Eötvös Loránd Tudományegyetem
Természettudományi Kar

Prímek a középiskolai szakkörön

Szakdolgozat

Készítette: Zsilinszky Dorina

Matematika BSc

Tanári szakirány

Témavezető:

Dr. Freud Róbert

egyetemi docens

Algebra és Számelmélet Tanszék

Budapest

2015

Tartalomjegyzék

Bevezetés és köszönetnyilvánítás

> „A matematika a tudományok királynője, és a matematika királynője a számelmélet." Gauss (1777-1855)

Szakdolgozatom célja a prímek témakörének szubjektív feldolgozása, a hozzájuk kapcsolódó érdekes tételek, tulajdonságok összegyűjtése, rendszerezése. Ezt a meglehetősen tág és sokszínű témát olyan szempontból dolgoztam fel, ahogyan én azt el tudnám képzelni egy esetleges szakköri munka során.

Választásomat két dolog motiválta elsősorban. Egyrészt, leendő tanárként szerettem volna olyan témában jobban elmélyülni, amelynek közvetlen kapcsolata van az iskolai tananyaggal. Mivel a számelmélet, ezen belül is a prímek témaköre szerepel a gimnáziumi anyagban, azonban nem kerül bővebb kifejtésre, így kiváló főszereplője lehet a középiskolai szakkörnek, ahol a diákok alaposabban megismerkedhetnek a prímek tulajdonságaival. Másrészt, a számelméletet már az egyetemi tanulmányaim legelején megkedveltem. A számelmélet az egyik olyan ága a matematikának, amely napjainkban is dinamikusan fejlődik. Számos olyan témakör van a prímekkel kapcsolatban is, ahol egy sejtést megfogalmazva triviális állítást kapunk, azonban ha megváltoztatjuk kissé az eredeti sejtést, vagy a feltételeket, akkor rögtön egy megoldatlan problémával találjuk szembe magunkat. Számomra ez lenyűgöző, és úgy gondolom, ez talán a diákokat is tudja vonzani. Legfőképpen, hogy javarészt olyan problémák ezek, amiket ők is, a meglévő matematikai fogalmaik birtokában meg tudnak érteni és meg tudnak vizsgálni.

Dolgozatomban részletesen foglalkozom a prímekkel kapcsolatos klasszikus problémákkal, a prímszámok előfordulásával végtelen számtani sorozatokban, a Mersenne- és Fermat-prímekkel, végül pedig a tökéletes számokkal. Mindegyik fejezetben szerepelnek az adott témakörhöz kapcsolódó tételek, illetve kidolgozott feladatok. A feladatok megoldása önálló munkám eredménye, ezen kívül számos esetben összegeztem az adott feladattal kapcsolatos észrevételeimet, illetve lehetséges általánosításokat. A tételek bizonyítása többnyire szintén saját munka, néhány helyen mutatok példát többféle bizonyítási módszerre is. Emellett, néhány Arany Dániel és KöMal versenyfeladatot is megemlítek, amelyek egy-egy adott fejezethez szorosan kapcsolódnak. Mivel szakdolgozatom nem kifejezetten a versenyfelkészítést célozza, így részletesen ezzel a témakörrel nem foglalkoztam. Ahol lehetett, igyekeztem összekapcsolni a különböző fejezeteket.

Szeretnék ezúton is köszönetet mondani témavezetőmnek, Freud Róbertnek, aki nélkül ez a szakdolgozat nem készülhetett volna el. A már elkészült munkámmal kapcsolatos rendszeres visszajelzései és az előttem álló fejezetek feldolgozásához adott tanácsai elengedhetetlen segítséget és támogatást jelentettek számomra.

1. Általános, elemi feladatok, klasszikus problémák

1.1. Bevezető feladatok

Az első fejezetben olyan feladatokat fogunk megnézni, amelyek mindenféle előismeret nélkül megoldhatóak, így kiválóan szolgálhatnak a téma bevezetőjéül a szakkörön.

1.1.1 Feladat. Adjuk meg az összes olyan n pozitív egészet, amelyre az alábbi számok mindegyike prímszám:

a) n, $n+2$ és $n+4$:

Megoldás. Először írjunk fel néhány ilyen számhármast, és nézzük meg, hogy mi történik!

Ha $n = 3 \to 3, 5, 7$
Ha $n = 5 \to 5, 7, 9$
Ha $n = 7 \to 7, 9, 11$
Ha $n = 11 \to 11, 13, 15$

Azt láthatjuk, hogy a három szám közül az egyik mindig osztható lesz 3-mal. Érdemes lehet tehát a 3-mal való oszthatóságot vizsgálnunk!

Ha $n \neq 3$, akkor ha

- $n = 3k$, akkor n nem prímszám
- $n = 3k+1$, akkor $n+2 = 3(k+1)$, azaz $n+2$ nem prímszám
- $n = 3k+2$, akkor pedig $n+4 = 3(k+2)$, azaz $n+4$ nem prímszám

Tehát $n \neq 3$ esetén nincs olyan n, amelyre mind a három felsorolt szám prímszám lenne. Azaz, pontosan egy megoldás létezik, $n = 3$.

b) n és n^2+8:

Megoldás. Írjunk fel először megint néhány példát!

Ha $n = 2 \to 2, 12$
Ha $n = 3 \to 3, 17$
Ha $n = 5 \to 5, 33$
Ha $n = 7 \to 7, 57$
Ha $n = 11 \to 11, 129$

Itt is azt látjuk, hogy a két szám közül az egyik osztható lesz 3-mal. Nézzük meg ismét a 3-mal való oszthatóságot!

