 15 perces szögemelkedéssel 8 tizedes pontossággal!

3. OMAR KHAJJAM (1048-1131)

Harmadfokú egyenleteket oldott meg kúpszeletek segítségével. Negyedfokú egyenletekkel azért nem foglalkozott, mert azok a valóságban nem léteznek, ugyanis szerinte negyedik dimenzió nincs. Negatív számokat ő sem használt, így a harmadfokú egyenleteknek 27 típusát kellett vizsgálnia. Egy általános harmadfokú egyenlet a következő alakra hozható:

$$x^3 + bx^2 + cx + d = 0$$

Vezessük be az alábbi helyettesítést, amely egy parabola egyenlete:

$$x^2 = 2py$$

Ekkor a következő hiperbolát kapjuk:

$$2pxy + 2bpy + cx + d = 0$$

Az eredeti egyenlet megoldásait a hiperbola és a parabola metszéspontjainak *x* koordinátái adják. Az érdemei közé tartozik még, hogy az arányokat is igyekezett számoknak tekinteni (racionális szám fogalmának a kialakítása). Adott közelítő eljárásokat az irracionális számokhoz, vagyis elindította azt a folyamatot is, amelynek révén az irracionális számok később elnyerték a „szám” rangját. Ezzel nagyban hozzájárult a valós számok fogalmának a kialakításához is. Érdekes, hogy a negatív számokat nem tudta „szám”-nak tekinteni! A műveiben megtalálható kéttagú kifejezések különböző pozitív hatványai, vagyis a binomiális együtthatókat ismerte. Valószínűsíthető, hogy a kínaiaktól függetlenül jött rá a Pascal-háromszögre.

4. AL-KÁSI (?-1429)

Az arab matematika utolsó kiemelkedő alakja. Főként a számolási módszerek fejlesztésében ért el sikereket. Sajnos Európa a műveit későn ismerte meg, csak az eredmények „újrafelfedezése" után. Legjelentősebb írása, „*Az aritmetika kulcsa"* 1427-ben jelent meg. Ezen kívül még két fontos matematikai és több csillagászati értekezése is ismert.

Az aritmetika kulcsa öt könyvből áll. Itt található az első ismertetés a tizedes törtekről és a velük lehetséges műveletek szabályairól. Ezeket a hatvanados törtekkel párhuzamosan tárgyalja. A hatványalakban való számoláshoz megadja a negatív kitevőkkel való szorzás, osztás szabályait. Ezzel egységessé tette az egész és törtszámok írásának és a műveletek módját. Megadta a tizedes és a hatvanados törtek egymásba való átváltását is. Írásaiban megtalálható a harmadfokú egyenletek iterációval történő megoldása (Horner-elrendezés) A tetszőleges természetes szám kitevővel való gyökvonás lineáris interpolációval. AL-KÁSI arra volt a legbüszkébb, hogy pontosabban adta meg a π értékét, mint előtte bárki. (16 tizedes pontossággal) Ezt az *Értekezés a körről* című munkájában jegyezte le. Arkhimédész módszerét követve kiszámolta a $3 \cdot 2^{28}$ oldalú sokszög kerületét, és ezt elosztotta a sokszög köré írható kör sugarával. Olyan trigonometrikus táblázatokat készített, ami 9 jegyre volt pontos.

Egy másik felfedezése: Először Ptolemaiosz módszerével eljutott $\sin 3°$ értékéhez. Ezután levezette a szögharmadolás képletét Ptolemaiosz-tételéből és Euklidész azon tételéből, amely szerint a kör két egymást metsző húrja szeleteinek szorzata egyenlő. A képlet mai jelölésekkel:

$$\sin 3\alpha = 3 \cdot \sin \alpha - 4 \cdot (\sin \alpha)^3$$

Ez ma emelt szintű matematikai tananyag a gimnáziumban. Az ő munkáiban is megjelenik a Pascal-háromszög, vagyis a Binomiális-tétel ismerete.

2.8. A középkor és a reneszánsz matematikája

Az európai középkor az egyetlen olyan időszak, amelyhez gyakran hozzáteszik a „sötét” jelzőt. Ennek van is bizonyos alapja. A 6.-11. században megszakadt a kapcsolat a Kelettel, ahol a tudomány tovább fejlődött, míg Európában visszafejlődött.

A római birodalom nyugati, latin nyelvű részének az iskolai oktatás megszervezése a legnagyobb érdeme. A pedagógia történetének első államilag kinevezett és fizetett tanára a római QUINTILIANUS (35?-96?) volt. A retorikáról írt könyvét egészen a 19. századig használták. Ő alkotta meg az első iskolai tantervet, amit a középkorban „hét szabad művészet” néven ismertek. Az alsó csoportját a grammatika, retorika és a dialektika (*trivium*) alkották. A triviális jelző ma is őrzi az emlékét, mint az egyszerű szinonimáját. Ezekre épült a *quadrivium*: aritmetika, geometria, asztronómia és a zene. Ő írta le a matematika oktatás értelmét: „Élesíti az elmét, előmozdítja a felfogás gyorsaságát. Nem akkor használ, amikor már megtanulta valaki, hanem azon közben, amíg megtanulja.”

A középkorban a kolostorok voltak a kultúra fényei, ahol rendszeres oktatás folyt latin nyelven, a hét szabad művészet szerint. A középkor iskoláit a gépies memorizálás jellemezte. A számok írása római számjegyekkel történt. Ebből- a matematika szempontjából-, sivár korból is kiemelhetünk néhány nagyszerű gondolkodót:

1. BOETHIUS (480?-524)

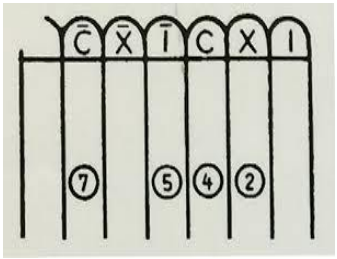
Előkelő római családból származott. Ő volt a középkor uralkodó filozófiai irányzatának, a *skolasztikának* a megalapozója. Latinra fordította Euklidész, Arisztotelész és Platón műveit. Írt egy matematika könyvet „Bevezetés az aritmetikába” címmel. Nem tartalmazott a görög tételeken kívül új ismereteket. Ebből a könyvből származik a ma is használt *prímszám* és *összetett szám* elnevezés. Matematikai munkásságához tartozik az is, hogy javította az abakuszon történő számolási eljárást, továbbá használta és népszerűsítette a hindu számírást. Azzal gyanúsítottak, hogy összeesküvést szervez az uralkodó ellen, ezért börtönbe került, majd kivégezték. A római egyház mártírként tiszteli, mert szerintük a tudóst a hite miatt ölték meg.

2. FLACCUS ALBINUS ALCUINUS (735-804)

Angol bencés szerzetes volt, akit Nagy Károly frank uralkodó 782-ben meghívott az udvarába. Feladata iskolák szervezése, a papok és a főurak tanítása volt. Írt egy hosszú időn át használt feladatgyűjteményt „Feladatok az ifjak elméjének élesítésére” címmel. Ez egy kevés aritmetikát, geometriát és csillagászatot tartalmazó találóskérdések formájába öltöztetett, érdekes feladatok gyűjteménye volt.

3. GERBERT (950?-1003)

Francia szerzetes, akiből később római pápa lett. Barcelonában tanulmányozta az arab matematikát, hazatérve tanította is a hindu-arab számírást. Az új számjegyek az abakuszán jelentek meg először. Az egyes vájatokba nem a megfelelő számú kavicsot tette, hanem egy zsetont, amelyre ráírta az újnak számító számjegyet.



Az abakuszon a rajzon szereplő vájatoktól sokkal több volt (27). A műveleti eredményeket nem az új számjegyekkel helyiértékesen írta ki, hanem római számokkal. Ez az abakusz már egy lépés volt az új számírásra való áttérés felé. Neki tulajdonítanak három matematikai tárgyú írást: 1. Az abakuszon számolás szabályai 2. Könyvecske az osztásról 3. Geometriai alapismeretek. Pápa korában (II. Sylvester 999-1003) szorgalmazta a hindu számírás elterjesztését. Ő honosította meg az *osztó* és az osztandó kifejezéseket. Foglalkozott csillagászattal és jártas volt az orgonakészítésben is. Ő küldte I. István királyunknak a koronát.

A 11. században szinte semmi előrelépés nem volt a matematikában. A 12. századot két fontos fejlemény jellemzi:

1. Megindult az egyházi iskolák egyetemmé való fejlődése. (Bologna, Párizs, Oxford)

2. Lefordították a legfontosabb görög és arab műveket latinra.

4. ADELARD (1090?-1160?)

Ő indította el a széles körű fordítói munkát 1126-ban. Angol szerzetes volt, aki álruhában látogatta az arab egyetemeket, ahol a nyelvet is megtanulta. Elsőként fordította le Euklidész *Elemek* című könyvét 1142-ben. Lefordította AL-HVARIZMI csillagászati táblázatait és „*A hindu számokról*” című művét is. Ennek nagy szerepe volt a mai számírás és számolási technika európai elterjedésében. 1155-ben latinra fordította Ptolemaiosz *Almageszt* című munkáját.

Adelard Angliában dolgozott, de az igazi nagy „fordító-üzem” a spanyolországi Toledoban működött. A matematika szempontjából a legtermékenyebb fordító CREMONAI GHERARDO (1114-1187) volt, aki 85 művet írt át latin nyelvre.

5. LEONARDO PISANO (1170?-1250?)

Ismertebb nevén FIBONACCI. A középkor legnagyobb matematikusa volt. A kereskedő apja révén megismerte az akkori arab és keresztény világ nagy részét. Nemcsak az arab nyelvet sajátította el, hanem megismerkedett az arab matematika akkori eredményeivel is. 1202-ben írta meg a *Liber abaci* (Az abakusz könyve) művét. Ebben rendezte és saját eredményeivel is kiegészítette az általa összegyűjtött aritmetikai és algebrai ismereteket. Ez a munka már lényegesen több egyszerű fordításnál, kétszáz senki sem tudta felülmúlni. 1228-ban írt egy hasonló jellegű geometriai összefoglalást *Practica geometria* (Gyakorlati geometria) címmel. Ezeken kívül még írt két könyvet, melyek egyenletek megoldásával foglalkoznak. Máig tartó világhírnevét egy „a nyulak szaporodásáról” szóló feladatának köszönheti. (A Fibonacci-sorozat az $a_1 = a_2 = 1, a_n = a_{n-1} + a_{n-2}$ alakban adható meg.)

Reneszánsz

A XV. század nagy változást hozott az európai gondolkodásban. Ekkor bontakozott ki a humanizmus. A középkorban főleg az aritmetika fejlődött, a reneszánsz korban az algebra került előtérbe. Sorra nyíltak meg új egyetemek. A matematika és a tudományok központja az angol és a francia területekről észak-itáliai (Bologna, Milánó) és közép-európai városokba (Nürnberg, Bécs, Prága) tevődött át. Magyarország sem maradt le a fejlődésről, hiszen Mátyás király egyetemet alapított Pozsonyban 1467-ben.

6. REGIOMONTANUS (1436-1476)

A korszak első nagy matematikusa. A német tudós eredeti neve Johannes Müller, de szülővárosa Königsberg latin nevét vette fel. Nagy műveltségű ember volt, foglalkozott a matematikán kívül csillagászattal, tudományos munkák fordításával is. Vitéz János esztergomi érsek meghívására Pozsonyban is tanított 1468-tól 1471-ig. Itt írta az *Ephemeries* című csillagászati művét, amelyet Kolumbusz is használt a felfedező útjain. Ő készítette 1473-ban az első olyan csillagászati táblázatot, amely bármely időpontra meghatározta a Nap és a Hold egymáshoz viszonyított helyzetét. (A földrajzi hosszúság meghatározásában volt fontos szerepe.)

1464-ben Rómában készítette el az „Öt könyv mindenféle háromszögekről" című fő művét. Ebben a trigonometriát háromszögek megoldására használja, függetleníti a csillagászattól, így lett a matematika külön fejezete. Ebben az írásában a feladatok megoldása algebrai eszközökkel történik, de jelölések alkalmazása nélkül. Ezzel indul el az analitikus geometria kialakulása. Készített egy 7 tizedesjegy pontosságú szinusz-táblázatot és egy tangens-táblázatot is. Ezért látta meg a $4sin^3\alpha + sin\alpha = 3sin\alpha$ egyenletnek és a szögharmadolásnak az összefüggését. A levelezéseiből tudjuk, hogy sok számelméleti kérdéssel is foglalkozott. Ő találta meg az ötödik tökéletes számot: 33550336. Ő vezette be az európai matematikába a gyökmennyiségek fogalmát, illetve kidolgozta a műveleti szabályokat. Megmutatta a gyökös mennyiségek és a törtkitevős hatványok kapcsolatát, ezzel elősegítve a logaritmus felfedezését.

Ebben a korban született meg a matematika újabb vívmánya, a rövidítéseket, jelöléseket használó ún. szimbolikus algebra. Ennek egyik jelentős képviselője:

7. NICOLAS CHUQUET (1445?-1500?)

1484-ben írta „A számok tudománya három részben" című könyvét. Bevezette a negatív kitevőjű hatványokat és a velük végezhető műveleteket. A szabályait alkalmazva rájött a logaritmus alapgondolatára. A negatív számokat már önálló számként is elfogadta, ellentétben sok kortárs matematikussal.

8. GIROLÁMO CARDANO (1501-1576)

Nürnbergben 1545-ben jelent meg műve „A nagy művészet, avagy az algebra szabályai” címmel. Ezzel a munkával az európai matematika először lépte túl a görög és az arab matematikát. Ez a könyv tartalmazza a harmad-és negyedfokú egyenletek megoldási módszereit. Ezt követően a magasabb fokú egyenletek megoldóképleteinek keresése indult el. E kutatásokból született meg az absztrakt algebra. A harmadfokú egyenlet megoldóképletének megszületését nagyban motiválta a komoly pénzdíjakkal és hírnévvel járó számolóversenyek. Itt gyakran kellett harmadfokú egyenleteket megoldani a versenyzőknek. Ezért érthető, hogy amikor **DEL FERRO** (1465-1526), a bolognai egyetem professzora felfedezett egy módszert, azt senkinek sem árulta el. Később **TARTAGLIA** (1500?-1557) bresciai számolómester újra felfedezte az eljárást és elárulta (titoktartás mellett) Cardanonak. Del Ferro halála után az irataiban megtalálta Cardano a módszer leírását, ezért felmentve érezte magát a titoktartás alól és publikálta az eredményt.

Ekkor Cardano a milánói orvosi kollégium igazgatója és a pavai egyetem rektora volt. Ez a két titulus kevés pénzzel járt, ezért kockázással, kártyázással és sakkozással egészítette ki a jövedelmét. A szerencsejátékok törvényeit igyekezett megfejteni, így született meg „A kockajátékról” című könyve. Ezt tekintjük a valószínűségszámítás első megjelenésének.

9. RAFFAELLO BOMBELLI (1526-1572)

Bolognai mérnök-matematikus, a reneszánsz kor utolsó nagy olasz algebristája. Írt egy három részes algebra könyvet, mellyel az algebrai szimbolika fejlődéséhez nagyban hozzájárult. Az első rész a gyökmennyiségekkel, a második egyenletekkel foglalkozik. A harmadik részben mintegy 300 feladat szerepel. A *casus irreducibilis* problémáját ő oldotta meg, korát jóval megelőzve. Nagyban hozzájárult az algebrai szimbolika kialakulásához, de az egyenlőség jelét még nem használta.

A szimbolika fejlődésében a francia **VIÉTE** (1540-1603), az angol **HARRIOT** (1560-1621) és **OUGHTRED** (1574-1660) munkássága nagyon jelentős.

A reneszánsz kor két fontos számítástechnikai felfedezéssel is hozzájárult a matematika fejlődéséhez:

1. SIMON STEVIN (1548-1620) holland matematikus vezette be az algebrában a tizedes törteket 1585-ben. A mai alakjukat 1617-ben nyerték el.

2. A logaritmus feltalálása. Ezt **JOOST BÜRGI** (1552-1632), **JOHN NAPIER** (1550-1617) és **HENRY BRIGGS** (1561-1630) munkásságának köszönhetjük. Nem sokáig váratott magára a logarléc feltalálása sem. Ennek az ősét, a logaritmus skálát **EDMUND GUNTER** (1581-1626) londoni matematikus készítette el 1624-ben.

2.9. Az újkori számelmélet

Ebben a fejezetben a 17.-18. századi fejlődést tekintjük át röviden. A matematikában forradalmi változást hozott a 17. század közepe, a görögök óta a legnagyobbat. Kialakult az analitikus geometria, majd ennek nyomán a matematikai analízis. Az egyenletek ismeretleneit kiszámító elemi matematika átadta helyét a változókat tartalmazó függvények vizsgálatának. A század végére már nem lehetett megérteni a matematikát komoly elő tanulmányok nélkül. A matematika utolsó, egyben legnagyobb amatőrje a francia Fermat. A számelmélet önálló tudományággá válásához még a svájci Euler és a német Gauss zseniális képességeire és az analízis megfelelő fejlettségére is szükség volt.

PIERRE DE FERMAT (1601-1665): Jogász, a toulouse-i fellebbviteli bíróság tagja. Fermat Descartes-tól függetlenül felfedezte az analitikus geometria alapját. "Bevezetés a síkbeli és térbeli helyek elméletébe" című értekezése már 1636-ban megjelent, Descartes "Geometriá"-ja előtt. Blaise Pascallal folytatott levelezésén keresztül tudjuk, hogy a valószínűségszámítás elméletének társfelfedezője.

A kor matematikusaival nem tartotta a kapcsolatot, bár két angol matematikusnak, Digbynek és Wallisnak rendszeresen írt. A francia Mersenne matematikus szerzetes atyával is levelezésben állt, aki másoknak is közvetítette ötleteit. Fermat egyedül dolgozó ember volt, és mivel ritkán jegyzett fel bizonyításokat vagy magyarázatot arra, hogyan kapta meg az eredményeket, a kortársainak szinte lehetetlenné tette azok megértését. Ugyanakkor előszeretettel jelentette be az újságokban, hogy megoldott egy matematikai problémát, de a megoldás levezetésének leírását nem adta meg, a többiekre hagyva annak kitalálását. Munkáinak java csak halála után, 1679-ben, illetve később jelent meg.

A Nagy Fermat-sejtés: „Egy köböt pedig lehetetlen szétbontani két köbre, egy negyedik hatványt két negyedik hatványra, és általában a négyzet kivételével egy hatványt egy ugyanolyan két hatványra. Erre találtam egy valóban csodálatos bizonyítást, de a lapszél túl keskeny ahhoz, hogy befogadja” – ezt jegyezte fel latinul Diophantosz Aritmetika c. könyvének margójára. A matematikusok egészen 1994-ig, több mint 300 éven át keresték a megoldást, míg Andrew Wiles angol matematikus nyolcévi munka után bizonyította az állítást.

Néhány további felfedezése:

1. Kis Fermat-tétel: Ha p prímszám és a nem osztható p-vel, akkor $(a^{p-1} - 1)$ osztható p-vel. Mai jelölésekkel: $a^{p-1} \equiv 1 \pmod{p}$

Fermat 1636-ban jött rá e tételre, és egy 1640. október 18-i levelében írta meg e felfedezését Frenicle-nek. Az tétel első bizonyítást Gottfried Wilhelm Leibniz adta.

2. Fermat-számok: $F_n = 2^{2^n} + 1$. Azt hitte, hogy ezek mindig prímszámot adnak, de Euler bizonyította, hogy már $n = 5$ esetén sem igaz.

Az első nyolc Fermat-szám:

$F_0 = 2^1 + 1 = \underline{3}$

$F_1 = 2^2 + 1 = \underline{5}$

$F_2 = 2^4 + 1 = \underline{17}$

$F_3 = 2^8 + 1 = \underline{257}$

$F_4 = 2^{16} + 1 = \underline{65537}$

$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$

$F_6 = 2^{64} + 1 = 18446744073709551617 = 274177 \times 67280421310721$

$F_7 = 2^{128} + 1 = 340282366920938463463374607431768211457 =$
$59649589127497217 \times 5704689200685129054721$

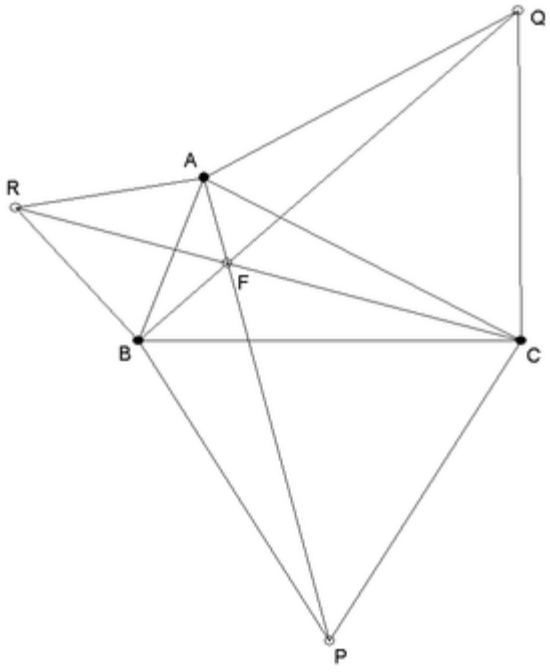
Jelenleg csak az első 12 Fermat-szám prímtényezőkre bontását ismerjük. Prímteszt a Fermat számokra: A Fermat-szám pontosan akkor prímszám, ha teljesül a következő:

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

Sok sejtést lehet a Fermat-számokról felállítani és ezek mindegyike reménytelenül nehéz. Sejtjük, de nem tudjuk bizonyítani, hogy az ismerteken kívül nincs több prím. De még azt sem tudjuk, hogy végtelen sok összetett Fermat-szám van, hogy mind négyzetmentes, vagy akár, hogy végtelen sok négyzetmentes Fermat-szám van.

3. Fermat-elv: Az optikával kapcsolatos Fermat-elv azt mondja ki, hogy a fénysugár egy tetszőleges optikai rendszerben mindig olyan pályát követ, amelyre nézve a kezdő és végpontok közötti terjedési idő extrém, általában a lehető legkisebb értéket veszi fel.

4. Fermat-pont (izogonális-pont): A geometriában az a pont, amit egy háromszög csúcsaival összekötve az összekötő szakaszok együttes hossza minimális. Feladványul adta Evangelista Torricellinek a pont megszerkesztését.



5. Végtelen leszállás: Huygens kéziratai között 1879-ben találtak egy Fermat levelet, amelyben megtalálható a végtelen leszállás bizonyítási módszer leírása. Ez a teljes indukciós bizonyítás indirekt változata.

LEONHARD EULER (1707-1783): A matematika történetének második legtermékenyebb tudósa. (Erdős Pálnak jelent meg több tudományos munkája). Halálakor 560 megjelent műve volt, posztumusz cikkeit a Szentpétervári Akadémia folyamatosan adta ki. 1843-ban, amikor úgy tűnt, mindet feldolgozták, a lista 756 tagot tartalmazott. Ekkor váratlanul 61 kéziratot találtak. A huszadik század elején összeállított listán 866 írása van.

Daniel Bernoulli hívta meg 1727-ben (ekkor 20 éves volt) a Szentpétervári Tudományos Akadémiára. 1731-ben a fizika professzora, majd két évvel később a matematikai osztály vezetője lett. 1740-ben a jobb szemére megvakult, de egy sikeres műtét visszahozta a látását. Később azonban újra elvesztette, és a műtét következtében 1771-ben a másik szemére is megvakult. (Munkáinak több mint a felét vakon készítette el, majd lediktálta tanítványainak, kollégáinak.) Óriási teljesítmény! A matematika szinte valamennyi ágában maradandót alkotott.

A sok eredménye közül néhány:

- A számelméletben megtalálta a 8. tökéletes számot és 59 barátságos számpárt.
- Bizonyította, hogy minden páros tökéletes szám $2^k(2^{k+1}-1)$ alakú.
- Megmutatta, hogy az ötödik Fermat-szám összetett: F_5 osztható 641-gyel.
- Első publikált bizonyítását adta Fermat állításának: minden $4k+1$ alakú prímszám két négyzetszám összege.
- Ő jelölte először π-vel a kör kerületének és átmérőjének arányát, *e*-vel a $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ sorozat határértékét, amit később róla neveztek el.
- Levezette az $e^{i\pi}+1=0$ egyenlőséget. (Ezt a matematika ékkövének nevezik.)
- Az analitikus geometria keretében szinte egymaga megalkotta a ma használatos trigonometriát.
- 1748-ban megjelent könyvében szereplő koordináta-rendszernek két tengelye volt, melyeken már negatív értékek is szerepeltek. Gyakran használt polárkoordinátákat is.
- Síkgeometriában felfedezte és a nevét viseli a háromszög Euler-egyenese (1744).
- Felfedezte a Feuerbach-kört. (Sajnos nem róla nevezték el.)
- Bebizonyította a róla elnevezett Euler-tételt, mely felírja a háromszög köréírt és beírt körének középpontjai közötti távolságot a két kör sugara segítségével.
- Bizonyította a róla elnevezett Euler-féle poliédertételt, mely összefüggést ad egy poliéder csúcsainak, éleinek és lapjainak száma között (1744).
- Elsőként haladta meg a kúpszeletek tárgyalása során Apollóniosz eredményeit.
- A gráfelmélet nyitányát jelenti a Königsbergi hidak általa megoldott problémája.
- Megoldotta a karcsú rudak rugalmas kihajlásának problémáját.
- A hidrodinamikát ma is az ő felfogásában tárgyalják.
- Az örvényszivattyúk és turbinák méretezését ma is az Euler-turbinaegyenlet szerint végzik.
- A pörgettyűmozgást az Euler-féle kinetikai egyenletek segítségével vizsgálta.
- Foglalkozott valószínűségszámítással, komplex számokkal, harmonikus sorokkal, moduláris aritmetikával, differenciálegyenletekkel.
- A csillagászatban foglalkozott a bolygók pályáinak kiszámításával.
- Az optikában a kromatikus aberráció matematikai elemzésével.
- Írt könyvet a hidraulikáról, hajótervezésről, tüzérségről, zenéről. Jelentős térképészeti munkát is végzett.

CARL FRIEDRICH GAUSS (1777-1855): Német matematikus, csillagász és fizikus. Őt tartják minden idők egyik legnagyobb matematikusának. Így is nevezik: "A matematikusok fejedelme." Euler mellett ő a matematika legsokoldalúbb tudósa. A tudomány számos területének fejlődéséhez járult hozzá. A számelmélethez, az analízishez, a differenciálgeometriához, a geodéziához, a mágnesességhez, a csillagászathoz és az optikához.

A legenda szerint tehetsége már hároméves korában megmutatkozott, amikor fejben kijavított egy összeadási hibát, melyet apja vétett, amikor papíron számolta a pénzügyeit. Egy másik híres történet, amely arról szól, hogy az általános iskolai tanára, diákjait azzal akarta lefoglalni, hogy 1-től 100-ig adják össze az egész számokat. A fiatal Gauss mindenki megdöbbenésére másodpercek alatt előrukkolt a helyes megoldással. (Rájött a számtani sorozat összegképletére.)

1796-ban (19 évesen) tört be a tudományos életbe, amikor sikerült megmutatnia, hogy bármely olyan szabályos sokszög, amely oldalainak száma Fermat-prím, megszerkeszthető körző és vonalzó segítségével. Ez jelentős felfedezés volt a szerkesztési problémák területén. Gauss annyira elégedett volt ezzel az eredménnyel, hogy azt kérte, egy szabályos 17-szöget vésseneka sírkövére. A sírköves ezt visszautasította, de szülővárosában (Braunschweig) a tiszteletére emelt szobor talapzatán látható a szabályos 17 oldalú sokszög.

1796 a legtermékenyebb év volt mind Gauss, mind a számelmélet számára. A heptadekagon szerkesztését március 30-án publikálta. Az osztási maradékok azonosságán alapuló kongruencia relációját bevezetve, megteremtette a moduláris számelméletet. Híres tételét a kvadratikus reciprocitásról április 8-án bizonyította.

Ennek a figyelemre méltó tételnek a segítségével a matematikusok meghatározhatják a megoldhatóságát bármely másodfokú kongruenciának. A prímszámtétel, melyet május 31-én sejtett meg, használható képet ad a prímszámok egész számok közti eloszlásáról. Gauss július 10-én azt is észrevette, hogy bármely pozitív egész felírható legfeljebb három háromszögszám összegeként. Október 1-jén publikált egy eredményt polinomok megoldásainak számával kapcsolatban, amely 150 évvel később végül a Weil-sejtéshez vezetett.

1799-es doktori értekezésében Gauss egy bizonyítást adott az algebra alaptételére. Ez a fontos tétel azt állítja, hogy minden legalább elsőfokú, valós vagy komplex együtthatós polinomnak van komplex gyöke. Gauss disszertációja az összes korábbi bizonyítás kritikáját tartalmazta és adott egy újat. Életében még három bizonyítást adott erre a tételre. Az utolsó, 1849-es bizonyítása mai mércével mérve is nagyon igényes. Próbálkozásai útközben nagymértékben pontosították a komplex számok fogalmát.

1800-ban publikálta máig is használatos húsvétképletét.

Gauss a számelmélethez is jelentősen hozzájárult 1801-es könyvével, a *Disquisitiones Arithmeticae*-vel, amely a moduláris aritmetika tiszta bemutatását tartalmazza, valamint a kvadratikus reciprocitás tételének első két bizonyítását. Ugyanezen év január 1-jén Giuseppe Piazzi olasz csillagász felfedezte a Ceres kisbolygót. Ez a momentum sarkallta Gausst arra, hogy megírja munkáját a kisbolygók nagybolygók által megzavart mozgásának elméletéről, amelyet végül 1809-ben publikált. Piazzi még csak néhány hónapja figyelte a Cerest, amikor az átmenetileg eltűnt a Nap ragyogása mögé. További hónapokkal később, amikor a Ceresnek ismét meg kellett volna jelennie, nem sikerült megtalálni. Gauss, aki ekkor 23 éves volt, hallott a problémáról, így hát nekiveselkedett. Három hónap munkát követően, 1801 decemberében megjósolt egy pozíciót a Ceresnek és ez fél fokra pontosnak bizonyult. Zách János Ferenc 1801. december 31-én Gothában, újra felfedezte a kisbolygót. A Cereshez kapcsolódó számításai alapján kidolgozta a perturbációelméletet. Számításai közben olyannyira modernizálta a 18. század pályajóslásának nehézkes matematikáját, hogy a néhány évvel később *Az égitestek mozgásának elmélete* címen publikált műve a csillagászati számítás mérföldkőjének számít. Bevezette a Gauss-féle gravitációs állandót, tartalmazta a legkisebb négyzetek módszerét. Ezt mind a mai napig használják minden tudományágban a mérési hiba hatásának minimalizálására. Gauss ezt a módszert 1809-ben be tudta bizonyítani a normális eloszlású hibák feltétele mellett.

Az 1810-es évek végén Gausst megkérték arra, hogy hajtson végre geodéziai méréseket, számításokat Hannover államban, hogy összekapcsolódjon a meglévő dán térképhálózattal. A vizsgálat részeként Gauss feltalálta a heliotrópot, amely a Nap sugarainak visszaverésével működött, tükörkészletet és egy kis teleszkópot felhasználva.

Gauss azt állította, hogy felfedezte a nemeuklideszi geometriák lehetőségét, de sohasem publikálta. Bolyai János 1829-ben fedezte fel a nemeuklideszi geometriát, a munkáit 1832-ben tette közzé. Miután ezt látta Gauss, azt írta Bolyai Farkasnak: *„Ezt dicsérni saját magam dicséretével járna. Mivel a munka teljes tartalma … szinte teljesen megegyezik saját gondolataimmal, amelyek az utolsó 30-35 évben lefoglalták az agyamat.”*

A hannoveri vizsgálat később a Gauss-eloszlás (normál eloszlás) kidolgozásához vezetett. Ez felkeltette Gauss érdeklődését a differenciálgeometria iránt. Ezen a területen egy fontos tétellel állt elő: a *theorema egregiummal*, amely a görbület fogalmának egy fontos tulajdonságát állapítja meg. Hétköznapi nyelven a tétel azt állítja, hogy a felület görbülete teljes egészében meghatározható szögek és távolságok mérésével a felületen. Azaz a felület görbületi viszonyainak, ezáltal a háromdimenziós térbe való „beágyazottságának” módja anélkül is megismerhető, hogy a felületből kilépnénk, és magát a teljes teret is ismernénk.

1831-ben Gauss nagyszerűen működött együtt Wilhelm Weber fizikaprofesszorral. Ez új ismeretekhez vezetett a mágnesség terén és Kirchhoff huroktörvényének felfedezéséhez az elektromosságtanban. Gauss és Weber az első elektromos távírót 1833-ban készítette el, amely az obszervatóriumukat a göttingeni fizikai intézettel kapcsolta össze. Egy mágneses obszervatóriumot építtetett az obszervatórium udvarán és Weberrel megalapította a „mágneses klub”-ot, amely a Föld mágneses mezőjének mérését támogatta szerte a világon. Kifejlesztett egy módszert a mágneses mező horizontális intenzitásának mérésére, amely egészen a XX. század második feléig használatban volt. Ez elősegítette a Föld mágneses mezője belső (mag és kéreg), valamint külső részének (magnetoszféra) elkülönítésének matematikai elméletét.

2.10. A számelmélet modern tagolódása

A számelmélet kérdései iránt a 19.-20. században még inkább fokozódott az érdeklődés. A számfogalom fejlődése, illetve a matematika más területein elért eredmények hatása komoly előrelépést hozott. A tisztázatlan problémák megoldására a matematika különböző területein kidolgozott módszereket kezdtek alkalmazni. Ez a számelméletben is elindított egyfajta differenciálódást, amely folyamat még most sem tekinthető befejezettnek. Ma már kilenc területről beszélünk:

1. Elemi számelmélet: Idetartoznak a minden részterületen közös fogalmak és tételek.

1. oszthatóság, 2. prímek, 3. maradékos osztás, az euklideszi algoritmus,

4. a számelmélet alaptétele, 5. moduláris aritmetika (maradékosztályok és kongruenciák),

6. egyszerű Diofantoszi egyenletek

2. Analitikus számelmélet: A számelméleti problémákat a függvényanalízis eszközeivel vizsgálja. A diszkrét matematika területéhez sorolt számelmélet megközelítése a folytonosság vizsgálatára létrejött szemlélettel és módszerekkel. Például: prímszámtétel, Riemann-sejtés

3. Algebrai számelmélet: A számelméleti problémákat az absztrakt algebra módszereivel vizsgálja. Ezek: algebrai számok, algebrai egészek, Galois-elmélet, véges testek számelmélete, p-adikus számok, ideálok elmélete.

4. Kombinatorikus számelmélet: Ez a nagyrészt Erdős Pál által létrehozott terület a természetes számok kombinatorikusan megfogalmazható tulajdonságaival foglalkozik. Gyakorta használ lineáris algebrai eszközöket is.

5. Prímszámelmélet: A prímszámok eloszlásával, tulajdonságaikkal foglalkozik.

6. Additív számelmélet: Például: Goldbach-sejtés, Waring-probléma.

7. Diofantoszi egyenletek: Például: Pitagoraszi számhármasok, Pell-egyenlet, Catalan-sejtés, kétnégyzetszám-tétel, Nagy Fermat-tétel, abc-sejtés.

8. Geometriai számelmélet: Például: Rácsgeometria, Minkowski-tétel, pakolási problémák, algebrai geometriai problémák, Nagy Fermat-tétel.

9. Számításelméleti számelmélet: Például: Prímteszt, Prímfaktorizáció, Kriptográfia.

A huszadik század végén az egyik legnagyobb közfigyelmet kiváltó matematikai felfedezése számelméleti jellegű volt: megoldódott a Nagy Fermat-sejtés kérdése. További fontos változás, hogy az 1960-as években még szinte lenézett, alkalmazhatatlan elmetornának gondolt diszkrét matematika és különösen a számelmélet az alkalmazott matematika egyik nagyon fontos területévé vált.

3. Amit már tudunk a prímekről

Tekintsük át, hogy napjainkban mit tudunk a prímszámokról. Az anyag mennyisége miatt nem minden állítás bizonyítását tudjuk végig követni.

3.1. A prímszámok végtelensége

A tétel és bizonyítása először Eukleidész könyvében jelent meg. Azóta sokan és sokféleképpen adtak erre az állításra bizonyítást. A következőkben nézzünk meg 12-t ezekből. Az olvasónak lehet az is egy feladat, hogy keressen ezektől eltérőket is.

Tétel: Végtelen sok prímszám létezik.

1. Bizonyítás:

Ezt a legrégebbi bizonyítást Eukleidész *Elemek* című munkájából ismerjük. A matematika történet első és talán a legszebb indirekt bizonyítása.

Tegyük fel, hogy csak véges sok prímszám létezik. Legyenek ezek: $p_1, p_2, \cdots, p_r$. Képezzük az alábbi számot:

$$A = p_1 \cdot p_2 \cdot \cdots \cdot p_r + 1$$

Az A szám nyilván a $p_1, p_2, \cdots, p_r$ prímszámok egyikével sem osztható. Azonban minden 1-nél nagyobb számnak létezik prímosztója. Ez viszont különbözik a $p_1, p_2, \cdots, p_r$ prímektől, ami ellentmond az indirekt feltevésnek.

A bizonyításból az is látható, hogy $p_n < 2^{2^n}, ahol\ p_n\ az\ n-edik$ prímszámot jelöli. Ennél pontosabb felső becslést a 2.2. fejezetben nézhetünk meg.

2. Bizonyítás:

Definíció: Az $F_n = 2^{2^n} + 1$ alakú számokat,(ahol $n = 0, 1, \cdots$, természetes szám), Fermat számoknak nevezzük. Néhány Fermat szám:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_5 = 641 \cdot 6700417$$

(Ezekről bővebben a 3.4. fejezetben olvashatunk.)

Bebizonyítjuk, hogy bármely két Fermat szám relatív prím, így végtelen sok prímszámnak kell lennie.

Ezért lássuk be a

$$\prod_{k=0}^{n-1} F_k = F_n - 2\,,(\,ahol\; n \geq 1)$$

rekurziót, amiből az állítás már következik. Valóban, ha *m* osztja például F_k-t és F_n-t, ahol $k < n$, akkor *m* osztja $2 = F_n - \prod_{k=0}^{n-1} F_k$-t is, tehát $m = 1\; vagy\; m = 2$. De $m = 2$ nem lehet, mert minden Fermat szám páratlan.

A rekurziót *n* szerinti teljes indukcióval bizonyítjuk.

1. Ha $n = 1$, akkor $F_0 = 3\; és\; F_1 - 2 = 3$.

2. Tegyük fel, hogy az állítás $n = m$-ig igaz.

3. Bizonyítsuk be, hogy $n = m + 1$-re is igaz.

Az indukciós feltevésből következik az alábbi:

$$\prod_{k=0}^{m} F_k = \left(\prod_{k=0}^{m-1} F_k\right) F_m = (F_m - 2)F_m =$$

$$= \left(2^{2^m} - 1\right)\left(2^{2^m} + 1\right) = 2^{2^{m+1}} - 1 = F_{m+1} - 2$$

3. Bizonyítás:

Definíció: Az $M_p = 2^p - 1$ alakú számokat, ahol *p* prímszám, Mersenne számnak nevezzük.

Egy Lagrange-tétel segítségével bizonyítjuk az állítást.

Tétel: Ha *G* egy véges multiplikatív csoport és *U* egy részcsoportja, akkor $|U|$ osztja $|G|$-t.

Tegyük fel, hogy véges sok prímszám van és *p* a legnagyobb. Megmutatjuk, hogy $2^p - 1$ bármely *q* osztója nagyobb, mint *p*. Ebből következik a prímszámok végtelensége. Legyen *q* a $2^p - 1$ valamely prímosztója, azaz $2^p \equiv 1\; (mod\; q)$. Mivel *p* prím, ez azt jelenti, hogy Z_q test $Z_q - \{0\}$ multiplikatív csoportjában a 2 elem rendje *p*. Ennek a csoportnak *q*-1 eleme van.

A Lagrange-tétel szerint minden elem rendje osztja a csoport rendjét, így p osztója $q-1$-nek, tehát $p < q$. Tehát ellentmondásra jutottunk.

4. Bizonyítás:

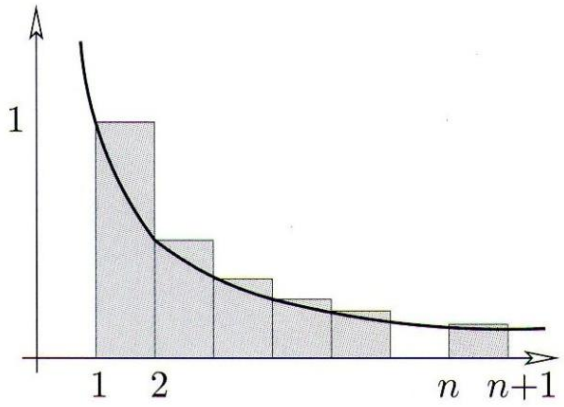
A bizonyítást az analízis eszközeivel végezzük el.

Definíció: Az *x* természetes alapú logaritmusa:

$$log\ x = \int_1^x \frac{1}{t} dt$$

Definíció: Legyen a $\pi(x)$ az *x* valós számnál kisebb vagy egyenlő prímszámok száma.

Számozzuk meg a prímszámokat növekvő sorrendben ($p_1, p_2, p_3, \cdots$) és vegyük *x* természetes alapú logaritmusát. Hasonlítsuk össze az $f(t) = \frac{1}{t}$ függvény grafikonja alatti terület egy a függvény grafikonját felülről közelítő lépcsős függvénnyel.



Így $n \leq x \leq n+1$ esetén az alábbi egyenlőtlenséget kapjuk:

$$log\ x \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} \leq \sum \frac{1}{m}$$

Itt az összegzést minden olyan *m* természetes számra kiterjesztjük, aminek csak $p \leq x$ prímosztója van. Minden ilyen *m* egyértelműen felírható a következő alakban:

$$\sum \frac{1}{m} = \prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

A belső összeg egy $\frac{1}{p}$ hányadosú mértani sor, azaz:

$$log\ x \leq \prod_{p \leq x} \frac{1}{1-\frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p^k}{p^k-1}$$

Mivel $p^k \geq k+1$, ezért:

$$\frac{p^k}{p^k-1} = 1 + \frac{1}{p^k-1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

Ebből következik az alábbi összefüggés:

$$log\ x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

Tudjuk, hogy $log\ x$ nem korlátos, tehát $\pi(x)$ sem az. Vagyis végtelen sok prímszám van.

5. Bizonyítás:

Ez a bizonyítás Hillél Fürstenberg nevéhez köthető, mely topológiát használ fel.

Nézzük az alábbi topológiát az egész számok **Z** halmazán:

az $a, b \in \boldsymbol{Z}, b > 0$ számokra legyen $N_{a,b} = \{a + nb : n \in \boldsymbol{Z}\}$.

Minden $N_{a,b}$ halmaz egy kétirányú végtelen számtani sorozat.

Definíció: Egy $O \subseteq \boldsymbol{Z}$ halmaz nyílt, ha vagy O üres, vagy minden $a \in O$-hoz van olyan $b \in \boldsymbol{Z}$, amelyre $N_{a,b} \subseteq O$.

Nyilvánvaló, hogy nyílt halmazok uniója is nyílt. Belátjuk, hogy véges sok nyílt halmaz metszete is nyílt. Ehhez elég, hogy két nyílt halmaz metszete is nyílt. Legyen $O_1 és\ O_2$ két nyílt halmaz. Ekkor tetszőleges $a \in O_1 \cap O_2$-höz létezik $b_1, b_2 \in \boldsymbol{Z}$, hogy $N_{a_1,b_1} \subseteq O_1$, illetve $N_{a_2,b_2} \subseteq O_2$, de ekkor $a \in N_{a_1,b_1 \cdot b_2} \subseteq O_1 \cap O_2$. Ez a halmazcsalád tehát egy valódi topológiát generál **Z**-n.

Nézzünk meg két állítást:

1. Bármely nem üres nyílt halmaz végtelen.

2. Minden $N_{a,b}$ halmaz zárt is.

Az 1. állítás következik a definícióból.

A 2. állításhoz vegyük észre az alábbi összefüggést:

$$N_{a,b} = \boldsymbol{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

Ami bizonyítja, hogy $N_{a,b}$ egy nyílt halmaz komplementere, tehát zárt. Mivel minden $n \neq 1$ és $n \neq -1$ számnak van *p* prímosztója, ezért benne van $N_{0,p}$-ben, amiből következik, hogy:

$$\boldsymbol{Z} \setminus \{1, -1\} = \bigcup_{p} N_{0,p}$$

Ha a *p* prímszámok halmaza véges lenne, akkor $\bigcup_p N_{0,p}$ a második állítás alapján előállna zárt halmazok véges uniójaként, és így ő maga is zárt lenne. Tehát az $\{1, -1\}$ nyílt halmaz lenne, ami viszont ellentmond az 1. állításnak. Tehát végtelen sok prímszám van.

6. Bizonyítás:

Erdős Pál megoldása a prímszámok végtelenségén túl azt is megmutatja, hogy a $\sum \frac{1}{p}$ sor divergens. Legyen $p_1, p_2, p_3, \cdots$ a prímszámok növekvő sorozata, és tegyük fel, hogy a $\sum \frac{1}{p}$ sor konvergens. Ekkor kell lennie olyan *k* természetes számnak, melyre

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$$

Nevezzük $p_1, p_2, \cdots, p_k$-t *kis* prímeknek, és $p_{k+1}, p_{k+2}, \cdots$-t *nagy* prímeknek. Tetszőleges *x* természetes számra az alábbi adódik:

$$\sum_{i \geq k+1} \frac{x}{p_i} < \frac{x}{2} \qquad (1)$$

Legyen N_x azon $m \leq x$ pozitív egészek száma, amelyeknek legalább egy *nagy* prímosztójuk van, K_x pedig azoké, amelyeknek minden prímosztójuk *kicsi*. Megmutatjuk, hogy alkalmas *x*-re $N_x + K_x < x$, ami a várt ellentmondásra vezet, mert definíció szerint $N_x + K_x = x$. Az $\left\lfloor \frac{x}{p_i} \right\rfloor$ azokat az $m \leq x$ pozitív egészeket számolja, amelyek p_i többszörösei. Vagyis (1) egyenlőtlenség alapján:

$$N_x \leq \sum_{i \geq k+1} \left\lfloor \frac{x}{p_i} \right\rfloor < \frac{x}{2} \qquad (2)$$

Vizsgáljuk most K_x-t. A csak *kis* prímosztókkal rendelkező $m \leq x$-eket átírjuk $m = a_m b_m^2$ alakba, ahol a_m a négyzetmentes rész. Minden a_m tehát különböző *kis* prímeknek a szorzata, azaz legfeljebb 2^k féle négyzetmentes rész van. Továbbá, mivel $b_m \leq \sqrt{m} \leq \sqrt{x}$, azt kapjuk, hogy legfeljebb $\sqrt{x}$ féle négyzetes rész van, és ezért $K_x \leq 2^k \sqrt{x}$. Ha $2^k \sqrt{x} \leq \frac{x}{2}$, akkor $K_x \leq 2^k \sqrt{x} \leq \frac{x}{2}$. Ekkor (2) alapján $N_x + K_x < x$.

Megjegyzés: Az $x > 2^{2k+2}$ esetén valóban teljesül az alábbi egyenlőtlenség:

$$2^k \sqrt{x} < \frac{x}{2}$$

7. Bizonyítás:

Euler bizonyítása. Tegyük fel, hogy csak véges sok prímszám létezik.

Legyenek ezek:2, 3, 5,..,p. Vizsgáljuk az alábbi azonosságot:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots =$$

$$= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right) \cdot \ldots \cdot \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) =$$

$$= \frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} \cdot \ldots \cdot \frac{1}{1 - \frac{1}{p}}$$

Az első sorban lévő kifejezés értéke a végtelenhez tart, míg a harmadik sorban lévő egy véges számérték. Ellentmondásra jutottunk, tehát hibás volt a feltételezés.

8. Bizonyítás:

Tegyük fel, hogy csak véges sok prímszám létezik. Legyenek ezek:2, 3, 5,...p. Vizsgáljuk az alábbi azonosságot:

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=$$

$$=\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\cdots\right)\cdot\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\frac{1}{3^6}+\cdots\right)\cdot\ldots\cdot\left(1+\frac{1}{p^2}+\frac{1}{p^4}+\frac{1}{p^6}+\cdots\right)=$$

$$=\frac{1}{1-\frac{1}{2^2}}\cdot\frac{1}{1-\frac{1}{3^2}}\cdot\ldots\cdot\frac{1}{1-\frac{1}{p^2}}$$

Az első sorban lévő kifejezés értéke egy irracionális szám $\left(\frac{\pi}{6}\right)$, míg a harmadik sorban lévőé egy racionális számérték. Ellentmondásra jutottunk, tehát hibás volt a feltételezés.

9. Bizonyítás:

Tegyük fel, hogy csak véges sok prímszám létezik. Ha *k* darab prímszám van, akkor a belőlük képezhető $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_k^{\alpha_k}$ alakú természetes számok száma, ahol a kitevők nem nagyobbak *n*-nél: $(n+1)^k$. E számok között szerepelnie kell az $1,2,3,\cdots,2^n$ számok mindegyikének, tehát $(n+1)^k>2^n$ lenne, de ez az egyenlőtlenség nem teljesül elegendően nagy *n*-re. Ellentmondásra jutottunk, tehát hibás volt a feltételezés.

10. Bizonyítás:

Tegyük fel, hogy csak véges sok prímszám létezik. Ha *k* darab prímszám van, akkor legyen $n=p_1\cdot p_2\cdot p_3\cdot\cdots\cdot p_k$. Ekkor az egyedüli, *n*-hez relatív prímszám az 1, tehát:

$\varphi(n)=1$. Vagyis: $\varphi(n)=(p_1-1)\cdot(p_2-1)\cdot\cdots\cdot(p_k-1)=1$. Azonban ez az egyenlőség nem teljesülhet. Ellentmondásra jutottunk, tehát hibás volt a feltételezés.

Megjegyzés: Az $1,2,\cdots,n-1$ számok közül az *n*-hez relatív prímszámok számát az Euler-féle $\varphi(n)$ függvény adja meg:

$$\varphi(n)=n\cdot\prod_{p|n}\left(1-\frac{1}{p}\right)$$

11. Bizonyítás:

Ha tudunk olyan végtelen sorozatot létrehozni, melynek elemei páronként relatív prímek, akkor abból már következik, hogy végtelen sok prímszám van. A 2. Bizonyításnál is hasonló módon jártunk el.

Legyenek *a* és *b* egymáshoz relatív prím természetes számok. A sorozat a következő:

$$a_0 = a, \qquad a_{n+1} = a_0 \cdot a_1 \cdot \cdots \cdot a_n + b \, , ahol \; n = 0, 1, 2, \cdots$$

Lássuk be, hogy a sorozat elemei páronként relatív prímek. Legyen *d* egy közös prímosztója a_i-nek és a_j-nek, ahol $i < j$. Az $a_j = a_0 \cdot a_1 \cdot \cdots \cdot a_i \cdot \cdots \cdot a_{j-1} + b$ előállítás miatt *d* osztója *b*-nek. Mivel $a_i = a_0 \cdot a_1 \cdot \cdots \cdot a_{i-1} + b$ és *d* osztója a_i-nek, így *d* osztója

$a_0 \cdot a_1 \cdot \cdots \cdot a_{i-1}$-nek, tehát *d* osztója a sorozat valamely, a_i-t megelőző elemének is. Ezt folytatva kapjuk, hogy *d* osztója *a*-nak is és *b*-nek is. Ez viszont ellentmond a kezdeti feltevésnek.

12. Bizonyítás:

Felhasználjuk a Fibonacci sorozatra vonatkozó Lucas tételt. Jelölje f_n a sorozat *n*-edik tagját. Ekkor $(f_m \, , f_n \,) = f_{(m,n)}$. Ha csak véges sok prímszám van: $p_1, p_2, \cdots, p_k$, akkor a Lucas tétel szerint az $f_{p_1}, f_{p_2}, \cdots, f_{p_k}$ elemek páronként relatív prímek, és mivel a felsoroltakon kívül más prím nincs, így mindegyik f_{p_i}-nek csak egy prímosztója lehet. Ennek mond ellent, hogy $f_{19} = 4181 = 113 \cdot 37$.

3.2. A prímszámok eloszlása

Ebben a fejezetben megnézünk néhány elemi becslést a prímek számáról.

Tetszőleges $x \geq 2$ valós szám esetén jelölje $\pi(x)$ az *x*-nél nem nagyobb pozitív prímszámok számát. A következő tétel a $[2, n]$ intervallumba eső prímszámok szorzatára ad felső becslést.

1. Tétel: Tetszőleges $n \geq 2$ egész szám esetén:

$$\prod_{p \leq n} p < 4^n$$

Bizonyítás: (Erdős Pál és Kalmár László bizonyítása) A bizonyítást *n* szerinti teljes indukcióval végezzük. Az $n = 2$ esetén $2 < 4^2$, $n = 3$ esetén $2 \cdot 3 < 4^3$, tehát igaz az állítás.

Tegyük fel, hogy a tétel igaz $(n-1)$-ig. Bebizonyítjuk, hogy ekkor *n*-re is igaz, ha $n \geq 4$.

1. eset: Ha *n* páros, azaz $n = 2k \geq 4$. Ekkor:

$$\prod_{p \leq 2k} p = \prod_{p \leq 2k-1} p < 4^{2k-1} < 4^{2k}$$

2. eset: Ha *n* páratlan, azaz $n = 2k + 1 \geq 4$. Ekkor:

$$\prod_{p \leq 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right),$$

ahol az indukciós feltétel miatt:

$$\prod_{p \leq k+1} p < 4^{k+1}, hiszen\ 2 < k + 1 < n$$

Továbbá:

$$\prod_{k+2\le p\le 2k+1} p \mid (k+2)(k+3)\cdots(2k+1) = \frac{(2k+1)!}{(k+1)!} = k!\cdot\binom{2k+1}{k}$$

Mivel ez a szorzat $k!$-hoz relatív prím, ezért osztója a $\binom{2k+1}{k}$ egész számnak. Tehát:

$$\prod_{k+2\le p\le 2k+1} p \le \binom{2k+1}{k} = \frac{3\cdot 5\cdot 7\cdot\cdots\cdot(2k+1)\cdot 2^k}{(k+1)!} <$$

$$< \frac{4\cdot 6\cdot 8\cdot\cdots\cdot(2k+2)\cdot 2^k}{(k+1)!} = 2^{2k} = 4^k$$

Vagyis:

$$\prod_{p\le 2k+1} p < 4^{k+1}\cdot 4^k = 4^{2k+1}$$

Tehát igaz az állítás. A tétel minden *x* valós szám esetén is igaz.