Ha $n \neq 3$, akkor ha

- $n = 3k$, akkor n nem prímszám
- $n = 3k + 1$, akkor $n^2 + 8 = 9k^2 + 6k + 9 = 3l$, azaz nem prímszám
- $n = 3k + 2$, akkor $n^2 + 8 = 9k^2 + 12k + 12 = 3l$, azaz nem prímszám

Tehát $n \neq 3$ esetén nincs olyan n, ami kielégítené a feltételeket. Láttuk, $n = 3$ esetén viszont megint jó lesz.
Azaz pontosan ez az egy megoldás létezik.

c) n, $n + 6$, $n + 12$, $n + 18$ és $n + 24$:

Megoldás. Próbáljuk meg megkeresni, melyik számmal való oszthatóságot lenne érdemes vizsgálni!

Ha $n = 2 \to 2$, 8, 14, 20, 26
Ha $n = 3 \to 3$, 9, 15, 21, 27
Ha $n = 5 \to 5$, 11, 17, 23, 29
Ha $n = 7 \to 7$, 13, 19, 25, 31
Ha $n = 11 \to 11$, 17, 23, 29, 35

Ha megvizsgáljuk, azt láthatjuk, hogy mindegyik esetben szerepel 5-tel osztható szám a felsorolásban. Érdemes lehet tehát az 5-tel való oszthatóságot vizsgálni.
Ha $n \neq 5$, akkor ha

- $n = 5k$, akkor n nem prímszám
- $n = 5k + 1$, akkor $n + 24 = 5k + 25 = 5l$, azaz nem prímszám
- $n = 5k + 2$, akkor $n + 18 = 5(k + 4)$, azaz nem prímszám
- $n = 5k - 2$, akkor $n + 12 = 5(k + 2)$, azaz nem prímszám
- $n = 5k - 1$, akkor $n + 6 = 5(k + 1)$, azaz nem prímszám

Tehát $n \neq 5$ esetén nincs olyan n, ami kielégítené a feltételeket. Láthattuk, hogy viszont $n = 5$-re jó lesz.
Azaz pontosan ez az egy megoldás létezik.

d) n, $n^3 - 6$ és $n^3 + 6$:

Megoldás. Először néhány példán keresztül próbáljuk megsejteni megint, hogy mit kell keresni!

Ha $n = 2 \to 2$, 2, 14
Ha $n = 3 \to 3$, 21, 33
Ha $n = 5 \to 5$, 119, 131
Ha $n = 7 \to 7$, 337, 349

Talán az első pár sorból sejthetjük, hogy mindig lesz egy 7-tel osztható szám a felsoroltak között. Igazoljuk ezt a sejtést!

Ha $n \neq 7$, akkor ha

- $n = 7k$, akkor n nem prímszám
- $n = 7k + 1$ vagy $n = 7k + 2$ vagy $n = 7k + 4$, akkor $n^3 + 6 = 7l$, azaz nem prímszám
- $n = 7k + 3$ vagy $n = 7k - 2$ vagy $n = 7k - 1$, akkor $n^3 - 6 = 7l$, azaz nem prímszám

Tehát $n \neq 7$ esetén nincs olyan n, amelyre mind a három szám prím lenne.

Ennek mélyebb magyarázata:
Mivel a 7 prím, ezért ha $7 \mid n$ vagy $7 \mid n^3 - 6$ vagy $7 \mid n^3 + 6$

$$\Leftrightarrow 7 \mid n(n^3 - 6)(n^3 + 6)$$

$$\Leftrightarrow n(n^3 + 1)(n^3 - 1) \equiv 0 \pmod 7$$

$$\Leftrightarrow n(n^6 - 1) = n^7 - n \equiv 0 \pmod 7$$

$$\Leftrightarrow n^7 \equiv n \pmod 7$$

Ez pedig a kis Fermat-tétel $p = 7$-re.
A feladat megoldásához még hozzátartozik, hogy $n = 7$-re ellenőrizni kell, hogy prím lesz-e a másik két szám:
$n^3 - 6 = 337$ és $n^3 + 6 = 349$ is prímszám.
Azaz, pontosan ez az egy megoldás létezik, hiszen minden további n esetén az egyik szám osztható lesz 7-tel, azaz nem lesz prímszám.

1.1.2 Feladat. Mely n pozitív egészekre lesz prímszám:

a) $n^3 - n + 3$:

Megoldás.

$$n^3 - n + 3 = n(n^2 - 1) + 3 = n(n - 1)(n + 1) + 3$$

$n - 1, n, n + 1$ közül az egyik biztosan osztható 3-mal, így $n^3 - n + 3$ az n-től függetlenül $3k$ alakú lesz. Azaz általában nem lesz prím, kivéve, ha $n = 1$, mert akkor

$$n^3 - n + 3 = 3$$

Más megoldás nincs, mert minden más n-re $n^3 - n + 3 > 3$ és osztható 3-mal, azaz összetett.

b) $n^3 - 27$:

Megoldás.

$$n^3 - 27 = n^3 - 3^3$$

Azaz, mivel $n-3 \mid n^3-27$, ezért általában (azaz, ha $|n-3| > 1$) nem lesz prímszám. Viszont, ha $|n-3| = 1$, azaz, ha $n = 2$ vagy $n = 4$, akkor ez az összefüggés nem ad nemtriviális osztót, tehát ezeket az eseteket külön meg kell vizsgálnunk.
Ha $n = 4$, akkor $n^3 - 27 = 37$, ami prím, illetve, ha $n = 2$, akkor $n^3 - 27 = -19$, ami szintén prím, tehát pontosan ez a kettő megoldás létezik.

c) $n^8 + n^7 + n^6 + n^5 + n^4 + n^3 + n^2 + n + 1$

Megoldás:

$$n^8 + n^7 + n^6 + n^5 + n^4 + n^3 + n^2 + n + 1 = n^6(n^2 + n + 1) + n^3(n^2 + n + 1) + n^2 + n + 1 =$$
$$= (n^6 + n^3 + 1)(n^2 + n + 1)$$

Ez a kifejezés minden $n > 0$ esetben összetett szám lesz, hiszen mindkét tényező nagyobb, mint 1.