2. Tétel: Tetszőleges $x \ge 2$ valós szám esetén:

$$\pi(x) < \left(4+\frac{3}{4}\right)\cdot\frac{x}{\log_2 x}$$

Bizonyítás: A $\prod_{p\le x} p$ szorzatot becsüljük alulról. A szorzat $\sqrt{x}$ alatti tényezőit 2-vel, a többit $\sqrt{x}$-szel becsüljük alulról, $x \ge 4$ esetén:

$$4^x > \prod_{p\le x} p = \left(\prod_{p\le\sqrt{x}} p\right)\left(\prod_{\sqrt{x}<p\le x} p\right) \ge$$

$$\ge \left(\prod_{p\le\sqrt{x}} 2\right)\left(\prod_{\sqrt{x}<p\le x} \sqrt{x}\right) = 2^{\pi(\sqrt{x})}\cdot\left(\sqrt{x}\right)^{\pi(\sqrt{x})}$$

Tehát:

$$2^{2x} > 2^{\pi(\sqrt{x})}\cdot\left(\sqrt{x}\right)^{\pi(x)-\pi(\sqrt{x})}$$

Áttérve kettes alapú logaritmusra a következőt kapjuk:

$$2x > \pi\left(\sqrt{x}\right) + \left[\pi(x) - \pi\left(\sqrt{x}\right)\right] \cdot \log_2 \sqrt{x}$$

Az $x \geq 4$ miatt $\log_2 x \geq 0$ és $\pi\left(\sqrt{x}\right) < \sqrt{x}$, ezért:

$$\pi(x) < \frac{4x - 2\pi(x)}{\log_2 x} + \pi\left(\sqrt{x}\right) = \frac{x}{\log_2 x} \cdot \left[4 + \frac{\pi\left(\sqrt{x}\right)}{x} \cdot (\log_2 x - 2)\right] \leq$$

$$\leq \frac{x}{\log_2 x} \cdot \left[4 + \frac{1}{\sqrt{x}} \cdot (\log_2 x - 2)\right]$$

Mivel $x \geq 4$, ezért van olyan $k \geq 2$ egész szám, amelyre $2^k \leq x < 2^{k+1}$, ezért:

$$0 \leq \frac{1}{\sqrt{x}} \cdot (\log_2 x - 2) < \frac{1}{2^{\frac{k}{2}}} \cdot (k + 1 - 2) \leq \frac{3}{4},$$

ahol az $\frac{1}{2^{\frac{k}{2}}} \cdot (k + 1 - 2) \leq \frac{3}{4}$ egyenlőtlenség $k = 2, k = 3, k = 4$ esetén fennáll, és $k \geq 4$-re:

$$\frac{k-1}{2^{\frac{k}{2}}} = \frac{(k+1)-1}{2^{\frac{k+1}{2}}} \cdot \left(1 - \frac{1}{k}\right) \cdot \sqrt{2} > \frac{(k+1)-1}{2^{\frac{k+1}{2}}}$$

Ezzel igazoltuk, hogy $x \geq 4$-re:

$$\pi(x) < \left(4 + \frac{3}{4}\right) \cdot \frac{x}{\log_2 x}$$

A $2 \leq x < 4$ esetén:

$$\pi(x) \leq 2 < 4 + \frac{3}{4} = \left(4 + \frac{3}{4}\right) \cdot \frac{2}{\log_2 4} < \left(4 + \frac{3}{4}\right) \cdot \frac{x}{\log_2 x}$$

Tehát igaz az állítás.

3. Tétel: Tetszőleges $x \geq 2$ valós szám esetén:

$$\pi(x) > \left(1 - \frac{3}{4}\right) \cdot \frac{x}{\log_2 x}$$

Bizonyítás: A bizonyításnál felhasználjuk a következő tételt.

Tétel: (Legendre-formula) Legyenek *n* és *k* pozitív egész számok, *p* pozitív prímszám, továbbá $p^k \leq n < p^{k+1}$. Ekkor az $n!$ kanonikus felbontásában a *p* kitevője:

$$\alpha_{p,n!} = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

Megjegyzés: A tétel egyszerűen következik abból, hogy az $1, 2, \cdots, n$ számok között $\left[\frac{n}{p}\right]$ darab *p*-vel, $\left[\frac{n}{p^2}\right]$ darab p^2-tel és általában $\left[\frac{n}{p^j}\right]$ darab p^j-nel osztható szám van. A szögletes zárójel a szám egészrészét jelöli.

E tétel alapján:

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{\beta_p} \ , ahol\ \beta_p = \sum_{j=1}^{\gamma_p} \left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right) \text{ és } p^{\gamma_p} \leq 2n < p^{\gamma_p + 1}$$

Egy *y* valós szám esetén $2[y] \leq 2y < 2[y] + 2$ miatt $2[y] \leq [2y] \leq 2[y] + 1$, vagyis

$$0 \leq [2y] - 2[y] \leq 1, tehát\ 0 \leq \beta_p \leq \gamma_p, ezért:$$

$$\binom{2n}{n} \leq \prod_{p \leq 2n} p^{\gamma_p} \leq (2n)^{\pi(2n)}$$

Másrészt $n \geq 2$-re:

$$\binom{2n}{n} = \frac{3 \cdot 5 \cdot 7 \cdot \cdots \cdot (2n-1) \cdot 2^n}{n!} > \frac{2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n-2) \cdot 2^n}{n!} = \frac{2^{2n-1}}{n} = \frac{2^{2n}}{2n}$$

Tehát pozitív egész *n*-re (Az egyenlőség $n = 1$ esetén teljesül):

$$2^{2n} \leq (2n)^{\pi(2n)+1}, azaz\ \pi(2n) \geq \frac{2n}{\log_2(2n)} - 1$$

Ezt $x \geq 2$ valós szám esetén alkalmazhatjuk $n = \left[\frac{x}{2}\right]$-szel:

$$\pi(x) \geq \pi\left(2\left[\frac{x}{2}\right]\right) \geq \frac{2\left[\frac{x}{2}\right]}{\log_2\left(2\left[\frac{x}{2}\right]\right)} - 1 > \frac{x-2}{\log_2 x} - 1 =$$

$$= \frac{x-2}{\log_2 x}\left(1 - \frac{1}{x}(2 + \log_2 x)\right)$$

Ha $x \geq 8$, akkor van olyan $k \geq 3$ egész, amelyre $2^k \leq x < 2^{k+1}$, ezért:

$$\frac{1}{x}(2 + \log_2 x) \leq \frac{1}{2^k}(k+3) \leq \frac{3}{4}$$

Ez $k = 3$ esetén nyilvánvaló, míg $k \geq 4$-re:

$$\frac{k+3}{2^k} \leq \frac{2k-1}{2^k} \leq \frac{3}{4}$$

Tehát $x \geq 8$ esetén:

$$\pi(x) > \left(1 - \frac{3}{4}\right) \cdot \frac{x}{\log_2 x}$$

A $2 \leq x < 4$ esetén:

$$\frac{x}{\log_2 x} < \frac{4}{1} = 4$$

A $4 \leq x < 8$ esetén:

$$\frac{x}{\log_2 x} < \frac{8}{2} = 4$$

Tehát minden $2 \leq x$ esetén igaz az állítás.

4. Tétel: (Csebisev tétele) Tetszőleges pozitív egész számhoz létezik olyan *p* prímszám, melyre:

$$n < p \leq 2n$$

Bizonyítás: (Erdős Pál bizonyítása) Nézzük $n \geq 5$ egész esetére a $\binom{2n}{n} = \prod_{p \leq 2n} p^{\beta_p}$ felső becslését úgy, hogy szétvágjuk a szorzatot $\sqrt{2n}$-nél, $\frac{2n}{3}$-nál és *n*-nél. Az előző tétel bizonyításában láttuk, hogy:

$$\prod_{p \leq \sqrt{2n}} p^{\beta_p} \leq \prod_{p \leq \sqrt{2n}} p^{\gamma_p} \leq (2n)^{\pi(\sqrt{2n})} \leq (2n)^{\sqrt{2n}-1}$$

Ha $\sqrt{2n} < p \leq \frac{2n}{3}$, akkor $\beta_p \leq \gamma_p = 1$ és az 1. Tétel alapján:

$$\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\beta_p} \leq \prod_{p \leq \frac{2n}{3}} p < 4^{\frac{2n}{3}}$$

Definiáljuk az üres szorzatot 1-nek. Így az eredmény akkor is érvényes lesz, ha $\sqrt{2n}$ $és$ $\frac{2n}{3}$ között nincs prímszám (pl. $n = 5, n = 6, n = 7$). Ha $\frac{2n}{3} < p \leq n$, akkor $\gamma_p = 1$ és $1 \leq \frac{n}{p} < \frac{3}{2}$, valamint $2 \leq \frac{2n}{p} < 3$ révén $\beta_p = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 \cdot 1 = 0$. Ha $n < p \leq 2n$, akkor

$\gamma_p = 1$ $és$ $\beta_p = 1 - 2 \cdot 0 = 1$.

Összegyűjtve a becsléseket és az előző tételeket felhasználva az $n \geq 5$-re, abban az esetben, ha van prím az $]n, 2n]$ intervallumban:

$$\frac{2^{2n}}{2n} < \binom{2n}{n} < (2n)^{\sqrt{2n}-1} \cdot 4^{\frac{2n}{3}} \cdot \prod_{n < p \leq 2n} p$$

Ha nincs prím az $]n, 2n]$ intervallumban, akkor:

$$\frac{2^{2n}}{2n} < \binom{2n}{n} < (2n)^{\sqrt{2n}-1} \cdot 4^{\frac{2n}{3}}$$

Vagyis:

$$\left(\frac{2^{\sqrt{2n}}}{\left(\sqrt{2n}\right)^6}\right)^{\frac{\sqrt{2n}}{3}} < 1$$

A $k = \left[\sqrt{2n}\right] \geq 30$ esetén:

$$\frac{2^{\sqrt{2n}}}{\left(\sqrt{2n}\right)^6} > \frac{2^k}{(k+1)^6} > 1, mivel\ \frac{2^{30}}{31^6} = \left(\frac{32}{31}\right)^6 > 1$$

A $k \geq 30$ esetén:

$$\frac{2^{k+1}}{(k+2)^6} = \frac{2^k}{(k+1)^6} \cdot \frac{2}{\left(1+\frac{1}{k+1}\right)^6} \geq \frac{2^k}{(k+1)^6} \cdot \frac{2}{\left(1+\frac{1}{31}\right)^6} > \frac{2^k}{(k+1)^6}$$

Ugyanis:

$$\left(1+\frac{1}{31}\right)^6 < 1{,}1^6 < 1{,}34^2 < 2$$

Tehát $\left[\sqrt{2n}\right] \geq 30$, azaz $n \geq 450$ esetén biztos, hogy van prímszám az $]n, 2n]$ intervallumban. Ellenőrizhető, hogy az $]n, 2n]$ intervallumban $1 \leq n < 450$ esetén is van prímszám. Biztosan jó a következő prímszámok valamelyike. (Mindegyik kisebb, mint az előtte lévő kétszerese.)

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

Megjegyzések:

1. Csebisev tétele így is megfogalmazható: Tetszőleges pozitív *n* egészre: $\pi(2n) > \pi(n)$.

2. A Csebisev tétel előzménye volt J.L.F. Bertrand (1822-1900) francia matematikus 1845-ben megfogalmazott sejtése: Ha $n > 3$ egész szám, akkor van olyan *p* prímszám, melyre:

$n < p < 2n - 2$. Általánosságban nem tudta bizonyítani, de $n < 3 \cdot 10^6$-ra ellenőrizte.

3. Csebisev 1850-ben bizonyította a következő állítást, amely a fenti tételénél erősebb: Minden $n > 3$ egész számra teljesül, hogy $\pi(2n - 3) > \pi(n)$.

Ezek után nézzünk meg egy becslést az *n*-edik prímszámra. Jelölje a pozitív prímszámok növekvő sorozatát $p_1 = 2, p_2 = 3, p_3 = 5, \cdots, p_n$ az *n*-edik prímszám. Ha a Csebisev tételt *n* helyett p_n-re alkalmazzuk, akkor a $p_{n+1} < 2p_n$ egyenlőtlenséget kapjuk, ami minden pozitív egész *n*-re teljesül.

5. Tétel: Ha p_n az *n*-edik pozitív prímszám, akkor

$$\frac{1}{5} n \log_2 n < p_n < \frac{8}{3} n \log_2 n$$

Bizonyítás: A $\pi(x)$-re kapott becslésekből meghatározhatjuk p_n nagyságrendjét. Mivel tetszőleges pozitív *n* egészre $\pi(p_n) = n$ és $p_n > n$, a 2. tétel alapján $n \geq 2$ esetén:

$$n = \pi(p_n) < 5 \cdot \frac{p_n}{\log_2 p_n} < 5 \cdot \frac{p_n}{\log_2 n}$$

Tehát $p_n > \frac{1}{5} \cdot n \cdot \log_2 n$. A 3. tétel alapján:

$$n = \pi(p_n) > \frac{1}{4} \cdot \frac{p_n}{\log_2 p_n}$$

Ebből csupán $p_n < 4 \cdot n \cdot \log_2 p_n$ adódik. Érdemes a 3. tétel helyett annak bizonyításából az $x \geq 2$ valós számra nyert $\pi(x) > \frac{x-2}{\log_2 x} - 1$ becslést használni nagyobb *x*-ekre. Ha $n \geq 8$ egész szám, akkor $\frac{1}{n} \cdot \log_2 n \leq \frac{3}{8}$. Nézzük a becslést $x = \frac{8}{3} \cdot n \cdot \log_2 n$ esetére, ahol $n \geq 8$ egész szám.

Eszerint:

$$\pi\left(\frac{8}{3}\cdot n\cdot\log_2 n\right) > \frac{\frac{8}{3}\cdot n\cdot\log_2 n-2}{\log_2\left(\frac{8}{3}\cdot n\cdot\log_2 n\right)}-1 \geq \frac{\frac{8}{3}\cdot n\cdot\log_2 n-2}{\log_2(n^2)}-1 =$$

$$= \frac{4}{3}\cdot n-\frac{1}{\log_2 n}-1 \geq n+\frac{n-4}{3} > n = \pi(p_n)$$

Így $p_n < \frac{8}{3}\cdot n\cdot\log_2 n$ teljesül $n \geq 8$ esetén és érvényes $2 \leq n \leq 7$ esetén is. Ha $2 \leq n \leq 3$, akkor:

$$\frac{p_n}{n\cdot\log_2 n} \leq \frac{5}{2\cdot\log_2 2} = \frac{5}{2}$$

Ha $4 \leq n \leq 7$, akkor:

$$\frac{p_n}{n\cdot\log_2 n} \leq \frac{17}{4\cdot\log_2 4} = \frac{17}{8}$$

Tehát igaz az állítás.

Ezt az eredményt alkalmazhatjuk prímszámok reciprokösszegeinek becslésére is. Ha k nemnegatív egész szám, akkor az 5. tétel szerint:

$$\sum_{n=2^k+1}^{2^{k+1}}\frac{1}{p_n} > \frac{3}{8}\cdot\sum_{n=2^k+1}^{2^{k+1}}\frac{1}{n\cdot\log_2 n} \geq \frac{3}{8}\cdot\sum_{n=2^k+1}^{2^{k+1}}\frac{1}{2^{k+1}\cdot(k+1)} = \frac{3}{16\cdot(k+1)}$$

Így tetszőleges *N* pozitív egészre:

$$\sum_{n=1}^{2^N}\frac{1}{p_n} = \frac{1}{2}+\sum_{k=0}^{N-1}\sum_{2^k+1}^{2^{k+1}}\frac{1}{p_n} > \frac{3}{16}\cdot\sum_{k=0}^{N-1}\frac{1}{k+1} = \frac{3}{16}\cdot\sum_{j=1}^{N}\frac{1}{j}$$

Mivel tetszőleges *K* pozitív egészre:

$$\sum_{j=1}^{2^K} \frac{1}{j} = 1 + \sum_{k=0}^{K-1} \sum_{j=2^k+1}^{2^{k+1}} \frac{1}{j} > \sum_{k=0}^{K-1} \sum_{j=2^k+1}^{2^{k+1}} \frac{1}{2^{k+1}} = \frac{K}{2}$$

Ezek alapján a következő tételt kapjuk:

6. Tétel: Ha p_n az *n*-edik pozitív prímszám és *K* pozitív egész szám, akkor:

$$\sum_{n=1}^{2^{2^K}} \frac{1}{p_n} > \frac{3}{32} \cdot K$$

Ebből a tételből már leolvasható, hogy a prímszámok reciprokösszege divergens. Erről a következő részben olvashatunk.

3.3. A prímszámok reciprokösszege

Ebben a fejezetben bebizonyítjuk, hogy a prímszámok reciprokaiból képzett végtelen sor divergens. Ez azt jelenti, hogy a prímek reciprokai „lassan” fogynak, vagyis a prímek „lassan” növekednek. Tehát a prímek viszonylag „sűrűn” helyezkednek el a pozitív egészek között. Ezzel szemben a négyzetszámok reciprokaiból képzett végtelen sor konvergens, azaz a négyzetszámok a pozitív egészeknek egy „ritka” részsorozatát alkotják.

A tételt először Euler mondta ki, ezért az ő bizonyítását nézzük meg. Ez a bizonyítás a divergencia tényén kívül azt is megmutatja, hogy

$$\sum_{p \le n} \frac{1}{p} > \log\log n - 2 \qquad (1)$$

A tételre Erdős Pál is adott egy szellemes indirekt bizonyítást, de ennek ismertetésétől most eltekintünk.

1. Tétel: A prímszámok reciprokaiból képzett végtelen sor divergens, azaz:

$$\sum_{p} \frac{1}{p} = \infty.$$

Bizonyítás: A bizonyításnál az alábbi tételeket használjuk fel:

2. Tétel:

$$\sum_{k=1}^{x} \frac{1}{k} > \log x \,, ha\ x \ge 2.$$

3. Tétel:

$$log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \le x + x^2 \,, ha\ 0 \le x \le \frac{1}{2}$$

4. Tétel:

$$\sum_{k=1}^{l} \frac{1}{k^2} < 2\,, minden\ l > 0\ esetén.$$

Az $x \geq 3$ esetén nézzük a következő szorzatot:

$$A_x = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p}}\right) \qquad (2)$$

ahol:

$$p^{v_p - 1} \leq x < p^{v_p} \qquad (3)$$

Megmutatjuk, hogy

$$A_x > \sum_{k=1}^{x} \frac{1}{k} \qquad (4)$$

Például $x = 10$ esetén:

$$A_{10} = \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4}\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3}\right)\left(1 + \frac{1}{5} + \frac{1}{5^2}\right)\left(1 + \frac{1}{7} + \frac{1}{7^2}\right)$$

Ha $k \leq 10$, akkor *k* kanonikus előállításában csak a 2, 3, 5, 7 prímek szerepelhetnek, és legfeljebb akkora hatványon, mint amilyenen az A_{10} egyes tényezőiben. Tehát tetszőleges $k \leq 10$ szám egyértelműen előáll ezen prímhatványok szorzataként. A_{10}-ben a szorzást végrehajtva minden tag $\frac{1}{k}$ alakú, és tetszőleges $k \leq 10$ esetén az $\frac{1}{k}$ tag tényleg fellép. Tehát a $\sum_{k=1}^{10} \frac{1}{k}$ minden tagja megjelenik A_{10}-ben, azaz:

$$\sum_{k=1}^{10} \frac{1}{k} < A_{10}$$

Ugyanilyen gondolatmenettel az A_x-nél azt kapjuk, hogy:

$$A_x > \sum_{k=1}^{x} \frac{1}{k} \qquad (5)$$

A 2. Tétel és (5) alapján:

$$A_x > \log x \qquad (6)$$

Mivel A_x minden tényezője egy-egy mértani sor, összegezve az egyes tényezőkben, és növelve:

$$A_x = \prod_{p \le x} \frac{1 - \left(\frac{1}{p}\right)^{v_p+1}}{1 - \frac{1}{p}} < \prod_{p \le x} \frac{1}{1 - \frac{1}{p}} \qquad (7)$$

Felhasználva (6)-ot és (7)-et a következőt kapjuk:

$$\log x < \prod_{p \le x} \frac{1}{1 - \frac{1}{p}} \qquad (8)$$

Mivel $x \geq 3$, így (8) mindkét oldala pozitív, ezért áttérhetünk logaritmusra:

$$\log\log x < \sum_{p \le x} \log \frac{1}{1 - \frac{1}{p}} \qquad (9)$$

Alkalmazva a 3. Tételt és (9)-et:

$$loglogx < \sum_{p \le x} \frac{1}{p} + \sum_{p \le x} \frac{1}{p^2} \qquad (10)$$

A 4. Tétel alapján:

$$\sum_{p \le x} \frac{1}{p^2} < \sum_{k=1}^{x} \frac{1}{k^2} < 2 \qquad (11)$$

Végül pedig (10) és (11) miatt:

$$\sum_{p \le x} \frac{1}{p} > \log\log x - 2$$

Nézzünk meg néhány tételt még a prímszámok reciprokösszegével kapcsolatban!

5. Tétel: A $\sum_{p\leq x}\frac{\log p}{p}$ sor aszimptotikusan egyenlő $\log x$-szel, vagyis:

$$\lim_{x\to\infty}\frac{\sum_{p\leq x}\frac{\log p}{p}}{\log x}=1$$

Bizonyítás: A bizonyításnál az alábbi tételeket használjuk fel:

6. Tétel:

$$\sum_{v=1}^{n}\log v=\sum_{p\leq n}\log p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)$$

Ez az $n!$ kanonikus előállítására vonatkozó Legendre-féle formula logaritmizált alakja.

7. Tétel:

$$n\cdot\log n-n<\sum_{v=1}^{n}\log v<(n+1)\cdot\log(n+1)-n$$

8. Tétel:

$$\log(1+x)\leq x$$

9. Tétel:

$$\sum_{k=2}^{\infty}\frac{\log k}{k(k-1)}<4$$

10. Tétel:

$$\sum_{p\leq n}\log p<n\cdot\log 4$$

A 6. és 7. Tétel segítségével becsüljük felülről és alulról az alábbi sort:

$$\sum_{p\leq n}\frac{\log p}{p}$$

Felső becslés:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)=\sum_{v=1}^{n}\log v<(n+1)\cdot\log(n+1)-n \qquad (12)$$

Azonban:

$$(n+1)\cdot\log(n+1)-n=n\cdot\log(n+1)+\log(n+1)-n=$$

$$=n\cdot\log\frac{n+1}{n}+n\cdot\log n+\log(n+1)-n=$$

$$=n\cdot\log\left(1+\frac{1}{n}\right)+n\cdot\log n+\log(n+1)-n \qquad (13)$$

A 8. Tételt az $x=\frac{1}{n}$-re alkalmazva:

$$n\cdot\log\left(1+\frac{1}{n}\right)\le n\cdot\frac{1}{n}=1 \qquad (14)$$

Tehát (13) és (14) miatt:

$$(n+1)\cdot\log(n+1)-n\le 1+n\cdot\log n-n+\log(n+1) \qquad (15)$$

A (12) és (15) alapján:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)<1+n\cdot\log n-n+\log(n+1) \qquad (16)$$

Ha a (16) bal oldalát alulról becsüljük, akkor az alábbiakat kapjuk:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)\ge\sum_{p\le n}\log\ p\left[\frac{n}{p}\right]\ge$$

$$\ge\sum_{p\le n}\log\ p\left(\frac{n}{p}-1\right)=n\cdot\sum_{p\le n}\frac{\log p}{p}-\sum_{p\le n}\log\ p \qquad (17)$$

A 10. Tétel és (17) felhasználásával:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)\ge n\cdot\sum_{p\le n}\frac{\log p}{p}-n\cdot\log 4 \qquad (18)$$

A (16) és (18) alapján *n*-nel végig osztva és rendezve adódik:

$$\sum_{p\le n}\frac{\log p}{p} < \log n + \log 4 - 1 + \frac{\log(n+1)}{n} + \frac{1}{n} \qquad (19)$$

Vagyis ha *n* elég nagy, akkor (19) alapján kapjuk a következő összefüggést:

$$\sum_{p\le n}\frac{\log p}{p} < \log n + 2 \qquad (20)$$

Alsó becslés:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)=\sum_{v=1}^{n}\log v > n\cdot\log n - n \qquad (21)$$

Másrészt:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)<\sum_{p\le n}\log\ p\left(\frac{n}{p}+\frac{n}{p^2}+\cdots\right)=$$

$$=n\cdot\sum_{p\le n}\frac{\log p}{p}+n\cdot\sum_{p\le n}\log\ p\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \qquad (22)$$

Azonban az $\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$ konvergens mértani sor, és így:

$$\sum_{p\le n}\log\ p\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\sum_{p\le n}\log\ p\cdot\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}}=\sum_{p\le n}\log\ p\cdot\frac{1}{p(p-1)} \qquad (23)$$

A 9. Tételt felhasználva:

$$\sum_{p\le n}\frac{\log p}{p(p-1)}<\sum_{k=2}^{n}\frac{\log k}{k(k-1)}<\sum_{k=2}^{\infty}\frac{\log k}{k(k-1)}<4 \qquad (24)$$

A (22), (23) és (24) miatt:

$$\sum_{p\le n}\log\ p\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)<n\sum_{p\le n}\frac{\log p}{p}+4n \qquad (25)$$

A (21) és (25) egyenlőtlenségeket felhasználva és *n*-nel végig osztva adódik:

$$\sum_{p\le n}\frac{\log p}{p} > \log n - 5 \qquad (26)$$

Végül a (20) és (26) alapján a következőt kapjuk:

$$\left|\sum_{p\le n}\frac{\log p}{p} - \log n\right| \le 5 \qquad (27)$$

Ebből pedig következik, hogy

$$\lim_{n\to\infty}\frac{\sum_{p\le n}\frac{\log p}{p}}{\log n} = 1 \qquad (28)$$

11. Tétel: Létezik olyan *c* konstans, hogy elég nagy *n*-re

$$\left|\sum_{p\le n}\frac{1}{p} - \log\log n\right| < c.$$

Bizonyítás: A bizonyításnál az alábbi tételeket használjuk fel:

12. Tétel:

$$x - \log(1+x) < x^2 \;\; ha\; 0 < x \le \frac{1}{2}$$

13. Tétel:

$$\sum_{k=2}^{\infty}\frac{1}{k^2\cdot\log k}\; sor\; konvergens.$$

14. Tétel:

$$\left|\sum_{k=2}^{n}\frac{1}{k\cdot\log(k+1)} - \log\log n\right| < c.$$

A tételt a parciális summázás (Ábel-átrendezés) segítségével bizonyítjuk.

15. Tétel: (Ábel-átrendezés) Legyenek $c_k, d_k, k = 1, \cdots, n$ valós számok és jelölje s_k a

$$\sum_{i=1}^{k} d_i$$

Összeget bármely $k = 1, \cdots, n$ esetén. Ekkor a

$$\sum_{k=1}^{n} c_k d_k$$

Összeg átrendezhető a következő módon:

$$\sum_{k=1}^{n} c_k d_k = \sum_{k=1}^{n} (c_k - c_{k+1}) s_k + c_n s_n$$

A $\sum_{p \le n} \frac{1}{n}$ sort rendezzük át a $\sum_{p \le n} \frac{\log p}{p}$ sor szerint, melyről az 5. Tétel alapján tudjuk, hogy aszimptotikusan $\log n$. Legyen

$$f(n) = \sum_{p \le n} \frac{\log p}{p} \qquad (29)$$

és

$$g(n) = \sum_{p \le n} \frac{1}{p} \qquad (30)$$

Az $f(n)$ definíciója miatt:

$$f(k) - f(k-1) = \begin{cases} 0\,, & ha\ k\ nem\ prím \\ \dfrac{\log p}{p}\,, & ha\ k = p\ prím \end{cases}$$

Ebből:

$$\frac{f(k) - f(k-1)}{\log k} = \begin{cases} 0\,, & ha\ k\ nem\ prím \\ \dfrac{1}{p}\,, & ha\ k = p\ prím \end{cases}$$

Tehát:

$$g(n) = \sum_{k=2}^{n} \frac{f(k) - f(k-1)}{\log k} = \sum_{k=1}^{n-1} \frac{f(k+1) - f(k)}{\log(k+1)} \qquad (31)$$

Most (31)-et átrendezzük $f(n)$ szerint. Legyen

$$f_1(n) = f(n) - \log n \qquad (32)$$

A (27) egyenlőtlenség felhasználásával $n > n_0$ esetén:

$$|f_1(n)| \leq 5 \qquad (33)$$

Így (31) és (32) miatt:

$$g(n) = \sum_{k=1}^{n-1} \frac{f_1(k+1) - f_1(k)}{\log(k+1)} + \sum_{k=1}^{n-1} \frac{\log(k+1) - \log(k)}{\log(k+1)} \qquad (34)$$

Először megvizsgáljuk a (34) jobb oldalának második tagját:

$$\sum_{k=1}^{n-1} \frac{\log(k+1) - \log(k)}{\log(k+1)} = \sum_{k=1}^{n-1} \frac{\log\left(1 + \frac{1}{k}\right)}{\log(k+1)} =$$

$$= \sum_{k=2}^{n} \frac{\log\left(1 + \frac{1}{k}\right)}{\log(k+1)} + \frac{\log 2}{\log 2} - \frac{\log\left(1 + \frac{1}{n}\right)}{\log(n+1)} =$$

$$= \sum_{k=2}^{n} \frac{\log\left(1 + \frac{1}{k}\right)}{\log(k+1)} + 1 - \frac{\log(n+1)}{\log(n+1)} + \frac{\log n}{\log(n+1)} =$$

$$= \sum_{k=2}^{n} \frac{\log\left(1 + \frac{1}{k}\right)}{\log(k+1)} + \frac{\log n}{\log(n+1)} \qquad (35)$$

Alkalmazzuk a 12. Tételt $x = \frac{1}{k}$-ra. Ekkor:

$$\frac{1}{k} - \log\left(1 + \frac{1}{k}\right) < \frac{1}{k^2}$$

Végig oszthatunk a $\log(k+1) > 0$ kifejezéssel, így az alábbit kapjuk:

$$\sum_{k=2}^{n} \frac{1}{k \cdot \log(k+1)} - \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} < \sum_{k=2}^{n} \frac{1}{k^2 \cdot \log(k+1)} \tag{36}$$

Felhasználva a 13. Tételt:

$$\sum_{k=2}^{n} \frac{1}{k \cdot \log(k+1)} - \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} < \sum_{k=2}^{n} \frac{1}{k^2 \cdot \log k} < \sum_{k=2}^{\infty} \frac{1}{k^2 \cdot \log k} = c_1 \tag{37}$$

ahol c_1 pozitív konstans. Másrészt a 8. Tétel alapján:

$$\sum_{k=2}^{n} \frac{1}{k \cdot \log(k+1)} - \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} > 0 \tag{38}$$

Vagyis:

$$\left| \sum_{k=2}^{n} \frac{1}{k \cdot \log(k+1)} - \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} \right| < c_1 \tag{39}$$

Így a 14. Tétel és (39) miatt:

$$\left| \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} - \log\log n \right| < c_2 \tag{40}$$

ahol c_2 pozitív konstans. Végül (35) és (40) alapján elég nagy *n*-re:

$$\left| \sum_{k=1}^{n-1} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} - \log\log n \right| \leq$$

$$\leq \left| \sum_{k=2}^{n} \frac{\log\left(1+\frac{1}{k}\right)}{\log(k+1)} - \log\log n \right| + \left| \frac{\log n}{\log(n+1)} \right| < c_2 + 1 = c_3 \tag{41}$$

Most vizsgáljuk meg (34) jobb oldalának első tagját is (ez a hibatag), a (33)-beli n_0-lal:

$$\sum_{k=1}^{n-1}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}=\sum_{k=1}^{n_0}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}+\sum_{k=n_0+1}^{n-1}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}=$$

$$=c_4+\sum_{k=n_0+1}^{n-1}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}=c_4+\frac{f_1(n_0+2)-f_1(n_0+1)}{\log(n_0+2)}+$$

$$+\frac{f_1(n_0+3)-f_1(n_0+2)}{\log(n_0+3)}+\cdots+\frac{f_1(n-1)-f_1(n-2)}{\log(n-1)}+\frac{f_1(n)-f_1(n-1)}{\log n} \qquad (42)$$

A (42)-t parciálisan szummázva a következőt kapjuk:

$$\sum_{k=1}^{n-1}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}=c_4+\frac{f_1(n)}{\log n}-\frac{f_1(n_0+1)}{\log(n_0+2)}+$$

$$+f_1(n_0+2)\left(\frac{1}{\log(n_0+2)}-\frac{1}{\log(n_0+3)}\right)+\cdots+$$

$$+f_1(n-1)\left(\frac{1}{\log(n-1)}-\frac{1}{\log n}\right) \qquad (43)$$

Így a (33) és a (43) miatt:

$$\left|\sum_{k=1}^{n-1}\frac{f_1(k+1)-f_1(k)}{\log(k+1)}\right|\le c_4+\frac{5}{\log 2}+\frac{5}{\log 2}+5\cdot\sum_{v=n_0+2}^{n-1}\left(\frac{1}{\log v}-\frac{1}{\log(v+1)}\right)=$$

$$=c_5+5\left(\frac{1}{\log(n_0+2)}-\frac{1}{\log n}\right)<c_5+\frac{5}{\log(n_0+2)}=c_6 \qquad (44)$$

Ahol c_5 és c_6 pozitív konstansok. Tehát (34), (41) és (44) felhasználásával arra az eredményre jutunk, hogy elég nagy *n*-re:

$$|g(n)-\log\log n|<c_7 \qquad (45)$$

Ahol:

$$g(n)=\sum_{p\le n}\frac{1}{p}$$

3.4. Modern eredmények

Nézzünk meg néhány modern becslést a prímszámok számára. Ezek élesebbek, mint amiket korábban megismertünk. A 3.2 fejezetben szereplő 2. és 3. Tétel szerint, ha $x \geq 2$, akkor:

$$1 - \frac{3}{4} < \frac{\pi(x)}{\frac{x}{\log_2 x}} < 4 + \frac{3}{4}$$

Ezek a becslések gyengék ahhoz, hogy Csebisev tételét kiadják. Az említett két tétel bizonyításából belátható, hogy nagy *x*-re az alsó és felső becslésnél is lényegesen csökkenthető a $\frac{3}{4}$, sőt még a 4 is, ha ügyesebb szétvágást alkalmazunk.

1. Feladat: Bizonyítsuk be, hogy adott $\varepsilon > 0$-hoz létezik olyan $x_0(\varepsilon)$ korlát, hogy $x \geq x_0(\varepsilon)$ esetén:

$$(1 - \varepsilon)\frac{x}{\log_2 x} < \pi(x) < (2 + \varepsilon)\frac{x}{\log_2 x}$$

Ebből még mindig nem jön ki közvetlenül Csebisev tétele, de a szorzók aránya a korábbi 19-ről a 2 közelébe került.

1. Tétel: Létezik olyan $e > 1$ alapszám, amelynél a logaritmusfüggvény $(1,0)$-beli érintőjének iránytangense 1.

2. Tétel: Az *e* számra igaz a következő két egyenlőség:

$$e = \lim_{n\to\infty}\left(1 + \frac{1}{n}\right)^n \quad \text{és} \quad e = \sum_{n=0}^{\infty}\frac{1}{n!}$$

3. Tétel: A természetes (e) alapú logaritmusra igaz a következő egyenlőtlenség:

$$\log x \leq x - 1$$

Természetes alapú logaritmusra átfogalmazva az 1. Feladatot: A $\varepsilon > 0$ és $x \geq x_0(\varepsilon)$ esetén:

$$(1-\varepsilon)(\log 2)\frac{x}{\log x} < \pi(x) < (2+\varepsilon)(\log 2)\frac{x}{\log x}$$

A $(\log 2)$ közelítő értéke 0,693. Így elég nagy *x*-re a $\pi(x)$ és az $\frac{x}{\log x}$ hányadosa 0,69 és 1,39 közé esik.

Sejtések a $\pi(x)$ közelítésére

Gauss 1792-ben arra a sejtésre jutott, hogy $\int_2^x \frac{dt}{\log t}$ lehet a jó közelítés. Legendre 1798-ban kimondta azt a sejtését, hogy $\pi(x)$ jól közelíthető az $\frac{x}{A\cdot\log x+B}$ kifejezéssel, ahol *A* és *B* állandók, s ezt 1808-ban már $\frac{x}{\log x-1{,}08366}$ alakban fogalmazta meg. Ha azonban legfeljebb $\frac{x}{log^3 x}$ nagyságrendű eltérést engedünk meg $\pi(x)$-től, akkor Legendre konkrét közelítése és Gauss sejtése nem fér össze egymással. Ugyanis sorfejtéssel, illetve parciális integrálással a fenti hibahatáron belül az $\frac{x}{\log x} + 1{,}08366 \cdot \frac{x}{log^2 x}$, illetve az $\frac{x}{\log x} + \frac{x}{log^2 x}$ becslést adnák. Ha $\frac{x}{log^2 x}$ nagyságrendű eltérést engedünk meg, akkor nincs köztük lényeges különbség.
Bármelyik sejtés ezen a hibahatáron belüli teljesüléséből következne, hogy létezik a

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}}$$

határérték és az értéke 1. Csebisev bebizonyította, hogy ha létezik a fenti határérték, akkor értéke 1. A határérték létezését nem sikerült igazolnia. Viszont megmutatta, hogy nagy *x*-ekre Legendre becslése biztosan nem lehet túl pontos. Azóta kiderült, hogy kb. 10^6-ig még Legendre becslése pontosabb, de $5 \cdot 10^6$ felett már Gauss közelítése jobb.

Az 1. Feladat állításánál sokkal pontosabb becslést igazolt Csebisev. Bebizonyította, hogy létezik olyan x_1 korlát, melyre $x \geq x_1$ esetén:

$$0{,}92129 \cdot \frac{x}{\log x} < \pi(x) < 1{,}10556 \cdot \frac{x}{\log x}$$

Legyen $s > 1$ valós szám. Nézzük a következő függvényt:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

A Euler-féle szorzatelőállítás minden $s > 1$ esetén:

$$\zeta(s) = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}$$

G.F.B. Riemann (1826-1866) német matematikus a $\zeta(s)$ függvényt az $s = 1$ kivételével minden komplex s-re értelmezte. Ez a $\pi(x)$ becslésében döntő hatású észrevétel volt. Riemann 1859. november 3-án a Berlini Akadémián tartott székfoglaló előadásának anyaga 1860-ban jelent meg nyomtatásban. Ebben a 9 oldalas dolgozatban vázolt egy lehetőséget a $\pi(x)$ pontosabb becslésére. Észrevételei fantasztikus hatással voltak a matematika fejlődésére, annak ellenére, hogy számos bizonyítatlan felvetés szerepelt a dolgozatban. Máig sem sikerült igazolni a Riemann-féle $\zeta(s)$ függvény komplex gyökeire vonatkozó nevezetes sejtést, miszerint $0 \leq Re\ s \leq 1$ $és$ $\zeta(s) = 0$ $esetén$ $Re\ s = \frac{1}{2}$. 1986-ig ezt már ellenőrizték másfél milliárd gyökre, de teljes bizonyítása még nincs. Bizonyítható, hogy Riemann sejtése azzal ekvivalens, hogy létezik olyan $c > 0$ állandó, hogy minden $x \geq 2$ esetén:

$$\left| \pi(x) - \int_2^x \frac{dt}{\log t} \right| < c x^{\frac{1}{2}} \log x$$

Ettől a ma ismert legjobb becslések is messze vannak. A $\lim_{x \to \infty} \pi(x) x^{-1} \log x$ létezésének igazolása is csupán 1896-ban sikerült.

Prímszámtétel: Létezik az alábbi határérték és az értéke 1.

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

Ezt Riemann gondolatai alapján bizonyította be egymástól függetlenül Hadamard (1865-1963) francia matematikus és Poussin (1866-1962) belga matematikus. 1899-ben Poussin azt is igazolta, hogy létezik olyan c_1 és c_2 pozitív állandó, hogy minden $x \geq 2$ esetén

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| < c_1 x e^{-c_2(\log x)^{\frac{1}{2}}}$$

Az itteni hibatag tetszőleges fix *K*-ra kisebb $\frac{x}{log^K x}$-nél, ha *x* elég nagy.

Gyengébb, de nagy konstanst nem tartalmazó becslést adott 1962-ben J.B. Rosser és

L. Schoenfeld amerikai matematikusok. Ha $n \geq 67$ egész szám, akkor:

$$\frac{n}{\log n - \frac{1}{2}} < \pi(n) < \frac{n}{\log n - \frac{3}{2}}$$

Az 1896-ban bizonyított prímszámtételre sokáig csak függvénytani bizonyítások születtek. Az első elemi számelméleti bizonyítást Erdős Pál és a norvég Selberg adta 1948-ban. A prímszámok analitikus eszközökkel való vizsgálata az elemi becsléseknél sokkal élesebb eredményeket ad, de ezek bizonyítása nagyon nehéz eszközöket kívánnak. Ezek meghaladják e könyv kereteit. Ezekkel a módszerekkel nem csak a prímszámok számára adhatunk becsléseket, hanem egyéb, prímekhez kapcsolódó mennyiségek is jól becsülhetők.

A prímek elméletének több magyar vonatkozása is van. Világhírű pl. Pintz János prímhézagokra vonatkozó eredményei.

4. Megoldatlan problémák

A prímszámok a matematika egyik legegyszerűbben megadott, ugyanakkor talán a legtitokzatosabb halmazát alkotják. Sok olyan kérdést tehetünk fel, amit egy általános iskolás tanuló is megért, azonban a legjobb matematikusok sem tudják megválaszolni. Néhány híres, egyszerűen megfogalmazható, de reménytelenül nehéz megoldatlan problémát vizsgálunk meg a következő fejezetekben.

4.1. Ikerprímek

Definíció: Azokat a prímeket, melyekre p és $p+2$ is prímszám, ikerprímeknek nevezzük.

Megoldatlan probléma, hogy véges vagy végtelen sok van-e ezekből. A sejtés szerint végtelen sok ilyen prímpár létezik. A *2* helyett bármilyen más *2k* páros számra is megoldatlan, hogy van-e végtelen sok prímpár, amelyben a különbség pontosan *2k*. Általánosításképpen prímpárok helyett prímhármasokat, prímnégyeseket, s.í.t., vizsgálhatunk. Egyszerűen belátható, hogy $n, n+2$ és $n+4$ mindegyike csak $n=3$ esetén prímszám. Elképzelhető, hogy végtelen sok olyan *n* van, amelyre $n, n+2$ és $n+6$ mindhárman prímek, vagy

$n, n+2, n+6$ és $n+8$ mindegyike prímszám.

Az ikerprím probléma úgy is megfogalmazható, hogy a szomszédos prímek különbsége vajon végtelen sokszor lesz-e „nagyon kicsi”. Egy másik nevezetes sejtés szerint két egymást követő négyzetszám között mindig található prímszám. E szerint a szomszédos prímek különbsége nem nőhet „túl gyorsan”.

Az ikerprímek, ha végtelen sokan vannak is, mindenképpen „nagyon ritkán” helyezkednek el a prímszámok között. Ugyanis az ikerprímek reciprokösszege konvergens, míg a prímeké divergens. (lásd 3.3 fejezet)

Ikerprímek 2000-ig (61 pár)

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463), (521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661), (809, 811), (821, 823), (827, 829), (857, 859), (881, 883), (1019, 1021), (1031, 1033), (1049, 1051), (1061, 1063), (1091, 1093), (1151, 1153), (1229, 1231), (1277, 1279), (1289, 1291), (1301, 1303), (1319, 1321), (1427, 1429), (1451, 1453), (1481, 1483), (1487, 1489), (1607, 1609), (1619, 1621), (1667, 1669), (1697, 1699), (1721, 1723), (1787, 1789), (1871, 1873), (1877, 1879), (1931, 1933), (1949, 1951), (1997, 1999)

Az első 20 000 ikerprím az alábbi helyen megtekinthető:

http://arnflo.se/~site_files/Other/twinprimes

Ikerprím rekordok

Sorszám	**Iker prímek**	**Számjegyek száma**	**Dátum**
1.	$\mathbf{3756801695685 \cdot 2^{666669} - 1}$	200700	2011. 12. hó
2.	$\mathbf{65516468355 \cdot 2^{333333} - 1}$	100355	2009. 08. hó
3.	$\mathbf{70965694293 \cdot 2^{200006} - 1}$	60219	2016. 04. hó
4.	$\mathbf{66444866235 \cdot 2^{200003} - 1}$	60218	2016. 04. hó
5.	$\mathbf{4884940623 \cdot 2^{198800} - 1}$	59855	2015. 07. hó
6.	$\mathbf{2003663613 \cdot 2^{195000} - 1}$	58711	2007.01. hó
7.	$\mathbf{38529154785 \cdot 2^{173250} - 1}$	52165	2014. 07. hó
8.	$\mathbf{194772106074315 \cdot 2^{171960} - 1}$	51780	2007. 06. hó

9.	$\mathbf{100314512544015 \cdot 2^{171960} - 1}$	51780	2006. 06. hó
10.	$\mathbf{16869987339975 \cdot 2^{171960} - 1}$	51779	2005. 09. hó
11.	$\mathbf{33218925 \cdot 2^{169690} - 1}$	51090	2002. 09. hó
12.	$\mathbf{22835841624 \cdot 7^{54321} - 1}$	45917	2010. 11. hó
13.	$\mathbf{1679081223 \cdot 2^{151618} - 1}$	45651	2012. 02. hó
14.	$\mathbf{9606632571 \cdot 2^{151515} - 1}$	45621	2014. 07. hó
15.	$\mathbf{84966861 \cdot 2^{140219} - 1}$	42219	2012. 04. hó
16.	$\mathbf{12378188145 \cdot 2^{140002} - 1}$	42155	2010. 12. hó
17.	$\mathbf{23272426305 \cdot 2^{140001} - 1}$	42155	2010. 12. hó
18.	$\mathbf{8151728061 \cdot 2^{125987} - 1}$	37936	2010. 05. hó
19.	$\mathbf{2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1}$	35851	2013. 12. hó
20.	$\mathbf{598899 \cdot 2^{118987} - 1}$	35825	2010. 04. hó

Részeredmények:

Viggo Brun 1915-ben bebizonyította, hogy *x*-ig az ikerprímek száma legfeljebb

$$c \cdot \frac{x}{(\log x)^2}$$

alkalmas *c*-vel, és hogy az ikerprímek reciprokösszege konvergál. A másik irányban igazolta, hogy végtelen sok olyan páratlan *n* szám van, hogy *n* és *n+2* is legfeljebb 9 prímszám szorzata.

1973-ban Chen igazolta, hogy van végtelen sok olyan p prímszám, hogy $p+2$ prímszám vagy két prímszám szorzata.

1940-ben Erdős Pál megmutatta, hogy létezik olyan $c < 1$ konstans és végtelen sok p prím, hogy

$q - p < c \cdot \ln p$, ahol q a p-t követő prímet jelöli.

Ez az eredmény már jelentősen javult, hiszen 1986-ban Helmut Maier megmutatta, hogy $c < 0{,}25$ konstans is biztosan létezik. 2004-ben Daniel Goldston és Cem Yıldırım belátta, hogy a $c = 0{,}085786\ldots$ konstans is megfelel a feltételeknek. Ezt 2005-ben megjavították (Goldston, Pintz és Yıldırım), belátva azt, hogy minden 0-nál nagyobb c konstans megfelel, sőt

$$q - p < C \cdot \sqrt{\ln p}\,(\ln \ln p)^2$$

is igaz végtelen sokszor alkalmas C-vel.

2013 áprilisában Jitang Csang, a Durhamban található New Hampshire-i Egyetem professzora bebizonyította, hogy végtelen sok olyan prímszámpár létezik, amelyek különbsége kevesebb, mint 70 millió. Ez azért nagy eredmény, mert a különbség véges szám. Az MTA Rényi Intézet kutatója, Pintz János akadémikus professzor elmondta: „a lényeg, hogy végtelen sokszor valamilyen konkrét véges határ alatt marad a szomszédos prímek különbsége."

4.2. Goldbach-sejtés

A Goldbach-sejtés, ahogyan azt a neve is mutatja, ma sem bizonyított tétel. A sejtés két állítást mond ki:

1. Minden 2-nél nagyobb páros szám előállítható két prímszám összegeként.

2. Minden 5-nél nagyobb páratlan szám előállítható három páratlan prímszám összegeként.

Goldbach ezeket 1742-ben Eulernek küldött levelében jegyezte le. Érdekes tény, hogy a 2. állítás következik az 1.-ből, amire Euler jött rá. Így az első sejtést erős Goldbach-sejtésnek, a másodikat gyenge Goldbach-sejtésnek nevezzük. Mivel egy páratlan számból pl. 3-at elvéve páros számot kapunk, és ha ez két prímszám összege, akkor az eredeti páratlan szám három prímszám összege.

4.3. Speciális alakú prímek

Ebben a fejezetben vizsgáljuk meg a $2^k + 1$ és a $2^k - 1$ alakú prímszámokat! Az előbbieket Fermat-prímeknek, az utóbbiakat Mersenne-prímeknek nevezzük. A mai napig megoldatlan kérdés, hogy létezik-e végtelen sok ilyen típusú prímszám.

1. Fermat-prímek

Tekintsük a $2^k + 1$ alakú számokat, ahol $k \geq 1$. Nézzük meg az első nyolc közül melyek lesznek prímek:

$k = 1\colon\ 2^1 + 1 = 3\ prím, \qquad k = 2\colon\ 2^2 + 1 = 5\ prím$

$k = 3\colon\ 2^3 + 1 = 9\ nem\ prím, \qquad k = 4\colon\ 2^4 + 1 = 17\ prím$

$k = 5\colon\ 2^5 + 1 = 33\ nem\ prím, \quad k = 6\colon\ 2^6 + 1 = 65\ nem\ prím$

$k = 7\colon\ 2^7 + 1 = 129\ nem\ prím, \quad k = 8\colon\ 2^8 + 1 = 257\ prím$

Definíció: Az $F_n = 2^{2^n} + 1$ alakú számokat, ahol $n \geq 1$ Fermat-számoknak, az ilyen alakú prímeket pedig Fermat-prímeknek nevezzük.

Tétel: Ha $k \geq 0$ $és$ $2^k + 1$ prímszám, akkor létezik $n \geq 0$ $úgy, hogy$ $k = 2^n$.

Bizonyítás: Ha $k = 2^n \cdot m, ahol\ m\ páratlan, akkor$ $2^k + 1 = \left(2^{2^n}\right)^m + 1$ osztható $2^{2^n} + 1 - gyel$. Ebből következik, hogy $2^{2^n} + 1 = 2^k + 1$. Vagyis $m = 1$.

Pierre Fermat (1601-1665) francia matematikus és fizikus egy 1640-ben írott levelében azt sejtette, hogy az F_n számok mindegyike prím.

Az $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ prímek. Az $F_5 = 641 \cdot 6700417$, vagyis nem prímszám. Ezt Euler igazolta 1732-ben. Ebből következik, hogy a tétel megfordítása nem igaz. Ezt kongruenciák tulajdonságaival az alábbi módon bizonyíthatjuk:

$641 = 640 + 1 = 5 \cdot 2^7 + 1, így\ 5 \cdot 2^7 \equiv -1\ (mod\ 641)$, ezt negyedik hatványra emelve:

$5^4 \cdot 2^{28} \equiv 1\ (mod\ 641)$. Másrészt $641 = 625 + 16 = 5^4 + 2^4, ebből\ 2^4 \equiv -5^4\ (mod\ 641)$

Az utóbbi két kongruenciát összeszorozva:

$$5^4 \cdot 2^{32} \equiv -5^4\ (mod\ 641)$$

Ha elosztjuk 5^4-nel, ahol $(5^4, 641) = 1$, a következőt kapjuk:

$$2^{32} + 1 = 2^{2^5} + 1 \equiv 0\ (mod\ 641)$$

Landry 1880-ban igazolta, hogy F_6 összetett szám:

$$F_6 = 274177 \cdot 67280421310721$$

A Fermat-prímekről tudjuk, hogy:

1. F_n összetett és ismert F_n prímtényezős felbontása

$n = 5, 6, 7, 8 - ra$ ($két\ prímtényező$)

$n = 9 - re$ ($három\ prímtényező$)

$n = 10 - re$ ($négy\ prímtényező$)

$n = 11 - re$ (öt $prímtényező$)

2. F_n összetett és ismert F_n legalább egy prímtényezője, de nem ismert a teljes felbontása, ha

$n = 12, 13, 15, 16, 17, 18, 19, 21, 23, 25, 26, 27, 28, 29, 30, 31, 32, 36, 37, 38, 39, 42, 43, \cdots$

3. F_n összetett, de nem ismert F_n egyetlen prímfaktora sem, ha $n = 14, 20, 22, 24$

4. Jelenleg 225 Fermat-számról tudjuk, hogy összetett.

5. Jelenleg öt Fermat-prímet ismerünk:

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$

A Fermat-prímekről nem tudjuk, hogy:

1. Az előbb felsorolt öt Fermat-prímektől különbözőek léteznek-e. (Egy sejtés szerint nem a válasz.)

2. F_n összetett-e vagy sem, ha $n = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, \cdots$

Újabb eredmények:

1. John Cosgrave 2003.10.10. :

$$3 \cdot 2^{2478785} + 1\ osztója\ F_{2478782} - nek$$

Ez a legnagyobb ismert összetett Fermat-szám.

2. M. Parcher 2005.05.15. :

$$2018719057 \cdot 2^{1162} + 1\ osztója\ F_{1160} - nak$$

3. Asko Vuori 2005.09.29. :

$$6213186413 \cdot 2^{605} + 1 \; osztója \; F_{600} - nak$$

A Fermat-prímek azért is érdekesek, mert Gauss egy nevezetes tétele szerint pontosan azok a szabályos *n*-szögek szerkeszthetők meg körzővel és vonalzóval, amelyekre *n* egyenlő 2 valamely hatványának és különböző Fermat-prímeknek a szorzatával.

A Fermat-számokra vonatkoznak az alábbi eredmények:

Tétel: (E. Lucas 1877.) Ha $n \geq 2$ és a *p* prímszám osztója az $F_n = 2^{2^n} + 1$ Fermat-számnak, akkor $p = 2^{n+2} \cdot k + 1 \; alak$ú, $ahol \; k \geq 1$.

Tétel: (Pepin-teszt) Az $n \geq 1$ esetben F_n akkor és csak akkor prím, ha

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$$

2. Mersenne-prímek

Tekintsük a $2^n - 1$ alakú számokat, ahol $n \geq 1$. Nézzük meg az első nyolc közül melyek lesznek prímek:

$n = 1$: $2^1 - 1 = 1 \; nem \; prím$

$n = 2$: $2^2 - 1 = 3 \; prím$

$n = 3$: $2^3 - 1 = 7 \; prím$

$n = 4$: $2^4 - 1 = 15 \; nem \; prím$

$n = 5$: $2^5 - 1 = 31 \; prím$

$n = 6$: $2^6 - 1 = 63 \; nem \; prím$

$n = 7$: $2^7 - 1 = 127 \; prím$

$n = 8$: $2^8 - 1 = 255 \; nem \; prím$

Ha az n összetett, akkor $2^n - 1$ is összetett szám, mert igaz a következő tétel.

Tétel: Ha $n \geq 1$ és $2^n - 1$ prímszám, akkor n prímszám.

Bizonyítás: Ha n nem prím, akkor felírható $n = a \cdot b$ alakban, ahol $a, b > 1$.

Így $2^n - 1 = (2^a)^b - 1$ osztható $2^a - 1$-gyel, és $a, b \geq 1$ miatt $2^a - 1 \neq 1$, $\frac{2^n-1}{2^a-1} \neq 1$, ami ellentmondás. Azonban: $n = 11$: $2^{11} - 1 = 2047 = 23 \cdot 89$ $nem\ prím$. Tehát a tétel megfordítása nem igaz.

Definíció: Az $M_p = 2^p - 1$ alakú számokat, ahol p prím Mersenne-számoknak nevezzük. Az ilyen alakú prímeket pedig Mersenne-prímeknek.

Marin Mersenne (1588-1648) francia matematikus, minorita szerzetes volt. Fermat, Descartes és más tudósokkal komoly tudományos levelezést folytatott. A minél nagyobb tökéletes számok előállításának reményében kereste az ilyen típusú prímeket. Mersenne tudta, hogy nehéz egy nagy számról eldönteni prím voltát. (Ahhoz, hogy egy 15 vagy 20-jegyű számról megállapítsuk prím-e, egy egész élet sem elég.)

1644-ben megadta az M_p prímek listáját, ahol $p \leq 257$. Szerinte

$p = 2,3,5,7,13,17,19,31,67,127,257$ esetén kapunk M_p prímeket, minden más p esetén összetett szám lesz.

Azonban ez $p = 67$ és $p = 257$ esetén nem igaz! Több mint kétszáz évig senki sem tudta, hogy Mersenne listája helyes-e. Az első hibát 1876-ban találta meg a francia Lucas. Bebizonyította, hogy $2^{67} - 1$ összetett, de tényezőkre nem tudta felbontani.

Végül az amerikai Cole találta meg 1903-ban az alábbi felbontást, miután több éven keresztül csak ezzel a kérdéssel foglalkozott:

$$2^{67} - 1 = 193707721 \cdot 761838257287$$

Mersenne listájában később további négy hibát találtak:

A hiányzó $2^{61} - 1, a\ 2^{89} - 1, és\ a\ \ 2^{67} - 1$ is prímszám, viszont a $2^{257} - 1$ összetett szám.

Eddig 51 Mersenne-prímet ismerünk. Ezeket az alábbi táblázat mutatja:

Sorszám	**Hatványkitevő**	**Számjegyek száma**	**Megtalálója**	**Időpont**
1.	2	1	görög matematikus	ie. 500 körül
2.	3	1	görög matematikus	ie. 500 körül
3.	5	2	görög matematikus	ie. 250 körül
4.	7	3	görög matematikus	ie. 250 körül
5.	13	4	ismeretlen	1456.
6.	17	6	P.A.Cataldi	1588.
7.	19	6	P.A.Cataldi	1588.
8.	31	10	L.Euler	1772.
9.	61	19	Pervusin	1883.
10.	89	27	Fauquembergue és Powers	1911.01.
11.	107	33	Fauquembergue és Powers	1914.06.11.
12.	127	39	E. Lucas	1876.01.10.

13.	521	157	Lehmer és Robinson	1952.01.30.
14.	607	183	Lehmer és Robinson	1952.01.30.
15.	1279	386	Lehmer és Robinson	1952.06.25.
16.	2203	664	Lehmer és Robinson	1952.10.07.
17.	2281	687	Lehmer és Robinson	1952.10.09.
18.	3217	969	H.Riesel	1957.09.08.
19.	4253	1281	A.Hurwitz	1961.11.03.
20.	4423	1332	A.Hurwitz	1961.11.03.
21.	9689	2917	D.B.Gillies	1963.05.11.
22.	9941	2993	D.B.Gillies	1963.05.16.
23.	11213	3376	D.B.Gillies	1963.06.02.
24.	19937	6002	B.Tuckerman	1971.03.04.
25.	21701	6533	L.C.Noll és L.Nickel	1978.10.30.
26.	23209	6987	L.C.Noll	1979.02.09.
27.	44497	13395	H.L.Nelson és D.Slowinski	1979.04.08.
28.	86243	25962	D.Slowinski	1982.09.25.
29.	110503	33265	W.Colquitt és L.Welsh	1988.01.28.
30.	132049	39751	D.Slowinski	1983.09.19.
31.	216091	65050	D.Slowinski	1985.09.01.
32.	756839	227832	D.Slowinski és P.Gage	1992.02.19.

33.	859433	258716	D.Slowinski és P.Gage	1994.01.04.
34.	1257787	378632	D.Slowinski és P.Gage	1996.09.03.
35.	1398269	420921	GIMPS/ J.Armengaud	1996.11.13.
36.	2976221	895932	GIMPS/G.Spence	1997.08.24.
37.	3021377	909526	GIMPS/R.Clarkson	1998.01.27.
38.	6972593	2098960	GIMPS/N.Hajratwala	1999.06.01.
39.	13466917	4053946	GIMPS/M.Cameron	2001.11.14.
40.	20996011	6320430	GIMPS/ M.Shafer	2003.11.17.
41.	24036583	7235733	GIMPS/ J.Findley	2004.05.15.
42.	25964951	7816230	GIMPS/ M.Nowak	2005.02.18.
43.	30402457	9152052	GIMPS/C.Cooper és S.Boone	2005.12.15.
44.	32582657	9808358	GIMPS/C.Cooper és S.Boone	2006.09.04.
45.	37156667	11185272	GIMPS/H.M.Elvenich	2008.09.06.
46.	42643801	12837064	GIMPS/O.M.Strindmo	2009.06.04.
47.	43112609	12978189	GIMPS/E.Smith	2008.08.23.
48.	57885161	17425170	GIMPS/ C.Cooper	2013.01.25.
49.	74207281	22338618	GIMPS/C.Cooper	2016.01.07.
50.	77232917	23249425	GIMPS/Jonathan Pace	2018.01.05.
51.	82 589 933	24 862 048	GIMPS / Patrick Laroche	2018.12.7.

Jelenleg az 51. Mersenne-prím a legnagyobb ismert prímszám. Az új legnagyobb prímszám megtalálója, a floridai Patrick Laroche a GIMPS programot használta fel Intel i5-4590T 4C/4T (Haswell) számítógépén.

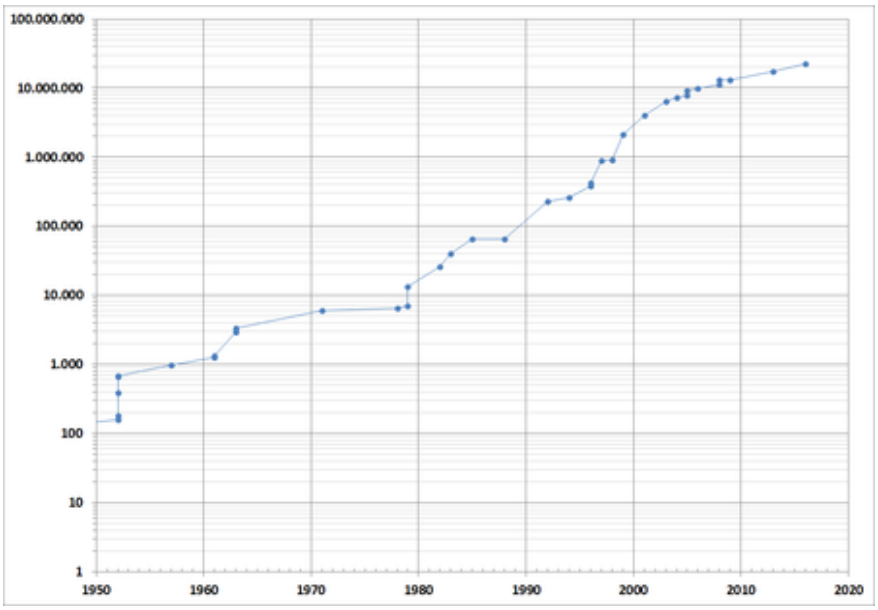
Új felhasználó, mert csak négy hónapja látott neki a keresésnek, és szerencséje is lehetett, mert 12 hét leforgása után már megtalálta az M82589933 számot.

Jonathan Pace az ötvenedik Mersenne prímszám megtalálója volt, egy évvel korábban. A GIMPS alkalmazást annak keletkezésétől használta 14 éven át, amikor sikerrel járt. A foglalkozása villamos mérnök, a jutalma 3000 USD volt. Valószínűleg nem a pénz motiválta!

Nagy prímek keresése:

1996-ban indult egy program, a Nagy internetes Mersenne-prím keresés (Great Internet Mersenne Prime Search, (GIMPS), melyben ma több mint 300 ezer személyi számítógépen fut a program. A kutatásban bárki részt vehet. A GIMPS szoftver igencsak sikeresként szerepel a prímek megtalálásában. A 2^20000000-1 és 2^85000000-1 közötti szakaszon már 12-t talált meg.

A kutatás akkor fejeződik be, ha valaki megtalálja az első, legalább 100 000 000 számjegyből álló Mersenne-prímet. A jutalma 100 000 USD.



Ábra az adott évben ismert legnagyobb Mersenne-prím számjegyeinek számáról.

A Mersenne-prímek kapcsolódnak a tökéletes számokhoz, hiszen Mersenne is ezek kapcsán vizsgálta ezeket a prímeket.

Ez a fogalom a Püthagoreusoktól származik (i.e. 550 körül), akik tökéletesnek neveztek egy *n* számot, ha *n* egyenlő az önmagától kisebb osztóinak az összegével. Mai jelöléssel: $\sigma(n) = 2n$.

A legkisebb tökéletes számokat Eukleidész is ismerte (i.e. 300 körül). Az Elemek című művében ő bizonyította a következő állítást:

Tétel: Ha $2^k - 1$ prímszám, akkor $n = 2^{k-1} \cdot (2^k - 1)$ tökéletes szám.

Euler közel 2000 évvel később igazolta a tétel megfordítását.

Tétel: Ha *n* páros tökéletes szám, akkor $n = 2^{k-1} \cdot (2^k - 1)$ alakú, ahol $2^k - 1$ prímszám.

Bizonyítás: Legyen $n = 2^a \cdot m,\ ahol\ a \geq 1\ és\ m\ páratlan.$

Így $\sigma(n) = \sigma(2^a \cdot m) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$ és innen $\sigma(n) = 2n$ alapján:

$$(2^{a+1} - 1)\sigma(m) = 2^{a+1} \cdot m$$

Ebből következik, hogy $(2^{a+1} - 1) - 1\ osztója\ a\ 2^{a+1} \cdot m$ kifejezésnek.

Mivel $(2^{a+1} - 1, 2^{a+1}) = 1$, ezért $2^{a+1} - 1$ osztója *m*-nek, vagyis $m = (2^{a+1} - 1) \cdot m_1$.

Ezt visszahelyettesítve:

$(2^{a+1} - 1)\sigma(m) = (2^{a+1} - 1)2^{a+1} \cdot m_1, és\ ebből: \sigma(m) = 2^{a+1} \cdot m_1.$

Az m_1 *és* m *osztói* $m - nek.$

$$m_1 < m\ és\ m_1 + m = m_1 + (2^{a+1} - 1) \cdot m_1 = 2^{a+1} \cdot m_1 = \sigma(m)$$

Így $m - nek\ m_1 - en$ *és* $m - en$ kívül nincs más osztója. Ebből azt kapjuk, hogy:

$m_1 = 1\ és\ m = 2^{a+1} - 1\ prímszám.$

Tehát az $a = k - 1$ jelöléssel $n = 2^{k-1} \cdot (2^k - 1), ahol\ 2^k - 1$ prímszám.

Így n akkor és csak akkor páros tökéletes szám, ha $n = 2^{k-1} \cdot M_p$ alakú, ahol M_p Mersenne-prím. Nem tudjuk, hogy létezik-e végtelen sok Mersenne-féle prímszám, így azt sem tudjuk, hogy van-e végtelen sok tökéletes szám. Arra a kérdésre sem ismerjük a választ, hogy létezik-e páratlan tökéletes szám.

Milyen tulajdonságok alapján kereshetők meg az M_p számok prímtényezői és dönthető el, hogy M_p prím vagy sem? A Mersenne-számok lehetséges prím tényezőire vonatkoznak az alábbi tételek.

Tétel: Legyen $p > 2$ prímszám! Ekkor M_p bármely pozitív osztója egyszerre

$2kp + 1$ *és* $8r \pm 1$ alakú.

Példa: Legyen $p = 47$. Ekkor $M_{47} = 2^{47} - 1$ tetszőleges q prímosztója $94k + 1$, illetve $8r \pm 1$ alakú. Az így adódó

$$x \equiv 1 \ (mod\ 94), \text{és}\ \ x \equiv \pm 1 \ (mod\ 8)$$

szimultán kongruencia rendszereket megoldva:

$$x \equiv 1 \text{ és } 95 \ \ (mod\ 376)$$

Az ilyen alakú prímek: $q = 1129, 1223, 2351, \cdots$

Ezek közül $2351\ osztója\ M_{47} - nek, tehát\ M_{47}$ összetett.

Lehetséges, hogy Mersenne is ismerte $M_{47} - nek$ ezt a prímosztóját és ezért tudatosan hagyta ki a $p = 47$ értéket a listájáról.

Bizonyítás: A Fermat-számokhoz hasonlóan elég az állítást prímosztókra igazolni. Tegyük fel, hogy a q prímre teljesül: q osztója $2^p - 1 - nek$, vagyis $2^p \equiv 1 \ (mod\ q)$.

Ekkor $o_q(2)$ osztója p-nek, továbbá $o_q(2) \neq 1$, tehát $o_q(2) = p$. Innen kapjuk, hogy p osztója $q - 1 - nek, azaz\ q = tp + 1$ alakú. Mivel q és p páratlan, ezért t páros vagyis

$q = 2kp + 1$ alakú.

A $q = 8r \pm 1$ állításhoz azt kell igazolni, hogy a *2* kvadratikus maradék *mod q*. Ez a $2^p \equiv 1 \ (mod\ q)$ kongruenciából *p* páratlanságának és a Legendre-szimbólum tulajdonságainak felhasználásával az alábbi módon adódik:

$$\left(\frac{2}{q}\right) = \left(\frac{2}{q}\right)^p = \left(\frac{2^p}{q}\right) = \left(\frac{1}{q}\right) = 1$$

Tétel: (Lucas-Lehmer-teszt)

Legyen $p > 2$ prím, továbbá $a_1 = 4$ *és* $a_{i+1} = a_i^2 - 2, ha\ i \geq 1$. Ekkor M_p pontosan akkor prím, ha M_p osztója $a_{p-1} - nek.$ (1)

Példa: Legyen $p = 5$. Ekkor:

$a_1 = 4,\ a_2 = 14,\ a_3 = 194 \equiv 8\ (mod\ 31)$ *és* $a_4 \equiv 62 \equiv 0\ (mod\ 31)$, tehát

$M_5 = 31\ prím.$

Az (1) feltétel teljesülésének ellenőrzésekor elég az a_i-knek csak a modulo M_p vett maradékát kiszámítani, összesen $p - 2 \approx log_2 M_p$ négyzetre emelési, valamint kivonási és redukciós lépést kell végrehajtani.

4.4. Prímképletek

Az elmúlt évszázadokban, sőt még napjainkban is vannak akik keresik a prímszámokat előállító képletet. Megadható-e olyan képlet, amely minden *n*-re előállítja az *n*-edik prímszámot? Van-e olyan (a természetes számokon értelmezett), a gyakorlatban is kiszámítható függvény, amelynek minden helyettesítési értéke prímszám? Vizsgáljuk meg a kérdést! Általános vélekedés szerint ilyen képletre nincs remény.

Fermat azt sejtette, hogy a $2^{2^k} + 1$ alakú számok tetszőleges *k* természetes szám esetén prímszámok. Ha $k = 0,1,2,3,4$, akkor tényleg prímet kapunk. Ezek:

$$3, 5, 17, 257, 65537$$

Azonban Euler megmutatta, hogy $k = 5$ esetén $2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700417$ már nem prím. A mai napig egyetlen prímet sem találtak, pedig további 40 Fermat-számot vizsgáltak számítógépek segítségével.

Euler észrevette, hogy az $n^2 + n + 41$ minden $0 \leq n \leq 39$ esetén prímszámot ad. (Az $n = 40$-re már összetett szám lesz.) Ebből azonnal adódik, hogy:

$$(n - 40)^2 + (n - 40) + 41 = n^2 - 79n + 1610$$

minden $0 \leq n \leq 79$ természetes szám esetén prímszám. Ha racionális együtthatós polinomokat is megengedünk, akkor akármilyen hosszú ilyen prímsorozatot tudunk gyártani.

Tétel: Legyen *k* tetszőleges pozitív egész. Ekkor van olyan f racionális együtthatós polinom, amelyre bármely $1 \leq i \leq k$ esetén $f(i)$ éppen az *i*-edik prímszám.

Azonban egy nem konstans polinom biztosan nem lehet prímképlet, mert nem vehet fel minden egész helyen prímet. Ugyanis igaz a következő két tétel.

Tétel: Egy nem konstans polinom nem veheti fel a 0 értéket végtelen sokszor.

Bizonyítás: A másod-és magasabb fokú polinomokra is teljesül, hogy ha valamely x_0 helyen gyöke van, akkor kiemelhető belőle egy $(x - x_0)$ szorzótényező. Ezért egy *n*-edfokú polinom legfeljebb *n* darab elsőfokú tényező szorzatára bontható, vagyis legfeljebb *n* darab gyöke lehet. Tehát legfeljebb *n* helyen veheti fel a 0 függvényértéket.

Következmény: Egy nem konstans polinom egyetlen függvényértéket sem vehet fel végtelen sokszor.

Tétel: Nincs olyan egész együtthatós, nem konstans polinom, amely minden természetes szám helyen prím értéket vesz fel.

Bizonyítás: Tekintsük az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ polinomot, ahol az

$a_0, a_1, a_2, \cdots, a_n$ együtthatók egész számok.

Ha $a_0 = 0$, akkor tetszőleges *n*-re az $x = n$ helyen felvett helyettesítési érték osztható *n*-nel, így ha például *n* összetett szám, akkor a helyettesítési sem lehet prím.

Ha $a_0 \neq 0$, akkor vizsgáljuk meg, hogy milyen értékeket vehet fel a polinom az

$x = 0, |a_0|, |2a_0|, |3a_0|, \cdots$ helyeken. Nyilván az összes ilyen helyen osztható lesz a helyettesítési érték a_0-val. Egy a_0-val osztható szám csak úgy lehet prímszám, ha vagy

$|a_0| = 1$, vagy a_0 maga ennek a prímnek asszociáltja. Az, hogy a fenti helyek mindegyikén ugyanannak a prímnek az asszociáltja legyen a helyettesítési érték, nem lehetséges, hiszen egy polinom nem veheti fel végtelen sokszor ugyanazt az értéket.

Ha $a_0 = 1$, akkor például az $x = 0$ helyen nem lesz prím a helyettesítési érték. Ugyanis $f(0) = a_0$, ami most 1, és az 1 nem prímszám. Vagyis a fenti polinom semmilyen esetben sem vehet fel csak prím értékeket. Tehát igaz az állítás.

Most nézzünk meg három olyan eredményt, amelyek elméleti szempontból jelentősek, de a gyakorlati kiszámíthatóság követelményének nem felelnek meg.

1. Legyen

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^{2^n}}} = 0{,}000200000000000300\cdots$$

azaz *c* egy olyan tizedes tört, amelyben sorra a prímek tízes számrendszerbeli alakját írjuk le, amelyeket megfelelő számú 0-val választunk el, hogy „biztosa ne érjenek egymásba”. Ekkor teljesül a következő egyenlőség:

$$p_n = \left[10^{2^{2^n}} \cdot c\right] - 10^{2^{2^n} - 2^{2^{n-1}}} \cdot \left[10^{2^{2^{n-1}}} \cdot c\right]$$

2. Létezik olyan $\alpha > 1$ valós szám, amelyre a következő formula minden *n* pozitív egész esetén prímszám:

$$\left[\alpha^{3^n}\right]$$

Megjegyzés: A fenti két állításban a sarkos zárójel a szám egészrészét jelenti.

3. Meglepő a következő eredmény is. Megadható olyan többváltozós egész együtthatós polinom, amelynek a változók nemnegatív értékein felvett pozitív helyettesítési értékei megegyeznek a prímszámok halmazával.

Ez a polinom ugyanazt a prímet több helyen is felveheti, illetve negatív értékeket is felvesz. Ilyen polinom létezését először Matijaszevics igazolta 1970-ben. Ekkor oldotta meg Hilbert tizedik problémáját. Bebizonyította, hogy nem létezik olyan általános algoritmus, amely bármely Diofantoszi egyenlet esetén eldönti, hogy van-e megoldása vagy sem. Módszeréből egyúttal a fent jelzett polinom létezése is kiderült. Az ilyen polinomokra vonatkozó jelenlegi rekord: Ha a minimális változószám 10, akkor a fokszám kb. $1{,}6 \cdot 10^{45}$.

4.5. Prímekből álló számtani sorozatok

A matematikusokat több mint kétszáz éve foglalkoztatja, hány tagból állhat egy prímszámokból álló számtani sorozat, és hány ilyen sorozat létezik. Van-e tetszőlegesen hosszú, prímekből álló számtani sorozat? A számelmélet e nevezetes sejtése tulajdonképpen egyik matematikus nevéhez sem fűződik. Feltehetően már Joseph Louis Lagrange és Edward Waring felvetette 1770-ben, amikor azt vizsgálták, egy *n* hosszúságú, prímszámokból álló számtani sorozat differenciája mekkora lehet.

1939-ben a holland matematikus, Johannes van der Corput és Theodor Estermann bebizonyította, hogy háromtagú, prímszámokból álló számtani sorozatból, mint például a 3, 5, 7 vagy a 47, 53, 59, végtelen számú létezik. A továbblépés csak 1981-ben sikerült Roger Heart-Brown matematikusnak. Ő igazolta, hogy van végtelen sok négytagú számtani sorozat, amiben van három prímszám és a negyedik tagja legfeljebb két prímszám szorzata. 1992-ben Balog Antal bebizonyította, hogy minden *k*-ra van *k* darab prímszám, $p_1, \cdots, p_k$, hogy $\frac{p_i+p_j}{2}$ átlagok, ahol $1 \leq i < j \leq k$, különböző prímszámok. E tételből és abból, hogy minden $n \geq 3, n \neq 6$ értékre van két ortogonális latin négyzet, már következik, hogy minden $n \geq 3$ esetén létezik különböző prímekből álló nxn-es bűvös négyzet.

Ám, hogy tetszőleges számú tagból állhat egy ilyen sorozat, és végtelen számú sorozat létezik minden tetszőleges számúból, azt 2004-ben sikerült Ben Green (University of British Columbia, Vancouver) és Terence Tao (University of California, Los Angeles) matematikusoknak bizonyítaniuk.

Tétel: Minden olyan prímszámokból álló A halmaz tartalmaz tetszőleges hosszúságú számtani sorozatot, aminek pozitív a relatív sűrűsége, azaz

$$\lim_{x\to\infty} \frac{inf A(x)}{\pi(x)} > 0$$

ahol $A(x)$ az A halmaz x-nél kisebb tagjainak a száma, $\pi(x)$ pedig a prímek száma x-ig.

A tételt 2006-ban Tao és Tamar Ziegler kiterjesztette polinom-érték különbségű sorozatokra. Bebizonyították, hogy ha $p_1(x), \cdots, p_k(x)$ egész együtthatós, nulla konstans taggal rendelkező polinomok, akkor van végtelen sok olyan egész (a, b) számpár, hogy $a + p_1(b), \cdots, a + p_k(b)$ valamennyien prímek.

2007-ben Tao igazolta a Gauss-prímekre a következő állítást:

Ha $b_1, \cdots b_k$ Gauss-egészek, akkor létezik r pozitív egész szám és a Gauss-egész, hogy $a + rb_1, \cdots, a + rb_k$ valamennyien Gauss-prímek.

A 2004-es tétel 49 oldalas bizonyítása sajnos olyan értelemben nem konstruktív, hogy csupán a létezését bizonyítja a tetszőleges számú prímszámból álló számtani sorozatoknak, illetve hogy ezekből végtelen számú lehet, olyan formulát nem ad az érdeklődők kezébe, amellyel ezek a sorozatok megjósolhatók. Ez a kutatási terület még nyitott a nagy számok kedvelői előtt.

Egy hüvelykujjszabállyal azonban tudunk segítséget nyújtani azoknak, akik prímszám-sorozatokat akarnak előállítani. Biztosan állíthatjuk, hogy ha hat elemből álló sorozatot szeretnénk, akkor a tagok közötti különbség legalább 30 vagy sokszorosa. A 30 a 6-nál kisebb prímszámok (1, 2, 3, 5) szorzatából áll össze. Ha 15-tagból álló sorozatot szeretnénk, akkor a tagok közötti különbség legalább 2x3x5x7x11x13 = 30 030.

A $k \geq 3$ egész számokra, egy **AP-*k*** olyan sorozat, ami k prímszámot tartalmaz egy számtani sorozat részeként. Az AP-k felírható $a \cdot n + b$ alakú k db prímszámként, fix a (ez a sorozat különbsége) és b egészekre, k egymást követő n egész értékre. Az AP-k-t általában $n = 0 - (k - 1)$ közötti értékekkel adják meg. Ez úgy érhető el, ha b az első prím a számtani sorozatban.

Ha egy AP-*k* nem a *k* prímszámmal kezdődik, akkor a sorozat különbsége a

k# = 2·3·5·...·*j* primoriális többszöröse, ahol *j* a legnagyobb prím ≤ *k*.

Bizonyítás: Legyen AP-*k* *a*·*n* + *b*, *k* egymást követő *n* értékre. Ha a *p* prím nem osztója *a*-nak, akkor a moduláris aritmetika szerint *p* a számtani sorozat minden *p*-edik elemét osztani fogja. Ha az AP *k* egymást követő értéke prímszám, akkor az *a*-nak oszthatónak kell lennie az összes *p* ≤ *k* prímszámmal.

Az előbbiekből az is következik, hogy az *a* különbségű AP nem tartalmazhat több egymást követő prímet, mint a legkisebb, *a*-t nem osztó prím számértéke.

Ha *k* prímszám, akkor az AP-*k* kezdődhet *k*-val, és a sorozat különbsége elég, ha (*k*−1)# többszöröse *k*# helyett. Megfigyelhető az AP-3 a {3, 5, 7} prímekkel és 2# = 2 különbséggel, vagy az AP-5 {5, 11, 17, 23, 29} és 4# = 6 különbséggel. A sejtések szerint ilyen példák minden *k* prímszámra hozhatók. Jelenleg (2016) a legnagyobb prím, amire ezt sikerült igazolni a *k* = 19, a következő AP-19-re, amit Wojciech Iżykowski talált meg 2013-ban:

19 + 4244193265542951705·17#·n, ahol *n* = 0 – 18.

Igaznak vélt sejtésekből, mint a Dickson-sejtés és az első Hardy–Littlewood-sejtés következik, hogy ha *p* > 2 a legkisebb prímszám, ami nem osztja *a*-t, akkor végtelen sok *a* különbségű AP-(*p*−1) létezik. Például 5 a legkisebb prím, ami nem osztója a 6-nak, ezért arra számítunk, hogy végtelen sok 6 különbségű AP-4-et találunk (szexi prím-négyesek). Az *a* = 2, *p* = 3 kiadja az ikerprím-sejtést, az "AP-2" 2 prímre (*b*, *b* + 2).

A legnagyobb ismert prímek számtani sorozatban

A *q* prímszám esetén, *q*# jelölje a 2·3·5·7·...·*q* primoriálist.

Jelenleg (2016.) a leghosszabb ismert AP-*k* közül a legnagyobb egy AP-26, amit 2015. február 19-én talált Bryan Little. Ez a negyedik ismert AP-26:

161004359399459161 + 47715109·23#·*n*, ahol *n* = 0 – 25. (23# = 223092870)

A harmadik ismert AP-26-ot Bryan Little találta 2014. február 23-án:

136926916457315893 + 44121555·23#·*n*, ahol *n* = 0 – 25. (23# = 223092870)

A második ismert AP-26-ot James Fry találta meg 2012. március 16-án:

3486107472997423 + 1666981·23#·*n*, ahol *n* = 0 – 25. (23# = 223092870)

Az első ismert AP-26-ot 2010. április 12-én Benoãt Perichon találta:

43142746595714191 + 23681770·23#·*n*, ahol *n* = 0 – 25. (23# = 223092870)

Korábban a rekord egy 2008. május 17-én Raanan Chermoni és Jaroslaw Wroblewski által megtalált AP-25 volt:

6171054912832631 + 366384·23#·*n*, ahol *n* = 0 – 24. (23# = 223092870)

A korábbi rekord egy Jaroslaw Wroblewski által 2007. január 18-án megtalált AP-24 volt:

468395662504823 + 205619·23#·*n*, ahol *n* = 0 – 23.

A következő táblázat megmutatja a legnagyobb ismert AP-*k*-kat a felfedezési évükkel és a záró prím számjegyeinek számával. Vegyük észre, hogy a legnagyobb ismert AP-*k* lehet egy AP-(*k*+1) vége is. Egyes csúcstartók először kiszámolnak fix *p*-vel nagyszámú *c*·*p*#+1 alakú prímszámot, majd a prímet adó *c* értékek között keresnek számtani sorozatokat. Ez látható egyes rekordok formájából is. A kifejezés könnyen átírható *a*·*n* + *b* alakra.

Legnagyobb ismert AP-*k* (2016.)

k	**Prímek *n* = 0 – *k*–1**	**Számjegyek**	**Év**	**Felfedező**
1	$2^{57885161} + 422 \cdot n - 1$	17425170	2013	GIMPS, Curtis Cooper
2	$2^{43112609} + (2^{57885161} - 2^{43112609}) \cdot n - 1$	17425170	2013	GIMPS, Edson Smith, Curtis Cooper
3	$(483590093385 + 1367824406910 \cdot n) \cdot 2^{1290000} - 1$	388342	2015	David Broadhurst, Ernst Fluttert, Randall Scalise, PrimeGrid

4	$1631979959 \cdot 2^{25000} + (164196977 \cdot 2^{80000} - 1631979959 \cdot 2^{25000}) \cdot n - 1$	24092	2010	David Broadhurst
5	$(43728051 + 18797279 \cdot n) \cdot 16267\# - 1$	7026	2015	Serge Batalov
6	$(234043271 + 481789017 \cdot (n + 1)) \cdot 7001\# + 1$	3019	2012	Ken Davis
7	$(234043271 + 481789017 \cdot n) \cdot 7001\# + 1$	3019	2012	Ken Davis
8	$(452558752 + 359463429 \cdot n) \cdot 2459\# + 1$	1057	2009	Ken Davis
9	$(65502205462 + 6317280828 \cdot n) \cdot 2371\# + 1$	1014	2012	Ken Davis, Paul Underwood
10	$(3186700865 + 61959394 \cdot (n + 1)) \cdot 653\# + 1$	283	2010	Ken Davis
11	$(3186700865 + 61959394 \cdot n) \cdot 653\# + 1$	283	2010	Ken Davis
12	$(1366899295 + 54290654 \cdot n) \cdot 401\# + 1$	173	2006	Jeff Anderson-Lee
13	$(1296982250 + 14976848 \cdot n) \cdot 191\# + 1$	85	2010	Mike Oakes
14	$(145978014 + 25313115 \cdot n) \cdot 157\# + 1$	71	2009	Mike Oakes
15	$(237375311 + 118560155 \cdot n) \cdot 109\# + 1$	54	2009	Mike Oakes
16	$44260422033654940208007879697 4991691613909 + 103\# \cdot (n + 1)$	42	2014	Jaroslaw Wroblewski
17	$4426042203365494020800787969 74991691613909 + 103\# \cdot n$	42	2014	Jaroslaw Wroblewski
18	$10^{29} + 999 + 1806448944300798320195 \cdot 19\# \cdot (n - 1)$	30	2014	Jaroslaw Wroblewski
19	$10^{29} + 999 + 1806448944300798320195 \cdot 19\# \cdot (n - 2)$	30	2014	Jaroslaw Wroblewski
20	$3533531731191494525351461 + 61\# \cdot n$	25	2014	Jaroslaw Wroblewski
21	$5547796991585989797641 + 29\# \cdot n$	22	2014	Jaroslaw Wroblewski
22	$22231637631603420833 + 8 \cdot 41\# \cdot (n + 1)$	20	2014	Jaroslaw Wroblewski
23	$2223163763160342083 3 + 8 \cdot 41\# \cdot n$	20	2014	Jaroslaw Wroblewski
24	$161004359399459161 + 47715109 \cdot 23\# \cdot (n + 2)$	18	2015	Bryan Little
25	$161004359399459161 + 47715109 \cdot 23\# \cdot (n + 1)$	18	2015	Bryan Little
26	$161004359399459161 + 47715109 \cdot 23\# \cdot n$	18	2015	Bryan Little

Az egymást követő prímekből álló számtani sorozat *(Consecutive primes in arithmetic progression,* **CPAP***)* legalább három egymást követő prímet jelent, melyek egy számtani sorozat egymást követő tagjai. Az AP-*k*-tól eltérően a sorozat tagjai között lévő valamennyi számnak összetettnek kell lennie. Például az AP-3 {3, 7, 11} nem CPAP, mert a közéjük eső 5 prímszám.

Egy $k \geq 3$ egész számhoz tartozó **CPAP-*k*** *k* db egymást követő prímszámot jelent, melyek egy számtani sorozat egymást követő elemei. Sejtések szerint létezik tetszőlegesen hosszú CPAP – ebből az következik, hogy végtelen sok CPAP-*k* létezik bármely *k*-ra. A CPAP-3 középső prímszámát kiegyensúlyozott prímnek is nevezik. A legnagyobb ismert ilyen prím 10 546 számjeggyel írható le.

Az első ismert CPAP-10-et 1998-ban találta Manfred Toplic. Ez a CPAP-10 a lehetséges legkisebb különbségű volt: 7# = 210. A másik ismert CPAP-10-et 2009-ben találták meg.

Ha létezik CPAP-11, a sorozat különbségének 11# = 2310-nek vagy ennek többszörösének kell lennie. A 11 prímszám első és utolsó tagja közti különbség tehát 23 100 (vagy ennek többszöröse). Az a követelmény, hogy a 11 prímszám között legalább 23 090 összetett szám legyen, rendkívüli módon megnehezíti egy CPAP-11 megtalálását. Dubner és Zimmermann becslése szerint legalább 10^{12}-szer olyan nehéz, mint amilyen a CPAP-10 megtalálása volt.

A következő táblázat megmutatja a legnagyobb ismert, egymást követő *k* prímszámból álló számtani sorozatokat, *k* = 3–10 esetekre:

Legnagyobb ismert CPAP-*k* (2016.)

k	Prímek *n* = 0 – *k*−1	Számjegyek	Év	Felfedező
3	$1213266377 \cdot 2^{35000} - 1 + 2430n$	10546	2014	David Broadhurst
4	$62037039993 \cdot 7001\# + 7811555723 + 30n$	3021	2013	David Broadhurst
5	$406463527990 \cdot 2801\# + 1633050283 + 30n$	1209	2013	David Broadhurst
6	$44770344615 \cdot 859\# + 1204600427 + 30n$	370	2003	Jens Kruse Andersen, Jim Fougeron

7	4785544287883 · 613# + x_{253} + 210n	266	2007	Jens Kruse Andersen
8	10097274767216 · 250# + x_{99} + 210n	112	2003	Jens Kruse Andersen
9	73577019188277 · 199#·227·229 + x_{87} + 210n	101	2005	Hans Rosenthal, Jens Kruse Andersen
10	1180477472752474 · 193# + x_{77} + 210n	93	2008	Manfred Toplic, CP10 project

x_d egy d-számjegyű szám, amire azért volt szükség, hogy a prímszámok közötti összetett számoknak legyen megfelelő mennyiségű kis prímtényezője.

x_{77} = 54538241683887582 66818970359011065905786593476460487384078192351342110349557 9

x_{87} = 27987250963458718633203913541404633072818099420909252304070352084381131932093038067786 7

x_{99} = 158794709 61807422940998741617438694572837152359045245986366779168744094414346216082132873514356409 1

x_{253} = 1617599298905 32047130480253835658739849997983625515667103047375128118119991131225955073437387452053614851930092432794750767474667985881678018247872443196658784367240877338844578814274027432962181187982734957524785184351401239931320121110127717568463672 7

5. Érdekességek

Tesztelje memóriáját!

Szeretne villogni ismerősei előtt rendkívüli memóriájával? Jegyezzen meg egy 155 számjegyből álló prímszámot 3 másodperc alatt! Például ezt:

828180797877767574737271706968676665646362616059585756555453525150494847464544434241403938373635343332313029282726252423222120191817161514131211109876543 21

Sikerült memorizálnia? Nem? Segítek!

82 81 80 79 78 77 76 75 74 73 72 71 70 69 68 67 66 65 64 63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48 47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Ha 82-től visszafelé leírjuk a számjegyeket 1-ig, akkor egy prímszámot kapunk. Ugye, hogy egyszerű!

Prímszám rekordok időrendben

(1456 előtt nincs írásos bizonyíték)

Sorszám	Számjegyek száma	Felfedezés éve	Felfedező
1.	4	1456	Névtelen
2.	6	1588	Pietro Cataldi
3.	10	1772	Leonhard Euler
4.	14	1855	Thomas Clausen
5.	39	1876	Édouard Lucas
6.	44	1951	Aimé Ferrier **(mechanikus számológép)**
7.	79	1951	Miller és Wheeler **(Cambridge EDSAC számítógép)**
8.	687	1952	Névtelen

9.	969	1957	Névtelen
10.	1 332	1961	Névtelen
11.	3 376	1963	Névtelen
12.	6 002	1971	Bryant Tuckerman
13.	6 533	1978	Laura A. Nickel és Landon Curt Noll
14.	13 395	1979	David Slowinski és Harry L. Nelson
15.	25 962	1982	David Slowinski
16.	39 751	1983	David Slowinski
17.	65 050	1985	David Slowinski
18.	65 087	1989	"Amdahl Six" csoport: John Brown, Landon Curt Noll , BK Parady, Gene Ward Smith, Joel F. Smith, Sergio E. Zarantonello. **A legnagyobb nem Mersenne-típusú prímszám.**
19.	227 832	1992	David Slowinski és Paul Gage
20.	258 716	1994	David Slowinski és Paul Gage
21.	378 632	1996	David Slowinski és Paul Gage
22.	420 921	1996	GIMPS, Joel Armengaud
23.	895 932	1997	GIMPS, Gordon Spence
24.	909 526	1998	GIMPS, Roland Clarkson
25.	2 098 960	1999	GIMPS, Nayan Hajratwala
26.	4 053 946	2001	GIMPS, Michael Cameron
27.	6 320 430	2003	GIMPS, Michael Shafer
28.	7 235 733	2004	GIMPS, Josh Findley
29.	7 816 230	2005	GIMPS, Martin Nowak
30.	9 152 052	2005	GIMPS, Curtis Cooper és Steven Boone
31.	9 808 358	2006	GIMPS, Curtis Cooper és Steven Boone
32.	12 978 189	2008	GIMPS, Edson Smith
33.	17 425 170	2013	GIMPS, Curtis Cooper
34.	22 338 618	2016	GIM PS, Curtis Cooper
35.	23 249 425	2017	GIMPS, Jonathan Pace
36.	24 862 048	2018	GIMPS, Patrick Laroche

A húsz legnagyobb ismert prímszám 2020-ban

Helyezés	A szám	A felfedezés időpontja	A számjegyek száma
1.	$2^{82589933}-1$	2018.12.07.	24 862 048
2.	$2^{77232917}-1$	2017.12.26.	23 249 425
3.	$2^{74207281}-1$	2016.01.07.	22 338 618
4.	$2^{57885161}-1$	2013.01.25.	17 425 170
5.	$2^{43112609}-1$	2008.08.23.	12 978 189
6.	$2^{42643801}-1$	2009.06.04.	12 837 064
7.	$2^{37156667}-1$	2008.09.06.	11 185 272
8.	$2^{32582657}-1$	2006.09.04.	9 808 358
9.	$10223\cdot 2^{31172165}+1$	2016.10.31.	9 383 761
10.	$2^{30402457}-1$	2005.12.15.	9 152 052
11.	$2^{25964951}-1$	2005.02.18.	7 816 230
12.	$2^{24036583}-1$	2004.05.15.	7 235 733
13.	$2^{20996011}-1$	2003.11.17.	6 320 430
14.	$1059094^{1048576}+1$	2018.10.31.	6 317 602
15.	$919444^{1048576}+1$	2017.08.29.	6 253 210
16.	$168451\cdot 2^{19375200}+1$	2017.09.17.	5 832 522
17.	$123447^{1048576}-123447^{524288}+1$	2017.02.23.	5 338 805
18.	$7\cdot 6^{6772401}+1$	2019.09.09.	5 269 954
19.	$8508301\cdot 2^{17016603}-1$	2018.03.21.	5 122 515
20.	$6962\cdot 31^{2863120}-1$	2020.02.29.	4 269 952

5.1. Különböző típusú prímek

1. Bali-Stein prímpárok

Olyan prímszám-párok, melyeknek 2-es számrendszerbeli alakján elvégezve a XOR műveletet, 2 valamely hatványát kapjuk. Más szavakkal a két prím különbségének eredménye 2 valamely hatványa.

(2-3); (3-7); (3-11); (3-19); (3-67); (17-19); (19-83); (83-2131); (101-613); (191-2239); (223-479); (577-1601); (719-2767); (839-2887); (1259-3307); (1301-1303); (1511-3559); (1997-2029); (2389-3413)...

2. Balogh-prímpárok

Az olyan három egymást követő iker prímpárt, melyek között csak összetett számok vannak, Balogh-prímpároknak nevezünk.

(2-3;5-7;11-13); (5-7;11-13;17-19); (179-181;191-193;197-199); (3359-3361;3371-3373;3389-3391); (4217-4219;4229-4231;4241-4243); (6761-6763;6779-6781;6791-6793)...

3. Balról csonkolható prímek

Az olyan prímszámot nevezzük balról csonkolhatónak, amelynek (tízes számrendszerben) balról elhagyva a kezdő számjegyeit mindig prímet kapunk.

2; 3; 5; 7; 13; 17; 23; 37; 43; 47; 53; 67; 73; 83; 97; 113; 137; 167; 173; 197; 223; 283; 313; 317; 337; 347; 353; 367; 373; 383; 397; 443; 467; 523; 547; 613; 617; 643; 647; 653; 673; 683…

4. Bell-prímek

Olyan Bell-számok, amelyek prímek. 2; 5; 877; 27644437; 35742549198872617291353508656626642567; 359334085968622831041960188598043661065388726959079837

5. Biztonságos prímek

Ahol a p és $(p-1) / 2$ egyaránt prímek.

5; 7; 11; 23; 47; 59; 83; 107; 167; 179; 227; 263; 347; 359; 383; 467; 479; 503; 563; 587; 719; 839; 863; 887; 983; 1019; 1187; 1283; 1307; 1319; 1367; 1439; 1487; 1523; 1619; 1823; 1907

6. Boldog prímek

Olyan boldog számok, amelyek prímek is.

7; 13; 19; 23; 31; 79; 97; 103; 109; 139; 167; 193; 239; 263; 293; 313; 331; 367; 379; 383; 397; 409; 487; 563; 617; 653; 673; 683; 709; 739; 761; 863; 881; 907; 937; 1009; 1033; 1039; 1093

7. Chen-prímek

p prím és $p + 2$ vagy prím vagy félprím, azaz két prímszám szorzata.

2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 47; 53; 59; 67; 71; 83; 89; 101; 107; 109; 113; 127; 131; 137; 139; 149; 157; 167; 179; 181; 191; 197; 199; 211; 227; 233; 239; 251; 257; 263; 269

8. Csillagprímek

$6n(n - 1) + 1$ alakú prímszámok.

13; 37; 73; 181; 337; 433; 541; 661; 937; 1093; 2053; 2281; 2521; 3037; 3313; 5581; 5953; 6337; 6733; 7561; 7993; 8893; 10333; 10837; 11353; 12421; 12973; 13537; 15913; 18481

9. Csupa 1 prímek

Olyan prímek, amelyek (tízes számrendszerben) csak az 1-es számjegyet tartalmazzák.

11; 1111111111111111; 11111111111111111111

A következőnek 317, az azt követőnek pedig 1031 számjegye van.

10. Dupla Mersenne-prímek

Olyan $2^{(2^p-1)}-1$ alakú prím, ahol p is prím.

7; 127; 2147483647; 170141183460469231731687303715884105727

11. Eisenstein-prímek

Olyan irreducibilis elemek a Gauss-egészek körében, amelyeknek az imaginárius része nulla.

2; 5; 11; 17; 23; 29; 41; 47; 53; 59; 71; 83; 89; 101; 107; 113; 131; 137; 149; 167; 173; 179; 191; 197; 227; 233; 239; 251; 257; 263; 269; 281; 293; 311; 317; 347; 353; 359; 383; 389; 401

12. Erdős-prímek

Olyan prímszámok, amelyek számjegyei összege is prím.

2; 3; 5; 7; 11; 23; 29; 41; 43; 47; 61; 67; 83; 89

13. Euklideszi prímek

Prímek, melyek Eukleidész-féle számok.

2; 3; 7; 31; 211; 2311; 200560490131

14. Faktoriális prímek

$n!$ – 1 vagy $n!$ + 1 alakú prímszámok.

2; 3; 5; 7; 23; 719; 5039; 39916801; 479001599; 87178291199; 10888869450418352160768000001; 265252859812191058636308479999999; 263130836933693530167218012159999999; 86833176188118864955181944012799999999

15. Fermat-prímek

Olyan prímek, melyek Fermat-számok, tehát $2^{2^n} + 1$ alakú prímszámok.

3; 5; 17; 257; 65537

Csak ezek a Fermat-prímek ismertek.

16. Fibonacci-prímek

Prímek a Fibonacci-sorozatban: $F_0 = 0$; $F_1 = 1$; $F_n = F_{n-1} + F_{n-2}$.

2; 3; 5; 13; 89; 233; 1597; 28657; 514229; 433494437; 2971215073; 99194853094755497; 106634041749171059581457216 9; 191347024000932780814494239 17

17. Gauss-prímek

A Gauss-egészek prím elemei ($4n + 3$ alakú prímek).

3; 7; 11; 19; 23; 31; 43; 47; 59; 67; 71; 79; 83; 103; 107; 127; 131; 139; 151; 163; 167; 179; 191; 199; 211; 223; 227; 239; 251; 263; 271; 283; 307; 311; 331; 347; 359; 367; 379; 383; 419; 431; 439; 443; 463; 467; 479; 487; 491; 499; 503

18. Genocchi-prímek

Az egyetlen pozitív Genocchi-prím a 17.

19. Ikerprímek

A $(p; p + 2)$ prím párok.

(3; 5); (5; 7); (11; 13); (17; 19); (29; 31); (41; 43); (59; 61); (71; 73); (101; 103); (107; 109); (137; 139); (149; 151); (179; 181); (191; 193); (197; 199); (227; 229); (239; 241); (269; 271); (281; 283); (311; 313); (347; 349); (419; 421); (431; 433); (461; 463); (521;523); (569;571)

20. Jobbról csonkolható prímek

Az olyan prímszámot nevezzük jobbról csonkolhatónak, amelynek (tízes számrendszerben) jobbról elhagyva a záró számjegyeit mindig prímet kapunk.

2; 3; 5; 7; 23; 29; 31; 37; 53; 59; 71; 73; 79; 233; 239; 293; 311; 313; 317; 373; 379; 593; 599; 719; 733; 739; 797; 2333; 2339; 2393; 2399; 2939; 3119; 3137; 3733; 3739; 3793; 3797

21. Kiegyensúlyozott prímek

Olyan prímszámok, melyek azonos távolságra vannak a két szomszédos prímmel:

5; 53; 157; 173; 211; 257; 263; 373; 563; 593; 607; 653; 733; 947; 977; 1103; 1123; 1187; 1223; 1367; 1511; 1747; 1753; 1907; 2287; 2417; 2677; 2903; 2963; 3307; 3313; 3637; 3733

22. Középpontos háromszögprímek

Prímek, melyek középpontos háromszögszámok. Alakjuk: $(3n^2 + 3n + 2) / 2$.

19; 31; 109; 199; 409; 571; 631; 829; 1489; 1999; 2341; 2971; 3529; 4621; 4789; 7039; 7669; 8779; 9721; 10459; 10711; 13681; 14851; 16069; 16381; 17659; 20011; 20359; 23251

23. Középpontos hatszögprímek

Prímek, melyek középpontos hatszögszámok. Alakjuk: $(7n^2 – 7n + 2) / 2$.

43; 71; 197; 463; 547; 953; 1471; 1933; 2647; 2843; 3697; 4663; 5741; 8233; 9283; 10781; 11173; 12391; 14561; 18397; 20483; 29303; 29947; 34651; 37493; 41203; 46691

24. Középpontos négyszögprímek

Prímek, melyek középpontos négyszögszámok. Alakjuk: $n^2 + (n + 1)^2$.

5; 13; 41; 61; 113; 181; 313; 421; 613; 761; 1013; 1201; 1301; 1741; 1861; 2113; 2381; 2521; 3121; 3613; 4513; 5101; 7321; 8581; 9661; 9941; 10513; 12641; 13613; 14281; 14621

25. Középpontos tízszögprímek

Prímek, melyek középpontos tízszögszámok. Alakjuk: $5(n^2 - n) + 1$

11; 31; 61; 101; 151; 211; 281; 661; 911; 1051; 1201; 1361; 1531; 1901; 2311; 2531; 3001; 3251; 3511; 4651; 5281; 6301; 6661; 7411; 9461; 9901; 12251; 13781; 14851; 15401; 18301; 18911; 19531

26. Kubai prímek

Alakjuk: $\frac{x^3-y^3}{x-y}, ahol\ x = y + 1$

7; 19; 37; 61; 127; 271; 331; 397; 547; 631; 919; 1657; 1801; 1951; 2269; 2437; 2791; 3169; 3571; 4219; 4447; 5167; 5419; 6211; 7057; 7351; 8269; 9241; 10267; 11719; 12097; 13267; 13669

Alakjuk: $\frac{x^3-y^3}{x-y}, ahol\ x = y + 2$

13; 109; 193; 433; 769; 1201; 1453; 2029; 3469; 3889; 4801; 10093; 12289; 13873; 18253; 20173; 21169; 22189; 28813; 37633; 43201; 47629; 60493; 63949; 65713; 69313

27. Kynea-prímek

Az $(2^n + 1)^2 - 2$ alakú prímek.

7; 23; 79; 1087; 66047; 263167; 16785407; 1073807359; 17180131327; 68720001023; 4398050705407; 70368760954879; 18014398777917439; 18446744082299486207

28. Leyland-prímek

Leyland-prímek az $x^y + y^x$ alakban felírható prímek, ahol $1 < x \leq y$.

17; 593; 32993; 2097593; 8589935681; 59604644783353249; 523347633027360537213687137; 43143988327398957279342419750374600193

29. Lucas-prímek

A Lucas-sorozat prím tagjai. A Lucas sorozat definíciója a következő:

$L_0 = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2}$

Megoszlanak a vélemények arról, hogy az $L_0 = 2$ beleszámít-e a Lucas-számok közé:

(2;) 3; 7; 11; 29; 47; 199; 521; 2207; 3571; 9349; 3010349; 54018521; 370248451; 6643838879; 119218851371; 5600748293801; 688846502588399; 32361122672259149

30. Markov-prímek

Olyan prímek, amelyekre létezik olyan *x* és *y*, hogy $x^2 + y^2 + p^2 = 3xyp$.

2; 5; 13; 29; 89; 233; 433; 1597; 2897; 5741; 7561; 28657; 33461; 43261; 96557; 426389; 514229

31. Mersenne-prímek

A $2^n - 1$ alakú prímszámok. Az első 12 az alábbi:

3; 7; 31; 127; 8191; 131071; 524287; 2147483647; 2305843009213693951; 618970019642690137449562111; 162259276829213363391578010288127; 170141183460469231731687303715884105727

32. Mills-prímek

A $\left[\theta^{3^n}\right]$ alakú prímek, ahol θ a Mills-állandó. Ez a formula minden pozitív n-re prímszámot ad.

2; 11; 1361; 2521008887; 16022236204009818131831320183

33. Mírp számok

A mírp számok *(prím visszafele olvasva, angolul emirp)* olyan prímek, melyeknek a decimális számjegyeit visszafelé olvasva is prímet kapunk, és nem palindrom prímek.

13; 17; 31; 37; 71; 73; 79; 97; 107; 113; 149; 157; 167; 179; 199; 311; 337; 347; 359; 389; 701; 709; 733; 739; 743; 751; 761; 769; 907; 937; 941; 953; 967; 971; 983; 991

34. Motzkin-prímek

2; 127; 15511; 953467954114363

35. Newman-Shanks-Williams-prímek

Olyan Newman-Shanks-Williams-számok, amelyek prímek.

7; 41; 239; 9369319; 63018038201; 489133282872437279; 19175002942688032928599

36. Padovan-prímek

A Padovan-sorozat prím tagjai.

$$P(0) = P(1) = P(2) = 1, P(n) = P(n-2) = P(n-3)$$

2; 3; 5; 7; 37; 151; 3329; 23833; 13091204281; 3093215881333057; 136300555243466607821742128462127993362710278088105335847 3

37. Palindrom prímek

Olyan prímek, amelyeknek decimális számjegyei palindromot alkotnak, azaz balról jobbra és jobbról balra olvasva ugyanazt a számot adják:

2; 3; 5; 7; 11; 101; 131; 151; 181; 191; 313; 353; 373; 383; 727; 757; 787; 797; 919; 929; 10301; 10501; 10601; 11311; 11411; 12421; 12721; 12821; 13331; 13831; 13931; 14341; 14741

38. Pell-prímek

A Pell-sorozat prím tagjai.

$$P_0 = 0, P_1 = 1, P_n = 2P_{n-1} + P_{n-2}$$

2; 5; 29; 5741; 33461; 44560482149; 1746860020068409; 68480406462161287469; 1355877461004671178070 1; 4125636888562548868221559797461449

39. Permutálható prímek

Olyan prím, ahol a (tízes számrendszerben vett) számjegyek tetszőleges permutációja prímet ad.

2; 3; 5; 7; 11; 13; 17; 31; 37; 71; 73; 79; 97; 113; 131; 199; 311; 337; 373; 733; 919; 991; 1111111111111111; 11111111111111111111

Sejtés, hogy minden további permutálható prím is csak 1-es számjegyből áll.

40. Perrin-prímek

A Perrin-sorozat prím tagjai: $P(0) = 3$; $P(1) = 0$; $P(2) = 2$; $P(n) = P(n-2) + P(n-3)$.

2; 3; 5; 7; 17; 29; 277; 367; 853; 14197; 43721; 1442968193; 792606555396977; 18727865918041723432 1; 662411604887801410715798647 97

41. Pierpont-prímek

A $\mathbf{2^u \cdot 3^v + 1}$ alakú prímek, ahol $\boldsymbol{u, v \geq 0}$ egész számok.

2; 3; 5; 7; 13; 17; 19; 37; 73; 97; 109; 163; 193; 257; 433; 487; 577; 769; 1153; 1297; 1459; 2593; 2917; 3457; 3889; 10369; 12289; 17497; 18433; 39367; 52489; 65537; 139969; 147457

42. Pillai-prímek

23; 29; 59; 61; 67; 71; 79; 83; 109; 137; 139; 149; 193; 227; 233; 239; 251; 257; 269; 271; 277; 293; 307; 311; 317; 359; 379; 383; 389; 397; 401; 419; 431; 449; 461; 463; 467; 479; 499

43. Pitagorasz-prímek

A $\boldsymbol{4n+1}$ alakú prímek.