Észrevétel. Általában, ha k összetett (pl $k = rs$), akkor $n^{k-1}+n^{k-2}+\ldots+n^2+n+1$ összetett lesz minden n-re, mert szorzattá lehet alakítani, és mindkét tényező nagyobb, mint 1.

$$n^{k-1} + n^{k-2} + \ldots + n^2 + n + 1 = (n^{s-1} + n^{s-2} + \ldots + n + 1)(n^{k-s} + n^{k-2s} + \ldots + 1)$$

d) $n^4 + 4$:

Megoldás:

$$n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 - 2n + 2)(n^2 + 2n + 2)$$

Általában nem lesz prímszám, hiszen két egész szorzatára bontható. Egyedül akkor lehet prímszám ez a kifejezés, ha a szorzatban az egyik tényező ± 1-gyel egyenlő, a másik tényező pedig egy prímszám. Vagyis

- $n^2 + 2n + 2 = -1$, azaz:
  $n^2 + 2n + 3 = 0 \rightarrow$ ennek az egyenletnek a pozitív egészek körében nincs megoldása
- $n^2 + 2n + 2 = 1$, azaz:
  $n^2 + 2n + 1 = 0 \rightarrow$ ennek csak $n = -1$ a megoldása, ami nekünk nem jó
- $n^2 - 2n + 2 = -1$, azaz:
  $n^2 - 2n + 3 = 0 \rightarrow$ ennek a pozitív egészek körében nincs megoldása
- $n^2 - 2n + 2 = 1$, azaz:
  $n^2 - 2n + 1 = (n-1)^2 = 0$
  Azaz $n = 1$ esetén van esély rá, hogy prím legyen, és tényleg: $n^4 + 4 = 5$, ami prímszám, tehát jó. Minden más (pozitív) n esetén az $n^4 + 4$ összetett lesz.

e) $n^8+n^6+n^4+n^2+1$:

Megoldás:

$$n^8+n^6+n^4+n^2+1=(n^4+n^2+1)^2-n^6-2n^4-n^2=(n^4+n^2+1)^2-(n^3+n)^2=$$
$$=(n^4-n^3+n^2-n+1)(n^4+n^3+n^2+n+1)$$

Tehát általában nem lesz prímszám, hiszen két számnak a szorzatára bontható. Egyedül akkor lehet prímszám ez a kifejezés, ha a szorzatban az egyik tényező ± 1-gyel egyenlő, a másik tényező pedig egy prímszám. Ez csak úgy lehetséges, ha

$$n^4-n^3+n^2-n+1=1$$

Azaz:

$$n^4-n^3+n^2-n=n^3(n-1)+n(n-1)=(n^3+n)(n-1)=n(n^2+1)(n-1)=0$$

Ez akkor teljesül, ha $n=1$ (mi most $n>0$ – ra nézzük):
Ha $n=1$, akkor $n^8+n^6+n^4+n^2+1=5$, ami prímszám, tehát jó. Minden egyéb n-re a kifejezés összetett szám lesz.

Észrevétel. Az ilyen típusú feladatokban az egyik leggyakoribb módszer – ahogy láttuk – a szorzattá alakítás. Ha egy kifejezést szorzattá alakítottunk, akkor általában nem lesz prímszám, eltekintve egy-két kivételtől. Ezeket a kivételeket megvizsgálva fel tudjuk sorolni azokat az n-eket, amelyekre a kifejezés prímszám lesz.

Megjegyzés. A feladat c) és e) része kapcsolódik a körosztási polinomok témaköréhez is. Ennek felfedezése segíthet a szorzattá alakításban is. Tudniillik a c) részben:

$$n^8+n^7+n^6+n^5+n^4+n^3+n^2+n+1=\frac{n^9-1}{n-1}=\frac{n^9-1}{\phi_1(n)}=\phi_9(n)\cdot\phi_3(n)=(n^6+n^3+1)(n^2+n+1)$$

amelyek viszont már irreducibilis, azaz felbonthatatlan tényezők (tehát tovább nem bonthatóak mint polinomok, de természetesen adott n-re lehetnek összetettek).

Valamint az e) részben:

$$n^8+n^6+n^4+n^2+1=\frac{n^{10}-1}{n^2-1}=\frac{n^{10}-1}{\phi_1(n)\phi_2(n)}=\phi_5(n)\cdot\phi_{10}(n)=$$
$$=(n^4+n^3+n^2+n+1)(n^4-n^3+n^2-n+1)$$

amelyek szintén már irreducibilis tényezők (ami itt sem jelenti azt, hogy adott n-re ne lehetnének összetettek).

1.1.3 Feladat. Halhatatlan kapitánynak három halhatatlan unokája van, akiknek az életkora három különböző prímszám, és ezek négyzetének az összege is prímszám. Hány éves lehet a kaptiány legkisebb unokája? (Ne felejtsük el, hogy az unokák halhatatlanok, tehát akár több millió évesek is lehetnek!)

Megoldás. Az unokák életkorát jelöljük p_1, p_2, p_3-mal! A feladat feltételei szerint ekkor $p_1^2 + p_2^2 + p_3^2$ is prím.