5; 13; 17; 29; 37; 41; 53; 61; 73; 89; 97; 101; 109; 113; 137; 149; 157; 173; 181; 193; 197; 229; 233; 241; 257; 269; 277; 281; 293; 313; 317; 337; 349; 353; 373; 389; 397; 401; 409; 421; 433; 449

44. Prím négyesek

A (p; p+2; p+6; p+8) rendezett négyesek, ahol mind a négy szám prím.

(5; 7; 11; 13); (11; 13; 17; 19); (101; 103; 107; 109); (191; 193; 197; 199); (821; 823; 827; 829); (1481; 1483; 1487; 1489); (1871; 1873; 1877; 1879); (2081; 2083; 2087; 2089); (3251; 3253; 3257; 3259); (3461; 3463; 3467; 3469); (5651; 5653; 5657; 5659); (9431; 9433; 9437; 9439)

45. Prím hármasok

A (p; p+2; p+6) vagy (p; p+4; p+6) rendezett hármasok, ahol mind a három szám prím.

(5; 7; 11); (7; 11; 13); (11; 13; 17); (13; 17; 19); (17; 19; 23); (37; 41; 43); (41; 43; 47); (67; 71; 73); (97; 101; 103); (101; 103; 107); (103; 107; 109); (107; 109; 113); (191; 193; 197); (193; 197; 199); (223; 227; 229); (227; 229; 233); (277; 281; 283); (307; 311; 313); (311; 313; 317); (347; 349; 353)

46. Proth-prímek

A $\mathbf{k \cdot 2^n + 1}$ alakú prímek, ahol k páratlan és $k < 2^n$.

3; 5; 13; 17; 41; 97; 113; 193; 241; 257; 353; 449; 577; 641; 673; 769; 929; 1153; 1217; 1409; 1601; 2113; 2689; 2753; 3137; 3329; 3457; 4481; 4993; 6529; 7297; 7681; 7937; 9473; 9601; 9857

47. Ramanujan-számok

Adott n számra a Ramanujan-szám (R_n) a legkisebb olyan szám, amelyre legalább n prím található az $x/2$ és x számok között minden $x \geq R_n$ számra.

2; 11; 17; 29; 41; 47; 59; 67; 71; 97; 101; 107; 127; 149; 151; 167; 179; 181; 227; 229; 233; 239; 241; 263; 269; 281; 307; 311; 347; 349; 367; 373; 401; 409; 419; 431; 433; 439; 461; 487; 491

48. Smarandache-Wellin-prímek

Az első n prímszám decimális reprezentációjának konkatenációjával keletkező prím.

2; 23; 2357

A negyedik Smarandache-Wellin-prím az első 128 prímszám konkatenációja így 719-re végződik.

49. Sophie Germain-prímek

Ahol p és $2p + 1$ egyaránt prím.

2; 3; 5; 11; 23; 29; 41; 53; 83; 89; 113; 131; 173; 179; 191; 233; 239; 251; 281; 293; 359; 419; 431; 443; 491; 509; 593; 641; 653; 659; 683; 719; 743; 761; 809; 911; 953

50. Stern-prímek

Olyan prímek, amelyek nem állnak elő egy kisebb prím és egy négyzetszám kétszeresének összegeként.

2; 3; 17; 137; 227; 977; 1187; 1493

51. Szexi prímek

Olyan prímek, ahol p és $p + 6$ egyaránt prímek. Az elnevezés a latin *sex* szóból származik, ami 6-ot jelent.

(5,11); (7,13); (11,17); (13,19); (17,23); (23,29); (31,37); (37,43); (41,47); (47,53); (53,59); (61,67); (67,73); (73,79); (83,89); (97,103); (101,107); (103,109); (107,113); (131,137); (151,157); (157,163); (167,173); (173,179); (191,197); (193,199)

52. Szuper prímek

Olyan prímek, amelyeknek a prímszámok sorozatában vett indexe is prímszám. Tehát például a 2., a 3., az 5. prímszám.

3; 5; 11; 17; 31; 41; 59; 67; 83; 109; 127; 157; 179; 191; 211; 241; 277; 283; 331; 353; 367; 401; 431; 461; 509; 547; 563; 587; 599; 617; 709; 739; 773; 797; 859; 877; 919; 967; 991

53. Szuper szinguláris prímek

Pontosan 15 darab szuper szinguláris prímszám van.

2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 41; 47; 59; 71

54. Thabit-prímek

A $\mathbf{3 \cdot 2^n - 1}$ alakú prímszámok.

2; 5; 11; 23; 47; 191; 383; 6143; 786431; 51539607551; 824633720831; 26388279066623; 108086391056891903; 55340232221128654847; 2266735911777429702574 07

55. Ulam-prímek

Olyan Ulam-számok, amelyek prímek.

2; 3; 11; 13; 47; 53; 97; 131; 197; 241; 409; 431; 607; 673; 739; 751; 983; 991; 1103; 1433; 1489; 1531; 1553; 1709; 1721; 2371; 2393; 2447; 2633; 2789; 2833; 2897

56. Unokatestvér prímek

A $(p; p + 4)$ prímszám párok.

(3; 7); (7; 11); (13; 17); (19; 23); (37; 41); (43; 47); (67; 71); (79; 83); (97; 101); (103; 107); (109; 113); (127; 131); (163; 167); (193; 197); (223; 227); (229; 233); (277; 281)

57. Wagstaff-prímek

A $\frac{2^n+1}{3}$ alakú prímszámok.

3; 11; 43; 683; 2731; 43691; 174763; 2796203; 715827883; 2932031007403; 768614336404564651; 201487636602438195784363; 845100400152152934331135470251; 56713727820156410577229101238628035243

A hozzájuk tartozó *n* értékek a következők:

3; 5; 7; 11; 13; 17; 19; 23; 31; 43; 61; 79; 101; 127; 167; 191; 199; 313; 347; 701; 1709; 2617; 3539; 5807; 10501; 10691; 11279; 12391; 14479; 42737; 83339; 95369; 117239; 127031; 138937; 141079; 267017; 269987; 374321

58. Wedderburn-Etherington-prímek

Olyan Wedderburn-Etherington-számok, amelyek prímek.

2; 3; 11; 23; 983; 2179; 24631; 3626149; 253450711; 596572387

59. Wieferich-prímek

Olyan prímek, amelyekre p^2 osztja a $2^{p-1} - 1$ számot.

1093; 3511

60. Wilson-prímek

Olyan *p* prímszámok, amelyekre p^2 osztja a $(p - 1)! + 1$ számot.

5; 13; 563

61. Wolstenholme-prímek

Olyan *p* prímek, amelyekre fennáll az alábbi kongruencia:

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$$

16843; 2124679

62. Woodall-prímek

Az $\boldsymbol{n \cdot 2^n - 1}$ alakú prímszámok.

7; 23; 383; 32212254719; 2833419889721787128217599; 1958459827775699263024005 11; 47769131098520414182480566228824883 19

5.2. Prímszámok 1-től 25000-ig

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253, 3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371, 3373,

3389, 3391, 3407, 3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539, 3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823, 3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127, 4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441, 4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733, 4751, 4759, 4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903, 4909, 4919, 4931, 4933, 4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021, 5023, 5039, 5051, 5059, 5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189, 5197, 5209, 5227, 5231, 5233, 5237, 5261, 5273, 5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393, 5399, 5407, 5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477, 5479, 5483, 5501, 5503, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657, 5659, 5669, 5683, 5689, 5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, 5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, 6131, 6133, 6143, 6151, 6163, 6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277, 6287, 6299, 6301, 6311, 6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421, 6427, 6449, 6451, 6469, 6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599, 6607, 6619, 6637, 6653, 6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763, 6779, 6781, 6791, 6793, 6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911, 6917, 6947, 6949, 6959, 6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237, 7243,

7247, 7253, 7283, 7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481, 7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573, 7577, 7583, 7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753, 7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883, 7901, 7907, 7919, 7927, 7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081, 8087, 8089, 8093, 8101, 8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233, 8237, 8243, 8263, 8269, 8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389, 8419, 8423, 8429, 8431, 8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581, 8597, 8599, 8609, 8623, 8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719, 8731, 8737, 8741, 8747, 8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863, 8867, 8887, 8893, 8923, 8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001, 9007, 9011, 9013, 9029, 9041, 9043, 9049, 9059, 9067, 9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203, 9209, 9221, 9227, 9239, 9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371, 9377, 9391, 9397, 9403, 9413, 9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497, 9511, 9521, 9533, 9539, 9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679, 9689, 9697, 9719, 9721, 9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833, 9839, 9851, 9857, 9859, 9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973, 10007, 10009, 10037, 10039, 10061, 10067, 10069, 10079, 10091, 10093, 10099, 10103, 10111, 10133, 10139, 10141, 10151, 10159, 10163, 10169, 10177, 10181, 10193, 10211, 10223, 10243, 10247, 10253, 10259, 10267, 10271, 10273, 10289, 10301, 10303, 10313, 10321, 10331, 10333, 10337, 10343, 10357, 10369, 10391, 10399, 10427, 10429, 10433, 10453, 10457, 10459, 10463, 10477, 10487, 10499, 10501, 10513, 10529, 10531, 10559, 10567, 10589, 10597, 10601, 10607, 10613, 10627, 10631, 10639, 10651, 10657, 10663, 10667, 10687, 10691, 10709, 10711, 10723, 10729, 10733, 10739, 10753, 10771, 10781, 10789, 10799, 10831, 10837, 10847, 10853, 10859, 10861, 10867, 10883, 10889, 10891, 10903, 10909, 10937, 10939, 10949, 10957, 10973, 10979, 10987, 10993, 11003, 11027, 11047, 11057, 11059, 11069, 11071, 11083, 11087, 11093, 11113, 11117,

11119, 11131, 11149, 11159, 11161, 11171, 11173, 11177, 11197, 11213, 11239, 11243, 11251, 11257, 11261, 11273, 11279, 11287, 11299, 11311, 11317, 11321, 11329, 11351, 11353, 11369, 11383, 11393, 11399, 11411, 11423, 11437, 11443, 11447, 11467, 11471, 11483, 11489, 11491, 11497, 11503, 11519, 11527, 11549, 11551, 11579, 11587, 11593, 11597, 11617, 11621, 11633, 11657, 11677, 11681, 11689, 11699, 11701, 11717, 11719, 11731, 11743, 11777, 11779, 11783, 11789, 11801, 11807, 11813, 11821, 11827, 11831, 11833, 11839, 11863, 11867, 11887, 11897, 11903, 11909, 11923, 11927, 11933, 11939, 11941, 11953, 11959, 11969, 11971, 11981, 11987, 12007, 12011, 12037, 12041, 12043, 12049, 12071, 12073, 12097, 12101, 12107, 12109, 12113, 12119, 12143, 12149, 12157, 12161, 12163, 12197, 12203, 12211, 12227, 12239, 12241, 12251, 12253, 12263, 12269, 12277, 12281, 12289, 12301, 12323, 12329, 12343, 12347, 12373, 12377, 12379, 12391, 12401, 12409, 12413, 12421, 12433, 12437, 12451, 12457, 12473, 12479, 12487, 12491, 12497, 12503, 12511, 12517, 12527, 12539, 12541, 12547, 12553, 12569, 12577, 12583, 12589, 12601, 12611, 12613, 12619, 12637, 12641, 12647, 12653, 12659, 12671, 12689, 12697, 12703, 12713, 12721, 12739, 12743, 12757, 12763, 12781, 12791, 12799, 12809, 12821, 12823, 12829, 12841, 12853, 12889, 12893, 12899, 12907, 12911, 12917, 12919, 12923, 12941, 12953, 12959, 12967, 12973, 12979, 12983, 13001, 13003, 13007, 13009, 13033, 13037, 13043, 13049, 13063, 13093, 13099, 13103, 13109, 13121, 13127, 13147, 13151, 13159, 13163, 13171, 13177, 13183, 13187, 13217, 13219, 13229, 13241, 13249, 13259, 13267, 13291, 13297, 13309, 13313, 13327, 13331, 13337, 13339, 13367, 13381, 13397, 13399, 13411, 13417, 13421, 13441, 13451, 13457, 13463, 13469, 13477, 13487, 13499, 13513, 13523, 13537, 13553, 13567, 13577, 13591, 13597, 13613, 13619, 13627, 13633, 13649, 13669, 13679, 13681, 13687, 13691, 13693, 13697, 13709, 13711, 13721, 13723, 13729, 13751, 13757, 13759, 13763, 13781, 13789, 13799, 13807, 13829, 13831, 13841, 13859, 13873, 13877, 13879, 13883, 13901, 13903, 13907, 13913, 13921, 13931, 13933, 13963, 13967, 13997, 13999, 14009, 14011, 14029, 14033, 14051, 14057, 14071, 14081, 14083, 14087, 14107, 14143, 14149, 14153, 14159, 14173, 14177, 14197, 14207, 14221, 14243, 14249, 14251, 14281, 14293, 14303, 14321, 14323, 14327, 14341, 14347, 14369, 14387, 14389, 14401, 14407, 14411, 14419, 14423, 14431, 14437, 14447, 14449, 14461, 14479, 14489, 14503, 14519, 14533, 14537, 14543, 14549, 14551, 14557, 14561,

14563, 14591, 14593, 14621, 14627, 14629, 14633, 14639, 14653, 14657, 14669, 14683, 14699, 14713, 14717, 14723, 14731, 14737, 14741, 14747, 14753, 14759, 14767, 14771, 14779, 14783, 14797, 14813, 14821, 14827, 14831, 14843, 14851, 14867, 14869, 14879, 14887, 14891, 14897, 14923, 14929, 14939, 14947, 14951, 14957, 14969, 14983, 15013, 15017, 15031, 15053, 15061, 15073, 15077, 15083, 15091, 15101, 15107, 15121, 15131, 15137, 15139, 15149, 15161, 15173, 15187, 15193, 15199, 15217, 15227, 15233, 15241, 15259, 15263, 15269, 15271, 15277, 15287, 15289, 15299, 15307, 15313, 15319, 15329, 15331, 15349, 15359, 15361, 15373, 15377, 15383, 15391, 15401, 15413, 15427, 15439, 15443, 15451, 15461, 15467, 15473, 15493, 15497, 15511, 15527, 15541, 15551, 15559, 15569, 15581, 15583, 15601, 15607, 15619, 15629, 15641, 15643, 15647, 15649, 15661, 15667, 15671, 15679, 15683, 15727, 15731, 15733, 15737, 15739, 15749, 15761, 15767, 15773, 15787, 15791, 15797, 15803, 15809, 15817, 15823, 15859, 15877, 15881, 15887, 15889, 15901, 15907, 15913, 15919, 15923, 15937, 15959, 15971, 15973, 15991, 16001, 16007, 16033, 16057, 16061, 16063, 16067, 16069, 16073, 16087, 16091, 16097, 16103, 16111, 16127, 16139, 16141, 16183, 16187, 16189, 16193, 16217, 16223, 16229, 16231, 16249, 16253, 16267, 16273, 16301, 16319, 16333, 16339, 16349, 16361, 16363, 16369, 16381, 16411, 16417, 16421, 16427, 16433, 16447, 16451, 16453, 16477, 16481, 16487, 16493, 16519, 16529, 16547, 16553, 16561, 16567, 16573, 16603, 16607, 16619, 16631, 16633, 16649, 16651, 16657, 16661, 16673, 16691, 16693, 16699, 16703, 16729, 16741, 16747, 16759, 16763, 16787, 16811, 16823, 16829, 16831, 16843, 16871, 16879, 16883, 16889, 16901, 16903, 16921, 16927, 16931, 16937, 16943, 16963, 16979, 16981, 16987, 16993, 17011, 17021, 17027, 17029, 17033, 17041, 17047, 17053, 17077, 17093, 17099, 17107, 17117, 17123, 17137, 17159, 17167, 17183, 17189, 17191, 17203, 17207, 17209, 17231, 17239, 17257, 17291, 17293, 17299, 17317, 17321, 17327, 17333, 17341, 17351, 17359, 17377, 17383, 17387, 17389, 17393, 17401, 17417, 17419, 17431, 17443, 17449, 17467, 17471, 17477, 17483, 17489, 17491, 17497, 17509, 17519, 17539, 17551, 17569, 17573, 17579, 17581, 17597, 17599, 17609, 17623, 17627, 17657, 17659, 17669, 17681, 17683, 17707, 17713, 17729, 17737, 17747, 17749, 17761, 17783, 17789, 17791, 17807, 17827, 17837, 17839, 17851, 17863, 17881, 17891, 17903, 17909, 17911, 17921, 17923, 17929, 17939, 17957, 17959, 17971, 17977, 17981, 17987, 17989, 18013, 18041, 18043,

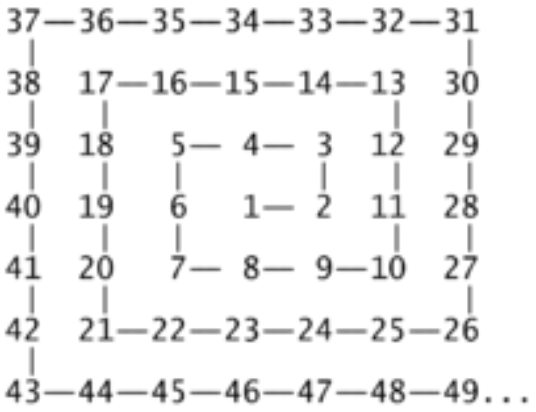
18047, 18049, 18059, 18061, 18077, 18089, 18097, 18119, 18121, 18127, 18131, 18133, 18143, 18149, 18169, 18181, 18191, 18199, 18211, 18217, 18223, 18229, 18233, 18251, 18253, 18257, 18269, 18287, 18289, 18301, 18307, 18311, 18313, 18329, 18341, 18353, 18367, 18371, 18379, 18397, 18401, 18413, 18427, 18433, 18439, 18443, 18451, 18457, 18461, 18481, 18493, 18503, 18517, 18521, 18523, 18539, 18541, 18553, 18583, 18587, 18593, 18617, 18637, 18661, 18671, 18679, 18691, 18701, 18713, 18719, 18731, 18743, 18749, 18757, 18773, 18787, 18793, 18797, 18803, 18839, 18859, 18869, 18899, 18911, 18913, 18917, 18919, 18947, 18959, 18973, 18979, 19001, 19009, 19013, 19031, 19037, 19051, 19069, 19073, 19079, 19081, 19087, 19121, 19139, 19141, 19157, 19163, 19181, 19183, 19207, 19211, 19213, 19219, 19231, 19237, 19249, 19259, 19267, 19273, 19289, 19301, 19309, 19319, 19333, 19373, 19379, 19381, 19387, 19391, 19403, 19417, 19421, 19423, 19427, 19429, 19433, 19441, 19447, 19457, 19463, 19469, 19471, 19477, 19483, 19489, 19501, 19507, 19531, 19541, 19543, 19553, 19559, 19571, 19577, 19583, 19597, 19603, 19609, 19661, 19681, 19687, 19697, 19699, 19709, 19717, 19727, 19739, 19751, 19753, 19759, 19763, 19777, 19793, 19801, 19813, 19819, 19841, 19843, 19853, 19861, 19867, 19889, 19891, 19913, 19919, 19927, 19937, 19949, 19961, 19963, 19973, 19979, 19991, 19993, 19997, 20011, 20021, 20023, 20029, 20047, 20051, 20063, 20071, 20089, 20101, 20107, 20113, 20117, 20123, 20129, 20143, 20147, 20149, 20161, 20173, 20177, 20183, 20201, 20219, 20231, 20233, 20249, 20261, 20269, 20287, 20297, 20323, 20327, 20333, 20341, 20347, 20353, 20357, 20359, 20369, 20389, 20393, 20399, 20407, 20411, 20431, 20441, 20443, 20477, 20479, 20483, 20507, 20509, 20521, 20533, 20543, 20549, 20551, 20563, 20593, 20599, 20611, 20627, 20639, 20641, 20663, 20681, 20693, 20707, 20717, 20719, 20731, 20743, 20747, 20749, 20753, 20759, 20771, 20773, 20789, 20807, 20809, 20849, 20857, 20873, 20879, 20887, 20897, 20899, 20903, 20921, 20929, 20939, 20947, 20959, 20963, 20981, 20983, 21001, 21011, 21013, 21017, 21019, 21023, 21031, 21059, 21061, 21067, 21089, 21101, 21107, 21121, 21139, 21143, 21149, 21157, 21163, 21169, 21179, 21187, 21191, 21193, 21211, 21221, 21227, 21247, 21269, 21277, 21283, 21313, 21317, 21319, 21323, 21341, 21347, 21377, 21379, 21383, 21391, 21397, 21401, 21407, 21419, 21433, 21467, 21481, 21487, 21491, 21493, 21499, 21503, 21517, 21521, 21523, 21529, 21557, 21559, 21563, 21569, 21577, 21587, 21589, 21599, 21601, 21611,

21613, 21617, 21647, 21649, 21661, 21673, 21683, 21701, 21713, 21727, 21737, 21739, 21751, 21757, 21767, 21773, 21787, 21799, 21803, 21817, 21821, 21839, 21841, 21851, 21859, 21863, 21871, 21881, 21893, 21911, 21929, 21937, 21943, 21961, 21977, 21991, 21997, 22003, 22013, 22027, 22031, 22037, 22039, 22051, 22063, 22067, 22073, 22079, 22091, 22093, 22109, 22111, 22123, 22129, 22133, 22147, 22153, 22157, 22159, 22171, 22189, 22193, 22229, 22247, 22259, 22271, 22273, 22277, 22279, 22283, 22291, 22303, 22307, 22343, 22349, 22367, 22369, 22381, 22391, 22397, 22409, 22433, 22441, 22447, 22453, 22469, 22481, 22483, 22501, 22511, 22531, 22541, 22543, 22549, 22567, 22571, 22573, 22613, 22619, 22621, 22637, 22639, 22643, 22651, 22669, 22679, 22691, 22697, 22699, 22709, 22717, 22721, 22727, 22739, 22741, 22751, 22769, 22777, 22783, 22787, 22807, 22811, 22817, 22853, 22859, 22861, 22871, 22877, 22901, 22907, 22921, 22937, 22943, 22961, 22963, 22973, 22993, 23003, 23011, 23017, 23021, 23027, 23029, 23039, 23041, 23053, 23057, 23059, 23063, 23071, 23081, 23087, 23099, 23117, 23131, 23143, 23159, 23167, 23173, 23189, 23197, 23201, 23203, 23209, 23227, 23251, 23269, 23279, 23291, 23293, 23297, 23311, 23321, 23327, 23333, 23339, 23357, 23369, 23371, 23399, 23417, 23431, 23447, 23459, 23473, 23497, 23509, 23531, 23537, 23539, 23549, 23557, 23561, 23563, 23567, 23581, 23593, 23599, 23603, 23609, 23623, 23627, 23629, 23633, 23663, 23669, 23671, 23677, 23687, 23689, 23719, 23741, 23743, 23747, 23753, 23761, 23767, 23773, 23789, 23801, 23813, 23819, 23827, 23831, 23833, 23857, 23869, 23873, 23879, 23887, 23893, 23899, 23909, 23911, 23917, 23929, 23957, 23971, 23977, 23981, 23993, 24001, 24007, 24019, 24023, 24029, 24043, 24049, 24061, 24071, 24077, 24083, 24091, 24097, 24103, 24107, 24109, 24113, 24121, 24133, 24137, 24151, 24169, 24179, 24181, 24197, 24203, 24223, 24229, 24239, 24247, 24251, 24281, 24317, 24329, 24337, 24359, 24371, 24373, 24379, 24391, 24407, 24413, 24419, 24421, 24439, 24443, 24469, 24473, 24481, 24499, 24509, 24517, 24527, 24533, 24547, 24551, 24571, 24593, 24611, 24623, 24631, 24659, 24671, 24677, 24683, 24691, 24697, 24709, 24733, 24749, 24763, 24767, 24781, 24793, 24799, 24809, 24821, 24841, 24847, 24851, 24859, 24877, 24889, 24907, 24917, 24919, 24923, 24943, 24953, 24967, 24971, 24977, 24979, 24989

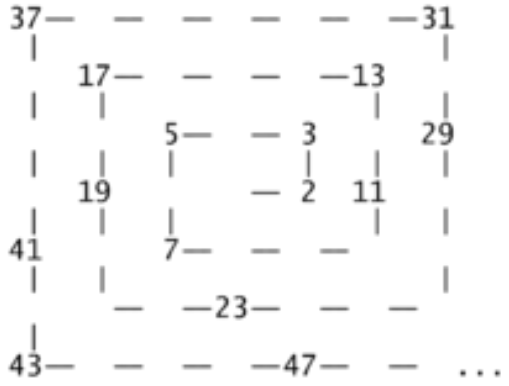
5.3. Ulam-spirál

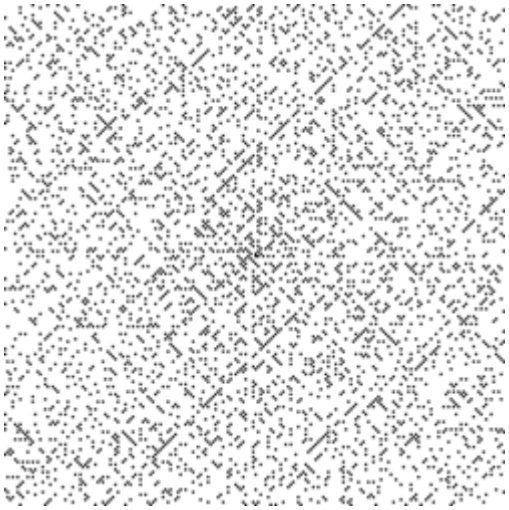
Az **Ulam-spirál** vagy **prím-spirál** a számelméletben a prímszámok egy spirális elrendezése, ami egy máig megmagyarázatlan mintát mutat. Nevét felfedezőjéről, Stanisław Ulam lengyel matematikusról kapta, aki 1963-ban egy értekezleten unalmában rajzolta fel a spirált.

Ulam egy négyzetrács mentén, spirálvonalban haladva felrajzolta az első 50 pozitív egész számot:



Ezután kihúzta azokat, amik nem prímek, és a következő ábrát kapta:





200×200-as Ulam-spirál.

Meglepetésére a prímek többnyire átlók mentén helyezkedtek el. A jelenség nagyobb léptékben is megfigyelhető, például az oldalsó ábrán látható 200×200-as spirálban, ahol a prímeket fekete pontok jelzik.

Mivel a páros számok a 2-t kivéve mind összetettek, és a spirálban a sakktábla sötét kockáihoz hasonló mintában helyezkednek el, az önmagában nem meglepő, hogy a prímszámok egy átlós rácsot alkotnak, az viszont igen, hogy e rács egyes vonalain sokkal gyakrabban fordulnak elő, mint másokon. Ez akkor is igaz lesz, ha a számokat nem egytől kezdve írjuk fel. Képletben megfogalmazva, sok olyan *b* és *c* konstans van, amire az

$f(n) = 4n^2 + bn + c$ függvény sűrűn ad helyettesítési értékként prímeket. A jelenség oka máig ismeretlen.

Elég messziről nézve az ábrát függőleges és vízszintes vonalak is kirajzolódnak. A svájci Leonhard Euler által talált $n^2 + n + 17$ kifejezés minden 0 és 15 közötti értékre prímszámot ad. Ezek a prímek: 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227 és 257 megjelennek az Ulam-spirál főátlóján. Euler később egy másik képletet is talált:

$n^2 + n + 41$, ami 0 és 40 közötti helyettesítési értékekre prímet ad. Ez egy másik átló, ami mentén különösen sok a prím: 10 millióig a helyettesítési értékek 47,5%-a prímet ad. Ulam további képleteket is talált, amik majdnem ilyen jók.

5.4. Prímszámokból álló bűvös négyzetek

Egy számokkal kitöltött nxn-es négyzetet akkor nevezünk bűvös négyzetnek, ha minden sorában, oszlopában, illetve az átlókban szereplő számok összege azonos. Most csak azokra nézünk néhány példát, amelyekben prímszámok szerepelnek. Egy $3x3$-as négyzet egy lehetséges elrendezése a következő is lehet:

$\frac{x+y}{2}$	z	$x+\frac{z-y}{2}$
$x-y+z$	$\frac{x+z}{2}$	y
$\frac{y+z}{2}$	x	$\frac{x-y}{2}+z$

Az *x, y* és *z* prímszámok legyenek. Írhatunk egy egyszerű programot, amelyik végig futtatja *x, y* és *z* értékeit egy adott intervallumba eső prímszámokon és ellenőrzi, hogy a táblázat minden eleme prímszám-e. Néhány példa:

17	**113**	**47**
89	**59**	**29**
71	**5**	**101**

53	**617**	**263**
521	**311**	**101**
359	**5**	**569**

137	**773**	**257**
509	**389**	**269**
521	**5**	**641**

389	**647**	**401**
491	**479**	**467**
557	**311**	**569**

359	**881**	**557**
797	**599**	**401**
641	**317**	**839**

73	**211**	**97**
151	**127**	**103**
157	**43**	**181**

Találhatunk olyan példát is, melyben minden szám végződése azonos:

571	**1051**	**181**
211	**601**	**991**
1021	**151**	**631**

823	**1093**	**643**
673	**853**	**1033**
1063	**613**	**883**

Találhatunk olyan példát is, melyben minden szám 7-re végződik:

307	**607**	**97**
127	**337**	**547**
577	**67**	**367**

37	**607**	**277**
547	**307**	**67**
337	**7**	**577**

Találhatunk olyan példát is, melyben minden szám 9-re végződik:

569	**59**	**449**
239	**359**	**479**
269	**659**	**149**

829	**1879**	**409**
619	**1039**	**1459**
1669	**199**	**1249**

Nézzünk egy $4x4$-esre bűvös négyzetre is példát:

37	**83**	**97**	**41**
53	**61**	**71**	**73**
89	**67**	**59**	**43**
79	**47**	**31**	**101**

Két tételt szeretnék ismertetni bizonyítás nélkül:

1. Tétel: Ha egy harmadrendű ($3x3$), csak prímszámokból álló bűvös négyzetben lévő számok egy számtani sorozat tagjai, akkor a sorozat differenciája osztható 210-zel.

2. Tétel: Ha egy negyedrendű ($4x4$), csak prímszámokból álló bűvös négyzetben lévő számok egy számtani sorozat tagjai, akkor a sorozat differenciája osztható 30030-cal.

5.5. Prímtesztek és Prímfaktorizáció

Léteznek olyan módszerek, amelyek viszonylag gyorsan eldöntik, hogy egy nagy szám prím-e vagy összetett. Az ilyen algoritmusokat nevezzük prímteszteknek.

Könnyű-e meghatározni egy szám prímtényezős felbontását? Látszólag igen, hiszen csak meg kell nézni, hogy osztható-e 2-vel, 3-mal, 5-tel, stb. Ha találunk egy prímosztót, akkor csak a hányadost kell tovább bontani. Ha pedig a szám négyzetgyökéig nem találtunk osztót, akkor az adott szám biztosan prím. Nagy számoknál már nem tudjuk ezt a módszert alkalmazni, hiszen nem ismerünk minden prímet, illetve rengeteg műveletet kellene a számítógépnek elvégeznie. Ez a próbaosztásos eljárás a gyakorlatban teljesen használhatatlan.

A gyors prímtesztek létezése első hallásra meglepőnek tűnik, annak tudatában, hogy egy nagy összetett szám prímtényezőkre való bontása milyen reménytelen feladat. Nézzük meg ezt a két problémát egy kicsit részletesebben.

Prímtesztek

A prímtesztek olyan eljárások, melyek egy adott számról eldöntik, hogy prím vagy összetett szám. Általában nem határozzák meg a szám egyetlen osztóját sem. Attól függően, hogy a teszt használ-e véletlen számokat, megkülönböztetünk determinisztikus és véletlen prímteszteket. Minden teszt valamilyen módon az Euler-Fermat tételen alapul.

Tétel: Minden egynél nagyobb egész *n* számra és minden *n*-hez relatív *a* egész számra igaz a következő kongruencia:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Bizonyítás: Legyen az $r_1, \cdots, r_{\varphi(n)}$ egy redukált maradékrendszer (RMR). Ekkor az $ar_1, \cdots, ar_{\varphi(n)}$ szintén RMR tetszőleges *n*-hez relatív prím *a*-ra, hiszen bármely kettő különbsége *ka* alakú, ahol *k* nem osztható *n*-nel.

Vegyük ezt a két felírását az egyértelmű RMR-nek:

$$\prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} ar_i \qquad (mod\ n)$$

Egy RMR elemeinek szorzata relatív prím a modulushoz, ezért egyszerűsíthetünk vele:

$$a^{\varphi(n)} \equiv 1 \quad (mod\ n)$$

Tehát igaz az állítás.

1. Fermat-prímteszt

Legyen *n* egy 1-nél nagyobb egész szám, melyről szeretnénk eldönteni, hogy prímszám-e. Válasszunk véletlenszerűen egy *n*-nél kisebb pozitív *a* egész számot. Ekkor az alábbi kongruencia biztosan teljesül ha *n* prím:

$$a^{n-1} \equiv 1 \quad (mod\ n) \qquad (1)$$

Ha *n* összetett, akkor legfeljebb 50% eséllyel teljesül. A fennmaradó kivételes esetekben *n*-et univerzális álprímnek nevezzük. Ekkor (1) minden *n*-hez relatív prím *a*-ra teljesül.

Bizonyítás:

Prímekre ez az Euler-Fermat tétel következménye, hiszen $\varphi(n) = n - 1$, ha *n* prím. Ha *n* összetett szám és *a* nem relatív prím hozzá, akkor *a*-nak minden hatványa többszöröse lesz *a* és *n* legnagyobb közös osztójának. Tehát (1) nem állhat fenn.

2. Solovay-Strassen-prímteszt

Legyen *n* egy 1-nél nagyobb páratlan egész szám. Ekkor az

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \qquad (mod\ n) \qquad (2)$$

kongruencia az $1, \cdots, n-1$ számok mindegyikére teljesül, ha *n* prím és az $1, \cdots, n-1$ számok kevesebb, mint felére teljesül, ha *n* összetett szám.

Bizonyítás:

1. Ha *n* prímszám, akkor az Euler-Fermat tétel szerint minden 1 és $n-1$ közötti *a* számra:

$$a^{n-1} \equiv 1 \pmod{n}$$

Továbbá $\boldsymbol{Z}_p$-ben csak ± 1 második egységgyök, ezért:

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$$

A Legendre-Jacobi szimbólum definíciója szerint: $\left(\frac{a}{n}\right) = \pm 1$. Tehát bizonyítandó:

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

akkor és csak akkor, ha $\left(\frac{a}{n}\right) = 1$, vagyis ha az alábbi kongruencia megoldható:

$$x^2 \equiv a \pmod{n}$$

Legyen g primitív gyök modulo *n*, és számoljunk a g szerinti diszkrét logaritmusokkal (indexekkel):

$$g^{2indx} \equiv g^{inda} \pmod{n}$$

Mivel g primitív gyök, azaz minden nem 0 maradékosztály előfordul valamilyen hatványaiként (ciklikusan fordulnak elő), a fenti állítások egyenértékűek a következővel:

$$2indx \equiv inda \pmod{n-1}$$

Mivel $2indx$ és $n-1$ is osztható 2-vel, ezért ha $inda$ páratlan, akkor a kongruencia nem oldható meg. Ha $inda$ páros, akkor:

$$2indx \equiv g^{\frac{inda}{2}} \pmod{\frac{n-1}{2}}$$

A megoldás:

$$x \equiv \pm g^{\frac{inda}{2}} \pmod{p}$$

Összefoglalva:

$$a^{\frac{n-1}{2}} \equiv 1 \quad (mod\ n)$$

Ez a kongruencia akkor és csak akkor igaz, ha $inda$ páros, vagyis $\left(\frac{a}{n}\right) = 1$.

2. Nézzük azt az esetet, amikor *n* összetett szám.

Nevezzük **cinkosnak** *a*-t egy összetett *n*-re vonatkozólag akkor, ha (2) teljesül, egyébként pedig **tanúnak**. Mivel $\left(\frac{a}{n}\right)$ csak *n*-hez relatív prím *a*-k esetén értelmezett, *n*-hez nem relatív prímekre (2) nem teljesül. A gyakorlatban $\left(\frac{a}{n}\right)$ kiszámításakor tényleg kiderül ha *a* és *n* nem relatív prím.

Első lépésben csak azt nézzük meg, hogy minden összetett *n*-re létezik *a* tanú. Ha *n* nem négyzetmentes (ossza mondjuk p^2), akkor egy g primitív gyök modulo p^2 tanú. Ugyanis az alábbi kongruencia nem teljesül:

$$g^{\frac{n-1}{2}} \equiv \pm 1 \qquad (mod\ n)$$

Indirekt bizonyítjuk az állítást. Tegyük fel, hogy teljesül a fenti kongruencia. Emeljük négyzetre:

$$g^{n-1} \equiv 1 \qquad (mod\ n)$$

Ebből következik p^2-re is:

$$g^{n-1} \equiv 1 \qquad (mod\ p^2)$$

Az Euler-Fermat tétel szerint:

$$g^{\varphi(p^2)} \equiv 1 \qquad (mod\ p^2)$$

Mivel g primitív gyök, a $mod\ p^2$ RMR minden elemét fel kell vennie g hatványainak, tehát semmilyen $\varphi(p^2)$-nél kisebb *j*-re nem állhat fenn a következő:

$$g^j \equiv 1 \qquad (mod\ p^2)$$

Vagyis a $g^{n-1} \equiv 1 \pmod{p^2}$-ből rögtön következik, hogy $\varphi(p^2)$ osztója $(n-1)$-nek. Azaz:

$p(p-1)$ osztója $(n-1)$-nek. Azonban p osztója p^2-nek osztója n-nek, ebből következik, hogy p osztója n-nek és $(n-1)$-nek. Ez ellentmondás, tehát igaz az állítás.

A továbbiakban legyen n négyzetmentes! Válasszuk a bizonyítást két részre aszerint, hogy minden n-hez relatív prím a-ra igaz a következő vagy sem:

$$a^{\frac{n-1}{2}} \equiv 1 \qquad (mod\ n) \qquad\qquad (3)$$

Ha (3) igaz minden n-hez relatív prím a-ra, akkor legyen:

$$n = q_1 \cdot \dots \cdot q_s \quad \left(\frac{h}{q_1}\right) = -1$$

Oldjuk meg az alábbi szimultán kongruencierendszert:

$$w \equiv h \pmod{q_1} \qquad w \equiv 1 \pmod{q_1}, ahol\ 2 \leq i \leq s$$

Ekkor (3) miatt:

$$w^{\frac{n-1}{2}} \equiv 1 \qquad (mod\ n)$$

Azonban:

$$\left(\frac{w}{n}\right) = \left(\frac{h}{q_1}\right) \cdot \left(\frac{1}{q_2}\right) \cdot \dots \cdot \left(\frac{1}{q_s}\right) = (-1) \cdot 1 \cdot \dots \cdot 1 = -1$$

Azt akartuk megmutatni, hogy létezik legalább egy tanú és ha (3) teljesül minden n-hez relatív a-ra, akkor meg is találtunk egyet:

$$1 \equiv w^{\frac{n-1}{2}} \not\equiv \left(\frac{w}{n}\right) = -1 \qquad (mod\ n)$$

Vizsgáljuk most a második esetet, amikor van olyan n-hez relatív prím a szám, amelyre (3) nem teljesül azaz:

$$a^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$$

Mivel egy inkongruencia fennáll a modulus legalább egy prímtényezőjére, válasszunk *n*-nek alkalmas q_1 prímtényezőjét, tehát:

$$a^{\frac{n-1}{2}} \not\equiv 1 \pmod{q_1}$$

Oldjuk meg ezzel az *a*-val az alábbi kongruenciarendszet:

$$z \equiv a \pmod{q_1}, \qquad z \equiv 1 \pmod{q_1}, \qquad ahol\ 2 \leq i \leq s$$

Erre a *z*-re:

$$z^{\frac{n-1}{2}} \not\equiv 1 \pmod{q_1}, \qquad z^{\frac{n-1}{2}} \equiv 1 \pmod{q_i}, \qquad ahol\ 2 \leq i \leq s$$

Tehát $z^{\frac{n-1}{2}}$ sem 1-gyel nem kongruens q_1-re, sem -1-gyel q_2-re. Így $z^{\frac{n-1}{2}}$ nem kongruens ± 1-gyel *n* minden prímtényezőjére, azaz:

$$z^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$$

Ez a *z* tanú, mert:

$$z^{\frac{n-1}{2}} \not\equiv \pm 1 = \left(\frac{z}{n}\right) \pmod{n}$$

Ezzel beláttuk, hogy összetett *n* esetén mindenképpen létezik *n* összetettségét igazoló tanú a Solovay-Strassen-prímtesztben.

Bebizonyítjuk, hogy ha már egyetlen tanú létezik, akkor a RMR legfeljebb fele cinkos.

Legyen *t* és *c* relatív prím *n*-hez, *t* tanú, *c* pedig cinkos. Indirekt módon bizonyítjuk, hogy a tc szorzat is tanú. Tegyük fel az ellenkezőjét, vagyis:

$$(tc)^{\frac{n-1}{2}} \equiv \left(\frac{tc}{n}\right) \pmod{n}$$

Használjuk ki, hogy *c* cinkos, vagyis:

$$c^{\frac{n-1}{2}} \equiv \left(\frac{c}{n}\right) \pmod{n}$$

Szorozzuk össze a két fenti kongruenciát:

$$(tc)^{\frac{n-1}{2}} \cdot c^{\frac{n-1}{2}} \equiv \left(\frac{tc}{n}\right) \cdot \left(\frac{c}{n}\right) \pmod{n}$$

A hatványozás és a Jacobi-szimbólum multiplikatív. Egy *n*-hez relatív prím *c* cinkos $\frac{n-1}{2}$-edik hatványa kongruens $\left(\frac{c}{n}\right)$-nel, $\left(\frac{c}{n}\right) = \pm 1$, tehát $c^{\frac{n-1}{2}}$ négyzete kongruens ± 1 négyzetével, vagyis 1-gyel. Ezt a három azonosságot felhasználva adódik a következő:

$$(tc)^{\frac{n-1}{2}} \cdot c^{\frac{n-1}{2}} = t^{\frac{n-1}{2}} \cdot \left(c^{\frac{n-1}{2}}\right)^2 \equiv t^{\frac{n-1}{2}} \pmod{n}$$

Ez azt jelenti, hogy *t* is cinkos, de ez ellentmond az indirekt feltevésnek. Tehát bebizonyítottuk, hogy cinkos és tanú szorzata tanú. Egyetlen *t* tanú létezéséből következik, hogy a $mod\ n$ RMR legalább fele tanú. Vegyük ugyanis $c_1, \cdots, c_k$ inkongruens cinkosokat és szorozzuk mindegyiket *t*-vel. A $tc_1, \cdots, tc_k$ mindegyike tanú és páronként inkongruensek.

(Lásd az Euler-Fermat tétel bizonyítását!)

3. Miller-Lenstra-Rabin-prímteszt

A prímteszt 1-nél nagyobb páratlan *n*-ekre működik. Írjuk $(n-1)$-et $2^k r$ alakba úgy, hogy *r* páratlan legyen és $k \geq 1$. Az Euler-Fermat tétel szerint ha *n* prím, minden $a \not\equiv 0 \pmod{n}$-re

$$a^{n-1} = a^{2^k r} \equiv 1 \pmod{n}$$

Ha *n* prím, akkor modulo *n* csak ± 1 lehet második egységgyök: $a^{2^{k-1} r} \equiv \pm 1 \pmod{n}$.

Ha $a^{2^{k-1} r} \equiv +1 \pmod{n}$, akkor $a^{2^{k-2} r} \equiv \pm 1 \pmod{n}$, és így tovább. Ennek alapján a teszt pontos megfogalmazása:

Legyen $n > 1$ és *r* páratlan, ahol $n - 1 = 2^k r$. Nevezzük jó sorozatnak $a^{2^0 r}, \cdots, a^{2^{k-1} r}$-et, ha $a^r \equiv 1 \pmod{n}$, vagy van olyan, mely (-1)-et ad *n*-re maradékul. Ha *n* prím, akkor minden $a = 1, \cdots, n-1$-re jó sorozatot kapunk. Ha *n* összetett, akkor az $a = 1, \cdots, n-1$ számok kevesebb, mint felére kapunk jó sorozatot.

Bizonyítás:

$\boldsymbol{Z}_p$-ben csak ± 1 a két második egységgyök. Emiatt $a^{2^k r} \equiv 1 \pmod{n}$-ből gyököt vonva ± 1-et kell kapnunk. Ha $(+1)$-et kapunk, akkor az eljárást megismételhetjük, amig *k*-adszor is gyököt vonva $a^r \equiv \pm 1 \pmod{n}$-et kapunk. Ezzel prím *n*-ekre beláttuk az állítást.

Nem négyzetmentes *n*-ekre a bizonyítás ugyanúgy megy, mint a Solovay-Strassen-prímteszt igazolásában láttuk.

Négyzetmentes *n*-ekre legyen *j* a legnagyobb szám, melyre még található olyan *a*, hogy:

$$a^{2^j r} \not\equiv 1 \pmod{n} \qquad (4)$$

(A maximum létezik, például $a = -1, j = 0$ esetén $(-1)^{2^0 r} = -1$.)

Ekkor *n*-nek valamely q_1 prímosztójára: $a^{2^j r} \not\equiv 1 \pmod{q_1}$. Oldjuk meg ezzel az *a*-val az alábbi kongruenciarendszert:

$$t \equiv a \pmod{q_1}, \quad t \equiv 1 \pmod{q_1}, \qquad ahol\ 2 \leq i \leq s$$

A feltétel szerint:

$$t^{2^j r} \equiv a^{2^j r} \not\equiv 1 \pmod{q_1}$$

Azonban:

$$t^{2^j r} \equiv 1^{2^j r} \equiv 1 \not\equiv -1 \pmod{q_1}, \qquad ahol\ 2 \leq i \leq s$$

Így $t^{2^j r}$ sem 1-gyel, sem (-1)-gyel nem kongruens modulo *n*, míg *j*-nél nagyobb számokra (így $V = j + 1$-re): $t^{2^V r} \equiv 1 \pmod{n}$, tehát *t* tanú.

Megmutatjuk, hogy ennek a *t* tanúnak és egy *n*-hez relatív prím *c* cinkosnak a szorzata tanú.

Egy *j*-nél nagyobb *x* számra:

$$(tc)^{2^x r} \equiv 1 \pmod{n}$$

Mivel *c* cinkos: $c^{2^j r} \equiv \pm 1 \pmod{n}$. A *t*-ről feljebb láttuk, hogy $t^{2^j r} \not\equiv \pm 1 \pmod{n}$. A kettő összevetéséből:

$$(tc)^{2^j r} \not\equiv \pm 1 \pmod{n}$$

Ebből a Solovay-Strassen-prímteszt bizonyításának utolsó bekezdésében látott módon kapjuk, hogy az $1,2,\cdots,n-1$ számok több mint fele tanú.

4. Lucas-prímteszt

Legyen *n* kettőnél nagyobb egész szám. Akkor és csak akkor létezik olyan 1 és *n* közötti *a* szám, melyre $a^{n-1} \equiv 1 \pmod{n}$, de $(n-1)$ minden *q* prímosztójára teljesül az alábbi, ha *n* prím:

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$$

Bizonyítás:

Ha *n* prím, akkor létezik primitív gyök modulo *n*, azaz a feltételt kielégítő *a* szám. Ha létezik ilyen *a* szám, akkor annak a rendje $(n-1)$-nek osztója, de nem osztója egyetlen valódi osztójának sem. Tehát az *a* szám rendje $(n-1)$, ezért az *n* prímszám.

Megjegyzés: Az állítás akkor is igaz marad, ha csak annyit teszünk fel, hogy $(n-1)$ minden *q* prímtényezőjéhez létezik egy olyan *q*-tól függő a_q egész szám, melyre:

$$a_q^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$$

5. Proth-prímteszt

Legyen $n = k \cdot 2^l + 1$, ahol *k* egy 2^l-nél kisebb páratlan szám. Az *n* akkor és csak akkor prím, ha található olyan *a* szám, melyre:

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

Megjegyzés: Ha *n* prím, akkor a kvadratikus nemmaradékok modulo *n* alkalmasak. Mivel a kvadratikus maradékok és kvadratikus nemmaradékok fele-fele arányban fordulnak elő a $(mod\ n)$ RMR-ben, így minden próbálkozásban 50% esélyünk van alkalmas a-t választani. Ha *n* összetett, akkor gyakran igaz a következő:

$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \quad (mod\ n)$$

Ebből biztosan kiderül, hogy összetett.

Bizonyítás:

Ha *n* prím, akkor a kvadratikus nemmaradékok modulo *n* alkalmasak.

Ha *n* összetett, akkor indirekt módon tegyük fel a következőt:

$$a^{\frac{n-1}{2}} \equiv -1 \quad (mod\ n)$$

Legyen az *n* szám egy prímosztója *p*. Ekkor: $2^l \mid o(a) \mid p-1$, mert:

$$a^{\frac{n-1}{2}} \equiv a^{\frac{k\cdot 2^l+1-1}{2}} \equiv a^{k\cdot 2^{l-1}} \equiv -1 \quad (mod\ n)$$

Négyzetre emelve: $a^{k\cdot 2^l} \equiv 1 \quad (mod\ n)$. Tehát $o(a)$ prímtényezős felbontásában *l*-edik hatványon szerepel a 2, vagyis $2^l \mid o(a)$. Továbbá $o(a) \mid \varphi(p) = p-1$, azaz $2^l \mid p-1$.

Kongruenciával kifejezve: $p \equiv 1 \quad (mod\ 2^l)$. Ezért $p = 1 + c \cdot 2^l$, továbbá:

$$n \equiv k \cdot 2^l + 1 \equiv 1 \quad (mod\ 2^l)$$

Mivel mind *p*, mind *n* kongruens 1-gyel modulo 2^l, ezért:

$$\frac{n}{p} \equiv 1 \quad (mod\ 2^l)$$

Vagyis:

$$n = p \cdot \frac{n}{p} = (1 + c \cdot 2^l)(1 + d \cdot 2^l) > 1 + cd2^{2l} > 1 + k \cdot 2^l = n$$

Ez pedig ellentmondás.

6. Pepin-prímteszt

Legyen $F_n = 2^{2^n} + 1$. Az $n > 0$ esetén az F_n akkor és csak akkor prím, ha

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

Bizonyítás:

Emeljük négyzetre a kongruenciát:

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

Így $o(3) \mid 2^{2^n}$, de $o(3) \nmid 2^{2^{n-1}}$. Ezért $o(3) = 2^{2^n}$. Vagyis legalább ennyi relatív prím van 0 és F_n között F_n-hez, tehát F_n prím. Az Euler-feltétel szerint:

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$$

A $2^2 \equiv 1 \pmod 3$. Ezt $(n-1)$-szer négyzetre emelve: $2^{2^n} \equiv 1 \pmod 3$. Emiatt:

$$F_n \equiv -1 \pmod 3$$

$$F_n - 1 = 2^{2^n} \equiv 0 \pmod 4$$

A kvadratikus reciprocitási tétel szerint:

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1$$

7. Pocklington-prímteszt

Legyen $N > 1$ egész szám, $q > \sqrt{N} - 1$ prímosztója az $N - 1$-nek. Az *N* biztosan prím, ha találunk olyan *a* számot, amelyre:

$$a^{N-1} \equiv 1 \pmod N \quad \text{és} \quad \left(a^{\frac{N-1}{q}} - 1, N\right) = 1$$

Megjegyzés: Ha az első feltétel nem teljesül, akkor az Euler-Fermat tétel miatt *N* biztosan összetett szám. Ha

$$1 < \left(a^{\frac{N-1}{q}} - 1, N\right) < N,$$

akkor *N*-nek még egy osztóját is megtaláltuk. Ezért tekinthetnénk prímfaktorizációnak, amely előtt végrehajtottunk egy Fermat-prímtesztet.

Bizonyítás:

Indirekt módon tegyük fel, hogy *N* összetett. Ezért létezik $p \leq \sqrt{N}$ prímosztója. Tehát $p \leq q$, így $(p-1, q) = 1$. Ezért egy alkalmas *u*-ra:

$$uq \equiv 1 \pmod{p-1}$$

Az $a^{N-1} \equiv 1 \pmod{N}$ miatt $a^{N-1} \equiv 1 \pmod{p}$. Ezért:

$$(a^{N-1})^u = \left(a^{\frac{N-1}{q}}\right)^{uq} \equiv a^{\frac{N-1}{q}} \equiv 1 \pmod{p}$$

Ez viszont ellentmond az alábbi feltételnek:

$$\left(a^{\frac{N-1}{q}} - 1, N\right) = 1$$

Tehát igaz az állítás.

Álprímek

1. Fermat-féle álprímek

Az *n* páratlan összetett számot *b* alapra nézve Fermat-féle álprímeknek nevezzük, ha $lnko(b,n) = 1$ *és* $b^{n-1} \equiv 1 \pmod{n}$ teljesül.

Tétel: Minden *b* alapra nézve végtelen sok álprím van.

Bizonyítás: Legyen $p > 2$ *és* $n = \frac{b^{2p}-1}{b^2-1}$ *és* $b \not\equiv \pm 1 \pmod{p}$. Ekkor *n* álprím *b* alapra nézve. Ugyanis:

$$n = \frac{b^p - 1}{b-1} \cdot \frac{b^p + 1}{b+1} = (b^{p-1} + b^{p-2} + \cdots + b + 1)(b^{p-1} - b^{p-2} \pm \cdots - b + 1)$$

Így *n* páratlan és összetett. A $b^{2p} \equiv 1 \pmod{n}$, hiszen $n = \frac{b^{2p}-1}{b^2-1} \mid b^{2p} - 1$, de a kis Fermat-tétel szerint:

$$b^{2p} \equiv b^2(b^{p-1})^2 \equiv b^2 \pmod{p}$$

Mivel $n(b^2 - 1) = b^{2p} - 1$, ezért $n(b^2 - 1) \equiv b^{2p} - 1 \pmod{p}$, így

$n(b^2 - 1) \equiv b^2 - 1 \pmod{p}$, mivel a feltételek szerint $lnko(b^2 - 1, p) = 1$, hiszen $b \pm 1$ nem osztható *p*-vel. A kongruenciát egyszerűsítve kapjuk:

$n \equiv 1 \pmod{p}$, de *n* páratlan, ezért $n \equiv 1 \pmod{2p}$ is igaz, azaz $2p \mid n - 1$.

Így $n \mid b^{2p} - 1 \mid b^{n-1} - 1, azaz\ b^{n-1} \equiv 1 \pmod{n}$ is teljesül, vagyis *n* álprím *b* alapra nézve. Ha $p > b + 1$, akkor $b \not\equiv \pm 1 \pmod{p}$ magától érthetően, így végtelen sok *p* prím található a tételhez, azaz végtelen sok álprím van minden *b* alapra. Tehát igaz az állítás.

Tétel: Ha $lnko(b_1, n) = lnko(b_2, n) = 1$ és *n* álprím b_1, b_2 alapokra, akkor *n* álprím $b_1 b_2$ és $b_1 b_2^{-1}$ alapokra is.

Bizonyítás: A $b_1^{n-1} \equiv 1 \pmod{n}$ *és* $b_2^{n-1} \equiv 1 \pmod{n}$ a feltételek miatt, de akkor

$(b_1 b_2)^{n-1} \equiv b_1^{n-1} b_2^{n-1} \equiv 1 \pmod{n}$, vagyis a $b_1 b_2$ alapra nézve is álprím. Továbbá

$(b_1 b_2^{-1})^{n-1} \equiv b_1^{n-1}(b_2^{n-1})^{-1} \equiv 1 \pmod{n}$, vagyis a $b_1 b_2^{-1}$ alapra nézve álprím.

Tétel: Legyen $lnko(b, n) = 1$. Ha *n* csak egyetlen *b*-re is bukja a $b^{n-1} \equiv 1 \pmod{n}$ Fermat-tesztet, akkor a $(mod\ n)$ maradékosztályok legalább felét bukja.

Bizonyítás: Az előző tétel miatt *b* alapok, melyekre $b^{n-1} \equiv 1 \pmod{n}$ teljesül $\boldsymbol{Z}_n$ multiplikatív csoportjában egy részcsoport, így, ha ez nem egyenlő $\boldsymbol{Z}_n^*$ csoporttal (vagyis létezik *b*, melyre $lnko(b, n) = 1$ *és* $b^{n-1} \not\equiv 1 \pmod{n}$), akkor mivel részcsoport, így rendje legfeljebb $\frac{|\boldsymbol{Z}_n^*|}{2}$. Ez azt jelenti, hogy a redukált maradékosztályok legalább felét bukja a teszt. Tehát igaz az állítás.

Megjegyzés:

1. Ha az *n* páratlan összetett szám nem minden relatív prím *b* alapra nézve Fermat-féle álprím, akkor a redukált maradékosztályok legalább felére nem álprím, így

$b^{n-1} \equiv 1 \pmod{n}$ ellenőrzése jó valószínűségi prímtesztelést ad. Először *n*-et teszteljük egy véletlen $1 < b < n$ alapra, ha $lnko(b,n) > 1$, akkor *n* összetett. Ha nem, akkor

$b^{n-1} \equiv 1 \pmod{n}$-et kiszámítjuk $O(log^3 n)$ bitoperációval ismételt hatványozással.

Ha a maradék nem kongruens 1-gyel modulo *n*, akkor *n* megint nem prím, egyébként egy másik $1 < b' < n$-re teszteljük. Ha a két teszt független, akkor legfeljebb $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ valószínűséggel éli túl a két tesztet. A *K* darab *b*-vel tesztelve legfeljebb $\frac{1}{2^K}$ valószínűséggel éli túl.

2. A Legendre szimbólum tulajdonsága, hogy *p* páratlan prím és $lnko(b,n) = 1$ esetén $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$ teljesül.

2. Carmichael számok (Univerzális álprím)

Az *n* összetett számot Carmichael számnak nevezzük, ha minden *n*-hez relatív prím alapra Fermat-féle álprím, azaz $lnko(a,n) = 1 \; esetén \; a^{n-1} \equiv 1 \pmod{n}$.

Tétel: (Korselt-kritérium)

Az *n* összetett szám akkor és csak akkor Carmichael szám, ha *n* négyzetmentes és minden *p* prímosztójára $p - 1 \mid n - 1$ teljesül.

Megjegyzések:

1. A tételből következik, hogy minden Carmichael szám páratlan, hiszen bármely négyzetmentes páros összetett számnak (melynek tehát csak egyszeres prímtényezője a 2) van legalább egy páratlan prímtényezője, ezért a $p - 1 \mid n - 1$ kifejezés szerint páros oszt páratlant, ami ellentmondás.

2. A kritériumból következik az is, hogy a Carmichael számok ciklikusak.

3. Az eddigiekből az is következik, hogy egyik Carmichael számnak sincsen pontosan két prímtényezője (nem félprímek).

Tétel: (Alford, Granville, Pomerance 1994.)

Végtelen sok Carmichael szám van. Ha *n* elég nagy, akkor legalább $n^{\frac{2}{7}}$ Carmichael szám van *n*-ig.

Megjegyzések:

1. Korselt volt az első, aki megállapította a Carmichael-számok alapvető tulajdonságait, de anélkül, hogy egyetlen példa is ismert lett volna előtte.

2. 1910-ben Carmichael találta meg az első, egyben legkisebb ilyen számot, az 561-et, innen a „Carmichael-szám” elnevezés.

3. Az, hogy az 561 Carmichael-szám, jól látható a Korselt-féle kritérium alapján:

Igaz, hogy az $561 = 3 \cdot 11 \cdot 17$ négyzetmentes, továbbá $2 \mid 560$ *és* $10 \mid 560$ *és* $16 \mid 560$.

4. Valójában az első hét Carmichael-számot a cseh matematikus, Václav Šimerka találta meg 1885-ben (ezzel Carmichael mellett Korseltet is megelőzve). Ezek: 561, 1105, 1729, 2465, 2821, 6601, 8911.

5. J. Chernick 1939-ben igazolt egy tételt, aminek segítségével a Carmichael számok egy részhalmaza előállítható A $(6k+1)(12k+1)(18k+1)$ alakú számok Carmichael számok abban az esetben, ha a szorzat mindhárom tényezője prímszám. Nyitott kérdés, hogy ez a képlet végtelen sok Carmichael számot előállít-e.

6. Gérard P. Michon hasonló módszert alkotott Carmichael számok létrehozására:

Legyen *m* 3-mal osztható és $m \equiv 326 \pmod{616}$. Ha a $(7m+1)(8m+1)(11m+1)$ szorzat minden tényezője prím, akkor ez Carmichael szám.

7. Michon módszerével egy 1000 jegyű Carmichael szám előállítása:

$$(12936 \cdot 10^{329} - 59827428149) \cdot (14784 \cdot 10^{329} - 68374203599) \cdot (20328 \cdot 10^{329} - 94014529949)$$

8. Löh és Niebuhr 1992-ben néhány igen nagyméretű Carmichael számot állítottak elő, köztük egy több mint 16 millió jegyűt, 1 101 518 prímtényezővel.

9. Erdős Pál csoportelméleti megfontolásai és modern számítógépes algoritmusok segítségével 2012 júliusában előállítottak egy több mint 10 milliárd prímtényezővel rendelkező és több mint 300 milliárd jegyű Carmichael számot.

3. Euler-féle álprímek

Legyen *n* páratlan összetett szám. Ha $lnko(b,n) = 1$ *és* $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$, *(ahol* $\left(\frac{b}{n}\right)$ Jacobi szimbólum) teljesül, akkor *n*-et Euler-féle álprímnek nevezzük *b* alapra nézve.

Tétel: Ha *n* Euler-féle álprím *b* alapra nézve, akkor ugyanerre az alapra nézve Fermat-féle álprím is. Visszafelé nem feltétlenül igaz.

Bizonyítás: A feltétel szerint $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$, de $\left(\frac{b}{n}\right) \equiv \pm 1 \pmod{n}$. Így az előbbi kongruenciát négyzetre emelve: $b^{n-1} \equiv 1 \pmod{n}$, vagyis *b*-re nézve Fermat-féle álprím. Tehát igaz az állítás. A fordított irányhoz ellenpélda: $b = 3, n = 91$.

Tétel: Minden *a* alapra végtelen sok Euler-féle álprím van.

4. Catalan álprímek

Az *n* páratlan összetett természetes szám akkor **Catalan-álprím,** ha *n* teljesíti a következő kongruenciát:

$$(-1)^{\frac{n-1}{2}} \cdot C_{\frac{n-1}{2}} \equiv 2 \pmod{n}$$

A C_m az *m*-edik Catalan számot jelöli. A kongruencia igaz minden páratlan prímszámra is.

Eddig mindössze három Catalan-álprím ismeretes: 5907, 1194649 és 12327121, melyek közül a két utóbbi szám Wieferich-prím négyzete. Általában is igaz, hogy ha *p* Wieferich-prím, akkor p^2 Catalan-féle álprím.

5. Erős álprímek

Legyen *n* természetes páratlan összetett szám. Ha

$n - 1 = 2^s \cdot m, ahol\ s > 0$ *és* $m\ páratlan, lnko(b,n) = 1$ *és* $b^m \equiv 1 \pmod{n}$, vagy létezik $r: 0 \leq r < s, hogy\ b^{2^r m} \equiv -1 \pmod{n}$, akkor *n*-et erős álprímnek nevezzük *b* alapra nézve.

Tétel: (A.O.L. Atkin és R. Larson) Ha *n* erős álprím adott *a* alapra, akkor Euler-féle álprím is az *a* alapra.

Tétel: (Malm) Ha *n* $(4k+3)$ alakú Euler-féle álprím adott *a* alapra, akkor erős álprím is az adott *a* alapra. Vagyis a $(4k+3)$ alakú számok körében a két fogalom megegyezik.

Bizonyítás: Legyen az *n* egy $(4k+3)$ alakú egész szám. Ezért $n-1=2d$, ahol *d* páratlan. A feltétel szerint Euler-féle álprím, ezért $a^{\frac{n-1}{2}} \equiv a^d \equiv \left(\frac{a}{n}\right) \pmod{n}$. A Jacobi szimbólum a ± 1, így az *n* erős álprím is az adott *a* alapra. Tehát igaz az állítás.

Tétel: Ha *n* páratlan összetett szám és $n \neq 9$, akkor *n* erős álprím a redukált maradékosztályok legfeljebb $\frac{1}{4}$-ére. Legyen $n = 2^s \cdot q + 1, ahol\ s \geq 1$. Ekkor:

$$|R_n| = |\{1 \leq a \leq n\} \mid lnko(a,n) = 1 \text{ és } a^q \equiv 1 \pmod{n}\ vagy$$

$$a^{2^j q} \equiv -1 \pmod{n}, ahol\ 0 \leq j \leq s-1 | \leq \frac{1}{4}\varphi(n)$$

Következmény:

Ha *n* páratlan egész szám és *k* darab véletlen $0 < b_1 < b_2 < \cdots < b_k < n, lnko(b,n) = 1$ számmal teszteljük *n*-et a Miller-Rabin teszttel, akkor legfeljebb $\frac{1}{4^k}$ valószínűséggel éli túl a tesztet.

Prímfaktorizáció

A prímfaktorizáció során egy adott összetett szám prímtényezőinek a meghatározását kell elvégezni. A próbaosztásos módszer nagy összetett számok esetén a gyakorlatban nem működik. A nehézséget az jelenti, hogy olyan sok próbálkozást kellene számítógéppel végrehajtani, amihez évmilliárdok sem elegendők! A próbaosztásos módszerek továbbfejlesztett változatai is nagyon „lassúak”. Például egy 500 jegyű összetett számot, amelynek nincsenek kis prímosztói, illetve nincs valamilyen speciális tulajdonsága, a napjaink leggyorsabb számítógépei sem képesek belátható időn belül tényezőkre bontani. Turing gépen nem ismert polinom idejű algoritmus erre a feladatra. Jelenleg csupán Dixon algoritmusa bizonyítottan szubexponenciális futásidejű.

A prímfaktorizáció története

A prímfaktorizáció problémájának megszületése i.e. 300 környékére tehető, ekkor született ugyanis a görög Euklidész. Bár munkássága főként a geometria révén ismert, ő definiálta először a prímszámokat és kimondott a számelmélet alaptételével ekvivalens állításokat is. A számelmélet alaptétele kimondja, hogy minden egész szám felírható prímszámok szorzataként, lényegében egyértelműen. A prímfaktorizáció feladata ennek a felírásnak a megkeresése. Mivel a prímfaktorizációnak az 1970-es évekig nem volt nagy gazdasági és elméleti jelentősége, ezért a kor matematikusai kevés figyelmet fordítottak a kérdésre. Egészen Fermatig nem is született a próbaosztásnál gyorsabb algoritmus a feladat megoldására, az ő gondolatai viszont visszaköszönnek még a mai modern algoritmusokban is, így tőle érdemes számítani a probléma történelmét.

Fermat algoritmusának alapja, hogy minden páratlan *N* szám felírható két négyzetszám különbségeként, mivel ha $N = ab$, akkor $N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$. Ekkor a jól ismert azonosság miatt $N = x^2 - y^2 = (x + y)(x - y)$, azaz ha valamilyen módon találunk olyan *x*,*y* párt amire $N = x^2 - y^2$, akkor osztót is találtunk. Fermat módszere különböző *x*-ekre ellenőrzi, hogy $x^2 - N$ négyzetszám-e, mert ha igen, akkor meg is találtuk a keresett $x, y = \sqrt{x^2 - N}$ párt. Ez az algoritmus nagyon gyors, ha a keresett osztók közel vannak egymáshoz, egyébként viszont a próbaosztásnál is lassabb. Az algoritmus ötletén alapszik a kvadratikus szita és a GNFS algoritmus is, melyeket később tárgyalunk.

Euler nevéhez fűződik a relatív prímeket számláló Euler-függvény, illetve kidolgozott egy speciális alakú számokat faktorizáló algoritmust is. Fermat módszeréhez hasonlóan ő is négyzetszámokkal dolgozik, de az algoritmusában a faktorizálandó egészet négyzetszámok összegeként kell felírni, kétféleképpen. (Nem minden egész írható fel így, ebből adódik a speciális alak.)

Ezt követően Legendre munkássága lendítette előre a faktorizáció problémáját. Kétszáz évvel később a Legendre-szimbólum használata lesz a kvadratikus szita alapja, a kongruens négyzetek ötletére pedig több algoritmus is születik (a modern algoritmusok nagy része ezt használja).

1801-ben Gauss kiadta élete fő művét, a *Disquisitiones Arithmeticae*-t, amely több módszert és ötletet is tartalmaz az egészek prímfelbontásáról. Gauss munkája és főleg az eliminációs eljárása nélkül a későbbiekben tárgyalt algoritmusok nem működhetnének.

Az 1800-as évek végén többen mechanikus, illetve elektromos gépekkel igyekeztek kiváltani a hosszadalmas kézi számolásokat. 1896-ban Lawrence mutatta be terveit egy szitáló gépről, mely egy mozgó papírt lyukasztott ki azokon a pontokon, ahol az algoritmus megengedett maradékhoz ért. Lawrence gépe végül soha nem épült meg, de ötlete hasonló elvekkel működő gépek születését vonta maga után.

1910-ben Maurice Kraitchik, G'erardin és a Carissan testvérek is építettek ilyen gépeket. Közülük a Carissan testvérek munkája érte el a legjobb eredményt gyorsaságban, de az ő gépüket is kézzel kellett még hajtani.

Az első automatikus szitáló gépet D. H. Lehmer építette 1926-ban, majd - követve a technika fejlődését - újabbakat készített. Az első még egy bicikli láncot hajtó villanymotorból állt, később napelemeket (1932), 16 mm-es mozi filmet (1936), végül analóg késleltetőket (1965) használt gépeihez.

Az 1940-as évek közepén a számítógépek fejlődése elérte azt a pontot, hogy legyőzhették a mechanikus gépek gyorsaságát, bár ekkor még nem léteztek jó implementációk a meglévő algoritmusokra.

1970-ben Daniel Shank változtatott ezen, algoritmusa (SQUFOF) megtette az első lépést a számítógépek győzelme felé. Ezután évekig az ő módszerét használták jó eredményekkel.

1974-ben Pollard a $(p-1)$, 1975-ben pedig a ρ-módszer bemutatásával szerzett hírnevet, algoritmusai speciális célúak, azaz nem alkalmazhatóak minden számra. Az első általánosan alkalmazható eljárást Morrison és Brillhart mutatta be szintén 1975-ben. Az algoritmusuk (CFRAC) néhány évig a leggyorsabbnak számított.

1983-ben C. Pomerance QR-algoritmusával sikeresen faktorizált 70-jegyű számokat, a CFRAC osztásait elkerülő (általános célú) algoritmus ezzel átvette a leggyorsabbnak járó helyet. (Valójában a szitáló gépek nagyon gyorsnak számítanak még ma is, Williams egy faktorizáló gépe $2 \cdot 10^{12}$ próbát végzett másodpercenként, ami egy átlagos számítógépnél kb. 1 milliószor gyorsabb számolást jelent!

Az áttörést valójában a programok párhuzamosíthatósága és a bonyolultabb algoritmusok jelentették, amiket már igen nehéz volna mechanikus gépeken "futtatni".

1987-ben Lenstra keze által megszületett a máig leggyorsabb speciális célú algoritmus (ECM), melynek érdekessége, hogy módszere teljesen eltér az addig alkalmazottaktól.

1988-ban Pollard körlevélben tájékoztatta kutató társait új ötletéről (SNFS), az ebből születő algoritmus fejlesztett változata (GNFS) az általános célú algoritmusok között a leggyorsabbá vált. Az elmúlt 30 évben az GNFS sebessége különböző matematikai ill. implementációs trükkökkel nőtt, de más nagy eredmény nem született a témában.

1994-ben Peter Shore bemutatta az első kvantumszámítógépekre írt algoritmusát, mellyel polinom időben faktorizálható bármely összetett szám. Az algoritmus erősen épít kvantum-jelenségekre, így amíg várnunk kell a kvantumszámítógépek igazi megszületésére és elterjedésére, addig ez az algoritmus főként elméleti jelentőséggel bír.

Faktorizációs algoritmusok

A faktorizációs algoritmusok két csoportra oszthatók, a speciális és az általános célú algoritmusok csoportjára. A speciális célú algoritmusok az egész számok egy halmazára alkalmazhatók sikeresen (ilyen például azon számok halmaza, melyeknek csak kis osztóik vannak vagy az osztók szomszédjai ilyenek). A speciális célú algoritmusok ezeken a számokon gyorsak, de a halmazon kívül vagy lassúak, vagy teljesen kudarcot vallanak. Az általános célú algoritmusok bármely egész számra alkalmazhatóak, de ugyanannyi idő alatt faktorizálják a sima egészeket, mint például az RSA modulusokat. Így egy véletlenszerűen választott számra csak akkor érdemes alkalmazni őket, ha a speciális célú algoritmusokkal már kudarcot vallottunk. Minden a - következőkben - tárgyalt algoritmus felteszi, hogy a faktorizálandó szám összetett, így minden esetben tesztelnünk kell először annak prím voltát. Ezt hatékonyan megtehetjük valamelyik valószínűségi prímteszttel vagy ha biztosra akarunk menni használhatjuk a polinom idejű AKS-algoritmust is.

1. Speciális célú algoritmusok

A speciális célú algoritmusok a nehezen faktorizálható számokon általában elbuknak, de egy véletlenszerűen választott számnak nagy valószínűséggel vannak kis osztói, ezeket pedig a leggyorsabban a speciális célú algoritmusokkal találhatjuk meg.

Legtöbbször nem tudjuk, hogy a faktorizálandó szám melyik algoritmus speciális halmazába tartozik, ezért azt sem, hogy melyiket érdemes használnunk. A gyakorlatban, ha kis számot kell faktorizálnunk, akkor a próbaosztással és a ρ módszerrel próbálkozzunk. Egyéb esetekben az ECM algoritmussal választhatjuk le a kis osztókat, s ha még így sem jártunk teljes sikerrel, akkor érdemes áttérni az általános célú algoritmusokra és bevetni a QR algoritmust vagy a GNFS-t. A legegyszerűbb speciális célú algoritmus a próbaosztás.

1. Próbaosztás (trial division)

A próbaosztás a leglassabb, viszont a legkönnyebben megérthető algoritmus, mellyel találkozhatunk a témában. Alapgondolata, hogy ha *n* a faktorizálandó egész, akkor teszteljünk le minden 1-nél nagyobb, de *n*-nél kisebb egész számot, hogy osztója-e *n*-nek. Ha osztót találtunk írjuk le, majd folytassuk a tesztelést az *n/{a talált osztó}* számmal. Nyilván *n* minden osztója beleesik az 1, . . . , *n* intervallumba, így előbb vagy utóbb megtaláljuk a teljes felbontást. Érdemes meggondolni, hogy az egészek 80%-ának van 100-nál kisebb osztója, 92%-ának pedig 1000-nél kisebb. Így bár ez az algoritmus egy olyan számot, aminek csak nagy osztói vannak nagyon lassan faktorizál, de egy "átlagos" számnak gyorsan talál osztót.

Mivel a prímeken kívül minden *n* egésznek van osztója a $\{2,3,4,\cdots,\lfloor\sqrt{n}\rfloor\}$ halmazban, így valójában a tesztelést nem szükséges folytatnunk $\lfloor\sqrt{n}\rfloor$ után. Könnyen látható az is, hogy a próbaosztás (az osztások sorrendje miatt) minden esetben prím osztókat talál. Kihasználhatjuk ezt úgy, hogy a tesztelés során minden összetett számot kihagyunk. A $\{2,3,4,\cdots,k\}$ halmazban nagyjából $\frac{k}{\log k}$ prím található a prímszámtétel szerint, így jelentősen csökken a tesztelések száma ezzel a módszerrel.

Az összetett számok kihagyása felveti a kérdést, hogy hogyan menjünk végig a prímeken. Ősi módszer Eratoszthenész szitája, mellyel kiszitálhatjuk *n*-ig az összetett számokat *O(n(log n)(log(log(n))))* bitművelettel. Ekkor tárolhatjuk egy listában a megmaradt prímeket, így elkerülve, hogy minden használatkor elő kelljen állítani azokat. A lista tárolása viszont tárhelyigényes, ami nem mindig áll rendelkezésre, például számológépek esetén sem. Prímlista helyett generálhatunk olyan pszeudo-prím sorozatot, ami lefedi a prímek halmazát. Ilyen például a következő:

$$2, 3, 6k \pm 1 \;\; ahol\; k > 0\; egész\; szám$$

Könnyen igazolható, hogy a sorozat tényleg jó, hiszen ha $l \in \{0, 2, 3, 4\}$, akkor minden $6k+l$ alakú szám *2* vagy *3* többszöröse. Természetesen kapunk néhány összetett számot is a sorozatban, de az a kevés osztás amit ezekre kell fordítanunk, nem nagy ár a lista elkerüléséért.

Több módot is választhatunk a sorozat előállítására. Például ha *5*-tel kezdünk, majd felváltva *2*-t és *4*-et adunk az aktuális számhoz, akkor megkapjuk a sorozatot és ráadásul elkerüljük a szorzásokat is. Ezt a megoldást vázoljuk a következőkben:

1. Ha $n \equiv 0 \pmod 2$, legyen $p = 2$ és álljunk le, az eredmény p.

2. Ha $n \equiv 0 \pmod 3$, legyen $p = 3$ és álljunk le, az eredmény p.

3. Legyen $p = 3$ Legyen $b = 2$.

4. Amíg $p < \sqrt{n}$, legyen $p = p + b$.

Ha $n \equiv 0 \pmod p$, álljunk le, az eredmény p.

Legyen $b = 6 - b$. A próbaosztás idő komplexitása $O(\sqrt{n})$.

Látni fogunk ennél sokkal gyorsabb algoritmusokat is a következőkben, de ezért bonyolultsággal fogunk fizetni.

2. A ρ módszer (The rho method, Pollard's rho)

1975-ben Pollard bemutatta az új Monte Carlo módszerét, aminek egy változatával 5 évvel később sikeresen faktorizálták a 8. Fermat-számot. A ρ módszer alapja, hogy ha elő tudunk állítani olyan a_1, a_2 egészeket melyekre $a_1 \equiv a_2 \pmod{p}$, ahol *p* az *n* egy nemtriviális osztója, akkor a különbségüket véve *p* egy többszörösét kapjuk, amiből *lnko* művelettel jó eséllyel kinyerhető *p,* (ha éppen n többszörösét kapjuk, akkor nem tudjuk kinyerni).

Mivel éppen *p*-t keressük, ezért nem tudjuk eldönteni az a_1, a_2 egészekről hogy kongruensek-e, viszont kiszámolhatjuk rögtön $lnko(n, a_2 - a_1)$-et és ha szerencsések vagyunk, akkor egy osztót kapunk.

A gyakorlatban a_1, a_2 helyett egy $a_1, a_2, \cdots, a_k$ sorozatot használunk, melyet rekurzívan, egy *f* egész együtthatós polinommal állítunk elő:

$$a_{m+1} = f(a_m) \pmod{n}$$

Ez a sorozat nyilván ciklikus és $(mod\ p)$ sokkal hamarabb válik azzá, mint $(mod\ n)$. Ha ennek a ciklusnak a hossza *t*, akkor $a_m \equiv a_{m+t} \pmod{p}$, de nagy valószínűséggel $a_m \not\equiv a_{m+t} \pmod{n}$ és így kinyerhetjük a keresett osztót a fent leírt módon. Általában $f(a) = a^2 + c$ alakú polinomokat használunk, valamely $c \geq 1$ egésszel és $a_0 = 1$ kezdőértékkel. Pollard algoritmusa Floyd módszerét használja a ciklus megkeresésére:

1. Legyen $a = b = 2, c = 1$.

2. Legyen $f_c(x) = x^2 + c \pmod{n}$.

3. Legyen $a = f_c(a), b = f_c(f_c(b))$.

4. Legyen $d = lnko(a - b, n)$.

5. Ha $1 < d < n$, az eredmény $p = d$.

6. Ha $d = 1$, akkor menjünk 3-ra.

7. Ha $d = n$, akkor legyen $c = c + 1$ és menjünk 2-re.

Az említett 8. Fermat szám faktorizációját Richard P. Brent találta meg 1980- ban. A faktorizáció 2 óráig tartott egy UNIVAC számítógépen. (A UNIVAC a UNIVersal Automatic Computer kifejezés rövidítése, ez volt 1951-ben az első kereskedelmi számítógép Amerikában, alkotói J. Presper Eckert és John Mauchly, az ENIAC feltalálói.)

Brent módosított algoritmusa körülbelül 25%-al gyorsabb, mint az eredeti Pollard féle, ezért általában az ő verzióját használják a gyakorlatban. A különbség csak a ciklus megkeresésében van, Brent a saját módszerét használta erre.

Pollard ρ algoritmusának idő komplexitására csak sejtésünk van: ha p a faktorizálandó n egy osztója és $p = O(\sqrt{n})$, akkor a várható futási idő:

$$O(\sqrt{p}) = O\left(n^{\frac{1}{4}}\right)$$

3. A p − 1 módszer (Pollard's p − 1 method)

Pollard másik faktorizációs módszere a *p−1* módszer, melyet szintén 1975-ben mutatott be. A módszer a Kis Fermat-tételt használva hatékonyan bontja prímtényezőkre azokat az egészeket, amelyeknek valamelyik *p* prímosztója esetén *p−1 B*-sima, ahol *B* viszonylag kicsi.

Az algoritmus ötlete, hogy ha *p − 1 B*-sima, akkor egy *n*-hez relatív prím *a*-ra $a^{B!} - 1$ osztható *p*-vel a Kis Fermat-tétel szerint, de reményeink szerint *n*-el nem, mert ekkor az osztó kinyerhető *lnko* számolással. A gyakorlatban *B!*-nál alacsonyabb kitevőt is használhatunk, mivel az algoritmus trükkje abban rejlik, hogy $a^c - 1$-nek rengeteg osztója van, ha *c* sima.

Az algoritmus:

1. Válasszuk ki a *B* simasági korlátot.

2. Válasszunk *a*-t.

3. Minden $q \leq B$ prímre:

- Legyen $s = \left[\frac{ln(n)}{ln(q)}\right]$.

- Legyen $a = a^{q^s} \pmod n$.

4. Legyen $p = lnko(a-1, n)$.

5. Ha $1 < p < n$, akkor az eredmény *p* egyébként válasszunk új *a*-t és menjünk 3-ra.

Pollard *p − 1* algoritmusának várható futásideje:

$$O\left(B\frac{ln(n)}{ln(B)}\right)$$

4. A p + 1 módszer (Williams's p + 1 method)

Hugh C. Williams 1982-ben mutatta be módszerét, amely Pollard *p − 1* módszerének egy variánsa Lucas sorozatokkal. A módszer alapja V_M kiszámolása különböző *M*-ekre, ugyanis ha a faktorizálandó *n* egy *p* prímfaktorára $\left(\frac{P^2-4Q}{P}\right) = -1$ és $p+1 \mid M$, akkor $V_M - 2$ osztható *p*-vel. Jó eséllyel $n \nmid V_M - 2$ és így *p* kinyerhető *lnko* számolással.

Természetesen nem tudjuk előre $\left(\frac{P^2-4Q}{P}\right)$ értékét, így érdemes több *P*-vel próbálkoznunk. Ha $\left(\frac{P^2-4Q}{P}\right) = 1$, akkor Williams *p + 1* módszere azonos Pollard *p − 1* módszerének egy lassabb változatával.

M-re gyakran az 1, 2!, 3!, 4!, . . . sorozatot használjuk, ekkor $Q = 1$ és $P \neq \pm 2$ esetén érdemes $V_{k!}$-t a $V_{(k-1)!}$-ból számolni a következő rekurzióval:

$$U_{mk} = U_k(P)U_m\big(V_k(P)\big)$$

$$V_{mk} = V_m\big(V_k(P)\big)$$

Pollard és Williams módszereit Eric Bach és Jeffrey Shallit általánosította körosztási polinomokra. Módszerükkel hatékonyan faktorizálható *n*, ha $\varphi_k(p)$ sima. Sajnos $k = 2$ fölött egyre kisebb az esély rá, hogy $\varphi_k(p)$ sima legyen, így ezek a módszerek a gyakorlatban nem olyan hatékonyak.

5. Faktorizálás elliptikus görbékkel (Elliptic Curve Method,ECM)

Három évvel a *p + 1* módszer bemutatása után, 1985-ben Lenstra az elliptikus görbék használatát javasolta faktoriálishoz, ötletét Brent csiszolta tovább. Ezzel megszületett a leggyorsabb speciális célú algoritmus. Az ECM alapjaiban hasonlít Pollard *p − 1* módszeréhez, a különbség az algebrai struktúra amiben dolgoznak. Pollard a *Z/nZ* multiplikatív csoportot használja, Lenstra pedig az elliptikus görbékkel definiált csoportját (szintén *mod n*).

Az algoritmus:

1. Válasszunk véletlenszerűen egy elliptikus görbét Z/nZ felett. Ezt megtehetjük úgy, hogy véletlenszerűen választunk egy $P = (x, y) \neq (0,0)$ számpárt *x, y (mod n)* értékekkel, valamint egy szintén véletlenszerű *a*-t, majd az $y^2 = x^3 + ax + b \ \ (mod\ n)$ egyenletet átrendezve meghatározzuk *b*-t.

2. Válasszunk egy *B* simasági korlátot. Legyen *e* a *B*-nél kisebb prímek szorzata.

3. Számoljuk ki a görbén *eP (mod n)*-et. A szorzást számoljuk ismételt összeadással. Ha a formulában szereplő hányados (a meredekség) *u/v és lnko(u, n) = 1*, akkor *v = 0 (mod n)* esetén a görbén definiált ∞ elemet kaptuk. Ha *lnko(v, n)* nem 1 vagy *n*, akkor az összeadás egy a görbén nem értelmezett pontot ad, ez mutatja, hogy az elliptikus görbénk nem csoport *mod n*. (De fontosabb, hogy *lnko(v, n)* nemtriviális osztó!)

4.

- Ha ki tudtuk számolni *eP*-t, vagyis nem ütköztünk nem invertálható elembe, akkor kezdjük elölről az algoritmust új görbével és kezdőértékkel.

- Ha a számítás során *kP* = ∞-be ütközünk, akkor kezdjük elölről az algoritmust új görbével és kezdőértékkel.

(Hiszen ezen a ponton nem tudnánk túljutni, mivel ∞ + . . . + ∞ = ∞)

- Ha a számítás során valahol *lnko(v, n)* nem 1 vagy *n*, akkor megtaláltunk egy nemtriviális osztót.

Az algoritmus működése azon alapszik, hogy ha *p* és *q* két különböző prímosztója

n-nek és $y^2 = x^3 + ax + b \pmod n$ fennáll, akkor az egyenlet igaz *mod p* és *mod q* is. Ezek a görbék már biztosan csoportot alkotnak, és Lagrange tétele szerint, ha az eredeti görbén egy *P* pontra *kP* = ∞ *(mod p)*, akkor *k* osztója a csoport rendjének. Ez természetesen *q*-ra is igaz, és ha az elliptikus görbét véletlenszerűen választottuk, akkor a két csoport rendje *p + 1*-hez, illetve *q + 1*-hez esik közel.

Mivel annak az esélye nagyon kicsi, hogy a két csoport rendjének faktorai megegyeznek, ezért amikor az algoritmus során *kP* = ∞ *(mod p)*, akkor valószínűleg *mod q* ez nem igaz. Ekkor *kP* nincs rajta az eredeti görbén és a számolás során talált *v*-re, *lnko(v, p) = p* vagy *lnko(v, q) = q*, de nem egyszerre. Így *lnko(v, n)* egy nemtriviális osztót ad.

Ha *p* az *n* legkisebb prímosztója, akkor az ECM algoritmus várható futásideje:

$$O\left(e^{\left(\sqrt{2}+o(1)\right)\cdot ln(p)\cdot ln(ln(p))}\right)$$

2. Általános célú algoritmusok

Az általános célú algoritmusok bármely összetett szám ellen bevethetők, egyetlen hátrányuk a speciális célú algoritmusokkal szemben, hogy ugyanannyi idő alatt faktorizálják a feladat szempontjából egyszerű számokat, mint a legnehezebbeket.

Ez azért okoz gondot, mert ezen algoritmusok számítógépes implementációi általában nagy memória és számításigénnyel rendelkeznek. Így előfordulhat, hogy sokkal tovább tart a könnyen felbontható számokat faktorizálni általános célú algoritmussal. Érdemes úgy gondolnunk rájuk, mint az utolsó alkalmazandó módszerekre, hacsak nem tudjuk előre, hogy mással nem érhetünk el eredményt. Minden itt tárgyalt algoritmusról elmondható, hogy Legendre kongruens négyzetekről szóló ötletén alapul.

Definíció (Legendre kongruenciája):

Legyen $x, y\ egész, 0 \leq x < y \leq n, x + y \neq n$. Ekkor Legendre kongruenciájának a következő egyenletet nevezzük:

$$x^2 \equiv y^2 \pmod{n}$$

Tegyük fel, hogy valamilyen módon találtunk egy *x, y* párt, mely kielégíti Legendre kongruenciáját. Ekkor jó eséllyel *lnko(n, x + y) vagy lnko(n, x − y)* egy nem triviális osztója *n*-nek, mivel:

$$x^2 \equiv y^2 \pmod{n} \leftrightarrow n \mid x^2 - y^2 \leftrightarrow n \mid (x+y)(x-y)$$

Könnyen igazolható (a lehetőségek felsorolásával), hogy 2/3 eséllyel kapunk nemtriviális osztót. A trükk az egészben a feltételek enyhítése. Fermat módszerénél olyan *x, y* párt kerestünk, melyre $x^2 - y^2 = n$, mert ekkor biztosan fel tudjuk bontani *n*-et. Sajnos ilyen *x, y* párból elég kevés van, gyakorlatilag az osztók számával arányos a mennyiségük.

Legendre módszerénél pedig *n* egy többszörösét faktorizáljuk és reménykedünk, hogy a *lnko* művelettel jó helyen vágtuk el a számot. Természetesen az algoritmusok jól kezelik a 2/3-os valószínűséget, minden módszer törekszik arra, hogy ha egyszer eljutunk idáig, akkor sikertelenség esetén kevés plusz számolással újra próbálkozhassunk.

1. Faktorizálás lánctörtekkel (Continued Fraction Method, CFRAC)

1931-ben D. H. Lehmer és R. E. Powers mutatták be az első modern lánctörtekkel faktorizáló algoritmust. A módszert Michael A. Morrison és John Brillhart fejlesztették tovább számítógépekre 1975-ben. Az algoritmusban ötvöződik a gyökök lánctörtekkel való jó közelítésének ereje Legendre módszerével, ezzel hosszú időre (a QR megjelenéséig) ez volt a leggyorsabb faktorizáló algoritmus nagy számokra.

Az algoritmus $\sqrt{n}$ közelítéseiből állít elő olyan y_i-ket, amikre $x_i^2 \equiv y_i \pmod{n}$, ahol x_i a $\sqrt{n}$ egy közelítése. Ha $\sqrt{n}$-et lánctörtekkel közelítjük, akkor mivel $\frac{P_i^2}{Q_i^2} \approx n$, ezért

$P_i^2 - Q_i^2 \approx 0$. Az itt fellépő eltérést jelöljük y_i-vel, s mivel ez láthatóan kicsi, így nagy valószínűséggel felbontható kis prímszámok szorzatára. Ha össze tudunk gyűjteni olyan

y_i-ket, melyeknek a kanonikus alakjában lévő prímek azonosak, akkor egy részük szorzatából előállíthatjuk a keresendő $y_{i1}y_{i2}\cdots y_{ik} = y^2$ négyzetszámot. Mivel a $x_i^2 \equiv y_i \pmod{n}$ kongruencia bal oldalán négyzetszámok vannak, így a szorzatuk is négyzetszám marad, vagyis megkapjuk a Legendre kongruencia egy megoldását:

$$x^2 = x_{i1}^2 x_{i2}^2 \cdots x_{ik}^2 \equiv y_{i1}y_{i2}\cdots y_{ik} = y^2$$

Az algoritmus vázlata:

1. Válasszunk egy *B* korlátot, majd az ennél kisebb prímek halmazát jelöljük *fb*-vel, ez lesz az un. faktorbázis.

2. Számítsuk ki $\sqrt{n}$ lánctört alakját, majd minden $\frac{P_i}{Q_i}$közelítésre számoljuk ki

$y_i = P_i^2 - Q_i^2 n$-et, és ha ez *fb*-sima, akkor tároljuk el a felbontását egy vektorban. A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevőket jelentsék a szám kanonikus alakjából.

Ismételjük addig ezt a lépést, amíg nem találunk |*fb*|-nél több *fb*-sima számot. Ha a lánctört hossza nem elég hosszú ehhez, akkor $\sqrt{n}$ helyett használjuk $\sqrt{kn}$-et valamilyen $k \in N$-el.

3. Az összegyűjtött vektorokból készítsünk mátrixot, melyre alkalmazzuk a Gauss eliminációt *(mod 2)*, így megkeresve a Legendre kongruencia megoldását.

4. Számítsuk ki *lnko(n, x ± y)*-t, ami *2/3* eséllyel nemtriviális osztó. Ellenkező esetben ugorjunk 2-re és cseréljünk le néhány vektort.

A CFRAC algoritmus várható futási ideje:

$$O\left(n^{\sqrt{1{,}5\cdot\frac{lnln(n)}{ln(n)}}}\right)$$

2. Kvadratikus szita (Quadratic Sieve, QS)

A kvadratikus szita Carl Pomerance által kifejlesztett módszer, melyet 1981-ben mutatott be. Több mint 10 évig - a GNFS megjelenéséig - ez volt a leggyorsabb faktorizáló algoritmus, sőt még ma is annak mondható a maximum 110 jegyű számok között. Az algoritmussal sikeresen faktorizáltak több RSA modulust is, a legjobb eredmények jelenleg a 130 jegyű számok környékén vannak.

A kvadratikus szita is Legendre kongruenciájára épít, vagyis kongruens négyzetszámokat kell keresnünk *(mod n)*, mert ekkor 2/3 eséllyel nemtriviális osztót is találunk egyben. Legyen:

$$Q(x) = \left(x + \left[\sqrt{n}\right]\right)^2 - n = \tilde{x}^2 - n, ahol\ x\ egész\ szám$$

Ekkor célunk találni olyan $\{x_1, x_2, \cdots, x_k\}$ halmazt, amire $Q(x_1)Q(x_2)\cdots Q(x_k)$ négyzetszám, jelöljük ezt y^2-tel. Mivel minden *x*-re $Q(x) \equiv \tilde{x}^2 \pmod n$, ezért:

$$y^2 = Q(x_1)Q(x_2)\cdots Q(x_k) \equiv (\tilde{x}_1\tilde{x}_2\cdots\tilde{x}_k)^2 \pmod n$$

Vagyis megvannak a keresett kongruens négyzetek.

Az, hogy a $Q(x_i)$-k szorzata négyzetszám, azt jelenti, hogy a szorzat kanonikus alakjában minden kitevő páros, ennek eldöntéséhez faktorizálnunk kell a $Q(x_i)$-ket. Ahhoz, hogy ez könnyű legyen, $Q(x_i)$-t minél kisebbnek kell választanunk, vagyis *x*-nek 0 közelinek kell lennie. Legyen tehát *M* egy általunk választott korlát, és $x \in [-M, M]$.

A $Q(x_i)$-kből akkor könnyű négyzetszámot összerakni, ha ugyanazoknak a prímeknek a különböző hatványai szerepelnek a kanonikus alakjukban. Ilyen számokat úgy érdemes keresni, hogy választunk egy $\{p_1, p_2, \cdots, p_B\}$ faktorbázist és megnézzük, hogy $Q(x)$ felbomlik-e a faktorbázison. Ha egy *p* prím osztója $Q(x)$-nek, akkor:

$$\left(x + \left[\sqrt{n}\right]\right)^2 \equiv n \pmod{p}$$

Vagyis *n* kvadratikus maradék *mod p*. Ez azt jelenti, hogy a faktorbázisban olyan *p* prímeknek kell lenniük, amire $\left(\frac{n}{p}\right) = 1$.

Mivel $Q(x)$ lehet negatív is, így a (-1)-et is be kell vennünk a faktorbázisba, ezen kívül még arra kell ügyelnünk, hogy se a faktorbázis mérete, se *M* ne legyen túl nagy. Az optimális futási idő eléréséhez a faktorbázis mérete legyen körülbelül:

$$B = \left(e^{\sqrt{ln(n)\cdot ln(ln(n))}}\right)^{\frac{\sqrt{2}}{4}}$$

Az intervallum korlátja pedig ennek köbe, azaz:

$$M = \left(e^{\sqrt{ln(n)\cdot ln(ln(n))}}\right)^{\frac{3\sqrt{2}}{4}}$$

Ha találunk *B* db olyan $Q(x_i)$-t amelyik teljesen felbomlik a faktorbázison, akkor a kitevőkből mátrixot készítve Gauss eliminációval $(mod\ 2)$ megtalálhatunk egy olyan $\{x_1, x_2, \cdots, x_k\}$ részhalmazt, amire $Q(x_1)Q(x_2)\cdots Q(x_k)$ négyzetszám. Tekintsük tehát a sikeresen faktorizált $Q(x_i)$-k kanonikus alakját, s a kitevőket tegyük be egy-egy vektorba. Az ilyen x_i és kitevő-vektor párokat relációnak hívjuk. A $Q(x_i)$-k összeszorzása ekkor ezen vektorok összeadására egyszerűsödik. Az pedig, hogy megtaláljuk azt a részhalmazt aminek a szorzata négyzetszám, az azt jelenti, hogy azt a részhalmazt keressük, ahol a vektorok összege éppen 0 $(mod\ 2)$, ez pedig egy egyenletrendszer megoldásával megtalálható. Véges test feletti Gauss eliminációra Wiedemann és Lánczos algoritmusa is rendelkezésre áll.

Az egyetlen megválaszolatlan kérdés az, hogy hogyan faktorizáljunk hatékonyan sok számot. Megtehetjük, hogy sorra vesszük a $Q(x_1), Q(x_2), \cdots$ sorozat elemeit, leellenőrizzük egyenként próbaosztással, hogy felbomlanak-e a faktorbázison. Ha igen, akkor megtartjuk őket, egyébként megyünk tovább amíg nem találunk *B* db olyat ami felbomlik. Ez persze túl lassú volna így. Helyette szerencsére megtehetjük, hogy az egész *[−M, M]* intervallumon egyszerre faktorizálunk.

A módszer azon alapul, hogy ha $x \equiv y \pmod p$, akkor $Q(x) \equiv Q(y) \pmod p$. Oldjuk meg a következő kongruenciát:

$$Q(x) = s^2 \equiv 0 \pmod p$$

Ezt megtehetjük a Shanks-Tonelli algoritmussal. Legyen a kapott két megoldás:

$$s_{p,1} \text{ és } s_{p,2} = -s_{p,1}$$

Ekkor $x_i = s_{p,1}, s_{p,2} + kp, (ahol\ k\ egész\ szám)$ esetén $Q(x_i)$ osztható lesz *p*-vel. Tegyük a $Q(x_i)$ értékeket egy vektorba, majd a faktorbázison végig haladva minden $s_{p,1}, s_{p,2} + kp$ -edik elemet osszuk el *p*-vel annyiszor, ahányszor tudjuk és tároljuk el, hogy hányszor sikerült $(mod\ 2)$. Ha ezt megcsináljuk a faktorbázis összes elemével, akkor a végén azon $Q(x_i)$-k helyén lesz 1, amik teljesen felbonhatóak a faktorbázison. Az ezekhez tartozó kitevő-vektorokat rakjuk egy mátrixba és oldjuk meg az így adódó egyenletrendszert. Mivel ekkor csak 2/3 eséllyel találunk nemtriviális osztót, ezért jó, ha *B*-nél több vektorunk van, mert ha elsőre nem járnánk sikerrel, akkor egy vektort lecserélve a mátrixban, újra próbálkozhatunk.

Az algoritmus vázlata:

1. Válasszunk egy *B* korlátot, majd készítsük el a *B* méretű faktorbázist olyan prímekből, melyekre $\left(\frac{n}{p}\right) = 1$.

2. Válasszunk *M*-et, majd számoljuk ki a $Q(x_i)$ értékeket minden *x* $\in$ *[−M, M]*-re. Szitálással faktorizáljunk legalább annyi $Q(x_i)$-t, mint amennyi *B*.

3. A kapott relációkra alkalmazzunk Gauss eliminációt $(mod\ 2)$, ezzel megoldva a Legendre kongruenciát.

4. A kapott *x, y* értékekkel számoljuk ki $p = lnko(n, x \pm y)$-t, ami 2/3 eséllyel nemtriviális osztó. Ha $p = 1$, menjünk az előző pontra és cseréljünk le a mátrixban egy vektort.

A QS algoritmus várható futási ideje:

$$O\left(e^{\sqrt{ln(n)\cdot ln(ln(n))}}\right)$$

3. GNFS (General Number Field Sieve, GNFS)

1988-ban John Pollard ötlete alapján elkészült a legmodernebb speciális célú algoritmus, a Special Number Field Sieve. A módszerrel azon $r^e \pm s$ alakú számok faktorizálhatók hatékonyan, ahol *r* és *s* kicsi. Az SNFS általánosításaként létrejövő algoritmus a GNFS, mely bármilyen alakú számra alkalmazható, de egy kicsivel lassabb az SNFS-nél. A GNFS a jelenlegi tudásunk szerint a leggyorsabb algoritmus a több mint 100 jegyű számok körében.

A GNFS megértéséhez érdemes látni a folyamatot, ahogy az algoritmus kifejlődött. A Legendre-kongruenciás módszerek Dixon algoritmusával kezdődtek, mely hasonló módon működik mint a kvadratikus szita, azzal a különbséggel, hogy a sima számokat nem szitálással, hanem véletlenszerűen választva próbálta összeszedni. A kvadratikus szita azzal javította ezt a módszert, hogy a sima számok keresését egy sokkal hatékonyabb algoritmussal helyettesítette. Mindkét algoritmus azon alapul, hogy két különböző gyűrűben, konkrétan

Z-ben és *Z/nZ*-ben keresünk négyzetszámokat és egy megfelelő leképezéssel a *Z*-beli négyzetszámot egy *Z/nZ*-beli négyzetszámba visszük. A két gyűrű közötti leképezést a

QS-ben a $\varphi(k) = k\ (mod\ n)$ függvény végzi, ami $k = x^2 - n$ esetén láthatóan megtartja a négyzetszám tulajdonságot *Z* és *Z/nZ* között.

A GNFS algoritmus két meggondolással javít ezen a módszeren. Az egyik, hogy a szitálásnál használt sima számokat előállító $x^2 - n$ polinomot lecserélhetjük magasabb fokúra is anélkül, hogy kevésbé sima számokat kapnánk. A másik pedig, hogy *Z* helyett használhatunk más gyűrűt is, ha a négyzetszámokat ugyanúgy le tudjuk képezni *Z/nZ*-beli négyzetszámokra.

Tegyük fel, hogy adott az *R* gyűrűnk és a $\varphi : R \rightarrow Z/nZ$ gyűrű-homomorfizmusunk. Ha találunk egy $\beta \in R$-et, melyre:

$$\varphi(\beta^2) = y^2 \pmod n \text{ és } x = \varphi(\beta) \pmod n$$

Akkor:

$$x^2 \equiv \varphi(\beta)^2 \equiv \varphi(\beta^2) = y^2 \pmod n$$

Ezzel megvan a Legendre-kongruencia egy megoldása. Látni fogjuk, hogy a kérdéses gyűrű és a hozzá tartozó homomorfizmus is viszonylag természetes módon konstruálható.

Polinom kiválasztása

Elsőként foglalkozzunk a megfelelő polinom kiválasztásával. Célunk olyan *f(x)* polinomot választani, mely sok sima számot állít elő, azaz hasznos. Két tulajdonsággal fogható meg hasznosság, az egyik, hogy *f(x)* értéke kicsi legyen, ezt a polinom méret tulajdonságának nevezzük. Minél kisebb a mérete egy polinomnak, annál jobb. A másik fontos tulajdonság, hogy a polinom által előállított számok lehetőleg minél több kis osztóval rendelkezzenek. Ezt úgy fogalmazhatjuk meg matematikailag jól, hogy az *f(x)* polinomnak sok gyöke legyen *mod p* kis *p*-re. Ezt a tulajdonságot *gyök* tulajdonságnak nevezzük.

A GNFS-ben olyan polinomokat használunk, melyek irreducibilisek *Z[x]*-ben és van egy gyökük *Z/nZ*-ben. Az *m* gyökkel rendelkező *f(x)* polinom megválasztása általában irreducibilis is egyben, mivel *f(m) = n* mellett, ha *f(x)* nem lenne irreducibilis, azaz például *f(x) = g(x)h(x)* igaz lenne, akkor *f(m) = g(m)h(m) = n* alakban meg is találnánk *n* egy osztóját.

A polinom megválasztásához használjuk az *n* egész *m*-alapú reprezentációját, ami ebben az alakban áll elő:

$$n = \sum_{i=0}^{d} a_i \cdot m^i \, , ahol \; 0 < a_i < m$$

Ekkor a *d* fokú, a_i együtthatós polinom automatikusan teljesíti is az elvárásainkat, így legyen tehát:

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \; és \; f(m) = 0 \;\; (mod\; n)$$

A polinom méret tulajdonságát úgy tudjuk csökkenteni, ha az a_i együtthatókat minél kisebbnek választjuk, különös tekintettel a_d és a_{d-1} nagyságára (*d*-t általában 3 és 6 közé választjuk, így ezek lesznek a dominánsok). Egy trükk, amivel ez elérhető amellett, hogy az *m* gyök megmaradjon, ha az együtthatókat így módosítjuk:

$$a_i = a_i - m \; és \; a_{i+1} = a_{i+1} + 1$$

A megfelelő hasznosság eléréséhez még az kell, hogy a polinom gyök tulajdonsága is megfelelő legyen. Nincs jó módszerünk arra, hogy könnyedén előállítsunk olyan polinomokat, melyeknek jó a gyök tulajdonsága is. A gyakorlatban általában sok lehetséges jelölt közül választjuk ki a legjobbat. Egy kis intervallumon szitálással megmérjük az összes jelölt gyök tulajdonságát és az így kapott legjobbat használjuk.

A hasznosság mérésére létezik egy heurisztika is, mellyel a legrosszabb polinomokat még a szitálás előtt eldobhatjuk. Ez a Murphy által kidolgozott *α(P)* függvény a következőképpen definiálható:

$$\alpha(P) = \sum_{p \le B} \left(1 - q_p \cdot \frac{p}{p+1}\right) \cdot \frac{\log p}{p-1}$$

A képletben a *B* egy simasági korlát, *p*-k prímek és q_p a *P* polinom gyökeinek száma *mod p*.

Így végül a polinom kiválasztása a következő módon történik:

1. Választunk *d*-t és m_0-t, melyre:

$$\left[n^{\frac{1}{d+1}}\right] \leq \frac{|a_d|}{m_0} \leq \left[n^{\frac{1}{d}}\right]$$

2. Válasszunk egy *(x, y)* intervallumot, amelyben a legjobb a_i együtthatókat keressük. Az intervallum olyan legyen, amire $0 < x < \frac{|a_d|}{m_0} < y < 0{,}5$ igaz.

3. Válasszunk egy intervallumot, melyben a legjobb *m*-et keressük. Válasszuk az intervallumot olyanra, hogy az a_{d-1} a lehető legkisebb legyen, vagyis

$$m \in \left\{m_0, \left[\left(\frac{n}{a_d}\right)^{\frac{1}{d}}\right]\right\}$$

4. Minden olyan a_d és *m* kombinációra, ahol a_d megfelelően sima, számoljuk ki az *m*-alapú reprezentációból $f_m(x)$-et, majd $\alpha\big(f_m(x)\big)$-et. Ha $\alpha\big(f_m(x)\big)$ kicsi, dobjuk el $f_m(x)$-et.

5. A megmaradó polinomokból szitálással válasszuk ki a legjobbat.

Kongruens négyzetek *Z[θ]*-ban

Legyen $f \in Z[x]$ polinom, melynek θ egy gyöke *C*-ben és *m* gyöke *Z/nZ*-ben, azaz $f(m) \equiv 0 \pmod n$. Ekkor használjuk a *Z[θ]* és *Z* gyűrűket és tekintsük a következő tételben szereplő homomorfizmust:

Tétel: Legyen $f \in Z[x]$ egy normált, irreducibilis polinom $\theta \in C$ gyökkel és legyen $m \in Z/nZ$ olyan, amelyre $f(m) \equiv 0 \pmod n$. Ekkor a $\varphi: Z[\theta] \to Z/nZ$ leképezés amire $\varphi(1) \equiv 1 \pmod n$ és ami θ-t *m*-be viszi, egy szürjektív gyűrű-homomorfizmus.

Ekkor, ha találunk olyan $S \subset Z^2$ halmazt, amelyre:

$$\prod_{(a,b)\in S}(a+b\theta) = \beta^2 \text{ és } \prod_{(a,b)\in S}(a+bm) = y^2$$

teljesül, ahol $\beta \in Z(\theta), y \in Z$, akkor az $x = \varphi(\beta) \in Z/nZ$ jelölés mellett alkalmazzuk φ-t:

$$x^2 \equiv \varphi(\beta)^2 \equiv \varphi(\beta^2) \equiv \varphi\left(\prod_{(a,b)\in S}(a+b\theta)\right) \equiv$$

$$\equiv \prod_{(a,b)\in S}(a+bm) \equiv y^2 \pmod{n}$$

Fontos megjegyeznünk, hogy az $a + b\theta$ alakú számok szorzataként előálló négyzetszámnak $Z[\theta]$-ban kell lennie, mert φ csak ott van értelmezve. A gyakorlatban ezt a feltételt enyhíthetjük annyival, hogy a négyzetszám $Q(\theta)$-ban is lehet, mert abból könnyű $Z[\theta]$- belit csinálni a következő módon. Legyen $\alpha \in Q(\theta)$ és $z \in Z$ úgy, hogy az alábbi teljesüljön:

$$\prod_{(a,b)\in S}(a+b\theta) = \alpha^2 \text{ és } \prod_{(a,b)\in S}(a+bm) = z^2 \qquad (1)$$

Ekkor $\alpha \in D$ (D a $Q(\theta)$-beli algebrai számok részgyűrűje) és $f'(\theta) \cdot \alpha \in Z[\theta]$.