Nézzük meg először, hogy p_i páros-e vagy páratlan. Maximum az egyik prím lehet páros, akkor ha $p_1 = 2$, de akkor a négyzetösszeg is páros lenne, ami ellentmondás. Tehát mind a három prím páratlan.
Nézzük most a 3-mal való oszthatóságot! Nyilván p_1, p_2, p_3 közül nem lehet mindegyik $3k$ alakú, tehát biztosan van köztük $3k+1$ és/vagy $3k+2$ alakú prím is.
Ha $p_i = 3k \pm 1$, akkor $p_i^2 = 3k + 1$. Tehát bármelyik prímszámra igaz a három közül, hogy $p_i^2 = 3k$ vagy $p_i^2 = 3k + 1$.
Viszont, nem lehet, hogy mindegyik $p_i^2 = 3k + 1$, hiszen akkor $p_1^2 + p_2^2 + p_3^2 = 3l$, ami ellentmondás. Ebből következik, hogy valamelyik prímre igaz, hogy $p_i = 3k$. Ez viszont csak akkor lehetséges, ha $p_1 = 3$, azaz a kapitány legkisebb unokája 3 éves.
Ilyen p_1, p_2, p_3 lehet például: 3, 5, 7 vagy 3, 7, 11. Azt látjuk, hogy a többi unoka életkora nem egyértelmű. Megoldatlan kérdés, hogy létezik-e végtelen sok ilyen számhármas.

1.2. Goldbach-sejtés

A Goldbach-sejtés egy olyan probléma, amit egyszerűen el lehet mesélni bárkinek, mindazonáltal a mai napig nincs teljesen megoldva, így mindenképpen érdemes szakkörön megmutatni a gyerekeknek.

„Páros" Goldbach-sejtés:
$4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 5 + 7$, ... : felírható-e 4-től kezdve minden páros szám két prímszám összegeként?

A fenti probléma a „páros" Goldbach-sejtés. Ebből azonnal következik a „páratlan" Goldbach, amely arra vonatkozik, hogy a 7-től kezdve minden páratlan szám felírható három prím összegeként:

$$7 = 2 + 2 + 3$$

$$9 = 2 + 2 + 5$$

$$11 = 12 - 1 = 4 + 7 = 2 + 2 + 7$$

$$13 = 14 - 1 = 6 + 7 = 3 + 3 + 7$$

$$\vdots$$

$$2k + 1 = (2k + 2) - 1 = (p_1 + p_2) - 1 = (p_1 - 1) + p_2 = (p_3 + p_4) + p_2 \quad (\text{ha } p_1 \geq 5)$$

Vagy:

$$2k+1 = (2k-2)+3 = p_1 + p_2 + 3 \quad (2k-2 \geq 4)$$

A „páros" Goldbach-sejtés ekvivalens azzal az állítással, hogy minden $n \geq 6$ egész szám felírható három prím összegeként, ugyanis:

- Ha n páratlan, akkor teljesül rá a „páratlan" Goldbach (ami a „páros" Goldbach-ból következik), tehát felírható három prím összegeként.
- Ha n páros, akkor a „páros" Goldbach-sejtést felhasználva, a következő felbontás jó lesz:
$$n = 2 + (n-2) = 2 + (p_1 + p_2)$$
Illetve, ha n páros, és felírható három prím összegeként, akkor az egyik prím a 2 kell legyen, így:
$$n = 2 + p_1 + p_2 \Longleftrightarrow n - 2 = p_1 + p_2$$

1.2.1 Feladat. Mely páros számok írhatók fel két (pozítív) összetett szám összegeként?

Megoldás.

Ha $n \geq 8$, és $4 \mid n$, akkor a következő felbontás jó lesz: $n = \frac{n}{2} + \frac{n}{2}$, hiszen $\frac{n}{2} > 2$ is páros, azaz összetett.
$n = 4k+2$, akkor $n = (2k+2) + 2k$, azaz akkor is lesz jó felbontás, ha $n \geq 10 \quad (k \geq 2)$.
Végül, ha $n \leq 6$, akkor nem írható fel két összetett szám összegeként, mert legalább az egyik tag mindenképpen prímszám vagy 1 lesz:
$6 = 1+5 = 2+4 = 3+3$
$4 = 1+3 = 2+2$
$2 = 1+1$

Összefoglalva: A páros számok közül pontosan azok írhatók fel két (pozitív) összetett szám összegeként, amelyekre teljesül, hogy $n \geq 8$.

1.3. Prímszámokból álló sorozatok

1.3.1 Feladat. Létezik-e végtelen hosszú, nemnulla differenciájú számtani sorozat csupa prímszámból?

Megoldás. Nem létezhet ilyen sorozat, mert minden $a \neq 0, 1$-re igaz, hogy ha a eleme a sorozatnak, akkor $a + ad = a(1+d)$ is eleme, ami nem prímszám.

Megjegyzés. Létezik akármilyen véges hosszú (nemkonstans) számtani sorozat csupa prímszámból. Ezt 2004-ben Ben Green és Terence Tao bizonyította be.

1.3.2 Feladat. Tekintsünk egy csupa prímszámból álló számtani sorozatot, jelöljük a tagok számát n-nel, a differenciát pedig d-vel. Bizonyítsuk be, hogy ha $n = 4$, akkor $6 \mid d$.

Megoldás. Jelöljük a tagokat $p, p+d, p+2d, p+3d$-vel!