Legyen $\beta = f'(\theta) \cdot \alpha$, $y = f'(\theta) \cdot z$ és $x = \varphi(\beta) \in Z/nZ$. Ekkor:

$$x^2 \equiv \varphi(\beta)^2 \equiv \varphi(\beta^2) \equiv \varphi\left(f'(\theta)^2 \cdot \prod_{(a,b)\in S}(a+b\theta)\right) \equiv$$

$$\equiv \varphi\left(f'(\theta)\right)^2 \cdot \prod_{(a,b)\in S}(a+b\theta) \equiv f'(m)^2 \cdot \prod_{(a,b)\in S}(a+bm) \equiv y^2 \pmod{n}$$

Vagyis a keresett kongruens négyzetek ilyenkor is elállíthatók.

Keressünk tehát egy olyan S halmazt, melyre igaz (1). Ezt úgy tehetjük meg, hogy olyan $(a, b) \in Z^2$ párokat keresünk, melyre $a+b\theta$ sima egy "algebrai" faktorbázis felett és $a+bm$ sima egy "racionális" faktorbázis felett, majd a *QS*-ben megismert módon lineáris algebra segítségével megkeressük az S halmazt. Az algebrai faktorbázis $Z[\theta]$-hoz, a racionális pedig Z-hez tartozik.

Természetes, hogy a racionális faktorbázis a megszokott módon prímszámokat tartalmaz, az viszont nem világos elsőre, hogy $Z[\theta]$-ban mi szerint faktorizálunk. Valójában $Z[\theta]$-ban általában még a számelmélet alaptétele sem érvényes, így a kérdés valóban okoz némi fejtörést. A GNFS megszületésekor (SNFS) azzal a feltevéssel éltek, hogy igaz az alaptétel és $Z[\theta] = D$. Általánosan persze egyik sem igaz, ennek ellenére az SNFS algoritmus nagyon hatékony a mai napig.

Simaság $Z[\theta]$-ban

A GNFS-ben használt megoldás az, hogy a $Z[\theta]$-ban lévő simaságot a gyűrű prímideáljai szerint vesszük, vagyis az $a + b\theta$ elem akkor sima az algebrai faktorbázis felett, ha az $< a + b\theta >$ főideál felbomlik a faktorbázisban lévő prímideálok szorzatára. Ahhoz, hogy a $Z[\theta]$-beli faktorizálást könnyedén elvégezhessük, át kell fogalmaznunk az ideálok oszthatóságával kapcsolatos kérdéseket kezelhetőbb formára.

Az derült ki, hogy ha elsőrendű prímideálokat használunk, akkor ezeket a reprezentálhatjuk (r, p) számpárok halmazaként, ahol $p \in Z$ prím, $r \in Z/pZ$ és

$f(r) \equiv 0 \pmod p$. Ezzel a formával számítógépen is jól kezelhetővé válnak az ideálok, ha a szükséges műveleteket is el tudjuk végezni ebben az ábrázolásban. Létezik olyan homomorfizmus, mellyel az oszthatósági kérdéseket könnyedén vizsgálhatjuk. Ez a tétel egyrészt azt mondja ki, hogy az $< a + b\theta >$ alakú ideálok (ahol a és b relatív prímek) elsőrendű prímideálok szorzatára bomlanak. Vagyis a faktorbázist van értelme ilyen prímideálok halmazának választani, másrészt jó feltételt ad arra, hogy egy elsőrendű prímideál osztója-e egy $< a + b\theta >$ alakú ideálnak. A tétel szerint egy elsőrendű prímideál pontosan akkor osztója az $< a + b\theta >$ ideálnak, ha a hozzá tartozó (r, p) párra $a \equiv -br \pmod p$ igaz. Végül az (a, b) elem akkor lesz sima az algebrai faktorbázis felett, ha a hozzá tartozó ideál normája az. Így pedig $Z[\theta]$-ban faktorizálni egy faktorbázis felett pont olyan egyszerű, mint a Z-ben.

Ahhoz, hogy az algebrai faktorbázist összeállítsuk, olyan *(r, p)* párokat kell keresnünk, melyekre $p \in Z$ *prím,* $r \in Z/pZ$ és $f(r) \equiv 0 \pmod p$ igaz. Másként fogalmazva ez éppen az *f(x)* polinom gyökeinek megkeresése *(mod p)*. Ezt a feladatot általában olyan egyszerűen oldjuk meg, hogy leellenőrizzük sorban az összes $r \in Z/pZ$ elemet, hogy kielégíti-e az egyenletet, de ez a módszer csak viszonylag kis *p* esetén hatékony. A GNFS-ben jellemzően nagy prímek is előfordulnak, így itt egy gyorsabb módszert érdemes használunk.

Négyzetszámok *Z[θ]*-ban

Most, hogy tisztáztuk a *Z[θ]*-beli faktorizálás mikéntjét, térjünk vissza az eredeti célunkhoz, miszerint kongruens négyzetszámokat akarunk előállítani *mod p*. A módszerünk az, hogy a *Z* és *Z[θ]* gyűrűkben egyszerre keresünk sima számokat, melyekből Gauss-eliminációval előállítjuk a kívánt négyzeteket. A probléma az, hogy a Gauss-eliminációval előállított *Z[θ]*-beli négyzetszámról jelenleg nem tudjuk garantálni, hogy az tényleg az, mivel *Z[θ]*-ban nem biztos, hogy igaz a számelmélet alaptétele. A GNFS-ben úgy érjük el, hogy négyzetszámot kapjunk, hogy nem csak azt a feltételt szabjuk, hogy a megfelelő kitevők párosak legyenek, hanem azt is hogy a megfelelő Legendre-szimbólumok is 1-et vegyenek fel. *Z*-ben ha *x* négyzetszám, akkor *mod p* is az minden *p* prímre, ezért ha egy *x*-re és valamilyen *p* prímre az $\left(\frac{x}{p}\right)$ Legendre-szimbólum értéke −1, akkor *x* biztosan nem négyzetszám. *Z[θ]*-ban ugyanilyen feltételt kvadratikus karakterek segítségével tehetünk.
Tétel: Legyen $S \subseteq Z^2$ olyan *(a, b)* számpárok halmaza, melyre:

$$\prod_{(a,b)\in S} (a + b\theta) = \alpha^2$$

valamilyen $\alpha \in Q(\theta)$-val. Vegyünk egy olyan elsőrendű *p* prímideált, amihez az *(r, p)* pár tartozik és amelyik nem osztja az $< a + b\theta >$ ideált semmilyen *(a, b)*-re, valamint $f'(r) \not\equiv 0$. Ekkor:

$$x_p(\alpha^2) := \prod_{(a,b)\in S} \left(\frac{a + br}{p}\right) = 1$$

Ahhoz tehát, hogy jó eséllyel négyzetszámot kapjunk, arra van szükség, hogy minél több prímideállal igaz legyen ez a feltétel. Természetesen ezzel a módszerrel nem lehet a gyakorlatban biztosra menni, de nagyon kis eséllyel fogunk hibázni. Szükségünk van így még egy faktorbázisra, mely azokat a prímideálokhoz tartozó *(r, p)* párokat fogja tartalmazni, melyekkel ez utóbbi feltételt írjuk elő. Ezt a faktorbázist kvadratikus faktorbázisnak nevezzük. Ebben a halmazban természetesen ugyanolyan tulajdonságú ideálok vannak, mint az algebrai faktorbázisban, de nem azonosak velük.

Van még egy fontos különbség a GNFS-ben a kvadratikus szitához képest. Itt a lineáris algebrai lépésben egy *Q(θ)*-beli négyzetszámot kapunk, amiből $f'(\theta)^2$-val való szorzással állítunk elő *Z[θ]*-belit. Ebből az is következik, hogy nem is ismerjük a négyzetszám gyökét *Z[θ]*-ban, azt külön ki kell számolnunk. Mivel a *Z*-beli négyzetszámot is beszorozzuk, ezért annak ugyanúgy nem ismerjük a gyökét. A *QS*-ben ezeket automatikusan megkaptuk a kanonikus alakokból. Bár a gyökvonás elvégzése nem tűnik komoly nehézségnek, mégis egy fontos és a futási időben sem elhanyagolható részét képezi ez az algoritmusnak. A *Z*-beli gyökvonásra számtalan módszer ismert, a *Z[θ]*-beli gyökvonás viszont egy kevésbé vizsgált terület.

Szitálás

A szitálás algoritmusa egy kicsit eltér a kvadratikus szitában használt módszertől, mivel itt más feltételek alapján keresünk sima számokat. A keresett elemek itt a következő tulajdonságokkal rendelkeznek:

- *lnko(a, b) = 1*
- $a + bm$ sima a racionális faktorbázis felett
- $N(a,b) = b^{deg(f)} f\left(\frac{a}{b}\right)$ sima az algebrai faktorbázis felett

Mivel *(a, b)* számpárokat keresünk, ezért 2-dimenzióban kellene szitálni, de ehelyett általában az egyik változót lerögzítve szokás a keresést végezni. Legyen tehát *b* rögzített érték mellett $a \in [-C, C]$. Ekkor $a + bm$ akkor osztható *p*-vel, ha $a = -bm + kp\ (k \in Z)$ alakú. Hasonlóan $a + b\theta$ akkor osztható az *(r, p)*-nek megfelelő prímideállal, ha

$a = -br + kp\ (k \in Z)$ alakú. Innentől kezdve a szitálást teljesen hasonlóan végezhetjük, mint a QS-be. Annyi különbséggel, hogy két vektorban kell egyszerre szitálnunk, s végül azokat az elemeket tartjuk meg, melyek mindkét vektorban 1-re csökkentek. Ha az $a \in [-C, C]$ intervallumon elvégeztük a szitálást, de még nincs elég relációnk, növeljük meg *b*-t és szitáljunk újra.

Lineáris algebra

A szitálással olyan *(a, b)* párokat kaptunk, amire $a+bm$ és $a+b\theta$ sima a racionális illetve az algebrai faktorbázis felett. Ahhoz, hogy megkeressük azt a részhalmazt, amelynek elemeit összeszorozva négyzetszámokat kapunk, meg kell oldanunk egy egyenletrendszert. Az eredményül kapott halmaztól azt várjuk el, hogy a szorzatok kanonikus alakja *Z*-ben és $Z[\theta]$-ban is nullvektor legyen *mod 2*. A kvadratikus bázissal hasonlóan járunk el. Az előzőek mellett azt is elvárjuk, hogy a szorzatok kvadratikus karakterei 1-ek legyenek. Mivel a kvadratikus karakter értékkészlete $\{-1, 0, 1\}$, de az eddigi műveleteket *mod 2* végeztük, ezért itt egy kis módosításra van szükség. Írjunk a mátrixba 1-et, ha a megfelelő kvadratikus karakter nem 1, egyébként nullát. Így egy-egy relációhoz tartozó sorvektor álljon a következő elemekből:

• Az első elem legyen 0, ha $(a + bm) > 0$, egyébként 1.

• A második elemtől kezdve írjuk le $(a + bm)$ kanonikus alakját a racionális faktorbázis felett. Írjunk 1-et, ha az adott prím páratlanszor, illetve 0-t ha párosszor osztja $(a + bm)$-t.

• Folytassuk a vektort *(a+bθ)* elem algebrai faktorbázison vett kanonikus alakjával. Hasonlóan csak a paritást írjuk le.

• Folytassuk a vektort a kvadratikus bázissal, írjunk 1-et, ha $\left(\frac{a+br_i}{p_i}\right) \neq 1$,

egyébként 0-t.

Végül a vektorokból mátrixot képezve kapunk egy (relációk száma) · (racionális faktorbázis elemszáma + algebrai faktorbázis elemszáma + kvadratikus faktorbázis elemszáma +1) méretű mátrixot. A keresett részhalmazt megkaphatjuk az *Ax = 0 (mod 2)* egyenletrendszer megoldásával, ahol *A* az előbbi mátrix.

Az algoritmus vázlata

Az eddigieket összefoglalva, a GNFS algoritmus a következő lépésekből áll:

1. Válasszunk egy *Z[x]*-beli irreducibilis polinomot, melyre *f(m) ≡ 0 (mod n)*.

2. Válasszuk meg a racionális, algebrai és kvadratikus faktorbázisok elemeit.

3. Szitálással keressünk olyan $(a, b) \in Z^2$ elemeket, melyekre:

• *lnko(a, b) = 1*

• $a + bm$ sima a racionális faktorbázis felett.

• $N(a, b) = b^{deg(f)} f\left(\frac{a}{b}\right)$ sima az algebrai faktorbázis felett.

Az ilyen elemeket relációknak nevezzük. Gyűjtsünk össze annyi relációt, amennyit csak tudunk, de legalább annyit, mint ahány elem a faktorbázisokban van összesen.

4. A relációkból készítsünk mátrixot, majd Gauss-eliminációval keressük egy-egy négyzetszámot *Z*-ben és *Z[θ]*-ban.

5. Számoljuk ki az előző pontban kapott négyzetszámok gyökeit az alábbiak segítségével:

$$y^2 = \prod_{(a,b)\in S} (a - bm) \quad \text{és} \quad x^2 = \prod_{(a,b)\in S} (a - b\theta)$$

6. Az *n* egy osztóját jó eséllyel megkapjuk *lnko(n, x+y)* és *lnko(n, x−y)* kiszámításával.

A GNFS algoritmus várható futásideje (sejtés):

$$O\left(e^{\left(\sqrt[3]{\frac{64}{9}}+O(1)\cdot\sqrt[3]{\log n}\cdot\sqrt[3]{(\log\log n)^2}\right)}\right)$$

5.6. Prímszámok és a kriptográfia

Ebben a részben napjaink leggyakrabban használt titkosítását szeretném bemutatni. Az eljárás arra a tényre támaszkodik, hogy egy nagy összetett számnak a prímtényezős felbontása évmilliárdokba telik a mai számítógépekkel és algoritmusokkal.

Titkosírással kapcsolatos feljegyzések már az ókortól kezdve megtalálhatóak a világ több részén. Természetes közegeként először a hadviselésben jelent meg, és azóta is megmaradt legfontosabb alkalmazási területeként. Az újkorig nagyrészt a monoalfabetikus helyettesítéssel működő rejtjelezés volt elterjedt. 1466-ban készült el az első általunk ismert polialfabetikus rejtjelezőgép Leon Battista Alberti keze által. Az újkor végén a gyors technikai fejlődés magával vonta a kommunikáció gyorsulását is, ez pedig a kriptográfia fejlődésével járt. A világháborúkban nagy szerepe volt a titkosírásnak, a csaták a kódok szintjén is zajlottak. A 20. század második felében a számítógépek megjelenésével új szintre lépett a kommunikáció is, az addig megfejthetetlennek hitt rejtjelek gyorsan elavulttá váltak.

1976-ban jelent meg Whitfield Diffie és Martin Hellman *Új direktívák a kriptográfiában* című könyve. Ők vezették be a kulcsmegosztáson alapuló kriptográfia fogalmát. Egy évvel később Ron Rivest, Adi Shamir és Len Adleman munkájának köszönhetően elkészült az első nyílt kulcsú titkosító eljárás. (A nevük kezdőbetűivel jelöljük: RSA). A módszer lényege, hogy az eljárást használók egy-egy kulcspárral rendelkeznek, melyek közül az egyiket szabadon terjeszthetik, a másikat pedig titokban kell tartaniuk. A nyilvános kulccsal kódolt üzenetet csak a titkos kulccsal lehet dekódolni és bár a kódolás algoritmusa mindenki számára ismert, a titkos kulcsot - és így az üzenetet - mégsem lehet könnyedén meghatározni.

Az RSA és más titkosítási rendszerek is matematikai alapon garantálják a dekódolás nehézségét. Olyan un. egyirányú függvényeket használnak, melyek gyorsan kiértékelhetők, de az inverzük meghatározása a gyakorlatban szinte lehetetlen. Ebben a fejezetben az RSA működését és a hozzá kapcsolódó prímfaktorizáció kérdéseit vizsgáljuk meg.

Megjegyzés: Aki szeretne bővebben foglalkozni a titkosítás és a kódfejtés történetével, annak ajánlom Simon Singh: Kódkönyv című művét (Park Könyvkiadó).

1. Az RSA-séma

Az RSA-séma használatához szükségünk van a publikus és titkos kulcsok előállítására:

Inicializálás:

1. Válasszunk két prímet, *p*-t és *q*-t.

2. Számoljuk ki $n = pq$-t, és $\phi(n) = (p - 1)(q - 1)$-et.

3. Válasszunk *d*-t, amire teljesül, hogy $lnko(d, \phi(n)) = 1$.

4. Válasszunk *e*-t, amire teljesül, hogy $ed \equiv 1 \ (mod\ \phi(n))$.

5. Az (e, n) párt publikus-, a (d, n) párt pedig a privát kulcsnak nevezzük.

Az *M* üzenet titkosítása:

1. Reprezentáljuk *M*-et *k* db számmal, legyenek ezek $M_1, \cdots, M_k$.

2. Minden $M_i \in M_0, \cdots, M_k$-re számoljuk ki $C_i = M_i^e \ \ (mod\ n)$-et.

3. A titkosított üzenet: $C = C_0, \cdots, C_k$

A $C = C_0, \cdots, C_k$ titkosított üzenet dekódolása:

1. Minden $C_i \in C_0, \cdots, C_k$-ra számoljuk ki $M_i = C_i^d \ \ (mod\ n)$-et.

2. A dekódolt üzenet: $M_i = M_0, \cdots, M_k$

Példa az RSA-séma alkalmazására

Tegyük fel, hogy András titkosított üzenetet szeretne küldeni Bélának. A következőképp kell eljárnia:

Inicializálás:

1. Legyen $p = 11$ és $q = 29$.

2. Ekkor $n = pq = 319$, és $\phi(n) = (p - 1)(q - 1) = 280$.

3. Legyen d = 17, mivel *lnko*(17, 280) = 1, ezért ez megfelelő választás.

4. Legyen e = 33-t, mivel $33 \cdot 17 = 561 \equiv 1$ (mod 280), ezért ez megfelelő választás.

5. A (33, 319) pár a publikus-, a (17, 319) pár pedig a privát kulcs.

Az *M*="nem túl biztonságos..." üzenet titkosítása:

1. Reprezentáljuk az üzenetet a betűk ASCII kódjának megfelelő számokkal:

M="nem túl biztonságos..." = 110, 101, 109, 032, 116, 250, 108, 032, 098, 105, 122, 116, 111, 110, 115, 225, 103, 111, 115, 046, 046, 046

2. Minden $M_i \in M_0, \cdots, M_k$-ra számoljuk ki $C_i = M_i^e \ \ (mod\ n)$-et:

$$110^{33}\ (mod\ 319) = 286$$

$$101^{33}\ (mod\ 319) = 19$$

$$\vdots$$

$$046^{33}\ (mod\ 319) = 162$$

3. A titkosított üzenet: *C*=286, 19, 274, 98, 29, 160, 234, 98, 43, 73, 265, 29, 210, 286, 202, 158, 284, 210, 202, 162, 162, 162

A *C*=286, 19, 274, 98, 29, 160, 234, 98, 43, 73, 265, 29, 210, 286, 202, 158, 284, 210, 202, 162, 162, 162 üzenet dekódolása:

1. Minden $C_i \in C_0, \cdots, C_k$-ra számoljuk ki $M_i = C_i^d \ \ (mod\ n)$-et:

$$286^{17}\ \ (mod\ 319) = 110$$

$$019^{17}\ \ (mod\ 319) = 101$$

$$\vdots$$

$$162^{17}\ \ (mod\ 319) = 46$$

2. A dekódolt üzenet *M* = 110, 101, 109, 032, 116, 250, 108, 032, 098, 105, 122, 116, 111, 110, 115, 225, 103, 111, 115, 046, 046, 046 = "nem túl biztonságos..."

2. Helyesség

Ebben a részben az RSA-séma helyességét bizonyítjuk. Tegyük fel, hogy kiválasztottuk az összes szükséges számot a módszer használatához. Ekkor azt kell belátnunk, hogy az *M* üzenetet kódolva, majd dekódolva visszakapjuk *M*-et, azaz:

$$(M^e)^d = M \pmod n$$

Az *e* és *d* megválasztásakor feltétel volt, hogy *e* a *d* multiplikatív inverze legyen, azaz:

$$ed \equiv 1 \pmod{\phi(n)} \Rightarrow ed = k \cdot \phi(n) + 1 \ (k \in N).$$

Ezt felhasználva a következőt kapjuk:

$$(M^e)^d = M^{ed} \pmod n$$

$$(M^e)^d = M^{k \cdot \varphi(n)+1} \pmod n$$

A "kis" Fermat tételből könnyen látható, hogy minden *p*-re és *M*-re, ahol $p \nmid M$:

$$M^{p-1} \equiv 1 \pmod p \ \rightarrow \ M^{k(p-1)} \equiv 1 \pmod p$$

$$M^{p-1} \equiv 1 \pmod p \ \rightarrow \ M^{k(p-1)+1} \equiv M \pmod p, ahol\ k \in N$$

Alkalmazva ezt *p*-re és *q*-ra is, ezt kapjuk:

$$M^{k(p-1)+1} \equiv M \pmod p$$

$$M^{k(q-1)+1} \equiv M \pmod q$$

Ezt felhasználva:

$$M^{k(p-1)(q-1)+1} \equiv M \pmod{pq}$$

$$M^{k \cdot \varphi(n)+1} \equiv M \pmod n$$

$$M^{ed} \equiv M \pmod n$$

Ezt kellett igazolni, tehát igaz az állítás.

Biztonság

Az előző pontban láttuk, hogy az RSA-séma helyesen működik, de arról még nem bizonyosodtunk meg, hogy tényleg biztonságban van az üzenetünk, ha ezt a módszert használjuk. Könnyen látható, hogy *n* osztóinak ismeretében megtalálhatjuk *d*-t, mivel csak meg kell oldanunk az $ed \equiv 1 \pmod{(p-1)(q-1)}$ lineáris kongruenciát, amit hatékonyan meg is tudunk tenni. Felmerül tehát a kérdés, hogy a prímfaktorizáció nehézsége elegendő védelem-e. Valójában azonban az nem bizonyított még, hogy egy RSA-val kódolt üzenet dekódolása éppen olyan nehézségű feladat mint a prímfaktorizáció, de azt látjuk hogy a visszafelé irány teljesül. De ha tudnánk, hogy a két probléma ekvivalens, akkor sem nyugodhatnánk még meg teljesen, mivel a prímfaktorizációról nem tudjuk, hogy valóban annyira nehéz probléma mint amilyennek reméljük.

Matematikailag a problémák nehézségét a bonyolultság-osztályokkal jellemezhetjük jól. Az RSA-val kapcsolatban az volna a jó, ha kiderülne, hogy az egészek prímfaktorizációja valamilyen nehéz bonyolultság-osztályba tartozik. Bár bizonyítva nincs ilyesmi, de annak alapján, hogy milyen régóta megoldatlan a probléma, megalapozottnak gondolhatnánk a sejtést, hogy ez a feladat nem oldható meg polinom időben. Gyakorlatilag semmilyen kézzel fogható bizonyítékunk nincs arra, hogy a módszer valóban biztonságos, ezért fel kell tennünk a kérdést, hogy miért is használjuk ezt a rendszert? A válasz egyszerűen annyi, hogy a kifejlesztése óta eltelt 45 évben semmilyen olyan módszer nem került napvilágra, amellyel hatékonyan megfejthető lenne egy RSA-val titkosított üzenet. Minden eddigi próbálkozás valamilyen a felhasználó által elkövetett - és így könnyen orvosolható - hibára vezethető vissza. Az ilyen támadások 4 osztályba sorolhatók:

1. Implementációs problémákat kihasználó támadások.

2. A homomorf struktúrát kihasználó támadások.

3. Rosszul választott paramétereket kihasználó támadások.

4. Könnyű faktorizációt kihasználó támadások.

1. Implementációs problémákat kihasználó támadások.

Az ebbe a kategóriába tartozó támadások az implementációhoz kapcsolódó hibákat vagy gyengeségeket kihasználva szereznek információt az üzenetről vagy a paraméterekről.

Idő alapú támadások:

Az idő alapú támadások a titkosítás folyamatának az idejét mérik, az ilyen támadásokhoz szükséges ismerni a titkosítást végző hardware-t is, ami általában egy különálló modul. Kocher megmutatta, hogy csupán az idő mérésével meghatározható a titkos kulcs. Az ilyen támadások ellen az egyik módszer amit használhatunk, hogy úgy alakítjuk ki az titkosítást végző algoritmust, hogy minden kódolást és dekódolást ugyanannyi idő alatt végezzen el. Ezt a gyakorlatban nem használják, mivel egyrészt nehéz kivitelezni, másrészt pedig rendkívül csökken az adott hardware hatékonysága, ha arra kényszerül folyton, hogy a gyors műveleteket is lassan végezze el.

A másik módszert 1982-ben Chaum mutatta be, technikáját vakításnak nevezte el. A módszer alapja, hogy a titkosított *C* üzenet helyett egy $C' = c \cdot r^e \pmod n$ üzenetet dekódoljon a rendszer, ahol *r* egy véletlenszerűen választott *Z/nZ*-beli szám. Ekkor a dekódolás után megkapott M'-ből megkaphatjuk az eredeti üzenetet, ha osztunk *r*-el:

$M = \frac{M'}{r}$. Ezzel a módszerrel kiküszöbölhetők az idő alapú támadások, mivel a dekódolás közben egy, a támadó számára ismeretlen szöveget dekódol a rendszer, így a támadással kinyerhető adatok sem lesznek a valóságnak megfelelőek.

Teljesítmény analízis:

A teljesítmény analízis az előző támadási formához nagyon hasonló, de itt nem az időt, hanem a titkosítást végző eszköz által felvett energia mennyiségét méri a támadó. Természetesen itt is szükséges ismernie a támadónak az adott hardware tulajdonságait és csak akkor használhatja ezt a módszert, ha a titkosítást végző modul energiafelvételéről pontos adatai vannak. Vagyis ha nem egy különálló modul végzi a titkosítást - mint mondjuk egy otthoni PC-ben - akkor lehetetlen megállapítani, hogy pontosan mekkora energiát igényelt a kódolás/dekódolás.

A legkönnyebb védekezés az ilyen támadás ellen, ha a támadót soha nem engedjük közel a hardware-hez, de megtehetjük azt is, hogy az áramfelvételt egy zajos jellel terheljük, így elkerülve az információ kinyerését. A teljesítmény analízishez hasonló támadások léteznek a titkosító modul által kibocsátott elektromágneses sugárzást mérve is, de az ilyen módszerek mind megakadályozhatók azzal, ha a támadót fizikailag elkülönítjük a titkosítást végző géptől.

2. A homomorf struktúrát kihasználó támadások.

Az RSA homomorf struktúrája azt jelenti, hogy a módszer által használt kódoló eljárás homomorf, azaz:

$$(M_1 M_2)^e \equiv M_1^e M_2^e \equiv C_1 C_2$$

Tegyük fel, hogy Támadó dekódolni akar egy *C* üzenetet. Ehhez felhasználja a naiv Andrást, akit rávesz, hogy dekódoljon egy $C' = C \cdot r^e \pmod n$ üzenetet, ahol $r \in Z_n$ véletlenszerű és *(e, n)* András nyilvános kulcsa. Ekkor azzal, hogy András dekódolja C'-t, dekódolja *C*-t is, de erről ő mit sem tud. Ha a dekódolt M' üzenetet Támadó megszerzi, akkor a vakítás technikájához hasonlóan *r*-el osztva megkaphatja az eredeti *M* üzenetet. Ez a módszer természetesen csak a nagyon ügyetlen András ellen vethető be, a gyakorlatban kevésbé hatékonyan alkalmazható.

3. Rossz paramétereket kihasználó támadások.

Abban az esetben, ha az *e* vagy *d* paramétert nem kellő körültekintéssel választjuk meg, néhány ezt kihasználó támadásnak tehetjük ki magunkat.

Kis *d* választása:

1989-ben Martin Wiener publikált egy lánctörteket használó módszert, mellyel kis *d* esetén felfedhető annak értéke. Megmutatta, hogy ha $d < n^{\frac{1}{4}}$, akkor nem biztonságos a titkosítás. 10 évvel később Boneh és Durfee módosította ezt a korlátot $n^{0,292}$-re, de javaslatuk szerint ne válasszunk $n^{\frac{1}{2}}$-nél kisebb *d*-t.

Kis *e* választása:

Bár az előző pont miatt azt gondolhatnánk, hogy a kis *e* választása hasonlóan veszélyes, valójában itt nem annyira rossz a helyzet. Kis *e* választása esetén csak akkor határozható meg *d* értéke, ha a támadónak rendelkezésére áll néhány lineárisan összefüggő kódolt üzenet. Ilyen lehet például egy ismétlődő elköszönés az üzenetek végén.

A gyakorlatban használt RSA algoritmusok a kódolás előtt módosítanak az üzeneten amiatt, hogy ezt elkerüljék, de Coppersmith megmutatta, hogy elég nagy módosításra van szükség ahhoz, hogy a támadás teljesen kivédhető legyen. A jó védekezés természetesen a nagy *e* választása.

Közös paraméterek használata:

Abban az esetben, ha valaki közös modulust használ két különböző felhasználóval való kommunikációja során, dekódolhatóak azon üzenetei, melyeket mindkét felhasználónak elküldött. Legyen C_1 *és* C_2 az M üzenet kódolt változatai, melyeket az e_1 illetve e_2 exponensekkel kódoltak. Ekkor mivel e_1 és e_2 relatív prímek, ezért a Támadó kereshet olyan *x, y* párt, amire $xe_1 + ye_2 \equiv 1 \pmod{n}$. Ekkor *M*-et előállíthatja a következő módon:

$$C_1^x C_2^y \equiv M^{xe_1+ye_2} \equiv M \pmod{n}$$

Érdemes megjegyezni, hogy ennél a támadásnál bár az üzenetet elolvasta a Támadó, azonban a *d*-t nem tudta meg.

4. Könnyű faktorizációt kihasználó támadások

Láttuk, hogy *n* faktorizálásával megszerezhető *d*, így ügyelnünk kell arra, hogy ezt megnehezítsük. A legkevesebb, amit tehetünk, hogy *p*-t és *q*-t nagynak választjuk, de ezen kívül Rivest és Silverman sok javaslatot tesz arra, hogy milyen prímeket ne válasszunk. Erős prímeknek nevezik azokat a *p* prímeket, melyek esetében $p + 1$-nek és $p - 1$-nek van nagy prímfaktora. Erős prímeket használva elkerülhetjük, hogy Pollard faktorizáló algoritmusai hatékonyan használhatóak legyenek. Hasonló feltételekkel választható olyan *n*, amellyel az összes ismert faktorizáló algoritmus nehezen boldogul.

6. Feladatok

Ebben a fejezetben prímszámokkal kapcsolatos feladatokat oldhatunk meg. Két csoportba soroltam őket:

1. Határozzuk meg, hogy…

A 17.-ik prímszám az 59. Ennyi feladat található ebben a fejezetben.

2. Bizonyítsuk be, hogy…

A 19.-ik prímszám a 67. Ennyi feladat található ebben a fejezetben.

A feladványok többségéhez elég a középiskolás ismeret is. A megoldásokat igyekeztem röviden és érthetően megfogalmazni.

6.1 Határozzuk meg, hogy…

1. Határozzuk meg, hogy az n milyen értéke esetén lesz az $n, n+4, és\ n+14$ is prímszám?

2. Határozzuk meg, hogy milyen p prímszám esetén lesz a $8p^2+1$ is prímszám?

3. Határozzuk meg, hogy mennyi négyjegyű prímszámot lehet képezni az $1, 2, 3, 4$ számjegyek felhasználásával?

4. Határozzuk meg három prímszám összegeként a 146-ot!

5. Határozzuk meg három prímszám összegeként a 99-et!

6. Határozzuk meg azokat az x, y, z egész számokat, melyekre

$$(3x+y+z)(x+2y+z)(x+y+z) = p, ahol\ p\ prímszám!$$

7. Határozzuk meg azokat az x egész számokat, melyekre

$$x^2+28x+889 = p^2, ahol\ p\ prímszám!$$

8. Határozzuk meg, hogy hányféleképpen lehet felbontani az $\frac{1}{pq}$ törtet két különböző természetes szám reciprokának összegére, ahol p és q különböző prímszámok?

9. Határozzuk meg, hogy hányféleképpen lehet kiválasztani a 100-nál kisebb prímszámok közül ötöt úgy, hogy ezek számjegyei között az 1,2,3,4,5,6,7,8,9 mindegyike egyszer szerepeljen?

10. Határozzuk meg azokat a p prímszámokat, melyekre $p^3 + p^2 + 11p + 2$ is prímszám!

11. Határozzuk meg, hogy mennyi különböző prímszámot lehet úgy megadni, hogy közülük bármely három összege is prímszám legyen?

12. Határozzuk meg azokat az x egész számokat, melyekre a $2x^2 - x - 36 = p^2$, ahol p prímszám!

13. Határozzuk meg azokat a p és q prímszámokat, amelyekre $p^q + q^p$ szintén prímszám!

14. Határozzuk meg azokat a p prímszámokat, melyekről tudjuk, hogy jegyeinek száma páros és palindrom szám! (Vagyis, ha fordított sorrendben írjuk le a jegyeit, akkor ugyanazt a számot kapjuk.)

15. Határozzuk meg azokat a p prímszámokat, amelyekre a $p^2 + 8$ is prímszám!

16. Legyen a p prímszám és $p-1$ négyzetmentes! (Nincs négyzetszám osztója.) Határozzuk meg, hogy a p 4-gyel osztva milyen maradékot ad!

17. Határozzuk meg azokat a p prímszámokat, melyekre $2p - 1$ és $2p + 1$ ikerprímek!

18. Határozzuk meg azokat az a egész számokat, melyekre $a^4 + 4$ prímszám lesz!

19. Határozzuk meg, hogy mennyi olyan egész szám van 1000 és 2000 között, amely a kettőn és ötön kívül más prímszámmal nem osztható!

20. Határozzuk meg, hogy az $(n+1) \cdot (n+2) \cdot \cdots \cdot 2n$ szorzat prímtényezős felbontásában a 2 hányadik hatványon szerepel!

21. Határozzuk meg a p, q, r prímszámokat, melyekről tudjuk, hogy $pqr = 5(p + q + r)$!

22. Határozzuk meg a $2x + 3y + 6z = 90$ egyenlet megoldását, ahol *x, y, z* prímszámok!

23. Határozzuk meg az $n^p = p^n$ egyenlet megoldását, ahol *n* természetes szám, *p* prímszám!

24. Határozzuk meg azokat a *p* prímszámokat, melyekre a $p^2 + 2$ is prímszám!

25. Határozzuk meg azokat az *n* természetes számokat, melyekre a

$p = n^3 - 7n^2 + 14n - 6$ prímszám lesz!

26. Határozzuk meg, hogy az 1,2,3,…,9 számjegyek egyszeri felhasználásával a prímszámokat úgy, hogy e prímszámok összege, valamint ezen belül az egyjegyű prímszámok összege a lehető legkisebb legyen!

27. Három természetes számról a következőket tudjuk:

1. Mind a három szám különböző.

2. Összegük 406.

3. Legnagyobb közös osztójuk kettőnél nagyobb prímszám. (p)

4. Ha az egyes számokat elosztjuk *p*-vel, akkor ismét három prímszámot kapunk.

$(p_1,\ p_2, p_3)$

Határozzuk meg ezeket a természetes számokat!

28. Határozzuk meg azokat az *x, y, z* természetes számokat, amelyekre teljesül a következő egyenlőség:

$2^x + 5^y = 19^z$!

29. Határozzuk meg egy $\overline{xyxyxy}$ alakú tízes számrendszerbeli szám legnagyobb prímosztóját!

30. Határozzuk meg azokat a *p* és *q* prímszámokat, amelyekre $p + q$ *és* $p^2 + q^2 - q$ szintén prímszámok!

31. Határozzuk meg, hogy milyen *p* és *q* prímszámokra és *n* természetes számra teljesül az alábbi egyenlőség!

$$\sqrt[n]{p+q} = p - q$$

32. Határozzuk meg azt a négy prímszámot, melyeknek a négyzetösszege 476!

33. Határozzuk meg az *a* és *b* relatív prímeket, amelyekről a következőket tudjuk:

1. Összegük 150.

2. Mindkettő kisebb 100-nál.

3. Különbségük 7 többszöröse.

34. Határozzuk meg azt a három prímszámot, amelyekről a következőket tudjuk! A legnagyobb 20-al több mint a legkisebb, a középső 4-gyel kisebb a legnagyobbnál.

35. Határozzuk meg azokat az *n* természetes számokat, amelyekre az $n^5 + n^4 + 1$ kifejezés értéke prímszám!

36. Határozzuk meg azokat a számokat, melyeket az alábbi módon kapunk! Legyen egy háromjegyű prímszám minden számjegye 1-nél nagyobb négyzetszám és ezt a prímszámot szorozzuk meg az első számjegyével.

37. Legyen $p > q$ olyan prímek, melyekre $p^q + q^p$ is prímszám! Határozzuk meg az alábbi kifejezés értékét:

$$101 \cdot p^2 \cdot (q+p) \cdot (q-p) \cdot (q^2 - p^3)$$

38. Legyen $p > q$ olyan prímek, melyekre $p^q + q^p$ is prímszám! Határozzuk meg az alábbi kifejezés értékét:

$$q \cdot p^p \cdot (q^{q+p} + q + p + 1)$$

39. Határozzuk meg azokat a p_1, p_2, p_3 prímszámokat, amelyekre teljesül az alábbi egyenlőség:

$$p_1 \cdot p_2^3 + p_1^3 \cdot p_2 = 10 \cdot p_3$$

40. Határozzuk meg azokat az $\overline{abcd} \leq 4000$ prímszámokat, amelyekre az alábbi két feltétel teljesül:

1. Az első két számjegyük olyan kétjegyű prímszám, melyben a számjegyek szorzata 1-től különböző négyzetszám.

2. Második két számjegyük olyan kétjegyű prímszám, amely számjegyeinek szorzatát fordított sorrendben felírva ismét négyzetszámot kapunk.

41. Határozzuk meg azokat a $1000 < p < 2000$ prímszámokat, amelyek számjegyeinek összege olyan kétjegyű szám, melynek mindkét számjegye páros és összegük 8!

42. Határozzuk meg azokat az $\overline{abc}$ háromjegyű prímszámokat, ahol $a \neq b$ és a számjegyeire az alábbi összefüggés teljesül:

$$\frac{\overline{ab}}{\overline{ac} - 7a} = \frac{\overline{ba}}{\overline{bc} - 7b}$$

43. Határozzuk meg azt a három prímszámot, melyekre teljesül az alábbi összefüggés:

$$p_1 \cdot p_2 \cdot p_3 = 197 \cdot (p_1 + p_2 + p_3)$$

44. Határozzuk meg az 1, 2, 3, $\cdots$, 196 számoknak egy olyan sorrendjét, hogy bármely két szomszédos szám összege prímszám legyen!

45. Határozzuk meg azokat a p prímszámokat, melyekre az alábbi tört értéke is prímszám!

$$\frac{p^3 + 99}{p - 1}$$

46. Határozzuk meg azokat a p prímszámokat, melyekre $14p + 1 = k^3$!

47. Határozzuk meg azokat a p prímszámokat, melyekre $p^n + 1 = k^2$!

48. Határozzuk meg a különböző r, p, q prímek szorzatát, ha $r = q + 2p$ és $p^2 + q^2 = 538$!

49. Határozzuk meg a különböző p_1, p_2, p_3, p_4 prímek szorzatát, melyekre az alábbi teljesül!

$$(p_1 + p_2 + p_3)^2 - p_4^2 = 231$$

50. Határozzuk meg azokat a p, q, r prímeket úgy, hogy a $p^4 + q^4 + r^4 - 3$ kifejezés értéke prímszám legyen!

51. Határozzuk meg azokat a pozitív egész *n* és *p* prímszámokat, amelyekre az alábbi kifejezés értéke egész szám!

$$\sqrt{\frac{n+p}{n-p}}$$

52. Határozzuk meg azokat a különböző *p, q, r* prímeket úgy, hogy a következő egyenlőségek teljesüljenek: $p-q=q-r=8$!

53. Határozzuk meg azokat a különböző *p, q* prímeket, melyekre:

$$\sqrt{pq^3}+\sqrt{qp^3}=\sqrt{1134}$$

54. Határozzuk meg azokat a különböző p_1, p_2, p_3, p_4 prímek szorzatát, melyekre:

$$p_1^2-(p_2+p_3+p_4)^2=136$$

55. Határozzuk meg azokat az *n* pozitív egész számokat, amelyekre az alábbi számok mindegyike prímszám lesz!

$$n, n+2, n+4$$

56. Határozzuk meg azokat az *n* pozitív egész számokat, amelyekre az alábbi számok mindegyike prímszám lesz!

$$n, n+6, n+12, n+18, n+24$$

57. Határozzuk meg azokat az *n* pozitív egész számokat, amelyekre az alábbi számok mindegyike prímszám lesz!

$$n, n^3-6, n^3+6$$

58. Határozzuk meg azokat az *n* pozitív egész számokat, amelyekre az alábbi kifejezés értéke prímszám lesz!

$$n^3-n+3$$

59. Határozzuk meg azokat az *n* pozitív egész számokat, amelyekre az alábbi kifejezés értéke prímszám lesz!

$$n^8+n^6+n^4+n^2+1$$

6.2 Bizonyítsuk be, hogy…

1. Bizonyítsuk be, hogy végtelen sok olyan a természetes szám van, amelyre egy tetszőleges n természetes szám esetén $b = n^4 + a$ szám nem prímszám!

2. Bizonyítsuk be, hogy ha $3 < p$ prímszám, akkor $8p + 1$ nem lehet négyzetszám!

3. Bizonyítsuk be, hogy ha a,b,c,d olyan természetes számok, amelyekre $a \cdot b = c \cdot d$, akkor sem $a + b + c + d$, sem $a^2 + b^2 + c^2 + d^2$ nem lesz prímszám!

4. Bizonyítsuk be, hogy az $A = 0{,}23571113171923\ldots$ szám irracionális! (Tizedes jegyeknek a prímszámokat írtuk növekvő sorrendben.)

5. Bizonyítsuk be, hogy $\binom{n}{p} - \left[\frac{n}{p}\right]$ osztható p-vel, ahol p prímszám!

6. A természetes számokat az ábra szerint egy négyzetrácsos lapra csigavonalban felírjuk, majd a prímszámokat megjelöljük. Bizonyítsuk be, hogy a 9-es és a 24-es alatti oszlopokban egyetlen számot sem jelöltünk meg!

73	72	71	70	69	68	67	66	65	100
74	43	42	41	40	39	38	37	64	99
75	44	21	20	19	18	17	36	63	98
76	45	22	7	6	5	16	35	62	97
77	46	23	8	1	4	15	34	61	96
78	47	24	9	2	3	14	33	60	95
79	48	25	10	11	12	13	32	59	94
80	49	26	27	28	29	30	31	58	93
81	50	51	52	53	54	55	56	57	92
82	83	84	85	86	87	88	89	90	91

7. Bizonyítsuk be, hogy minden $3 < p$ prímszám valamelyik szomszédja osztható 6-tal!

8. Bizonyítsuk be, hogy ha egy prímszámot 30-cal osztunk, akkor a maradék prímszám vagy 1 lesz!

9. Bizonyítsuk be, hogy ha p, q *és* r, s számpárok ikerprímek, ahol $3 < p, q, r, s$, akkor $p \cdot r - q \cdot s$ osztható 12-vel!

10. Bizonyítsuk be, hogy ha p, q, r egész számok páronként relatív prímek, akkor az

$A = p \cdot q + q \cdot r + p \cdot r$ *és* $B = p \cdot q \cdot r$ is relatív prímek! Igaz-e az állítás megfordítása?

11. Bizonyítsuk be, hogy az $a_n - 1$ számnak legalább $n\ darab$ különböző prím osztója van, ha az $a_1, a_2, a_3, \ldots$ sorozatot a következő módon definiáljuk:

$$a_1 = 5, \qquad a_{n+1} = a_n^2 \text{ , } (\, ahol\ n = 1,2, \ldots).$$

12. Bizonyítsuk be, hogy a p_n sorozatnak nem eleme az 5, ha a sorozatot a következő módon definiáljuk:

$p_1 = 2,\ p_{n+1}\ az\ 1 + p_1 p_2 \ldots p_n$ szám legnagyobb prímosztója!

13. Adott 1 *és* $(2n-1)^2$ között *n* darab páronként relatív prím. Bizonyítsuk be, hogy a megadott számok között van prímszám!

14. Bizonyítsuk be, hogy tíz egymás utáni egész szám között mindig van olyan, amelyik a másik kilenchez relatív prím!

15. Bizonyítsuk be, hogy bármely 4-nél nagyobb tizenkettő szomszédos egész szám között legalább nyolc összetett szám!

16. Bizonyítsuk be, hogy minden pozitív egész *n*-hez található *n* darab szomszédos pozitív egész szám úgy, hogy egyikük sem egyenlő egy prímszám pozitív egész kitevőjű hatványával!

17. Bizonyítsuk be, hogy ha $2^n - 1$ prímszám, ahol *n* természetes szám, akkor *n* is prímszám! Az állítás megfordítása igaz-e?

18. Bizonyítsuk be, hogy a $3 < p$ prímszám négyzete 24-gyel osztva 1 maradékot ad!

19. Bizonyítsuk be, hogy az 5-nél nagyobb ikerprímek összege osztható 12-vel!

20. Bizonyítsuk be, hogy ha $\frac{a^3+b^3}{2}$ prímszám, akkor $3a^2-6a+4$ *és* $3b^2-6b+4$ is az, ahol a és b természetes számok!

21. Bizonyítsuk be, hogy az $1999^{2016}+2014$ nem prímszám!

22. Bizonyítsuk be, hogy az $A=\sqrt{2249\cdots910\cdots09}+3$, (Ahol a 224 után (*k-2*) darab 9-es, az 1 után *k* darab 0 szerepel, és *k* nagyobb, vagy egyenlő 2.) számnak a prímtényezői: 2, 3, 5!

23. Bizonyítsuk be, hogy különböző prímszámok reciprokainak összege nem lehet egész szám, sem egy egész szám reciproka!

24. Bizonyítsuk be, hogy ha $5<p$ prímszám, akkor a 360 osztója a p^4-5p^2+4 számnak!

25. Bizonyítsuk be, hogy ha $p\neq q$ prímszámok, akkor $\sqrt{p}$ *és* $\sqrt{p\cdot q}$ irracionális számok!

26. Bizonyítsuk be, hogy minden *p* prímszám esetén $\sqrt{p^2+1}$ *és* $\sqrt{p^2-1}$ irracionális számok!

27. Bizonyítsuk be, hogy ha 2^n+1 prímszám, akkor $n=2^l$ alakú!

28. Bizonyítsuk be, hogy minden $3<p$ prímszám felírható $6n+1\ vagy\ 6n-1\ alakban, ahol\ n=1,2,\cdots$!

29. Bizonyítsuk be, hogy minden $2<p$ prímszám csak egyféleképpen írható fel két négyzetszám különbségeként!

30. Bizonyítsuk be, hogy 2^n-1 *és* 2^n+1 nem lehet egyszerre prímszám, ha

$2<n$ természetes szám!

31. Legyen *p* és *q* 2-nél nagyobb prímszámok! Bizonyítsuk be, hogy ha $2^{pq}-2$ osztható a pq szorzattal, akkor 2^p-2 *és* 2^q-2 is osztható a pq szorzattal!

32. Legyen *p* 2-nél nagyobb prímszám! Bizonyítsuk be, hogy $\frac{2}{p}$ csakis egyféleképpen írható fel a $\frac{2}{p}=\frac{1}{x}+\frac{1}{y}$ alakban, ahol *x* és *y* egymástól különböző pozitív egész számok!

33. Bizonyítsuk be, hogy ha $n-1$ és $n+1$ prímszámok, akkor az $n, n-12, n+12$ számok egyike osztható 30 −cal!

34. Legyen *n* páratlan szám! Bizonyítsuk be, hogy ahány *n*-hez relatív prímszám van az *n*-nél kisebb számok között, ugyanannyi *n*-hez relatív prímszám van a *2n*-nél kisebbek között! (Erdős Pál feladata.)

35. Legyenek az *a, b, c* számok páronként relatív prímszámok! Bizonyítsuk be, hogy az $a \cdot b \cdot c$ és $a \cdot b + b \cdot c + a \cdot c$ is relatív prímszámok! Igaz-e a tétel megfordítása?

36. Bizonyítsuk be, hogy két páratlan prímszám négyzetének különbsége osztható 24-gyel!

37. Bizonyítsuk be, hogy két iker prímszám összege osztható 12-vel, ha a prímszámok 3-nál nagyobbak!

38. Bizonyítsuk be, hogy ha *a, b, c* három egymást követő természetes szám, akkor

$b^2 - a^2$ és $c^2 - b^2$ relatív prímszámok!

39. Bizonyítsuk be, hogy $7 < p$ esetén a p és $p+2$ iker prímszámokkal szomszédos három szám szorzata osztható 240-nel!

40. A következő számok prímek: 7,37,337. Igaz-e, hogy ezt a sorozatot folytatva mindig prímszámot kapunk? Bizonyítsuk be, hogy nem!

41. Bizonyítsuk be, hogy minden pozitív egész *n*-hez található *n* darab szomszédos pozitív egész szám úgy, hogy egyikük sem egyenlő egy prímszám pozitív egész kitevőjű hatványával!

42. Bizonyítsuk be, hogy $1 < p$ egész szám pontosan akkor prímszám, ha *p* bármely négy pozitív egész összegére való felbontásában semelyik két tag szorzata sem egyenlő a másik két tag szorzatával!

43. Bizonyítsuk be, hogy ha *a* és *b* különböző egész számok, akkor végtelen sok olyan *n* természetes szám létezik, amelyre $(a+n)$ és $(b+n)$ relatív prímek!

44. Bizonyítsuk be, hogy ha az $x^2 + ax + 1 = b$ egyenlet gyökei egész számok, és $b \neq 1$, akkor $a^2 + b^2$ nem lehet prímszám!

45. Bizonyítsuk be, hogy ha a és b relatív prímszámok, akkor a következő törteket nem lehet egyszerűsíteni!

$$\frac{a+b}{a\cdot b} \text{ és } \frac{a-b}{a\cdot b}$$

46. Bizonyítsuk be, hogy ha egy *N* összetett szám legkisebb prímosztója nagyobb a szám köbgyökénél, akkor az *N* szám két prímszám szorzata!

47. Legyen $1 < a$ és $0 < n$ egész számok! Bizonyítsuk be, hogy a^{n+1} csak akkor lehet prímszám, ha a páros és az n 2-nek valamilyen hatványa!

48. Bizonyítsuk be, hogy minden 3-nál nagyobb prímszám négyzete 12-vel osztva 1 maradékot ad!

49. Bizonyítsuk be, hogy végtelen sok olyan prímszámot találhatunk úgy, hogy bármely kettő különbsége osztható egy tetszőlegesen megadott k számmal!

50. Bizonyítsuk be, hogy ha p és q 7-nél nagyobb prímszámok, akkor a

$(p^2-1)\cdot(p^2-1)\cdot(p^6-q^6)$ kifejezés osztható 290304-gyel!

51. Bizonyítsuk be, hogy minden $n \geq 2$ természetes szám felírható prímszámok összegeként!

52. Bizonyítsuk be, hogy létezik végtelen sok olyan prímszám, amelyek első számjegye 1-es!

53. Jelölje p_n az *n*-edik prímszámot. Bizonyítsuk be, hogy $p_{n+1} < 2\cdot p_n$ minden $n \geq 1$ egész szám esetén!

54. Jelölje p_n az *n*-edik prímszámot. Bizonyítsuk be, hogy $p_n < 2^n$ minden $n \geq 2$ egész szám esetén!

55. Bizonyítsuk be, hogy nem lehet egy pozitív egészekből álló végtelen számtani sorozat minden tagja prímszám!

56. Bizonyítsuk be, hogy végtelen sok olyan prímszám van, amely nem tagja egyetlen ikerprím számpárnak sem!

57. Bizonyítsuk be, hogy létezik olyan *n* pozitív egész szám, amelyre p^n utolsó öt számjegye 00001, ahol $p > 5$ prímszám!

58. Bizonyítsuk be, hogy 12 db $3 < p$ prímszám négyzetének összege osztható 12-vel!

59. Legyenek $a_1, a_2, a_3, a_4, a_5, a_6$ olyan pozitív egész számok, melyekre:

$$a_1^n + a_2^n + a_3^n = a_4^n + a_5^n + a_6^n$$

Bizonyítsuk be, hogy ekkor $a_1 + a_2 + a_3 + a_4 + a_5 + a_6$ összeg nem lehet prímszám!

60. Legyen *p* egy olyan prím, melyre $p^2 + p + 1$ *és* $p^2 - p + 1$ is prímszám! Bizonyítsuk be, hogy ha $p^4 + p^3 + p^2 + p + 1$ nem prímszám, akkor négyzetszám!

61. Bizonyítsuk be, hogy a $4n^3 + 6n^2 + 4n + 1$ kifejezés egyetlen pozitív egész *n*-re sem lesz prímszám!

62. Bizonyítsuk be, hogy nem léteznek olyan *p* és *q* prímszámok, amelyekre a $p^{2q} + q^{2p}$ összeg szintén prímszám!

63. Bizonyítsuk be, hogy ha egy 5-nél nagyobb prímszám négyzetét 30-cal osztjuk, akkor a maradék 1 vagy 19 lesz!

64. Bizonyítsuk be, hogy ha p *és* $8p - 1$ is prímszámok, akkor $8p + 1$ összetett szám!

Bizonyítsuk be, hogy ha p *és* $8p^2 + 1$ is prímszámok, akkor $8p^2 - 1$ is prímszám!

65. Bizonyítsuk be, hogy ha $p > 3$ prímszám, akkor p^2-t 12-vel osztva 1 maradékot ad!

66. Bizonyítsuk be, hogy ha *p,q,r* 3-nál nagyobb különböző prímszámok egy számtani sorozatot alkotnak, akkor a sorozat *d* különbsége osztható 6-tal!

67. Bizonyítsuk be, hogy az alábbi számsorozat elemei páronként relatív prímek!

$$2 + 1;\ 2^2 + 1;\ 2^4 + 1;\ 2^8 + 1;\ 2^{16} + 1;\ \cdots;\ 2^{2^n} + 1;\ \cdots$$

7. Megoldások

A megoldások többségéhez elegendő a gimnáziumi ismeret. Igyekeztem röviden és érthetően megfogalmazni a magyarázatokat. Bízom benne, hogy ez sikerült!

7.1 Határozzuk meg, hogy …

1.

1, Ha $n = 3k$ alakú: Mivel n prím, csak a $k = 1$ eset lehetséges, azaz $n = 3$.

2, Ha $n = 3k + 1$ alakú: Ekkor az $n + 14$ összetett szám, tehát nincs ilyen megoldás.

3, Ha $n = 3k - 1$ alakú: Ekkor az $n + 4$ összetett szám, tehát nincs ilyen megoldás.

A megoldás: 3, 7, 17.

2.