Vizsgáljuk meg, hogy a d szám milyen másik egész számokkal osztható. A p páratlan, hiszen ha páros lenne, akkor például $p+2d$ is páros lenne, ami ellentmondás. Ebből következik, hogy d páros, hiszen $p+d$-nek is prímszámnak kell lennie. Illetve, azt is tudjuk, hogy $p \neq 3$, hiszen különben $p+3d$ osztható lenne 3-mal, ami ellentmondás. Innen következik, hogy d osztható 3-mal, hiszen ha $d = 3k+1$ vagy $3k-1$, akkor $p = 3k+1$ esetén $p+2d$, illetve $p+d$ lenne 3-mal osztható, $p = 3k-1$ esetén pedig $p+d$, illetve $p+2d$ lenne osztható 3-mal. Azaz d osztható 3-mal, és így 6-tal is.

1.3.3 Feladat. Tegyük fel, hogy p és d pozitív egész számok, amelyekre a $p, p+d, p+2d, \ldots, p+10d$ számok mindegyike prímszám. Bizonyítsa be, hogy ekkor d értéke legalább 210. (Arany Dániel, 11/12 kezdő, III.kategória, 1.forduló)

Megoldás. Az előző feladathoz hasonlóan, vizsgáljuk meg, hogy a d szám milyen más egész számokkal osztható.

A 2-vel, 3-mal való oszthatóság bizonyítása teljesen ugyanúgy megy, mint az előző feladatban. Nézzük most az 5-tel való oszthatóságot! Először is, $p \neq 5$, különben $p+5d$ nem lenne prímszám. Ezen kívül, ha $d = 5k+1$ akkor p akármilyen maradékot is ad 5-tel osztva, $p+d$ vagy $p+2d$ vagy $p+3d$ vagy $p+4d$ mindenképpen osztható lesz 5-tel. Ha $d = 5k+2$ vagy $5k+3$ vagy $5k+4$ alakú, akkor p akármilyen maradékot ad 5-tel osztva, mindig találhatunk olyan számot a sorozatban, ami osztható lesz 5-tel. Tehát $5 \mid d$.
Már csak a 7-tel való oszthatóság van hátra. Az előzőekhez hasonlóan, elmondhatjuk, hogy $p \neq 7$, hiszen különben $p+7d$ nem lenne prímszám. Ezen kívül, ha $d \equiv 1 \pmod 7$ és $p \equiv l \pmod 7$ akkor a $p+(7-l)d$ szám osztható lesz 7-tel. Ha $d \equiv 2 \pmod 7$ és $p \equiv l \pmod 7$ akkor a $p+(7-4l)d$ szám például osztható lesz 7-tel (hozzátéve, hogy ha a $k = 7-4l$ negatív, akkor az 1 és 7 közé eső $k \equiv 7-4l$ számot kell venni helyette). Ha $d \equiv 3 \pmod 7$ és $p \equiv l \pmod 7$ akkor a $p+(7-5l)d \equiv 0 \pmod 7$, tehát az jó lesz. És így végig, ha $d \equiv 4, 5, 6 \pmod 7$ akkor is lehet találni olyan számot a sorozatban, ami 7-tel osztható lesz. Így marad az az eset, hogy $7 \mid d$. Ilyen módon, mivel a 2, 3, 5, 7 páronként relatív prímek egymáshoz, így $2 \cdot 3 \cdot 5 \cdot 7 = 210 \mid d$. Ebből következik, hogy d értéke legalább 210.

Általában : Ha tekintünk egy csupa prímszámból álló, n tagú sorozatot, akkor d osztható az összes n-nél kisebb prímszámmal. Ugyanis:
Indirekt tegyük fel, hogy $p < n$ a legkisebb olyan prím, amelyre $(p, d) = 1$. Ekkor a prímekből álló számtani sorozat első p tagja teljes maradékrendszert alkot modulo p, így van köztük p-vel osztható, de mivel minden tag prímszám, így ez a tag csak p lehet. Azaz $p = a + id$, de mivel feltettük, hogy p minimális, így $i = 0$ kell legyen, hiszen különben az a osztója a d-nek, és így szükségképpen a sorozat összes tagjának, ami nem lehetséges. Ezért $p = a$, viszont ez esetben $a + pd$, a sorozat $p+1$-edik tagja osztható p-vel, azaz nem prím, ami ellentmondás.

1.4. Speciális alakú prímek

Ebben a részben speciális alakú számokat fogunk vizsgálni. Megoldatlan kérdés, hogy létezik-e végtelen sok ilyen alakú prím, azt viszont könnyebben meg tudjuk mutatni, hogy végtelen sok összetett szám van az ilyen alakú számok között.

Állítás. *Végtelen sok* $2^k - 1$ *és* $2^k + 1$ *alakú összetett szám létezik.*

Ha k összetett, azaz például $k = r \cdot s \ \ (r, s > 1)$, akkor:

- $2^k - 1 = (2^r)^s - 1$. Azaz $2^r - 1 \mid (2^r)^s - 1$. Ekkor $1 < 2^r - 1 < (2^r)^s - 1$, így találtunk egy valódi osztót.
  Azaz: $2^k - 1$ összetett, ha k összetett, és csak akkor lehet prím, ha k prím.

- ha r páratlan, akkor $2^s + 1 \mid (2^s)^r + 1$, azaz ebben az esetben $2^k + 1$ összetett.
  Ez azt is jelenti, hogy $2^k + 1$ csak akkor lehet prím, ha k kettőhatvány, egyéb esetben összetett lesz.

Állítás. *Végtelen sok* $n^2 + 1$ *alakú összetett szám létezik.*

Ha n páros és n egy $r^2 + 1$ alakú páratlan számmal osztva r maradékot ad, azaz $n = r + j(r^2 + 1)$, akkor $n^2 + 1 = r^2 + 1 + i(r^2 + 1)$, azaz osztható lesz $r^2 + 1$-gyel, és ha $n > r$, akkor biztos, hogy összetett lesz.

Állítás. *Végtelen sok összetett szám létezik a (tízes számrendszerben) csupa egyes számjegyet tartalmazó számok között.*

Észrevehetjük, hogy például

$$\begin{aligned} 11 \cdot 101 &= 1111 \\ 11 \cdot 10101 &= 111111 \\ 11 \cdot 1010101 &= 11111111 \end{aligned}$$

És így tovább, mindig a kettővel több „ilyen számjegyet" tartalmazó számmal kell megszorozni a 11-et.
Már önmagában ez a konstrukció is megad végtelen sok ilyen számot, de a 11 helyére más $11\ldots1$ számot is írhatunk.

Például:

$$\begin{aligned} 111 \cdot 1001 &= 111000 + 111 = 111111 \\ 111 \cdot 1001001 &= 111111111 \\ 111 \cdot 1001001001 &= 111111111111 \end{aligned}$$

És így tovább. Azt láthatjuk, hogy ha n összetett szám, akkor az n darab egyesből álló szám is összetett lesz.

Állítás. *Végtelen sok összetett szám létezik a* $333\ldots31$ *alakú számok között.*

Ha megvizsgálunk néhány ilyen számot, akkor észrevehetjük:

$$\begin{aligned} 31 \cdot 3 &= 93 = 100 - 7 \\ 331 \cdot 3 &= 993 = 1000 - 7 \\ 3331 \cdot 3 &= 9993 = 10000 - 7 \end{aligned}$$

És így tovább, mindig igaz lesz, hogy $33\ldots31$ az valami $\frac{10^k-7}{3}$ alakú szám.

Nézzük például mod 31 ezeket a számokat! Ha $k = 2 + 30r$, akkor

$$10^k - 7 = 10^{2+30r} - 7 \equiv 10^{30r} \cdot 10^2 - 7 \equiv 10^2 - 7 = 93 \equiv 0 \pmod{31}$$

Ehhez alkalmaztuk a kis Fermat-tételt, mivel $(10^r, 31) = 1$ és 31 prím. Azonban tulajdonképpen ezt anélkül is meg lehet oldani, ugyanis a skatulyaelv miatt a 10 hatványai periodikusak modulo 31. Ha m a periódushossz, akkor

$$10^{2+r\cdot m} - 7 \equiv 10^2 - 7 \equiv 0 \pmod{31}.$$

Azaz:
$\frac{10^k-7}{3} \equiv \frac{10^2-7}{3} = 31 \equiv 0 \pmod{31}$, azaz összetett lesz.
Mivel végtelen sok ilyen k szám van, így végtelen sok ilyen összetett szám is lesz.

Megjegyzés. 31 helyett lehetne például 331-gyel is, csak akkor olyan k számot keresnénk, amelyre például $k = 3 + 330r$, mert akkor a kis Fermat-tételt alkalmazva:

$$10^k - 7 = 10^{3+330r} - 7 \equiv 10^3 - 7 = 993 \pmod{331}$$

$$\Rightarrow \frac{10^k - 7}{3} \equiv \frac{10^3 - 7}{3} = 331 \equiv 0 \pmod{331}$$

Azaz összetett lesz.

Általában. Vegyünk egy p prímet, amely osztja a $\frac{10^k-7}{3}$-t, vagyis a számlálót, és amelyre $(3, p) = 1$ (azaz $p \neq 3$).
Ekkor a 10 hatványai periodikusak modulo p (szintén a skatulyaelv miatt). Ha a periódushossz m, akkor

$$10^{k+t\cdot m} - 7 = 10^k - 7 \equiv 0 \pmod{p}$$

Így

$$\frac{10^{k+t\cdot m} - 7}{3} \equiv 0 \pmod{p} \quad \text{(ehhez kell: } (3, p) = 1)$$

A periodikusság miatt ez a konstrukció végtelen sok $333\ldots31$ alakú összetett számot fog adni.

Állítás. *Végtelen sok összetett szám létezik a Fibonacci-számok között.*

Fibonacci számok: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$ és általában $u_{n+1} = u_n + u_{n-1}$.

Írjuk fel néhány kisebb számra a Fibonacci-számok osztási maradékát!
Például, ha $m = 2$, akkor a 2-vel való osztási maradékok így következnek egymás után:
1, 1, 0, 1, 1, 0, 1, 1, 0, ... stb.
Ha $m = 3$, akkor a 3-mal való osztási maradékok: 1, 1, 2, 0, 2, 2, 1, 0, 1, ... stb.
Ha $m = 5$, akkor az 5-tel való osztási maradékok:
1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ... stb.

Azt láthatjuk, hogy az osztási maradékokban ezek a periódusok folyton ismétlődni fognak. Ebből az következik, hogy végtelen sok 2-vel, 3-mal és 5-tel osztható Fibonacci-szám létezik.

2. Prímszámok számtani sorozatokban

Ebben a fejezetben azt fogjuk megnézni, hogy mi történik a végtelen számtani sorozatokban a prímeket tekintve. Az 1.3.1 Feladatban láttuk, hogy egy végtelen számtani sorozat nem állhat csupa prímszámból. De vajon szerepelhet-e benne végtelen sok prímszám? Az biztos, hogy ha $(a,d) \neq 1$, akkor nem szerepelhet benne, hiszen akkor ha $(a,d) = k$, a sorozat minden tagja osztható lesz k-val. Láthatjuk, hogy $(a,d) = 1$ szükséges feltétel ahhoz, hogy végtelen sok prímszám szerepeljen a sorozatban. Azonban a jó hír az, hogy ez elégséges is.