Ha $p = 3$, akkor $8 \cdot 3^2 + 1 = 73$. Ez prímszám, tehát jó megoldás. A $p \neq 3$ prímek 3-mal osztva 1 vagy 2 maradékot adnak, vagyis $p = 3k \pm 1$ alakúak. Ezt behelyettesítve:

$$8 \cdot (3k \pm 1)^2 + 1 = 8 \cdot (9k^2 \pm 6k + 1) + 1 = 72k^2 \pm 48k + 9 = 3 \cdot (24k^2 \pm 16k + 3)$$

Ez a kifejezés osztható 3-mal, tehát nem lehet prímszám.

3.

A keresett számok csak $1 - re\ vagy\ 3 - ra$ végződhetnek. Ilyen szám 12 darab van, melyek közül csak négy prím. Ezek: $1423, 2143, 2341, 4231$.

4.

Három egész szám összege páros, ha:

1. Mind a három szám páros.

2. Egy páros és kettő páratlan.

1. Nincs három páros prím, tehát nincs ilyen megoldás.

2. Egyedül a 2 páros prím, tehát a felbontásban szerepelnie kell. Vagyis a 144-et kell két prím összegére bontani. A 144 végződését háromféle módon állíthatjuk elő:

a, $1 + 3$

b, $5 + 9$

c, $7 + 7$

A prímek végződés szerint csoportosítva:

1-re végződik: 11, 31, 41, 61, 71, 101, 131

3-ra végződik: 3, 13, 23, 43, 53, 73, 83, 103, 113

5-re végződik: 5

7-re végződik: 7, 17, 37, 47, 67, 97, 107, 127, 137

9-re végződik: 19, 29, 59, 79, 109, 139

a, eset: $146 = 2 + 31 + 113 = 2 + 41 + 103 = 2 + 61 + 83 =$

$= 2 + 71 + 73 = 2 + 43 + 101 = 2 + 13 + 131$

b, eset: $146 = 2 + 5 + 139$

c, eset: $146 = 2 + 7 + 137 = 2 + 17 + 127 = 2 + 37 + 107 = 2 + 47 + 97$

Tehát a 146-ot 11 féleképpen bonthatjuk fel három prímszám összegére.

5.

Három egész szám összege páratlan, ha:

1. Egy páratlan van köztük.

2. Mind a három páratlan.

1. Nincs két páros prím, tehát nincs ilyen megoldás.

2. A 99 végződését hét módon állíthatjuk elő:

a, $1 + 1 + 7$

b, $1 + 3 + 5$

c, $1 + 9 + 9$

d, $3 + 3 + 3$

e, $3 + 7 + 9$

f, $5 + 5 + 9$

g, $5 + 7 + 7$

Felhasználva az előző feladatban megadott csoportosítást, a következő 30 megoldást kapjuk:

a, eset: $99 = 11 + 41 + 47 = 11 + 71 + 17 =$

$= 31 + 31 + 37 = 31 + 61 + 7 = 41 + 41 + 17$

b, eset: $99 = 11 + 83 + 5 = 41 + 53 + 5 = 71 + 23 + 5$

c, eset: $99 = 11 + 29 + 59 = 41 + 29 + 29 = 61 + 19 + 19$

d, eset: $99 = 3 + 13 + 83 = 3 + 23 + 73 = 3 + 43 + 53 =$

$= 13 + 13 + 73 = 13 + 43 + 43 = 23 + 23 + 53$

e, eset: $99 = 3 + 7 + 89 = 3 + 17 + 79 = 3 + 37 + 59 = 3 + 67 + 29 =$

$= 13 + 7 + 79 = 13 + 67 + 19 = 23 + 17 + 59 = 23 + 47 + 29 =$

$= 43 + 37 + 19 = 53 + 17 + 29 = 73 + 7 + 19$

f, eset: $99 = 5 + 5 + 89$

g, eset: $99 = 5 + 47 + 47.$

6.

A baloldalon egész számok szerepelnek, így kettő abszolút értéke 1, a harmadiké p. Az előjeleket tekintve vagy két tényező negatív vagy mindhárom pozitív. Ezek alapján 12 esetet különböztethetünk meg.

$$(3x + y + z) = A, \qquad (x + 2y + z) = B, \qquad (x + y + z) = C$$

A	p	p	-p	-p	1	1	-1	-1	1	1	-1	-1
B	1	-1	1	-1	p	-p	p	-p	1	-1	1	-1
C	1	-1	-1	1	1	-1	-1	1	p	-p	-p	p

Az első négy, illetve az utolsó négy oszlopban $p \neq 2$ kell, hogy teljesüljön.

Mint egyenletrendszert tekintve a következő megoldást kapjuk:

$$\begin{cases} 3x + y + z = A \\ x + 2y + z = B \\ x + y + z = C \end{cases}$$

$$x = \frac{A - C}{2}, \qquad y = B - C, \qquad z = 2C - B - \frac{A - C}{2}$$

Az y mindig egész, az x és z csak akkor, ha A és C azonos paritású. Ez mind a 12 esetben teljesül, ha a p páratlan. Ha p=2, akkor csak négy megoldást kapunk.

7.

Átírva az egyenletet:

$$x^2 + 28x + 889 = (x + 14)^2 + 693 = p^2$$

Ebből:

$$p^2 - (x + 14)^2 = (p - x - 14)(p + x + 14) = 693$$

A következő egyenletrendszer alapján:

$$\begin{cases} p - x - 14 = a \\ p + x + 14 = b \end{cases}$$

$$p = \frac{a+b}{2}, \qquad x = \frac{b-a}{2} - 14$$

Mivel *a* és *b* csak páratlan lehet, *p* és *x* mindig egész szám lesz. Nem kaphatunk prímet, ha *a*-nak és *b*-nek van közös osztója, mert ha van, az is páratlan, ezért a 2-vel való osztás után is megmarad. A relatív prím *a, b* párokat még ellenőrizni kell, hogy összegük fele prím-e.

A $693 = 3^2 \cdot 7 \cdot 11$. Az előbbiek miatt a két 3-as tényezőnek vagy az *a*-ban vagy a *b*-ben kell maradnia, így a $693 = 9 \cdot 7 \cdot 11$ alak szerint a következő *a, b* párok lehetnek:

1. $a \cdot b = b \cdot a = 1 \cdot 693$, az összeg fele 347, ez prímszám.

2. $a \cdot b = b \cdot a = 9 \cdot 77$, az összeg fele 43, ez prímszám.

3. $a \cdot b = b \cdot a = 7 \cdot 99$, az összeg fele 53, ez prímszám.

4. $a \cdot b = b \cdot a = 11 \cdot 63$, az összeg fele 37, ez prímszám.

Tehát mind a négy felbontásból kapunk két-két megoldást. Az első esetben:

$$x = \frac{693 - 1}{2} - 14 = 332 \text{ és } x = \frac{1 - 693}{2} - 14 = -360$$

A többit is hasonlóan elvégezve a keresett értékek:

$$x = -360, -60, -48, -40, 8, 20, 32, 332$$

8.

A két természetes szám *a* és *b* reciprokai kisebbek $\frac{1}{pq}$ − nál, vagyis mindkettő nagyobb

pq-nál. Legyen $a = pq + c \text{ és } b = pq + d, ahol\ 0 < c, d$ egész számok és

$a < b, c < d$ teljesüljön.

Az

$$\frac{1}{pq+c}+\frac{1}{pq+d}=\frac{1}{pq}$$

egyenletből rendezés után:

$cd=p^2q^2$ és $d=\frac{p^2q^2}{c}>c$ *alapján*: $c<pq$, azaz c a p^2q^2-nek pq-nál kisebb osztója, d pedig a társosztója. A p^2q^2 osztói:

$$1,p,p^2$$

$$q,pq,p^2q$$

$$q^2,pq^2,p^2q$$

Számuk 9, ha pq-t elhagyjuk, akkor 4 párt adnak c, d, így a, b számára. Tehát az $\frac{1}{pq}$ törtet 8-féleképpen bonthatjuk két különböző természetes szám reciprokának az összegére, ha különbözőknek tekintjük azokat is, melyek csak sorrendben térnek el egymástól. Ha ezeket nem tekintjük különbözőknek, akkor 4 felbontás lehetséges.

9.

Az öt szám közül 4 kétjegyű és 1 egyjegyű. A kétjegyűek utolsó számjegye nem lehet páros és 5-ös, tehát csak 1, 3, 7, 9-re végződhet. Az egyjegyű prímek közül, tehát csak a 2 és az 5 jöhet szóba.

Nézzük meg először azt, amikor a 2-t választjuk. Ekkor a 4 kétjegyű első jegye a 4, 5, 6, 8 számok közül kerül ki. Ezek a prímek a következők:

41	-	61	-
43	53	-	83
47	-	67	-
-	59	-	89

Határozzuk meg, hogy hányféleképpen választhatunk ki ebből a táblázatból négy számot úgy, hogy mindegyik sorból és oszlopból pontosan egyet vegyünk ki. Ezt 4-féleképpen tehetjük meg.

Szintén 4 a lehetőségek száma, ha egyjegyűnek az 5-öt választjuk. A feladat kérdésére a válasz: Nyolcféleképpen választhatjuk ki az öt prímszámot.

10.

Minden $p \neq 3$ $prímszám$ $3k+1$ $vagy$ $3k+2$ $alak$ú, $ahol$ $k = 1, 2, \cdots$. Így három eset lehetséges:

1. Ha $p = 3$, akkor:

$$p^3 + p^2 + 11p + 2 = 71$$

Ez prímszám.

2. Ha $p = 3k + 1$, akkor:

$$p^3 + p^2 + 11p + 2 = 27k^3 + 36k^2 + 48k + 15$$

Ez a szám osztható 3-mal.

3. Ha $p = 3k + 2$, akkor:

$$p^3 + p^2 + 11p + 2 = 27k^3 + 63k^2 + 81k + 36$$

Ez a szám osztható 3-mal. Az egyetlen megoldás: $p = 3$.

11.

Csoportosítsuk a prímeket a 3-as maradékosztályok szerint. Egy-egy osztályból legfeljebb két számot vehetünk ki, mert ha három prím 3-mal osztva egyenlő maradékot ad, akkor az összegük osztható 3-mal. Ha mindegyik osztályból veszünk egyet, akkor azok összege is osztható 3-mal. Tehát legfeljebb két osztályból és mindegyikből legfeljebb két számot vehetünk. Így legfeljebb négy prímszámot adhatunk meg. Ilyen például: 7, 11, 13, 23 vagy 19, 23, 37, 41.

12.

A kifejezést alakítsuk szorzattá:

$$2x^2 - x - 36 = (2x - 9)(x + 4) = \mathrm{A} \cdot \mathrm{B} = p^2$$

Három eset lehetséges:

1. Ha $A = 1, B = p^2$, akkor:

$$\begin{cases} 2x - 9 = 1 \\ x + 4 = p^2 \end{cases}$$

Ebből: $x = 5$ és $p = 3$.

2. Ha $A = p^2, B = 1$, akkor:

$$\begin{cases} 2x - 9 = p^2 \\ x + 4 = 1 \end{cases}$$

Ebből: $x = -3$, nincs prím.

3. Ha $A = p, B = p$, akkor:

$$\begin{cases} 2x - 9 = p \\ x + 4 = p \end{cases}$$

Ebből: $x = 13$ és $p = 17$.

A keresett értékek: $x = 5$ és $x = 13$.

13.

Legyen $p > q$ prímszámok! A $p^q + q^p > 2$ és páratlan, vagyis az összeg egyik tagja ($pl. q^p$) páros, azaz $q = 2$ és és a p páratlan. Vizsgáljuk az összeget a következő alakban:

$$2^p + p^2 = (2^p + 1) + (p^2 - 1)$$

Mivel p páratlan, $(2^p + 1)$ osztható 3-mal. Ha p nem osztható 3-mal, akkor a négyzete 1 maradékot ad 3-mal osztva, vagyis $(p^2 - 1)$ szintén osztható 3-mal. Tehát azt kapjuk, hogy ha p páratlan és 3-mal nem osztható, akkor $2^p + p^2$ osztható 3-mal. Ez csak akkor prím, ha $2^p + p^2 = 3$, de ebből $p = 1$ következik, ami nem helyes. Azaz a p osztható 3-mal, de ekkor csak a $p = 3$ lehetséges. Az egyetlen megoldás: $q = 2$ és $p = 3$.

14.

Az első ilyen prímszám a 11. Mivel minden páros jegyű palindrom szám osztható 11-gyel, ezért ez az egyetlen megoldás.

15.

Tudjuk, hogy egy szám négyzete 3-mal osztva 0 vagy 1 maradékot ad, attól függően, hogy a szám osztható-e 3-mal vagy sem. Ha a p nem osztható 3-mal, akkor a $p^2 + 8$ igen. Mivel ez 3-tól nagyobb, nem lehet prímszám. Tehát ha $p^2 + 8$ nem osztható 3-mal, akkor p-nek oszthatónak kell lennie 3-mal. Ilyen prímszám csak egy van, $p = 3$.

16.

A p prímszám $4k + 1\ vagy\ 4k + 3$ alakú, ahol $k = 1, 2, \cdots$. Mivel $p - 1$ négyzetmentes, ezért p csak $4k + 3$ alakú lehet. Vagyis 4-gyel osztva 3 maradékot ad.

17.

A $2p - 1, 2p, 2p + 1$ egymást követő természetes számok, a feltétel szerint a

$2p - 1\ és\ 2p + 1$ prímek, ezért a 3 osztója a $2p$-nek. A $(3, 2) = 1$, ezért a 3 osztója p-nek. Ilyen prímszám csak egy van, $p = 3$.

18.

$$A = a^4 + 4 = (a^2 + 2)^2 - 4a^2 = (a^2 + 2 + 2a)(a^2 + 2 - 2a) =$$
$$= [(a + 1)^2 + 1][(a - 1)^2 + 1]$$

Az A csak akkor lehet prím, ha $(a + 1)^2 + 1 = \pm 1\ vagy\ (a - 1)^2 + 1 = \pm 1$. Ha $1 < |a|$, akkor mindkét tényező nagyobb mint 1, tehát csak két megoldása van: $a = 1\ és\ a = -1$.

19.

Ezen számok prímtényezős felbontása a következő: $2^a \cdot 5^b$. A feltétel miatt:

$$1000 \leq 2^a \cdot 5^b \leq 2000, ahol\ 1 \leq a \leq 10\ és\ 1 \leq b \leq 4$$

Ezek alapján a megoldás: 1000, 1024, 1250, 1280, 1600, 2000.

20.

$$(n+1)(n+2)\cdots 2n = \frac{1\cdot 2\cdot 3\cdot\cdots\cdot n(n+1)(n+2)\cdots 2n}{1\cdot 2\cdot 3\cdot\cdots\cdot n} =$$

$$= \frac{2^n(1\cdot 2\cdot 3\cdot\cdots\cdot n)\big(1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1)\big)}{1\cdot 2\cdot 3\cdot\cdots\cdot n} = 2^n\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1)$$

Tehát 2 a prímtényezős felbontásban az *n*-edik hatványon szerepel.

21.

Mindkét oldal osztható 5-tel, tehát az egyik prímszám 5. Ha $p = 5$, akkor $qr = 5 + q + r$. Ebből:

$$q = 1 + \frac{6}{r-1}$$

Az $(r-1)$-nek a 6 osztójának kell lennie, hogy q egész legyen.

Így $r = 2, 3, 4, 7$ *és* $q = 7, 4, 3, 2$. A két középső eset nem prím megoldást ad. Tehát a keresett három prímszám: 2, 5, 7.

22.

Az egyenletet átrendezve adódik: $2x = 3(30 - y - 2z)$

Mivel a jobb oldal osztható 3-mal, ezért az $x = 3$. Az $y + 2z = 28$, amiből következik, hogy *y* páros, tehát $y = 2$. Ezek szerint $z = 13$.

23.

Az egyenlőség akkor teljesül, ha $n = p^k$ alakú, vagyis $p^{kp} = p^n$. Ebből a $kp = n$ adódik.

1. Ha $k = 1$, akkor $p = n$, azaz minden *p* prím megoldás.

2. Ha $k = 2$ *és* $p = 2$, akkor $n = 4$ megoldás.

3. Ha $2 < k$, akkor $kp = p^k$, azaz $k = p^{k-1}$. A $p^{k-1} = [(p-1)+1]^{k-1}$. A jobb oldal *k* tagból áll, melyek mindegyike legalább 1, ezért a $p^{k-1} \neq k$. Tehát az egyenletnek nincs más megoldása.

24.

Végezzük el a következő átalakítást:

$$p^2 + 2 = p^2 - 1 + 3 = (p-1)(p+1) + 3$$

Ha $p \neq 3$, akkor a $(p-1)\ vagy\ (p+1)$ osztható 3-mal. Az összeg mindkét tagja osztható 3-mal, tehát maga az összeg is. Mivel $p^2 + 2 > 3$, ezért a 3 valódi osztó, tehát a $p^2 + 2$ nem prímszám. Vagyis a $p^2 + 2$ pontosan akkor prímszám, ha $p = 3$.

25.

A kifejezést alakítsuk szorzattá:

$$p = n^3 - 7n^2 + 14n - 6 = (n-3)(n^2 - 4n + 2)$$

Négy esetet különböztethetünk meg:

1. Ha $(n-3) = 1\ és\ (n^2 - 4n + 2) = p$, akkor $n = 4\ és\ (n^2 - 4n + 2) = 2$. Ez megoldás.

2. Ha $(n-3) = -1\ és\ (n^2 - 4n + 2) = -p$, akkor $n = 2\ és\ (n^2 - 4n + 2) = -10$.

Ez nem megoldás.

3. Ha $(n^2 - 4n + 2) = 1$, akkor nem kapunk megoldást.

4. Ha $(n^2 - 4n + 2) = -1$, akkor az $n = 1$ eset megoldás.

26.

A 2, 4, 5, 6, 8 számjegyek nem lehetnek többjegyű prímszámok utolsó jegyei, de az 1, 3, 7, 9 számjegyek közül kell egyet-egyet választani, hogy kétjegyű prímszámot kapjunk. Mivel az egyjegyű prímszámok összegének is minimálisnak kell lennie, a következő két megoldást kapjuk:

$$2 + 3 + 5 + 41 + 67 + 89 = 207$$

$$2 + 3 + 5 + 47 + 61 + 89 = 207$$

Mindkét esetben az egyjegyű számok összege 10.

27.

A feladat szerint:

$$pp_1 + pp_2 + pp_3 = k(p_1 + p_2 + p_3) = 406 = 2 \cdot 7 \cdot 29\,, ahol\ 2 < p\ és\ 1 < p_1 < p_2 < p_3$$

Tehát $p = 7\ vagy\ p = 29$ lehet.

Ha $p = 7$, akkor $p_1 + p_2 + p_3 = 2 \cdot 29 = 58$. Három prímszám összege csak úgy lehet páros, ha egyikük a 2. Azaz ha $p_1 = 2\ és\ p_2 + p_3 = 56$. Ezt az egyenlőséget három számpár elégíti ki: $(3 + 53), (13 + 43), (19 + 37)$.

Ha $p = 29$, akkor $p_1 + p_2 + p_3 = 2 \cdot 7 = 14$. Ezért $p_1 = 2$ kell, hogy legyen.

Ekkor $p_2 + p_3 = 12$. Ebben az esetben csak egy számpár felel meg: $(5 + 7)$. Tehát összesen négy megoldás lehetséges:

$$(14, 21{,}371), (14, 91{,}301), (14, 133{,}259), (58, 145{,}203)$$

28.

Belátjuk, hogy az egyenletnek nincs megoldása. Nézzük meg, hogy az egyes hatványok milyen maradékot adnak 15-tel osztva. A 2^x maradéka 1, 2, 4, vagy 8 lehet. Az 5^y maradéka 1, 5, vagy 10 lehet. A 19^z csak 1 vagy 4 maradékot adhat. Vagyis a bal oldal az alábbi maradékokat adhatja:

$$(1 + 1), (1 + 5), (1 + 10), (2 + 1), (2 + 5), (2 + 10), (4 + 1), (4 + 5),$$

$$(4 + 10), (8 + 1), (8 + 5), (8 + 10)$$

Azaz: 2, 3, 5, 6, 7, 9, 11, 12, 13, 14.

A jobb oldal viszont 1 vagy 4 maradékot adhat, így a két oldal nem lehet egyenlő.

29.

Az ilyen számokat a következő alakba tudjuk írni:

$$\overline{xyxyxy} = 10101 \cdot (10x + y) = 3 \cdot 7 \cdot 13 \cdot 37 \cdot (10x + y)$$

Ebből következik, hogy a $(10x + y)$ a legnagyobb kétjegyű prímszám lehet, vagyis a 97, ami a 979797 számhoz tartozik.

30.

Ha a $p+q$ is prímszám, akkor az egyikük csak a 2 lehet. Mivel a másik prímben

$q^2-q=q(q-1)$ páros pozitív szám, így csak $q=2$ lehetséges.

Ekkor: $p+q=p+2$ és $p^2+q^2-q=p^2+2$

Végezzük el a következő átalakítást:

$$p^2+2=(p^2-1)+3=(p-1)(p+1)+3$$

Ha p nem osztható 3-mal, akkor a $(p-1),(p+1)$ számok egyike 3-mal osztható, így a jobb oldalon a 3 többszöröse áll, ami nem lehet prímszám. Az egyetlen lehetőség a $p=3$. Ekkor: $p+2=5$ és $p^2+2=11$. Tehát ez jó megoldás, és ez az egyetlen.

31.

Az egyenletből következik, hogy $p>q$ és $p+q=(p-q)^2$.

A baloldal $(p-q)+2q$ alakba írható, vagyis a $(p-q)$ osztója $2q$-nak. Mivel q prímszám, ezért a $2q$ osztói: 1, 2, q, és $2q$. Ha $p-q=1$, akkor az első egyenlőségben $p+q=1$, ami lehetetlen. Ha $p-q=q$ vagy $p-q=2q$, akkor $p=2q\ vagy\ p=3q$, azaz a p nem prímszám. Így csak $p-q=2$ lehetséges, azaz p és q iker prímek. Ezek alapján:

$$p=2^{n-1}+1\ \text{és}\ q=2^{n-1}-1$$

Mivel a $2^{n-1}-1\,,2^{n-1}\,,2^{n-1}+1$ számok közül pontosan egy osztható 3-mal és ez nem a középső, ezért p és q egyike 3-mal osztható. Ha $p=3,akkor\ q=1$, ami nem megoldás. Ha $q=3,akkor\ p=5$. Ekkor $8=p+q=(p-q)^n=2^n$ adódik, ahonnan $n=3$.

32.

A feltétel szerint $p_1^2+p_2^2+p_3^2+p_4^2=476$. Egy négyzetszám 3-mal osztva 0 vagy 1 maradékot ad. A 476 maradéka 3-mal osztva 2, így a bal oldali összegnek pontosan 2 tagja osztható 3-mal, de mivel prímek, így tegyük fel, hogy $p_1=3$ és $p_2=3$.

Ebből: $p_3^2+p_4^2=458$. Legyen $p_3<p_4$. Ekkor $p_4^2\geq 229$, vagyis $p_4>15$, illetve

$p_4^2<458$, vagyis $p_4\leq 21$. Tehát p_4 értéke 17 vagy 19 lehet. Ha $p_4=17,akkor\ p_3=13$. Ha $p_4=19$, akkor p_3 nem egész szám. Tehát a feladatnak egy megoldása van: 3, 3, 13, 17.

33.

A feltétel szerint $a - b = 150$. Legyen $a = 75 + x,\ b = 75 - x$ különbségük $a - b = 2x$. Ez többszöröse 7-nek, ha $x = 7 \cdot m, ahol\ m > 0$. Eszerint $a = 75 + 7m$ *és* $b = 75 - 7m$. Ha *a* és *b* relatív prímek, akkor *m* nem lehet páratlan szám.

Azonban $75 + 7m < 100, ha\ 7m < 25, azaz\ m = 1, 2, 3\ lehet$, de ezekből csak $m = 2$ felel meg. Tehát $a = 75 + 14 = 89$ *és* $b = 75 - 14 = 61$. Ezek pedig valóban relatív prímek.

34.

A három prímszám legyen $p_1 < p_2 < p_3$. A feltételek szerint:

$$p_3 = p_1 + 20 \text{ és } p_2 = p_3 - 4 = p_1 + 16$$

Nézzük meg a 3-mal való oszthatóságokat! Ha p_1 3-mal osztva 1 maradékot ad, vagyis $p_1 = 3k + 1$, akkor:

$$p_3 = p_1 + 20 = 3k + 21 = 3(k + 7)$$

Ez osztható 3-mal, de $p_3 > 20$, ami nem lehet prímszám. Ha p_1 3-mal osztva 2 maradékot ad, vagyis $p_1 = 3k + 2$, akkor:

$$p_2 = p_1 + 16 = 3k + 18 = 3(k + 6)$$

Ez osztható 3-mal, de $p_2 > 20$, ami nem lehet prímszám. Ha p_1 osztható 3-mal, akkor csakis $p_1 = 3$ lehet. Ekkor:

$$p_2 = p_1 + 16 = 19 \text{ és } p_3 = p_1 + 20 = 23$$

Tehát a három prímszám: 3, 19, 23.

35.

Alakítsuk át a kifejezést az alábbi módon:

$$n^5 + n^4 + 1 = n^5 + n^4 + n^3 - n^3 + 1 = n^3(n^2 + n + 1) - (n^3 - 1) =$$

$$= n^3(n^2 + n + 1) - (n - 1)(n^2 + n + 1) = (n^2 + n + 1)(n^3 - n + 1)$$

Ez a szorzat csak akkor lehet prím, ha az egyik tényezője 1, a másik pedig egy p prímszám. Két eset lehetséges:

1. $n^2 + n + 1 = 1$ és $n^3 - n + 1 = p$

2. $n^2 + n + 1 = p$ és $n^3 - n + 1 = 1$

Az első esetben csak $n = 0$ lehet, miből $p = 1$ adódik. Ez nem megoldás. A második esetben $n(n^2 - 1) = 0$, amiből $n = 0$ vagy $n = 1$. Az $n = 0$ nem ad megoldást. Ha $n = 1$, akkor $p = 3$ adódik, ami jó megoldás. Tehát a kifejezés értéke csak $n = 1$ esetén lesz prímszám.

36.

Az adott háromjegyű szám számjegyei csak 4 és 9 lehet. Mind a három számjegy nem lehet azonos, mert akkor a szám osztható lenne 3-mal. A szám nem végződhet 4-re sem. A feladatnak megfelelő számok a következők lehetnek: 449, 499, 949. Mivel $949 = 13 \cdot 73$ nem prímszám, csak a másik kettő lehetséges. A keresett számok:

$$4 \cdot 449 = 1796 \text{ és } 4 \cdot 499 = 1996$$

37.

A 6.1.13 feladat megoldása alapján: $p = 3$ és $q = 2$. Ezt behelyettesítve a kifejezésbe:

$$101 \cdot p^2 \cdot (p + q) \cdot (p - q) \cdot (p^2 - q^3) = 101 \cdot 9 \cdot 5 \cdot 1 \cdot 1 = 4545$$

38.

A 6.1.13 feladat megoldása alapján: $p = 3$ és $q = 2$. Ezt behelyettesítve a kifejezésbe:

$$q \cdot p^p \cdot (q^{q+p} + q + p + 1) = 2 \cdot 3^3 \cdot (2^{2+3} + 2 + 3 + 1) = 2 \cdot 27 \cdot 38 = 2052$$

39.

Alakítsuk át az egyenlőséget az alábbi módon:

$$p_1 \cdot p_2 \cdot (p_1^2 + p_2^2) = 2 \cdot 5 \cdot p_3$$

Az egyenlőség jobb oldala három prímszám szorzata, tehát a baloldal is ilyen. A $p_1^2 + p_2^2$ nem lehet 2, sem 5. Vagyis a p_1 és p_2 egyike 2, a másik 5. Ekkor $p_1^2 + p_2^2 = 2^2 + 5^2 = 29$, valóban prímszám. A megoldás: $p_1 = 2, p_2 = 5, p_3 = 29$ vagy $p_1 = 5, p_2 = 2, p_3 = 29$

40.

A feltétel szerint $\overline{abcd} \leq 4000$, ezért az $a = 1, a = 2, a = 3$ lehet. Az $a \neq 2$, mert $\overline{ab}$ prímszám és $a \cdot b$ négyzetszám, de ha $a = 2$, akkor az utóbbi feltétel miatt b-nek is párosnak kell lennie, így $\overline{ab}$ nem lenne prím. Az $a \neq 3$, mert a 3-mal kezdődő kétjegyű prímek 31 és 37, de ezek számjegyeinek szorzata nem négyzetszám. Tehát $a = 1$. Ekkor b-nek négyzetszámnak kell lennie, vagyis $b = 1, b = 4, b = 9$ lehet. Ha $b = 1$, akkor $a \cdot b = 1$, ami a feltételnek nem felel meg. Ha $b = 4$, akkor $\overline{ab} = 14$, ami nem prímszám. Ha $b = 9$, akkor $\overline{ab} = 19$, ami megfelel.

A második két számjegy $\overline{cd}$ szintén prímszám, és a számjegyek szorzatát fordított sorrendbe írva négyzetszám kell, hogy legyen. A kétjegyű négyzetszámok fordított sorrendbe írva: 61, 52, 63, 94, 46, 18. Ezek közül nem állítható elő két egyjegyű szám szorzataként: 61, 52, 94, 46. A lehetséges értékek: $63 = 9 \cdot 7$ $és$ $18 = 2 \cdot 9$. Ezek szerint a $\overline{cd}$ értékei: 97, 79, 92, 29. Ezek közül a 92 nem prímszám. A kapott értékek alapján:

$$\overline{abcd} = 1929, \overline{abcd} = 1979, \overline{abcd} = 1997$$

Az 1929 osztható 3-mal, a másik kettő viszont prímszám.

41.

Legyen a keresett szám $\overline{1abc}$. A 8-at páros számok összegére háromféleképpen tudjuk felbontani: $8 = 8 + 0 = 6 + 2 = 4 + 4$. Ezért az $\overline{1abc}$ jegyeinek összege négyféle lehet: 80, 62, 26, 44. Egy négyjegyű szám jegyeinek összege legfeljebb $4 \cdot 9 = 36$ lehet, vagyis a négy lehetőség közül csak a 26 felel meg. Tehát: $1 + a + b + c = 26$, vagyis $a + b + c = 25$. Ez csak úgy lehetséges, hogy két db 9-es és egy db 7-es, vagy egy db 9-es és két db 8-as szerepel. Ezek alapján a szóba jöhető számok:

$$\overline{1abc} = 1997, 1979, 1799, 1988, 1898, 1889$$

A 8-ra végződőek nem prímek. Ellenőrzés után $1799 = 7 \cdot 257$, tehát nem prímszám, a többi viszont igen. A megoldás: $1997, 1979, 1889$.

42.

A feltételt alakítsuk át az alábbi módon:

$$\frac{10a+b}{10a+c-7a}=\frac{10b+a}{10b+c-7b}$$

$$\frac{10a+b}{3a+c}=\frac{10b+a}{3b+c}$$

$$30ab+3b^2+10ac+bc=30ab+3a^2+10bc+ac$$

$$3b^2-3a^2=9bc-9ac$$

$$3(b-a)(b+a)=9c(b-a)$$

A feltétel szerint $a \neq b$, ezért: $a+b=3c$. A c értéke nem lehet páros, mert $\overline{abc}$ prímszám. Az egyenlet baloldalának értéke kisebb, mint 18, ezért $c<6$. Tehát $c=1, c=3, c=5$ lehet. A $c=5$ nem lehetséges, mert akkor $\overline{abc}$ osztható lenne 5-tel. A $c=3$ sem lehetséges, mert akkor $a+b=9$, így az $\overline{abc}$ osztható lenne 3-mal. Tehát $c=1$. Ekkor $a=1, b=2$ vagy $a=2, b=1$. Első esetben: $\overline{abc}=121$, ez nem prímszám. Második esetben: $\overline{abc}=211$, ami prímszám. Más megoldása nincs a feladatnak.

43.

A 197 prímszám, tehát a baloldalon valamelyik tényező, pl. $p_1=197$. Ezek alapján az egyenlet az alábbi módon alakítható:

$$197 \cdot p_2 \cdot p_3 = 197 \cdot (197+p_2+p_3)$$

$$p_2 \cdot p_3 = 197+p_2+p_3$$

$$p_2 \cdot p_3 - p_2 - p_3 = 197$$

Mindkét oldalhoz adjunk 1-et, a baloldalt alakítsuk szorzattá:

$$p_2 \cdot p_3 - p_2 - p_3 + 1 = 198$$

$$(p_2-1)(p_3-1)=198$$

A $198 = 2 \cdot 3^2 \cdot 11$. A 198-nak $(1+1)(2+1)(1+1) = 12$ db osztója van, ami azt jelenti, hogy 12-féleképpen lehet két pozitív egész szorzatára bontani. Az összes esetet nem kell megvizsgálni, ugyanis a $(p_2 - 1)(p_3 - 1) = 198 = 2 \cdot 3^2 \cdot 11$ egyenlet baloldalának pontosan az egyik tényezője páros, a másik pedig páratlan. Ez abból következik, hogy a 198 prímtényezős felbontásában a 2 első hatványon szerepel. Ha pl. a $p_2 - 1$ páratlan, akkor a p_2 páros. Vagyis $p_2 = 2$ lehet csakis. Tehát a baloldal tényezői: $p_2 - 1 = 1$ és $p_3 - 1 = 198$ lehetnek. Ebből: $p_1 = 197, p_2 = 2, p_3 = 199$. Ezek mindegyike prímszám és a feltételnek is megfelelnek.

44.

Az adott számok csak úgy helyezkedhetnek el a sorban, hogy páros és páratlan számok váltakozva kövessék egymást. Írjuk fel a páratlan számokat növekvő sorban. Ezek közé kell elhelyezni a páros számokat úgy, hogy bármelyik két szomszédos szám összege prím legyen. Írjuk az első két szám közé a 196-ot. Ekkor $1 + 196 = 197$ prímszám és $196 + 3 = 199$ is prímszám. Ezt a gondolatot folytatva adódik a megoldás: A páros számokat csökkenő sorrendben írjuk be a páratlan számok közé.

$$1, 196, 3, 194, 5, 192, 7, 190, \cdots, 6, 193, 4, 195, 2$$

Megjegyzés: Az ilyen elrendezésre azért volt lehetőség, mert a 197 és 199 ikerprímek. Tehát ez az elrendezés bármely ikerprím számpár esetén lehetséges.

45.

Alakítsuk át törtet az alábbi módon:

$$\frac{p^3 + 99}{p-1} = \frac{p^3 - 1 + 100}{p-1} = \frac{p^3 - 1}{p-1} + \frac{100}{p-1} = \frac{(p-1)(p^2 + p + 1)}{p-1} + \frac{100}{p-1}$$

A jobb oldali első tag egész szám. Az eredeti tört akkor és csak akkor lesz egész, ha a $\frac{100}{p-1}$ is egész. Ez akkor teljesül, ha $p - 1$ osztója 100-nak. A 100 osztói: 1,2,4,5,10,20,25,50,100. Ez alapján a *p* értékei: 2,3,5,6,11,21,26,51,101. Ezek közül a prímszámok: 2,3,5,11,101.

Ha $p = 2$, akkor prímszámot kapunk:

$$\frac{p^3 + 99}{p - 1} = \frac{8 + 99}{2 - 1} = 107$$

Ha $p = 3$, akkor nem prímszámot kapunk:

$$\frac{p^3 + 99}{p - 1} = \frac{27 + 99}{3 - 1} = 63$$

Ha $p = 5$, akkor nem prímszámot kapunk:

$$\frac{p^3 + 99}{p - 1} = \frac{125 + 99}{5 - 1} = 56$$

Ha $p = 11$, akkor nem prímszámot kapunk:

$$\frac{p^3 + 99}{p - 1} = \frac{1331 + 99}{11 - 1} = 143 = 11 \cdot 13$$

Ha $p = 101$, akkor nem prímszámot kapunk:

$$\frac{p^3 + 99}{p - 1} = \frac{1030301 + 99}{101 - 1} = 10304$$

Tehát az egyedüli megoldás $p = 2$.

46.

Az egyenlőség baloldala páratlan, ezért a jobb oldal is páratlan, vagyis a $k = 2r + 1$ alakú. Ezek alapján:

$$14p + 1 = (2r + 1)^3 = 8r^3 + 12r^2 + 6r + 1$$

$$14p = 8r^3 + 12r^2 + 6r$$

$$7p = 4r^3 + 6r^2 + 3r$$

$$7p = r(4r^2 + 6r + 3)$$

Mivel a p prímszám, ezért három eset lehetséges:

1. $r = 1$ és $4r^2 + 6r + 3 = 13 = 7p$. Ez nem lehetséges.

2. $r = p$ és $4r^2 + 6r + 3 = 4p^2 + 6p + 3 = 7$. Ez sem lehetséges.

3. $r = 7$ és $4 \cdot 7^2 + 6 \cdot 7 + 3 = p = 241$. Ez prímszám.

Tehát a feladat feltételeinek egyetlen prím felel meg, a $p = 241$. Ugyanis:

$$14 \cdot 241 + 1 = 3375 = 15^3$$

47.

Ha p páros, azaz $p = 2$, akkor k páratlan, azaz $k = 2r + 1$ alakú. Ekkor:

$$2^n + 1 = (2r + 1)^2 = 4r^2 + 4r + 1, azaz\ 2^n = 4r(r + 1)$$

Mivel a jobb oldali szorzat egyik tényezője páratlan, a másik páros, a baloldal 2-nek hatványa, ezért az egyenlőség csak akkor teljesül, ha $r = 1$. Vagyis $2^n = 8 = 2^3, azaz\ n = 3$.

Ha p páratlan, akkor k páros, azaz $k = 2r$ alakú. Ekkor:

$$p^n + 1 = (2r)^2 = 4r^2$$

$$p^n = 4r^2 - 1 = (2r - 1)(2r + 1)$$

Ez az egyenlőség csak akkor teljesül, ha $(2r - 1)$ és $(2r + 1)$ is p-nek valamilyen egész kitevős hatványa. Vagyis: $2r - 1 = p^i$ és $2r + 1 = p^{n-i}$. Ha a második egyenletből kivonjuk az elsőt: $2 = p^{n-i} - p^i = p^i\left(p^{n-2i} - 1\right)$. Mivel a 2-t két egész szám szorzatára csak egyféleképpen bonthatjuk fel: $2 = 1 \cdot 2$, ezért az utóbbi egyenlőség csak akkor teljesülhet, ha

$p^i = 1$ és $p^{n-2i} - 1 = 2$. Ebből $i = 0$ lehet csakis. Tehát $p^n - 1 = 2, azaz\ p^n = 3$, vagyis $p = 3$ és $n = 1$. Ezek alapján csak két megoldást kaptunk a feladatra:

1. A $p = 2$ és $n = 3$. Ekkor $2^3 + 1 = 9 = 3^2$.

2. A $p = 3$ és $n = 1$. Ekkor $3^1 + 1 = 4 = 2^2$.

48.

Bármely $p \neq 3$ prím négyzete 3-mal osztva 1 maradékot ad. Eszerint a $p^2 + q^2 = 538$ egyenlőség baloldala 3-mal osztva 2 maradékot ad, de a jobb oldal viszont 1 maradékot ad. Tehát a baloldal valamelyik tagja osztható 3-mal.

Ha $q = 3$, akkor $p^2 + 9 = 538$, ebből $p^2 = 529 = 23^2$, tehát $p = 23$. Az első egyenlőség alapján: $r = q + 2p = 3 + 2 \cdot 23 = 49$. A 49 nem prímszám, vagyis ez nem megoldás.

Ha $p = 3$, akkor $q = 23$. Az első egyenlőség alapján: $r = q + 2p = 23 + 2 \cdot 3 = 29$. A 29 prímszám, vagyis ez jó megoldás. A keresett szorzat: $3 \cdot 23 \cdot 29 = 2001$.

49. A feltétel miatt valamelyik prím a 2. Ha $p_4 = 2$, akkor $(p_1 + p_2 + p_3)^2 = 235$. Ez nem lehet, mert a 235 nem négyzetszám. Legyen $p_1 < p_2 < p_3, és\ p_1 = 2$. Ezt beírva az eredeti egyenlőségbe:

$$(2 + p_2 + p_3)^2 - p_4^2 = 231$$

$$(2 + p_2 + p_3 + p_4)(2 + p_2 + p_3 - p_4) = 231$$

A $231 = 3 \cdot 7 \cdot 11$, ezért a kéttényezős szorzat négy esetet ad:

<u>1. eset:</u> $231 \cdot 1$. Ha $2 + p_2 + p_3 + p_4 = 231$ $és$ $2 + p_2 + p_3 - p_4 = 1$, akkor a kettő különbsége: $2p_4 = 230, azaz\ p_4 = 115$. Ez nem prím, tehát nem lehetséges.

<u>2. eset:</u> $77 \cdot 3$. Ha $2 + p_2 + p_3 + p_4 = 77$ $és$ $2 + p_2 + p_3 - p_4 = 3$, akkor a kettő különbsége: $2p_4 = 74, azaz\ p_4 = 37$, ami prímszám. Ekkor $p_2 + p_3 = 38$.

$p_2 = 3$ nem lehetséges, mert $p_3 = 35$ lenne, ami nem prím.

$p_2 = 5$ nem lehetséges, mert $p_3 = 33$ lenne, ami nem prím.

$p_2 = 7$ esetén $p_3 = 31$, ez jó megoldás.

$p_2 = 11$ nem lehetséges, mert $p_3 = 27$ lenne, ami nem prím.

$p_2 = 13$ nem lehetséges, mert $p_3 = 25$ lenne, ami nem prím.

$p_2 = 17$ nem lehetséges, mert $p_3 = 21$ lenne, ami nem prím.

$p_2 = 19$ nem lehetséges, mert $p_3 = 19$, ami nem különböző prím.

3. eset: $33 \cdot 7$. Ha $2 + p_2 + p_3 + p_4 = 33$ és $2 + p_2 + p_3 - p_4 = 7$, akkor a kettő különbsége: $2p_4 = 26, azaz\ p_4 = 13$, ami prímszám. Ekkor $p_2 + p_3 = 18$.

$p_2 = 3$ nem lehetséges, mert $p_3 = 15$ lenne, ami nem prím.

$p_2 = 5$ nem lehetséges, mert $p_3 = 13$, ami nem különböző prím.

$p_2 = 7$ esetén $p_3 = 11$, ez jó megoldás. Több eset nincs.

4. eset: $21 \cdot 11$. Ha $2 + p_2 + p_3 + p_4 = 21$ és $2 + p_2 + p_3 - p_4 = 11$, akkor a kettő különbsége: $2p_4 = 10, azaz\ p_4 = 5$, ami prímszám. Ekkor $p_2 + p_3 = 14$.

$p_2 = 3$ esetén $p_3 = 11$, ez jó megoldás.

$p_2 = 5$ nem lehetséges, mert $p_3 = 9$ lenne, ami nem prím.

$p_2 = 7$ nem lehetséges, mert $p_3 = 7$, ami nem különböző prím.

Tehát három megoldása van a feladatnak:

$$p_1 = 2, p_2 = 7, p_3 = 11, p_4 = 13$$

$$p_1 = 2, p_2 = 7, p_3 = 31, p_4 = 37$$

$$p_1 = 2, p_2 = 3, p_3 = 11, p_4 = 5$$

50.

A kifejezésnek páratlannak kell lennie, ezért a három prím közül mindhárom páros vagy 1db páros.

Ha mindhárom páros, akkor $p = q = r = 2$. Ekkor: $2^4 + 2^4 + 2^4 - 3 = 45$, de ez nem prímszám.

Ha 1 db páros (pl. $r = 2$), akkor $p^4 + q^4 + 2^4 - 3 = p^4 + q^4 + 13$. Ezt az összeget vizsgáljuk 3-mal való oszthatóság szerint. Minden prím (a 3-at kivéve) $3k \pm 1$ alakú. Legyen $p = 3k \pm 1$ és $q = 3n \pm 1$! Ekkor:

$(3k \pm 1)^4 + (3n \pm 1)^4 + 13 = 3K + 1 + 3L + 1 + 13 = 3K + 3L + 15$, $ahol\ K, L\ egész.$

Ez az összeg osztható 3-mal. Vagyis p és q egyike nem lehet $3k \pm 1$ alakú, tehát csak a 3 lehet. Mindkettő nem lehet 3, mert ekkor $3^4 + 3^4 + 13 = 175$, ami osztható 5-tel. Legyen pl. $q = 3$! Ekkor: $p^4 + 81 + 13 = p^4 + 94$, ahol $p > 3$. A prímek negyedik hatványa az 5 kivételével 1-re végződnek. Ezért $\cdots 1 + 94 = \cdots 95$, de ez osztható 5-tel, tehát nem prím. Azt kaptuk, hogy a három prím csak a 2, 3, 5 lehet valamilyen sorrendben. Ezek megfelelnek a feladat feltételeinek, ugyanis: $5^4 + 3^4 + 2^4 - 3 = 719$, ami prímszám.

51.

A kifejezés csak akkor lesz egész szám, ha egy $k > 0$ egész esetén:

$$\frac{n+p}{n-p} = k^2$$

Alakítsuk át a kifejezést és vizsgáljuk meg mikor lesz négyzetszám:

$$\frac{n+p}{n-p} = \frac{n-p+2p}{n-p} = 1 + \frac{2p}{n-p}$$

Ez akkor lesz egész, ha az $n - p$ osztója $2p$-nek, vagyis:

$$n - p = 1, 2, p, 2p, -1, -2, -p, -2p, azaz$$

$$n = p + 1, p + 2, 2p, 3p, p - 1, p - 2, 0, -p$$

Az utolsó két eset nem lehetséges. A többi esetben:

$$\frac{n+p}{n-p} = 1 + 2p, 1 + p, 3, 2, 1 - 2p, 1 - p$$

Ezek közül a 2, 3 nem négyzetszám, az utolsó kettő pedig negatív.

Ha $1 + 2p = k^2$, akkor $2p = k^2 - 1 = (k-1)(k+1)$. Ezek értékei:

$$k - 1\text{: } 1, 2, p, 2p$$

$$k + 1\text{: } 2p, p, 2, 1$$

Ezek szerin *k* és *p* lehetséges értékei:

$$k = 2, k = 3, k = 1, k = 0$$

$$p = \frac{3}{2}, p = 2, p = 0, p = -\frac{1}{2}$$

Ekkor $n = 2,5$. Ezek közül egyik sem jöhet számításba.

Ha $1 + p = k^2$, akkor $p = k^2 - 1 = (k-1)(k+1)$. Ezek értékei:

$$k - 1 = 1 \text{ és } k + 1 = p, vagy\ k - 1 = p \text{ és } k + 1 = 1$$

A második esetben nem kapunk megoldást. Az első esetben $k = 2$ és $p = 3$. Ekkor:

$$\frac{n+3}{n-3} = 4$$

Ebből $n = 5$. A feladat megoldása: $p = 3$ és $n = 5$.

52.

Az $r < q < p$ prímek számtani sorozatot alkotnak, melynek differenciája 8. Vagyis

$q = r + 8$ és $p = r + 16$. Vizsgáljuk meg a prímeket 3-mal való oszthatóságra!

Ha *r* 3-mal osztva 1 maradékot ad, azaz $r = 3k + 1$ alakú, akkor

$$q = r + 8 = 3k + 9 = 3(k + 3)$$

Tehát *q* osztható lenne 3-mal, ami nem lehetséges.

Ha *r* 3-mal osztva 2 maradékot ad, azaz $r = 3k + 2$ alakú, akkor

$$p = r + 16 = 3k + 18 = 3(k + 6)$$

Tehát *p* osztható lenne 3-mal, ami nem lehetséges.

Ha *r* 3-mal osztható, akkor $r = 3$ lehet csak. Ekkor:

$$q = r + 8 = 11 \text{ és } p = r + 16 = 19$$

Ezek mindegyike prím, tehát megfelelnek a feladat feltételeinek.

53.

Emeljük négyzetre a kifejezést, majd alakítsuk át:

$$\left(\sqrt{pq^3}+\sqrt{qp^3}\right)^2 = pq^3+qp^3+2\sqrt{p^4q^4} = pq(p^2+q^2)+2p^2q^2 =$$

$$= pq(p^2+q^2+2pq) = pq(p+q)^2 = 1134$$

Az $1134 = 2\cdot 3^4\cdot 7$, tehát két négyzetszám osztója lehet, a 9 és 81. Ezért

$$(p+q)^2 = 9\ vagy\ (p+q)^2 = 81$$

Ebből: $p+q = 3\ vagy\ p+q = 9$. A 3 nem bontható fel két prím összegére, így ez nem lehetséges. A $p+q = 9$ lehetséges, amiből $p = 7, q = 2\ vagy\ p = 2, q = 7$.

54.

Alakítsuk szorzattá a kifejezést:

$$(p_1+p_2+p_3+p_4)(p_1-p_2-p_3-p_4) = 136$$

Mivel $136 = 2^3\cdot 7$, ezért négyféleképpen bonthatjuk kéttényezős szorzattá:

1. eset: Ha $136 = 1\cdot 136$, akkor $p_1-p_2-p_3-p_4 = 1$ *és* $p_1+p_2+p_3+p_4 = 136$.

2. eset: Ha $136 = 2\cdot 68$, akkor $p_1-p_2-p_3-p_4 = 2$ *és* $p_1+p_2+p_3+p_4 = 68$.

3. eset: Ha $136 = 4\cdot 34$, akkor $p_1-p_2-p_3-p_4 = 4$ *és* $p_1+p_2+p_3+p_4 = 34$.

4. eset: Ha $136 = 8\cdot 17$, akkor $p_1-p_2-p_3-p_4 = 8$ *és* $p_1+p_2+p_3+p_4 = 17$.

Mivel $p_1+p_2+p_3+p_4+p_1-p_2-p_3-p_4 = 2p_1$ páros, így az első és negyedik eset nem lehetséges.

A 2. esetben:

$$\begin{cases} p_1-p_2-p_3-p_4 = 2 \\ p_1+p_2+p_3+p_4 = 68 \end{cases}$$

Ebből $2p_1 = 70$, vagyis $p_1 = 35$. Ez nem prímszám, tehát nem lehetséges.

A 3. esetben:

$$\begin{cases} p_1 - p_2 - p_3 - p_4 = 4 \\ p_1 + p_2 + p_3 + p_4 = 34 \end{cases}$$

Ebből $2p_1 = 38$, vagyis $p_1 = 19$. Ekkor $p_2 + p_3 + p_4 = 15$. A 15-öt fel tudjuk bontani három prím összegére: $15 = 3 + 5 + 7$. Tehát a kérdezett szorzat: $3 \cdot 5 \cdot 7 \cdot 19 = 1995$.

55.

A három szám közül az egyik mindig osztható 3-mal. Vizsgáljuk meg a 3-mal való oszthatóságokat!

Ha $n = 3$, akkor $n + 2 = 5$ *és* $n + 4 = 7$. Ez jó megoldás.

Ha $n \neq 3$, akkor három eset lehetséges:

1. $n = 3k$. Ekkor *n* nem prímszám.

2. $n = 3k + 1$. Ekkor $n + 2 = 3(k + 1)$, vagyis nem prímszám.

3. $n = 3k + 2$. Ekkor $n + 4 = 3(k + 2)$, vagyis nem prímszám.

56.

Vizsgáljuk meg az 5-tel való oszthatóságokat!

Ha $n = 5$, akkor $n + 6 = 11, n + 12 = 17, n + 18 = 23, n + 24 = 29$. Ez jó megoldás.

Ha $n \neq 5$, akkor öt eset lehetséges:

1. $n = 5k$. Ekkor *n* nem prímszám.

2. $n = 5k + 1$. Ekkor $n + 24 = 5k + 25 = 5(k + 5)$, vagyis nem prímszám.

3. $n = 5k + 2$. Ekkor $n + 18 = 5k + 20 = 5(k + 4)$, vagyis nem prímszám.

4. $n = 5k - 2$. Ekkor $n + 12 = 5k + 10 = 5(k + 2)$, vagyis nem prímszám.

5. $n = 5k - 1$. Ekkor $n + 6 = 5k + 5 = 5(k + 1)$, vagyis nem prímszám.

57.

Vizsgáljuk meg az 5-tel való oszthatóságokat!

Ha $n = 7$, akkor $n^3 - 6 = 337, n^3 + 6 = 349$. Ez jó megoldás.

Ha $n \neq 7$, akkor három eset lehetséges:

1. $n = 7k$. Ekkor *n* nem prímszám.

2. $n = 7k + 1\ vagy\ n = 7k + 2\ vagy\ n = 7k + 4$. Ekkor $n^3 + 6 = 7m$, vagyis nem prímszám.

3. $n = 7k + 3\ vagy\ n = 7k - 2\ vagy\ n = 7k - 1$. Ekkor $n^3 - 6 = 7l$, vagyis nem prímszám.

58.

A kifejezést alakítsuk szorzattá:

$$n^3 - n + 3 = n(n^2 - 1) + 3 = n(n - 1)(n + 1) + 3$$

Az $n - 1, n, n + 1$ három egymást követő pozitív természetes szám, tehát valamelyik osztható 3-mal. Tehát az $n^3 - n + 3$ kifejezés az *n*-től függetlenül mindig osztható 3-mal. Az egyetlen megoldás $n = 1$, mert $n^3 - n + 3 = 3$. Más megoldás nincs, mert 1-től nagyobb *n* esetén $n^3 - n + 3 > 3$ és osztható 3-mal, vagyis összetett szám.

59.

A kifejezést alakítsuk szorzattá:

$$n^8 + n^6 + n^4 + n^2 + 1 = (n^4 + n^2 + 1)^2 - n^6 - 2n^4 - n^2 =$$

$$= (n^4 + n^2 + 1)^2 - (n^3 + n)^2 = (n^4 - n^3 + n^2 - n + 1)(n^4 + n^3 + n^2 + n + 1)$$

Tehát a kifejezés általában nem lesz prímszám, mert két szám szorzatára bontható. Akkor lehet csak prím, ha az egyik tényező 1, a másik pedig prímszám. Ez csak úgy lehetséges, ha

$n^4 - n^3 + n^2 - n + 1 = 1$. Ezt átalakítva:

$$n^4 - n^3 + n^2 - n = n^3(n - 1) + n(n - 1) = (n^3 + n)(n - 1) = n(n^2 + 1)(n - 1) = 0$$

Ez akkor teljesül, ha $n = 1$. Ekkor $n^8 + n^6 + n^4 + n^2 + 1 = 5$, ami prímszám. Minden más n-re összetett szám lesz.

Megjegyzés: Az ilyen típusú feladatokban az egyik leggyakoribb módszer a szorzattá alakítás. Ha egy kifejezést szorzattá alakítottunk, akkor az általában nem lesz prímszám, néhány kivételtől eltekintve. Ezeket a kivételeket megvizsgálva, könnyen adódik a megoldás.

7.2 Bizonyítsuk be, hogy…

1.

Igazoljuk, hogy az $a = 4k^4, ahol\ 1 < k, és\ k \in N$ alakú számokra igaz az állítás.

Megmutatjuk, hogy az $n^4 + 4k^4$ szám felbontható két egész szám szorzatára, melyek egyike sem egyenlő 1-gyel, azaz nem prímszám.

$$b = n^4 + 4k^4 = (n^2 + 2k^2)^2 - 4n^2k^2 = (n^2 + 2k^2 - 2nk)(n^2 + 2k^2 + 2nk)$$

Itt a kisebbik tényezőre:

$$(n^2 + 2k^2 - 2nk) = (n - k)^2 + k^2 \geq 1$$

Az egyenlőség csak $n = k = 1$ esetén áll fenn. Tehát végtelen sok k $és$ $a = 4k^4$ szám felel meg az állításnak.