2.1 Tétel. **(Dirichlet-tétel)** Ha a $d > 0$ és a egészek relatív prímek, akkor az $a + kd$, $k = 0, 1, 2, \ldots$ számtani sorozat végtelen sok prímet tartalmaz. ♣

Ezt a tételt általánosságban nem bizonyítjuk be, csak néhány speciális esetét igazoljuk, többféle bizonyítási módszerrel.

2.2 Tétel. A $4k + 3$ alakú prímek száma végtelen. ♣

Bizonyítás. Tegyük fel indirekt, hogy véges csak véges sok ilyen prímszám létezik, legyenek ezek $p_1 = 3, \ldots, p_r$.
Olyan A számot szeretnénk gyártani, amely ezek egyikével sem osztható, viszont van $4k+3$ alakú prímosztója, hogy így ellentmondásra juthassunk. Vesszük a p_i-k szorzatát, és kicsit „elrontjuk", hogy megfeleljen az előbbi szempontoknak. Legyen $A = 4p_1 \ldots p_r - 1$!
Az A nyilván nem osztható a $p_1, \ldots, p_r$ prímek egyikével sem, eddig tehát jó. Már csak annak kell teljesülnie, hogy van $4k + 3$ alakú prímosztója.

Ennek belátásához írjuk fel A-t prímtényezők szorzataként: $A = q_1 \ldots q_s$ ($s = 1$, illetve $q_i = q_j$ is megengedett). Mivel A páratlan, ezért mindegyik $q_i > 2$. Továbbá, nem lehet minden $q_i \equiv 1 \pmod 4$, ugyanis ezeket összeszorozva $A \equiv 1 \pmod 4$ adódna, ami ellentmondás. Ebből következik, hogy a q_i prímek között kell lennie $4k + 3$ alakúnak is. Ez szükségképpen különbözik a $p_1, \ldots, p_r$ prímektől, így ellentmondásra jutottunk. □

2.3 Tétel. A $6k + 5$ alakú prímek száma végtelen. ♣

Bizonyítás. A bizonyítás hasonló módon megy, mint az előbb. Tegyük fel indirekt, hogy véges sok ilyen prím létezik, legyenek ezek $p_1 = 5, \ldots, p_r$.
Most is szeretnénk ügyesen egy olyan A számot gyártani, amely nem osztható ezekkel a prímekkel, de van $6k - 1$ alakú prímosztója. Legyen $A = 6p_1 \ldots p_r - 1$!
Ismét igaz, hogy A nem osztható a $p_1, \ldots, p_r$ prímek egyikével sem, az első fele tehát megvan.
A nekünk „jó" prímosztó megtalálásához megint írjuk fel A-t prímtényezők szorzataként: $A = q_1 \ldots q_s$ ($s = 1$, illetve $q_i = q_j$ is megengedett). Mivel A páratlan, így mindegyik $q_i > 2$.

Ha minden $q_i \equiv 1 \pmod 6$, akkor ezeket a kongruenciákat összeszorozva megintcsak $A \equiv 1 \pmod 6$ adódna, ami ellentmondás. Ebből az következik, hogy kell lennie a q_i prímek között nem $6k+1$ alakú prímnek is. Viszont, ha minden $q_i \equiv 1$ vagy 3, akkor ezeket összeszorozva

A biztosan nem lesz $6k-1$ alakú.
Tehát, a q_i prímek között kell lennie $6k+5$ alakúnak is, ami szükségképpen különbözik a $p_1, \ldots, p_r$ prímektől, tehát ellentmondásra jutottunk. □

Most az előzőektől kicsit különböző módszerekkel bizonyítunk olyan esetekben, amelyeket nem lehet ilyen egyszerűen elintézni. Ezekben a bizonyításokban a kvadratikus kongruenciákra vontakozó tételeket fogjuk felhasználni, amelyeket itt külön nem részletezünk.

2.4 Tétel. A $4k+1$ alakú prímek száma végtelen. ♣

Bizonyítás. Ez esetben nem tudjuk a $4k+3$ alakú prímek bizonyításához felhasznált gondolatmenetet követni.
Ha ugyanis $A = 4p_1 \ldots p_r + 1 = q_1 \ldots q_s$, és s páros szám, akkor még ha minden $q_i = 4k-1$ alakú is, akkor is $A = 4k+1$ lenne, és így nem jutnánk ellentmondásra. Más eszközökhöz kell tehát folyamodnunk:

Ismét tegyük fel indirekt, hogy véges sok ilyen prímszám létezik, legyenek ezek $p_1 = 5, \ldots, p_r$. Az megmarad, hogy olyan A számot keresünk, ami nem osztható ezekkel a prímekkel, viszont van $4k+1$ alakú prímosztója. Legyen $A = (2p_1 \ldots p_r)^2 + 1$!
Ekkor az A nem osztható a $p_1, \ldots, p_r$ prímek egyikével sem. Ez volt a könnyebbik része.

Innentől kicsit különbözik a bizonyítás menete annak érdekében, hogy találjunk egy $4k+1$ alakú prímosztót:

Legyen q az A egy tetszőleges prímosztója. Mivel A páratlan, így $q > 2$. A $q \mid A$ osztható ságot átírhatjuk

$$(2p_1 \ldots p_r)^2 \equiv -1 \pmod{q}$$

alakba. Ez azt jelenti, hogy az $x^2 \equiv -1 \pmod{q}$ kongruencia megoldható, vagyis

$$q \equiv 1 \pmod{4}.$$

Azaz megtaláltuk, amit kerestünk, egy újabb $4k+1$ alakú prímet, ami ellentmondás. □

Ha nem akarunk másodfokú kongruenciával dolgozni, akkor máshogy is befejezhetjük a bizonyítást.
Az indirekt feltevésből következik, hogy létezik az A-nak egy $4k-1$ alakú q prímosztója. A $q \mid A$ oszthatóságot átírhatjuk

$$a^2 = (2p_1 \ldots p_r)^2 \equiv -1 \pmod{q}$$

alakba. Ebből következik, hogy

$$a^{q-1} = (a^2)^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \equiv (-1)^{2k-1} = -1 \pmod{q}$$

Viszont, a kis Fermat-tétel miatt

$$1 \equiv a^{q-1} \pmod{q}$$

Azaz $1 \equiv -1 \pmod{q}$, amiből az következik, hogy $q = 2$, ami ellentmondás.