2.

Indirekt bizonyítjuk be. Tegyük fel, hogy $8p + 1$ négyzetszám. Ekkor ez egy páratlan szám négyzete:

$$8p + 1 = (2n + 1)^2$$

Mivel $3 < p, ezért\ 3 \leq n$ teljesül. Ebből:

$$8p = 4n^2 + 4n = 4n(n + 1)$$

$$p = \frac{n(n + 1)}{2}$$

Az n és $n+1$ közül az egyik páros és a fele egész. Így a *p* prímszámot két természetes szám szorzatára bontottuk, és $3 \leq n$ miatt mindkét tényező nagyobb 1-től. Ez ellentmondás, tehát a feltevés helytelen.

3.

A feltétel szerint $\frac{a}{c} = \frac{d}{b}$. Legyen a tovább már nem egyszerűsíthető alakja $\frac{u}{v}$. Legyen *j* és *k* az a természetes szám amivel egyszerűsítettünk. Felírható a következő:

$$a = ju, \qquad c = jv, \qquad d = ku, \qquad b = kv\,.$$

Eszerint:

$$a + b + c + d = j(u + v) + k(u + v) = (j + k)(u + v)$$

Ez pedig egy összetett szám, mert mindkét tényező értéke legalább 2. Ebből következik, hogy ha *x, y, u, v* olyan természetes számok, amelyekre $xy = uv$ és *n* tetszőleges természetes szám, akkor $(x^n + y^n + u^n + v^n)$ összetett szám. Ugyanis, ha $xy = uv$, akkor $x^n y^n = u^n v^n$, tehát az $a = x^n,\ b = y^n,\ c = u^n,\ d = v^n$ számokra alkalmazható az előző állítás.

4.

Tegyük fel, hogy ez a szám racionális. Ez azt jelentené, hogy a tizedes tört szakaszos lenne, azaz volna olyan *k* természetes szám, hogy a tizedes tört alakban egy helytől kezdve *k* egymás utáni számjegy rendre megegyezne az utána következő *k*-val, és így tovább.

Csebisev tétele értelmében minden prímszám és a kétszerese között van prímszám. Ebből többek között az is következik, hogy bármely *n* természetes számra van legalább két darab

n-jegyű prímszám. Válasszuk *n*-et *k* többszörösére úgy, hogy két *n*-jegyű prímszám már a tizedes tört szakaszos részére essen. Ezt elég nagy többszörös esetén mindig megtehetjük.

A szakaszosság miatt az első prímszám minden számjegye, mivel *n* többszöröse *k*-nak, megismétlődik. Ez azt jelenti, hogy a két prímszám azonos jegyekből áll, azaz azonos. Ez nem lehet igaz, így az a feltevésünk, hogy a felírt tizedes tört racionális, helytelen. Tehát a szám irracionális.

5.

Legyen $\left[\frac{n}{p}\right] = k, ekkor\ n = kp + m,\ \ ahol\ k, m\ egészek\ és\ 0 \leq m < p$. Azt kell bizonyítani, hogy $\binom{n}{p}\ \ p - vel\ osztva\ k$ maradékot ad.

$$\binom{n}{p} = \frac{(kp+m)(kp+m-1)\cdots kp\cdots(kp+m-p+1)}{p!} =$$

$$= k \cdot \frac{(kp+m)\cdots(kp+1)(kp-1)\cdots(kp+m-p+1)}{(p-1)!}$$

A számlálóban eredetileg *p* darab egymás után következő szám állott, ezek maradékai *p*-vel osztva mind különbözőek, tehát valamilyen sorrendben *0,1,2,…,p-1*. Közülük a *p*-vel osztható maradt ki, ezért a kifejezés így alakítható:

$$\binom{n}{p} = k \cdot \frac{qp + (p-1)!}{(p-1)!} = \frac{kqp}{(p-1)!} + k$$

Ez *p*-vel osztva valóban *k*-t ad maradékul, hiszen az összeg első tagja osztható *p*-vel mivel egész szám és nevezője relatív prím *p*-hez.

6.

Az 1-től balra lefelé induló átlóban a páratlan négyzetszámok szerepelnek, ugyanis mindegyik szám egy 1 középpontú, páratlan oldalszámú négyzet utolsó kockájában szerepel. A 9-es oszlopában álló számok közül a 10 az előző saroktól egy, a 27 kettő, az 52 három mezőre van. Általában a $(2k+1)^2$ sorszámú saroktól *k* mezővel kell továbbmenni. Így a 9-es alatti oszlopban lévő számok $(2k+1)^2 + k = (k+1)(4k+1), ahol\ 1 \leq k,$ két 1-nél nagyobb egész szám szorzataként írható fel, azaz nem prímek. A 24-es alatti oszlopban a 26-tal kezdve az 1-gyel kisebb számok állnak, vagyis a $(2k+1)^2 + k - 1 = k(4k+5)\ ahol\ 2 \leq k$. A $25 = 5 \cdot 5$ szintén összetett szám. Tehát igaz az állítás. Hasonló módon bizonyítható, hogy a 284 alatti oszlopban, a 14-estől és az 55-östől jobbra lévő sorban szintén nincs prímszám.

7.

A $3 < p$ prímszám mindkét szomszédja páros, tehát osztható 2-vel.

A $p-1,\ p,\ p+1$ egymást követő három természetes szám, tehát valamelyik osztható 3-mal. Mivel a p prím, az egyik szomszédja osztható 3-mal.Egy szám akkor osztható 6-tal, ha osztható 2-vel és 3-mal. Ezzel az állítást igazoltuk.

8.

1, Ha $p < 30$: Az állítás igaz.

2, Ha $30 < p$: Ekkor p-ből levonjuk a 30 egy alkalmas többszörösét. ($p - 30k = maradék$) Mivel 30 $osztható\ 2-vel, 3-mal$ és $5-tel, p$ viszont egyikükkel sem, így a maradék sem lehet ezekkel osztható. Tehát ugyanannyi maradékot ad $2-vel, 3-mal, 5-tel$ osztva, mint p . A maradékok a következők lehetnek: $1, 7, 11, 13, 17, 19, 23, 29$. Ezzel az állítást igazoltuk.

9.

Mivel p és q 3-nál nagyobb iker prímek, ezért a köztük lévő szám osztható 6-tal. Tehát a p és q számokat $6k+1\ illetve\ 6k-1$ alakban írhatjuk fel, ahol *k* egész szám. Hasonlóan *r* és *s* is $6l+1\ illetve\ 6l-1$ alakú, ahol *l* egész szám. A p és *r* 6-tal osztva vagy ugyanazt a maradékot adják vagy nem. A két lehetséges eset közül elég az egyiket vizsgálni a 12-vel való oszthatóságra, mert a másik eset csak -1-szeres szorzóban tér el.

$$A = (6k+1)(6l+1) - (6k-1)(6l-1)$$

$$B = (6k+1)(6l-1) - (6k-1)(6l+1)$$

A műveletek elvégzése után:

$$A = 12(k+l)$$

$$B = 12(l-k)$$

Mivel *k* és *l* egész számok, az *A* és *B* is osztható 12-vel.

10.

Ha a és b nem relatív prímek, akkor van egy közös k prímosztójuk. Mivel k osztja b-t, osztja a p, q, r számok egyikét. Tételezzük fel, hogy k a p osztója. Ekkor az $a - p(q + r)$ különbség mindkét tagja osztható k-val, tehát a vele egyenlő qr szorzat is osztható k-val. Vagyis q és r egyike osztható k-val. Ezzel beláttuk, hogy a p, q, r számok nem relatív prímek. Tehát ha p, q, r számok páronként relatív prímek, akkor a és b relatív prímek.

Ha a p, q, r számok közül mondjuk p-nek és q-nak van egy közös k prímosztója, akkor a $q(p + r) + pr$ összeg, azaz az a is osztható k-val. Viszont k-val osztható a $b = pqr$ szorzat is, tehát a és b nem relatív prímek. Tehát az állítás megfordítása is igaz.

11.

Azt kell belátni, hogy az $a_n - 1 = 5^{2^{n-1}} - 1$ számnak legalább n darab különböző prímosztója van. Teljes indukcióval bizonyítjuk.

1. Az $n = 1$ esetén az állítás igaz.

2. Tegyük fel, hogy $n = k$ esetén igaz.

3. Lássuk be, hogy $n = k + 1$ esetén is igaz:

$$a_{k+1} - 1 = 5^{2^k} - 1 = \left(5^{2^{k-1}} - 1\right)\left(5^{2^{k-1}} + 1\right) = (a_k - 1)(a_k + 1)$$

A feltevésünk miatt az $(a_k - 1)$ számnak legalább k darab különböző prímosztója van. Azt kell még igazolni, hogy az $(a_k + 1)$ számnak van olyan prímosztója, amely nem osztója $(a_k - 1)$-nek. Igaz a következő:

$$(a_k - 1, a_k + 1) = 2$$

Nyilvánvaló, ha $(a_k - 1, a_k + 1) = d$, akkor d osztója $a^k - 1$ és d osztója $a^k + 1$ és így d osztója az $(a^k + 1) - (a^k - 1) = 2$ kifejezésnek. Mivel $a^k - 1$ és $a^k + 1$ is páros, a 2 közös osztójuk, azaz a 2 osztója d-nek, tehát $d = 2$.

Az $(a-b)$ osztója az $a^n - b^n$ kifejezésnek. Ebből következik, hogy 4 osztója a $a^k - 1$ kifejezésnek és $(a_k - 1, a_k + 1) = 2$ miatt a 4 nem osztója $a^k + 1$ kifejezésnek.

Mivel $a_k + 1 > 2$, az $(a_k + 1)$-nek a 2-n kívül kell, hogy legyen más prímosztója is,

ami $(a_k - 1, a_k + 1) = 2$ miatt $(a_k - 1)$-nek nem prímosztója.

12.

Mivel $p_1 = 2, p_2 = 3$, ezért ha $3 \leq n$, akkor $1 + p_1 p_2 \cdots p_n$ 2-vel és 3-mal osztva 1-et ad maradékul, így minden prímosztója legalább 5.

Tegyük fel az állítás ellenkezőjét, azaz a sorozat *n*-edik eleme 5.

Ekkor $1 + p_1 p_2 \cdots p_{n-1}$ legnagyobb prímtényezője 5, tehát ennek a számnak 5-től különböző prímtényezője nem lehet. Ez azt jelenti, hogy $1 + p_1 p_2 \cdots p_{n-1}$ az 5 valamilyen hatványa: $p_1 p_2 \cdots p_{n-1} = 5^k - 1$.

A jobb oldal osztható 4-gyel, mert $(a-b)$ osztója az $a^n - b^n$ kifejezésnek. A baloldalon $(n-1)$ darab prím szorzata szerepel, melyek közül az első 2, a többi pedig 2-nél nagyobb. Ez a sorozat tehát nem osztható 4-gyel. Ez ellentmondás, tehát az 5 nem eleme a sorozatnak.

13.

Indirekt módon bizonyítjuk. Legyenek az adott számok:

$a_1, a_2, \cdots, a_n, ahol\ 1 < a_i < (2n-1)^2\ és\ legyen\ a_i\ legkisebb\ prímosztója\ p_i$. Mivel a_i nem prímszám, van p_i-n kívül még prímosztója, azaz $p_i^2 \leq a_i < (2n-1)^2$. Az így kapott p_i prímek különbözőek, mert ha $p_i = p_j$ lenne, akkor p_i osztója lenne a_i-nek és a_j-nek is, de a feltétel szerint a_i és a_j relatív prímek. Tehát kapunk *n* különböző prímet, melyek kisebbek $(2n-1)$-nél. Ez lehetetlen, hiszen $1\ és\ (2n-1)$ között $(n-2)$ darab páratlan szám van, és a 2-t kivéve minden prím páratlan. Tehát $1\ és\ (2n-1)$ között legfeljebb $(n-1)$ darab különböző prímszám található, ami ellentmondás. Vagyis az állítás igaz.

14.

Két egész szám közös osztója osztja a különbségüket is. Tíz egymás utáni szám közül kettőt választva a különbség legfeljebb 9, azaz a a közös osztó is legfeljebb 9. Ha a legnagyobb közös osztó nem 1, akkor az osztható a 2, 3, 5, 7 valamelyikével, de akkor a választott számok is oszthatók. Tehát ha találunk a tíz szám között olyat, amelyik a 2, 3, 5, 7 egyikével sem osztható, akkor az a másik kilenchez relatív prím.

Tíz egymást követő szám között öt páratlan van, ezek közül legfeljebb kettő osztható 3-mal és legfeljebb egy-egy osztható 5-tel, illetve 7-tel. Mindig marad legalább egy páratlan szám, amelyik 3, 5, 7 egyikével sem osztható. Ez a szám megfelel a követelményeknek.

15.

A tizenkét szomszédos szám közül hat páros, ezek egyike sem prímszám. A tizenkettő szám között négy osztható 3-mal, melyek fele páratlan. Ez a két páratlan szám szintén nem prímszám.

16.

Egy egész szám pontosan akkor nem prímhatvány, ha van két relatív prím valódi osztója. Keressük az *n* darab számot a következő alakban:

$$\{2 + M, 3 + M, \cdots, (n + 1) + M\}$$

Ha *k* osztója *M*-nek $2 \leq k \leq n + 1$ esetén és $M = k \cdot m_k$, akkor $k + M = k(1 + m_k)$. Ebből látszik, hogy ha *k* osztója m_k-nak, akkor is a *k* és $1 + m_k$ relatív prímek. Vagyis minden 1-től nagyobb *k* esetén a $k + M$ előáll két 1-nél nagyobb relatív prím szorzataként. Ha tehát k^2 osztója *M*-nek $2 \leq k \leq n + 1$ esetén, akkor a fenti alakban keresett számok egyike sem prímhatvány. A feltétel biztosan teljesül az $M = [(n + 1)!]^2$ választás esetén.

17.

Indirekt módon bizonyítjuk. Tegyük fel, hogy $A = 2^n - 1$ prímszám, de az *n* nem prímszám.

Legyen $n = a \cdot b, ahol\ 1 < a, b\ egész\ számok$. Ekkor:

$$A = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right)$$

Mivel $2 \leq a, ezért\ 3 \leq 2^a - 1$, a másik tényező pedig nem kisebb 5-től. Tehát az *A* összetett szám. Ez ellentmondás.

Az állítás megfordítása nem igaz. Ellenpélda: $2^{11} - 1 = 23 \cdot 89$.

18.

Ha $3 < p$, akkor 24 osztója a $p^2 - 1$ számnak, mert $p^2 - 1 = (p-1)(p+1)$ és mivel 3 nem osztója *p*-nek, ezért $p - 1 és\ p + 1$ közül az egyik osztható 3-mal. A *p* páratlan szám négyzete 8-cal osztva 1 maradékot ad, tehát a 8 osztója a $p^2 - 1$ számnak. Mivel $(3, 8) = 1$, ezért a 24 osztója a $p^2 - 1$ számnak.

19.

Legyen $p - 1 és\ p + 1$ ikerprímek, ahol $6 < p$. A két ikerprím összege $2p$, amiről be kell látni, hogy osztható 12-vel. Mivel *p* páros, ezért 4 osztója $2p$-nek. A $p - 1 és\ p + 1$ prímszámok, tehát 3 osztója *p*-nek. A $(3, 4) = 1$, ezét a 12 osztója $2p$-nek.

20.

A $p = \frac{a^3+b^3}{2}$ egész szám és 4-gyel nem osztható, tehát *a* és *b* páratlan számok. Ezért a

$c = \frac{a+b}{2}$pozitív egész szám. Alakítsuk *p*-t szorzattá és felhasználva a $b = 2c - a$ helyettesítést a következőt kapjuk:

$$p = c(3a^2 - 6ac + 4c^2) = c[3(c-a)^2 + c^2]$$

Ha $c \neq 1$, akkor $0 \leq 3(c-a)^2 + c^2 \neq 1$. Ebből következik, hogy *p* nem prím. Tehát $c = 1$. Ekkor $p = 3a^2 - 6a + 4, illetve\ p = 3b^2 - 6b + 4$. Így beláttuk azt is, hogy $a + b = 2$ és mivel *a* és *b* pozitív egészek, ezért $a = b = 1$. Vagyis $\frac{a^3+b^3}{2} = 1$, ez pedig nem prímszám. Tehát nincs olyan *a* és *b* természetes szám, melyekre az $\frac{a^3+b^3}{2}$ prím lenne.

Az előző érvelés akkor is igaz, ha *a* és *b* egész számok. Ebben az esetben már van megoldás. Például $a = 3, b = -1$.

21.

Az 1999 páros kitevőjű hatványa 1-re végződik. Ha ehhez a számhoz hozzáadunk 2014-et, akkor olyan számot kapunk, amely 5-re végződik, vagyis osztható 5-tel.

22.

A gyökjel alatti szám a következő alakban is felírható:

$$225 \cdot 10^{2k} - 10^{k+2} + 10^{k+1} + 9 = 225 \cdot 10^{2k} - 10^k(100 - 10) + 9 = (15 \cdot 10^k - 3)^2$$

Tehát:

$$A - 3 = 15 \cdot 10^k - 3$$

Ebből:

$$A = 15 \cdot 10^k$$

Ez pedig csak a 2, 3, 5 prímtényezőket tartalmazza.

23.

Legyen $p_1, p_2, \cdots, p_n$ prímszámok. Ekkor:

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} = \frac{p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}}{p_1 p_2 \cdots p_n}$$

A tört számlálója nem osztható p_1-gyel, mert az első tag nem osztható vele. Hasonlóan belátható, hogy a tört $p_2,\ p_3, \cdots, p_n$ prímek egyikével sem osztható. Tehát a tekintett összeg nem lehet egész szám. Ha $2 \leq n$, akkor a számláló nem lehet 1, tehát a keresett összeg nem lehet egész szám reciproka sem.

24.

Alakítsuk át a kifejezést az alábbi módon:

$$p^4 - 5p^2 + 4 = (p^2 - 4)(p^2 - 1) = (p - 2)(p + 2)(p - 1)(p + 1) \text{ és } 360 = 2^3 \cdot 3^2 \cdot 5$$

Elég azt belátni, hogy $3^2 \cdot 5$ osztója a $p^4 - 5p^2 + 4$ kifejezésnek.

25.

Indirekt módon bizonyítjuk.

1. Tegyük fel, hogy $\sqrt{p} = \frac{a}{b}, ahol\ (a,b) = 1\ és\ b \neq 0$. Ekkor:

$$pb^2|a^2 és\ p|a\ és\ p^2|a^2\ és\ p^2|pb^2\ és\ p|b^2\ és\ p|b$$

A $p|a\ és\ p|b$ ellentmond a feltételben szereplő $(a,b) = 1$ kikötésnek, tehát $\sqrt{p}$ irracionális.

2. Tegyük fel, hogy $\sqrt{p \cdot q} = \frac{a}{b}, ahol\ (a,b) = 1\ és\ b \neq 0$. Ekkor:

$$pqb^2|a^2 és\ p|a\ és\ p^2|a^2\ és\ p^2|pqb^2\ és\ p|qb^2$$

$$és\ mivel\ p\ nem\ osztója\ q-nak, ezért\ p|b^2\ és\ p|b$$

A $p|a\ és\ p|b$ ellentmond a feltételben szereplő $(a,b) = 1$ kikötésnek, tehát $\sqrt{p \cdot q}$ irracionális.

26.

1. Amennyiben $\sqrt{p^2+1}$ racionális szám, akkor egész szám is, azaz $\sqrt{p^2+1} = a > 0$. Tehát $p^2 = a^2 - 1 = (a-1)(a+1), azaz\ (a-1)|p^2, ebből\ a-1 = p\ vagy\ a-1 = 1.$ Mindkét esetben ellentmondáshoz jutunk, hiszen $p^2 = p(p+2)\ illetve\ p^2 = 2 \cdot 3$ adódik.

2. Ha $\sqrt{p^2-1} = b > 0$ igaz lenne, akkor $b^2 = p^2 - 1$ miatt $b^2 < p^2, b < p$ teljesülne. Másrészt $(p-1)^2 < p^2 - 1, ha\ 1 < p$. Tehát $(p-1)^2 < b^2, (p-1) < b$. Ez pedig ellentmondáshoz vezet, ugyanis $p-1 < b < p$ egész számok esetén nem lehetséges.

27.

Ha *n* páratlan, akkor $2^n + 1 = (2+1)(2^{n-1} - 2^{n+2} \pm \cdots \pm 2^0)$. Ekkor $2^n + 1$ osztható lenne 3-mal, tehát $2^n + 1$ csak úgy lehet prím, ha $2^n + 1 = 3$ vagy *n* páros szám. Az *n*-nek nem lehet 2-nél nagyobb prímosztója, ugyanis ha $2 < p\ és\ p|n\ azaz\ n = p \cdot k, k \neq 0$, akkor $2^n + 1 = (2^k)^p + 1 = (2^k+1)((2^k)^{p-1} - (2^k)^{p-2} \pm \cdots \pm 1)\ miatt\ 2^k + 1|2^n + 1$ lenne. Tehát az *n* prímtényezős felbontásában csak a 2 szerepelhet, azaz $n = 2^l$.

28.

A $p-1$ és $p+1$ számok párosak és valamelyikük osztható 3-mal.

1. Ha $3|p-1$, akkor $p-1=3k, ahol\ k=1,2,\cdots$. Mivel $p-1$ páros, ezért $k=2n$ alakú, ahol $n=1,2,\cdots$, azaz $p-1=3(2n)=6n$. Ebből $p=6n+1$.

2. Hasonlóan látható be a $3|p+1$ eset is.

29.

Először lássuk be, hogy létezik két olyan *x* és *y* egész szám, melyekre $x^2-y^2=p$.

Az $x^2-y^2=(x-y)(x+y)=p$. Négy esetet különböztethetünk meg:

1. $x-y=1$ és $x+y=p$

2. $x-y=p$ és $x+y=1$

3. $x-y=-1$ és $x+y=-p$

4. $x-y=-p$ és $x+y=-1$

Minden esetben a következőt kapjuk:

$$x^2=\frac{p^2+2p+1}{4}\ \text{és}\ y^2=\frac{p^2-2p+1}{4}$$

A megoldásból az is látszik, hogy x^2 és y^2 egyértelmű.

30.

A $2^n-1, 2^n, 2^n+1$ három szomszédos természetes szám, tehát valamelyikük osztható

3-mal. Mivel 2^nnem osztható 3-mal, így 2^n-1 és 2^n+1 közül az egyik osztható 3-mal, tehát egyszerre nem prímszámok.

31.

Induljunk ki a következő egyenlőségből:

$$2^{pq} - 2 = 2^{pq} - 2^p + 2^p - 2 = [(2^p)^q - 2^p] + (2^p - 2) \cdots \qquad (1)$$

A feltevés szerint $2^{pq} - 2$ osztható q-val, illetve a Fermat-tétel szerint $a^p - a$ osztható a p prímszámmal. Tehát az (1) jobb oldalán ha $a = 2^p$, akkor $(2^p)^q - 2^p$ osztható q-val. Ebből következik, hogy az (1) jobb oldalának második része, $(2^p - 2)$ osztható q-val. Azonban szintén a Fermat-tétel szerint $(2^p - 2)$ osztható p-vel is, így $(2^p - 2)$ osztható a pq szorzattal is. Mivel:

$$2^{pq} - 2 = 2^{pq} - 2^q + 2^q - 2 = [(2^q)^p - 2^q] + (2^q - 2) \cdots \qquad (2)$$

Ezért hasonló gondolatmenettel bizonyítható, hogy $(2^q - 2)$ is osztható a pq szorzattal.

32.

A kifejezést a következő alakban is felírhatjuk:

$$p(x + y) = 2xy$$

A jobb oldalon álló szorzat osztható p-vel, tehát x vagy y osztható p-vel. Mivel x és y szimmetrikusan szerepelnek az összefüggésben, akármelyik esetet vehetjük. Tegyük fel, hogy y a p többszöröse, azaz $y = kp$. Ekkor a $p(x + kp) = 2xkp$ egyenletből:

$$x = \frac{kp}{2k - 1}$$

Ha $k = 1$, akkor $y = x = p$, de ezt kizártuk.

Ha $k > 1$, akkor k $és$ $2k - 1$ számoknak nem lehet közös osztójuk, tehát $2k - 1$ a p osztója kell, hogy legyen. Azaz $2k - 1 = 1$ $vagy$ $2k - 1 = p$. Azonban $2k - 1 = 1$esetben $k = 1$, de ezt kizártuk. Ezek szerint $2k - 1 = p$, illetve $k = \frac{p+1}{2}$ az egyedüli lehetőség. Ekkor:

$$x = \frac{p + 1}{2} \text{ és y} = \frac{p(p + 1)}{2}$$

Ellenőrzés:

$$\frac{2}{p}=\frac{1}{\frac{p+1}{2}}+\frac{1}{\frac{p(p+1)}{2}}=\frac{2}{p+1}+\frac{2}{p(p+1)}=\frac{2}{p+1}\left(1+\frac{1}{p}\right)=\frac{2}{p+1}\cdot\frac{p+1}{p}=\frac{2}{p}$$

33.

Ha $n-1$ és $n+1$ prímek, akkor *n* páros szám és mivel három egymás után következő szám egyike osztható 3-mal, ezért *n* osztható 3-mal, tehát *n* osztható 6-tal, kivéve ha

$n-1=3\ vagy\ n+1=3.$

Továbbá *n* vagy többszöröse 5-nek vagy nem. Az első esetben *n* osztható 30-cal is, kivéve, ha $n=6$. A második esetben, mivel az öt egymásután következő $n-2, n-1, n,$

$n+1, n+2$ számok egyike osztható 5-tel, vagy $n-2$ vagy $n+2$ osztható 5-tel. Tehát vagy $n-12$ vagy $n+12$ is osztható 5-tel. Azonban *n* osztható6-tal, ezért $n-12$ és $n+12$ is osztható 6-tal, azaz $n-12$ vagy $n+12$ osztható 30-cal. Amint láttuk, az állítás csak akkor igaz, ha $n\neq 2, n\neq 4, n\neq 6$.

34.

Legyen $x<n$, mely *n*-hez relatív prím, vagyis $(x,n)=1$. Ha *x* páratlan szám, akkor $(x,2\,n)=1$. Ha *x* páros szám, akkor $(x,2n)=2$. Azonban most $(x+n)$ páratlan és $(x+n,2n)=1$, tehát vagy *x* vagy $(x+n)$ a $2n$-hez relatív prím. Ezekkel viszont kimerítettük a $2n$-hez relatív prímszámokat, mert ha $y\ (ahol\ y<n)$ az *n*-hez nem relatív prím, akkor sem *y* sem $y+n$ nem relatív prím a $2n$-hez.

Megfordítva: Ha $(z,2n)=1$, akkor *z* páratlan és $(z,n)=1$.

Két eset lehetséges: $z<n\ vagy\ n<z<2n$. Utóbbi esetben $(z-n)$ az *n*-nél kisebb páros szám, úgy hogy $(z-n,n)=1$.

35.

1. Ha egy p prímszám az a, b, c relatív prímszámok szorzatának osztója, akkor p az a, b, c számok csakis az egyikét osztja. Tegyük fel, hogy p az a osztója. Ekkor p az $ab + bc + ac$ összeg két tagját osztja, de nem osztója a bc tagnak, tehát nem lehet osztója az $ab + bc + ac$ összegnek sem. Így bármely p prímszám, mely az abc szorzatnak osztója, nem osztója az $ab + bc + ac$ összegnek, vagyis valóban relatív prímek.

2. Tegyük fel, hogy abc és $ab + bc + ac$ relatív prímek. Ebből következik, hogy az abc szorzat bármely két tényezője relatív prímszám. Ugyanis, ha pl. a és b számoknak volna közös osztójuk, akkor ez osztaná az abc szorzatot és a háromtagú összeg mindegyik tagját, tehát az összeget is. Azaz a feltevéssel ellenkező eredményre jutnánk.

36.

A prímszámok egyike sem lehet 3. Ugyanis, ha $p \neq 3$ prímszám és $q = 3$, akkor a $p^2 - 9$ nem osztható 3-mal, tehát nem osztható 24-gyel sem. A kifejezést alakítsuk át a következő módon:

$$p^2 - q^2 = (p^2 - 1) - (q^2 - 1)$$

Ha p a 3-tól különböző prímszám, akkor $(p^2 - 1)$ osztható 24-gyel. Ugyanis:

$(p^2 - 1) = (p - 1)(p + 1)$, ahol $(p - 1)$ és $(p + 1)$ két egymás utáni páros szám, tehát egyikük osztható 4-gyel, a szorzatuk pedig 8-cal. Mivel a p nem osztható 3-mal a $(p - 1)$ vagy $(p + 1)$ a 3 többszöröse, tehát szorzatuk osztható 3-mal. Hasonló módon belátható, hogy a $(q^2 - 1)$ is osztható 24-gyel, vagyis az állítás igaz.

37.

A 3-nál nagyobb számokból álló ikerpár két szomszédos 3-mal nem osztható páratlan szám. Mivel három szomszédos szám közt mindig van páros és 3-mal osztható, az ikerpárokat elválasztó számok 6-tal oszthatók. Két iker prímszám összege a közéjük eső szám duplája, tehát osztható 12-vel.

38.

Mivel *a, b, c* három egymást követő szám, ezért $a = b - 1$ *és* $c = b + 1$. Ezért:

$$b^2 - a^2 = (b - a)(b + a) = 2b - 1$$

$$c^2 - b^2 = (c - b)(c + b) = 2b + 1$$

Két szám közös osztója a két szám különbségének is osztója. Ebben az esetben a különbség 2, de ez nem lehet közös osztó, mert mindkét szám páratlan. Tehát a $2b - 1$ és $2b + 1$ valóban relatív prímek.

39.

Két iker prímszámmal szomszédos három szám, három egymás után következő páros szám, melyek közül legalább egy 4-gyel osztható. A három szomszédos szám a két iker prímszámmal együtt öt egymás után következő szám, melyek közül legalább egy osztható

3-mal, és egy 5-tel. Mivel ezek az osztható számok nem lehetnek 7-nél nagyobb prímszámok, ezért kell, hogy a három szomszédos szám közül legyen 3-mal, illetve 5-tel osztható szám. Mivel a 2, 3, és 5 relatív prímszámok, ezért a három szomszédos szám szorzata biztosan osztható $4 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 240$-nel.

40.

A sorozat negyedik, illetve ötödik tagja sem lesz prímszám.

$$3337 = 47 \cdot 71 \ , \ \ 33337 = 17 \cdot 37 \cdot 53$$

Belátjuk, hogy a sorozat végtelen sok összetett számit tartalmaz. Mivel 333333 osztható 7-tel, ezért $3333337 = 10 \cdot 333333 + 7$ is osztható 7-tel. A sorozatnak azok a tagjai, melyek alakja az alábbi, szintén oszthatók 7-tel:

$$\underbrace{333333}_{6db}\underbrace{333333}_{6db}\cdots\underbrace{333333}_{6db}7$$

41.

Egy egész szám pontosan akkor nem prímhatvány, ha van két relatív prím valódi osztója. Keressük az *n* darab számot a következő alakban:

$$\{2 + M, 3 + M, \cdots, (n + 1) + M\}$$

Ha *k* osztója *M*-nek $2 \leq k \leq n + 1$ esetén és $M = k \cdot m_k$, akkor $k + M = k(1 + m_k)$. Ebből látszik, hogy ha *k* osztója m_k-nak, akkor is a *k* és $(1 + m_k)$ relatív prímek. Vagyis minden

1-nél nagyobb *k* esetén a $k + M$ előáll két 1-nél nagyobb relatív prím szorzataként.

Ha tehát k^2 osztója *M*-nek $2 \leq k \leq n + 1$ esetén, akkor a fenti alakban keresett számok egyike sem prímhatvány. A feltétel biztosan teljesül az alábbi választás esetén:

$$M = [(n + 1)!]^2$$

42.

Azt kell belátni, hogy *p* pontosan akkor összetett szám, ha léteznek olyan *a, b, c, d* pozitív egész számok, melyekre teljesül a következő: $p = a + b + c + d$ és $ab = cd$.

1. Ha léteznek ilyen *a, b, c, d* pozitív egész számok, akkor

$pb = ab + b^2 + cb + db = cd + b^2 + cb + db = (c + b)(d + b)$.

Ha *p* prímszám lenne, akkor *p* vagy $(c + b)$-nek, vagy $(d + b)$-nek osztója lenne, de ez nem lehet, mert $p = a + b + c + d$ miatt $p > (c + b)$ és $p > (d + b)$. Tehát *p* összetett szám.

2. Ha *p* összetett szám, akkor létezik olyan $m > 1$ és $n > 1$ egész szám, melyekre $p = m \cdot n$. Ekkor: $p = (m - 1)(n - 1) + 1 + (m - 1) + (n - 1)$.

Ebben a felírásban az első két tag szorzata egyenlő a második két tag szorzatával és mind a négy tag pozitív. Vagyis létezik olyan felbontás, amit igazolni kellett.

43.

A két szám közül legyen $b > a$ és $n > |a|$ és $n > |b|$, *ahol* $b + n$ prímszám. Ekkor $1 \leq a + n \leq b + n$ teljesül. A $(b + n)$ csak eggyel és önmagával osztható, az $(a + n)$ viszont nem osztható $(b + n)$-nel, hiszen kisebb nála. Tehát az $(a + n)$ és $(b + n)$ relatív prímek. Az n számot pedig végtelen sok prímszám közül választhatjuk ki.

44.

A másodfokú egyenlet gyökei és együtthatói közötti összefüggés alapján:

$$x_1 \cdot x_2 = 1 - b \text{ és } x_1 + x_2 = -a$$

Ebből:

$$a^2 + b^2 = (x_1 + x_2)^2 + (1 - x_1 \cdot x_2)^2 = (1 + x_1^2)(1 + x_2^2)$$

Ha $b \neq 1$, akkor $x_1 \cdot x_2 \neq 0$, vagyis a fenti szorzat tényezői 1-től nagyobbak és a feltétel szerint egész számok. Tehát az $a^2 + b^2$ valóban összetett szám.

45.

Ha a két törtet lehetne egyszerűsíteni, vagyis számlálója és nevezője valamely *p* prímszámmal osztható, akkor az $a \cdot b$ szorzat osztható *p*-vel, de *a* és *b* relatív prímek, tehát vagy *a* vagy *b* osztható *p*-vel. Tegyük fel, hogy *a* osztható *p*-vel. Mivel $a \pm b$ is osztható *p*-vel ekkor *b*-nek is osztója a *p*. Azonban így *a* és *b* nem relatív prímek. Tehát nem lehet egyszerűsíteni a két törtet.

46.

Legyen az *N* összetett szám legkisebb prímosztója *p*. Ekkor: $N = p \cdot q$. A feltétel szerint: $p^3 > N = p \cdot q, vagyis\ p^2 > q$. Ha q összetett szám volna, pl $q = q_1 \cdot q_2$, akkor a feltétel értelmében $q_1 > p \text{ és } q_2 > p$. Ezek szerint $q_1 \cdot q_2 \geq p^2$ lenne, ami ellentmondás. Tehát q prímszám, ami az állítást igazolja.

47.

Mivel $a > 1 \text{ és } n > 0$, ezért $a^n + 1 \geq a + 1 > 2$, tehát $a^n + 1$ páratlan prímszám lehet. De $a^n + 1$ csak úgy lehet páratlan, ha az *a* páros. Hiába volna azonban *a* páros, az $a^n + 1$ mégsem lehetne prím, ha *n* nem volna 2 hatványa. Tegyük fel, hogy *n* nem hatványa 2-nek, azaz van legalább egy páratlan valódi osztója. Ez legyen *m*! Ekkor: $n = 2^k \cdot m$, ahol *k* nem negatív egész szám. Vagyis: $a^n + 1 = a^{2^k \cdot m} + 1 = \left(a^{2^k}\right)^m + 1^m$. Az *m*-ről feltettük, hogy páratlan. Tehát $a^n + 1$ két egyenlő páratlan kitevőjű hatvány összegeként írható fel. Ez az összeg viszont mindig osztható az alapok összegével, azaz $a^{2^k} + 1$-gyel. Tehát ha *n*-nek van egy páratlan osztója, akkor $a^n + 1$ biztosan nem lehet prímszám.

48.

Minden 3-nál nagyobb p prímszám, mivel 2-vel és 3-mal nem osztható, csak

$6k+1\ vagy\ 6k-1$ alakú lehet. Tehát:

$p^2=(6k\pm1)^2=36k^2\pm12k+1=12\cdot(3k^2\pm k)+1=12K+1$. Vagyis igaz az állítás.

49.

A *k* számmal osztva a végtelen sok prímszámot, a maradékok száma véges: $0,1,\cdots,k-1$. Ha tehát a végtelen sok prímszámot a *k*-val való osztás maradéka szerint véges számú csoportba osztjuk, akkor kell lennie legalább egy olyan csoportnak, amelyben végtelen sok prímszám található. Ezek mindegyike *k*-val való osztásnál ugyanazt az *r* maradékot adja:

$$p_1=k\cdot x_1+r, p_2=k\cdot x_2+r,\cdots,ahol\ 0\le r<k.$$

Ezen sorozat bármely két tagjának különbsége osztható *k*-val:

$$p_i-p_j=a(x_i-x_j).$$

Tehát igaz az állítás.

50.

$$290304=2^9\cdot3^4\cdot7$$

1. $p^2-1=(p-1)(p+1)$. Mivel p páratlan, ezért $(p-1)$ és $(p+1)$ két egymás után következő páros szám, melyek közül az egyik 4-gyel is osztható. Tehát p^2-1 osztható

2^3-nal. Továbbá $p-1,p,p+1$ három egymás utáni szám, vagyis az egyik biztosan osztható 3-mal, de a feltétel szerint ez nem lehet a p. Mivel 2^3 és 3 relatív prímek, ezért

p^2-1 osztható $2^3\cdot3-mal$ és így $(p^2-1)(q^2-1)$ osztható $2^6\cdot3^2-nel$.

2. $p^6-q^6=(p^2-q^2)(p^4+p^2q^2+q^4)$. Mivel p ***és*** q sem 2-vel, sem 3-mal nem osztható, ezért $p=6a\pm1, q=6b\pm1$ alakú és így:

$$p^2-q^2=(6a\pm1)^2-(6b\pm1)^2=36(a^2-b^2)\pm12(a-b)=$$
$$=12[3(a+b)\pm1](a-b)$$

Ha $(a-b)$ páros, akkor p^2-q^2 osztható 24-gyel, ha $(a-b)$ páratlan, akkor $3(a+b)\pm 1$ páros, vagyis p^2-q^2 ekkor is osztható 24-gyel. Tehát p^6-q^6 biztosan osztható 2^3-nal.

3. $p^6-q^6=(p^2-q^2)[(p^2-q^2)^2+3p^2q^2]$. Mivel a feltétel szerint

$p=3a\pm 1$ $és$ $q=3b\pm 1$ alakú, ezért:

$p^2=9a^2\pm 6a+1=3K+1$ $és$ $q=3L+1$ alakú, vagyis:

$p^2-q^2=3(K-L)$ és így $[(p^2-q^2)^2+3p^2q^2]$ is osztható 3-mal. Tehát p^6-q^6 osztható 2^3-nal.

4. Mivel *p* és *q* sem osztható 7-tel, ezért:

$$p=7a\pm 1\ vagy\ p=7a\pm 2\ vagy\ p=7a\pm 3$$

$$q=7b\pm 1\ vagy\ q=7b\pm 2\ vagy\ q=7b\pm 3$$

alakú. A binomiális tétel alapján:

$$(7k\pm 1)^6=7A+1$$

$$(7k\pm 2)^6=7B+64=7(B+9)+1$$

$$(7k\pm 3)^6=7C+729=7(C+104)+1$$

Ezek alapján:

$p^6-q^6=7D$ alakú, vagyis osztható 7-tel.

A felsorolt 1., 2., 3., 4. alapján:

$(p^2-1)\cdot(p^2-1)\cdot(p^6-q^6)$ osztható $2^6\cdot 3^2\cdot 2^3\cdot 3^2\cdot 7=2^9\cdot 3^4\cdot 7=290304$-gyel.

51.

1. Ha *n* páros szám, akkor:

$$n=2k=\underbrace{2+2+\cdots+2}_{k\ darab}$$

2. Ha *n* páratlan szám, akkor

$$n=2k+1=\underbrace{2+2+\cdots+2}_{k-1\ darab}+3$$

52.

A Csebisev-tétel szerint minden $k \geq 1$-re 10^k $és$ $2 \cdot 10^k$ számok között van prímszám, és ez olyan szám, amelynek első számjegye 1-es és $k+1$ jegyből áll. Vagyis különböző k értékekre, különböző ilyen prímeket kapunk. Tehát igaz az állítás.

53.

A Csebisev-tétel szerint: Ha $n \geq 2$ egész szám, akkor létezik olyan p prímszám, amelyre

$n < p < 2n$ teljesül. Ezek alapján p_n $és$ $2p_n$ között lennie kell prímszámnak, vagyis

$$p_{n+1} < 2 \cdot p_n$$

54.

Az előző feladatban szereplő Csebisev-tételt alkalmazzuk, és teljes indukcióval bizonyítunk.

1. Ha $n = 2$, akkor $p_2 = 3 < 2^2 = 4$. Ez igaz.

2. Tegyük fel, hogy $n = k$ esetén igaz. Vagyis: $p_k < 2^k$, ahol $k \geq 2$.

3. A Csebisev-tétel szerint 2^k $és$ 2^{k+1} között létezik prímszám, amely nagyobb, mint p_k. Tehát igaz az alábbi egyenlőtlenség:

$$p_{k+1} < 2^{k+1}$$

55.

Legyen $a, a+d, a+2d, \cdots, a+nd, \cdots$ egy számtani sorozat, ahol $a > 1$ $és$ $d \geq 0$.

Ha $d = 0$, akkor lehet minden tag prímszám, pl. $3, 3, 3, \cdots$. Ha $d > 0$, akkor lesz egy

$a + ad = a(1+d)$ tagja, ami összetett szám. Tehát nem lehet minden tagja prímszám.

Megjegyzés: Ben Green és Terence Tao 2004-ben bizonyították, hogy minden $k \geq 1$ számra, a prímszámok sorozatában létezik végtelen sok k hosszúságú számtani sorozat.

56.

A Dirichlet-tétel szerint végtelen sok $15k + 7$ alakú prímszám létezik, ahol $(15,7) = 1$. Ebben az esetben $(15k + 7) - 2 = 15k + 5$ osztható 5-tel, illetve $(15k + 7) + 2 = 15k + 9$ osztható 3-mal, vagyis nem prímszám. Tehát igaz az állítás.

57.

Egy *p* prímszám különböző hatványainak utolsó számjegye legfeljebb 10-féle lehet. (Ettől kevesebb lehet, mert prímszámról van szó!) Ha vesszük *p* 11db különböző hatványát, akkor ezek között biztosan lesz kettő, amelyek utolsó számjegye azonos. Az utolsó előtti számjegy helyére is legfeljebb 10-féle számjegy kerülhet, így az utolsó két számjegy legfeljebb 10^2-féleképpen végződhet. Ha vesszük *p*-nek $10^2 + 1$ db különböző hatványát, akkor ezek között biztosan van kettő, melyek utolsó két számjegye azonos. Ezt a gondolatot folytatva: Ha vesszük *p*-nek $10^n + 1$ db különböző hatványát, amelyek legalább *n* számjegyből állnak, akkor ezek között biztosan lesz kettő olyan, amelyeknek az utolsó *n* db számjegye azonos.

Tekintsük *p*-nek $10^5 + 1$ db olyan hatványát, amelyek legalább 5 számjegyűek. Ezek között az előző indoklás szerint, kell lennie két olyannak, amelyek utolsó 5 számjegye azonos. Legyen ez a két hatvány p^k *és* p^l, ahol $k > l$. Ezek különbsége osztható 10^5-nel, vagyis

$p^k - p^l = A \cdot 10^5$, ahol A egész szám. Ezt átalakítva: $p^l(p^{k-l} - 1) = A \cdot 10^5$. Ebből látszik, hogy 10^5 osztója a bal oldali szorzatnak. Mivel $p > 5$, ezért $(p, 10) = 1$ relatív prímek, ezért p^l *és* 10^5 is azok. Ebből következik, hogy 10^5 osztója kell, hogy legyen $p^{k-l} - 1$-nek, azaz: $p^{k-l} - 1 = B \cdot 10^5$, ahol B egész szám. Ebből: $p^{k-l} = B \cdot 10^5 + 1$. Ez az egyenlőség azt jelenti, hogy p^{k-l} utolsó 5 db számjegye: 00001.

Megjegyzés: A bizonyításból látható, hogy nem csak az utolsó 5 db számjegyre, hanem tetszőleges db számjegyre is megfogalmazható a feladat.

58.

Legyen $p \geq 5$ prímszám! Ezt a prímet 12-vel osztva a maradék nem lehet páros, mert $p = 12k + 2l$ páros szám. A prímet 12-vel osztva a maradék nem lehet 3-mal osztható sem, mert $p = 12k + 3l = 3(4k + l)$ osztható 3-mal, vagyis nem prímszám.

Tehát ha egy ilyen prímet 12-vel osztunk, akkor a maradék csak 1, 5, 7, 11 lehet, vagyis minden $p \geq 5$ prímszám a következő alakba írható: $p = 12k \pm 1 \; vagy \; p = 12k \pm 5$. Ezek négyzete:

$$p^2 = (12k \pm 1)^2 = 12^2k^2 \pm 24k + 1 \; vagy \; p^2 = (12k \pm 5)^2 = 12^2k^2 \pm 120k + 25$$

Mindkét esetben a p^2-t 12-vel osztva, a maradék 1 lesz. Vagyis 12 db ilyen prím négyzetének mindegyike 12-vel osztva 1 maradékot ad, tehát ezek összege valóban osztható 12-vel.

59.

Vizsgáljuk meg az egyenlőség két oldalának paritását. Egy pozitív egész szám *n*-edik hatványa akkor és csak akkor páros, ha az alap is páros.

Ha mindkét oldal páros, akkor három eset lehetséges:

1. Mind a hat szám páros.

2. Mindkét oldalon két-két páratlan és egy-egy páros szám van.

3. Az egyik oldalon két páratlan és egy páros, a másik oldalon három páros szám szerepel.

Ha mindkét oldal páratlan, akkor is három eset lehetséges:

1. Mind a hat szám páratlan.

2. Az egyik oldalon egy páratlan szám van, a másikon pedig három páratlan.

3. Mindkét oldalon egy-egy páratlan szám szerepel.

Tehát az egyenlőség akkor teljesül, ha a megadott hat szám között a páratlan számok száma páros. Ez viszont azt jelenti, hogy az $a_1 + a_2 + a_3 + a_4 + a_5 + a_6$ összeg biztosan páros, vagyis nem lehet prímszám.

Megjegyzés: A feladatot általánosíthatjuk. Bizonyítsuk be, hogy ha

$$a_1^n + a_2^n + \cdots + a_k^n = b_1^n + b_2^n + \cdots + b_k^n$$

akkor az $a_1^n + a_2^n + \cdots + a_k^n + b_1^n + b_2^n + \cdots + b_k^n$ összeg nem lehet prímszám!

60.

Vizsgáljuk meg, hogy p^2+p+1 $és$ p^2-p+1 milyen p prímek esetén lesz szintén prímszám. A $p=2$ esetén mindkét kifejezés prím.

Minden prímszám 3-mal osztva (kivéve a $p=3$ eset), 1 vagy 2 maradékot ad.

Vagyis $p=3k+1$ $vagy$ $p=3k+2$ alakú. Ezek négyzete:

$$p^2=(3k+1)^2=9k^2+6k+1 \; vagy \; p^2=(3k+2)^2=9k^2+12k+4$$

Mindkét esetben 3-mal osztva 1 maradékot adnak, tehát bármely 3-tól különböző prím négyzete: $p^2=3N+1$ alakú.

Ha a vizsgált prím $p=3k+1$, akkor $p^2+p+1=3N+1+3k+1+1=3L+3$, vagyis nem prímszám.

Ha a vizsgált prím $p=3k+2$, akkor $p^2-p+1=3N+1-3k-2+1=3M$, vagyis nem prímszám.

Még a $p=3$ esetet kell megvizsgálni. Ekkor:

$$p^2+p+1=9+3+1=13 \; és \; p^2-p+1=9-3+1=7$$

Vagyis a $p=3$ is megfelel. Tehát csakis $p=2$ $és$ $p=3$ esetén lesz mindkét kifejezés értéke prímszám. Ezekre az értékekre:

1. Ha $p=2$, akkor $p^4+p^3+p^2+p+1=16+8+4+2+1=31$. Ez prímszám.

2. Ha $p=3$, akkor $p^4+p^3+p^2+p+1=81+27+9+3+1=121=11^2$. Ez négyzetszám. Tehát igaz az állítás.

61.

Alakítsuk át a kifejezést az alábbi módon:

$$4n^3+6n^2+4n+1=n^4+4n^3+6n^2+4n+1-n^4=(n+1)^4-n^4=$$

$$=[(n+1)^2-n^2]\cdot[(n+1)^2+n^2]=$$

$$=(n^2+2n+1-n^2)\cdot(n^2+2n+1+n^2)=(2n+1)\cdot(2n^2+2n+1)$$

Egy p prím csak úgy bontható két pozitív egész szorzatára, ha $p = 1 \cdot p$. Mivel

$(2n+1) < (2n^2 + 2n + 1)$, ezért $(2n+1) = 1 \text{ és } (2n^2 + 2n + 1) = p$. Ha $(2n+1) = 1$, akkor $n = 0 \text{ és } p = 1$ lenne, ami nem lehetséges. Tehát igaz az állítás.

62.

Ha a $p^{2q} + q^{2p}$ összeg prím, akkor az csak páratlan lehet. Ebből következik, hogy a p és q egyike páros. Legyen $p = 2$! Ekkor:

$$p^{2q} + q^{2p} = 2^{2q} + q^4 = 4^q + q^4$$

A 4 hatványai páratlan kitevő esetén 4-re, páros kitevő esetén 6-ra végződnek. Mivel q páratlan, ezért 4^q utolsó számjegye 4. A 2 és 5 kivételével minden prímszám 4-dik hatványa 1-re végződik. Ezek szerint: $4^q + q^4 = \cdots 4 + \cdots 1 = \cdots 5$. Ez a szám viszont osztható 5-tel. Már csak a $q = 5$ esetet kell vizsgálni. Ha $q = 5$, akkor $4^5 + 5^4 = 1649 = 17 \cdot 97$, vagyis nem prímszám. Tehát igaz az állítás.

63.

Az 5-nél nagyobb prímszámok 30-cal osztva 1,7,11,13,17,19,23,29 maradékot adhatnak. Ezért ezek a számok az alábbi négy alakban írhatók fel, ahol $k \geq 0$ egész szám:

1. eset: $p = 30k \pm 1$.

2. eset: $p = 30k \pm 7$.

3. eset: $p = 30k \pm 11$.

4. eset: $p = 30k \pm 19$. Vizsgáljuk meg a négy esetet!

Az 1. esetben:

$$p^2 = (30k \pm 1)^2 = 900k^2 \pm 60k + 1 = 30(30k^2 \pm 2k) + 1$$

Ez 30-cal osztva 1 maradékot ad.

A 2. esetben:

$$p^2 = (30k \pm 7)^2 = 900k^2 \pm 420k + 49 = 30(30k^2 \pm 14k + 1) + 19$$

Ez 30-cal osztva 19 maradékot ad.

A 3. esetben:

$$p^2 = (30k \pm 11)^2 = 900k^2 \pm 660k + 121 = 30(30k^2 \pm 22k + 4) + 1$$

Ez 30-cal osztva 1 maradékot ad.

A 4. esetben:

$$p^2 = (30k \pm 17)^2 = 900k^2 \pm 1020k + 289 = 30(30k^2 \pm 34k + 9) + 19$$

Ez 30-cal osztva 19 maradékot ad. Tehát igaz az állítás.

64.

1. Állítás: Ha egy $p > 3$ prímszámot 3-mal osztva 2-t ad maradékul, akkor $8p - 1$ osztható 3-mal. A feltétel szerint a $8p - 1$ prím. Tehát *p*-nek 3-mal osztva 1-et kell maradékul adnia, ekkor viszont $8p + 1$ osztható 3-mal. Ha $p = 3$, akkor $8p + 1 = 25$, ami szintén összetett szám.

2. Állítás: Ha *p* nem osztható 3-mal, akkor a p^2 1 maradékot ad 3-mal osztva. Ekkor $8p^2 + 1$ osztható 3-mal. Ha $p = 3$, akkor $8p^2 + 1 = 73$ $és$ $8p^2 - 1 = 71$, ami az állítást bizonyítja.

65.

A 3-nál nagyobb prímszámokat 6-tal osztva 1 vagy 5 maradékot adnak. Ha ugyanis a maradék 2 vagy 4 volna, akkor a számnak párosnak kellene lennie. Ha 3 lenne a maradék, akkor a szám osztható lenne 3-mal. Tehát minden 3-nál nagyobb prímszámot $6k + 1$ vagy $6k + 5$ alakban lehet felírni. Ezek négyzete:

$$36k^2 + 12k + 1, illetve\ 36k^2 + 60k + 25$$

Mindkét kifejezés 1-et ad maradékul, ha 12-vel osztjuk. Tehát igaz az állítás.

66.

Három $6k + 1$ vagy $6k + 5$ alakú szám közül legalább kettő egyforma. (A 65.-ös feladat megoldása alapján.) Ezért a különbségük, amely *d* vagy *2d*, osztható 6-tal, tehát *d* biztosan osztható 3-mal. Továbbá két páratlan szám különbsége osztható 2-vel, akkor viszont *d* osztható 6-tal is. Tehát igaz az állítás.

67. Végezzük el a következő átalakításokat:

$$2^{2^n}-1=\left(2^{2^{n-1}}+1\right)\left(2^{2^{n-1}}-1\right)=\left(2^{2^{n-1}}+1\right)\left(2^{2^{n-2}}+1\right)\left(2^{2^{n-2}}-1\right)=\cdots=$$

$$=\left(2^{2^{n-1}}+1\right)\left(2^{2^{n-2}}+1\right)\left(2^{2^{n-3}}+1\right)\cdots(2^2+1)(2+1)(2-1)$$

Tehát a $2^{2^n}-1=\left(2^{2^n}+1\right)-1$ szám osztható az összes előtte elhelyezkedő számokkal a sorban. Ebből következik, hogy ha a $2^{2^n}+1$ és $2^{2^k}+1$ kifejezések (ahol $k<n$) van közös osztójuk, akkor a 2 számnak is osztónak kell lennie ezzel a közös osztóval. A 2 azonban nem lehet közös osztója a sorozat két egymás melletti elemének, mivel a sorozat elemei mind páratlan számok. Ebből pedig már következik, hogy a sorozat bármely két eleme egymáshoz képest relatív prímek.

Megjegyzés: A feladat állításából speciálisan az is következik, hogy végtelen sok prímszám van. Ha ugyanis véges sok prímszám volna, akkor nem létezhetne végtelen sok olyan szám, amelyek közül bármely kettő mindig relatív prím lenne.