Létezik egy teljesen elemi bizonyítása is annak, hogy az A-nak, illetve általában az $n^2 + 1$ alakú számoknak nem létezhet $4k - 1$ alakú prímosztója (azaz A-nak minden prímosztója $4k + 1$ alakú).

Bizonyítás. Indirekt tegyük fel, hogy létezik olyan $t = 4k - 1$, amelyre $t \mid n^2 + 1$. Legyen t minimális, illetve n is legyen minimális. Ekkor $n \leq t - 1$.
Mivel t osztja $n^2 + 1$-et, ezért van olyan s, amelyre: $ts = n^2 + 1$. Nézzük meg, hogy s 4-gyel osztva milyen maradékot ad!

– ha n páros, akkor $ts = n^2 + 1 = 4k + 1$, azaz $s = 4l - 1$.
– ha n páratlan, akkor $ts = n^2 + 1 = (2l + 1)^2 + 1 = 4l^2 + 4l + 2 = 4l(l + 1) + 2 = 8k + 2$. Ekkor $s = 2(4m - 1)$.

Az n-re adott felső becslést felhasználva:

$$ts = n^2 + 1 \leq (t - 1)^2 + 1 = t^2 - 2t + 2$$

Ha t-vel leosztunk, a következő összefüggést kapjuk s-re:

$$s = t - 2 + \frac{2}{t} < t$$

Ha $s = 4l - 1$, akkor kaptunk egy t-nél kisebb, $4k - 1$ alakú osztót, ami ellentmondás.
Ha $s = 2(4m - 1)$, akkor $\frac{s}{2} = 4m - 1$, azaz megint ellentmondásba ütköztünk, mert kaptunk egy t-nél kisebb, $4k - 1$ alakú osztót. □

2.5 Tétel. A $8k + 3$ alakú prímek száma végtelen. ♣

Bizonyítás. Tegyük fel indirekt, hogy véges sok van belőlük, legyenek ezek $p_1 = 3, p_2, ..., p_r$. Hogyan konstruáljuk meg az A számot? Milyen kvadratikus kongruenciát válasszunk? Az kell nekünk, hogy A-nak ne lehessen csupa $8k + 1$ alakú prímosztója. Modulo 8 létezik 4 féle redukált maradékosztály, ennek a felét szeretnénk kizárni egy alkalmas kvadratikus kongruenciával. Mely kvadratikus kongruenciák érzékenyek modulo 8?

	$\left(\frac{2}{q}\right)$	$\left(\frac{-1}{q}\right)$	$\left(\frac{-2}{q}\right)$
1	1	1	1
3	-1	-1	1
5	-1	1	-1
7	1	-1	-1

Az első és a második oszlop az erre vonatkozó tételek miatt igaz, a harmadik oszlop pedig az első kettő szorzataként áll elő, azaz a következő összefüggésből adódik:

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

Mi most a $8k+3$ alakú prímekkel foglalkozunk, tehát a $\left(\frac{-2}{q}\right)$-t kell választanunk, ami azt jelenti, hogy az A számnak valami n^2+2 alakú számnak kell lennie.
Legyen $A=(p_1p_2\dots p_r)^2+2$! Nyilván az A nem osztható a $p_1,...,p_r$ prímek egyikével sem. Ha találnánk egy $8k+3$ alakú prímosztót, akkor ellentmondásra jutnánk.

A fenti táblázat szerint minden prímosztó $8k+1$ vagy $8k+3$ alakú.
Viszont, ha az A-nak minden prímosztója $8k+1$ alakú lenne, akkor az A maga is $8k+1$ alakú lenne, ami ellentmondás.

Azaz, A-nak biztosan létezik $8k+3$ alakú prímosztója. Így viszont találtunk egy újabb ilyen alakú prímet, ami ellentmondás. □

Általában : Nézzük meg, hogy általában hogyan működik egy ilyen jellegű bizonyítás!

- a bizonyítás indirekt: feltesszük, hogy az $mk+l$ alakú prímekből véges sok van, ezeket jelöljük $p_1,\dots,p_r$-rel
- az A számot úgy konstruáljuk meg, hogy ne lehessen csupa $mk+1$ alakú prímosztója, majd prímtényezőkre bontjuk
- az A szám prímosztóit vizsgáljuk mod m, van nekünk $\varphi(m)$ redukált maradékosztályunk, ott találhatóak a prímek (1-2 kivételtől eltekintve)
- egy alkalmas kvadratikus kongruenciával egy részét kizárjuk, marad az 1 maradékosztály és még az l által reprezentált maradékosztály
- mivel úgy intéztük, hogy nem lehet minden prímosztó az 1 maradékosztályban, így találtunk egy újabb $mk+l$ alakú prímet, és így jutunk ellentmondásra

Megjegyzés. Mivel egy megfelelő kvadratikus kongruenciával a maradékosztályok felét tudjuk kizárni, így ez a fajta bizonyítás csak addig működik, amíg 4 redukált maradékosztályunk van, azaz amíg $\varphi(m)=4$.

2.1 Feladat. Hány olyan prímszám létezik, amelynek tízes számrendszerben az utolsó négy számjegye 4321?

Megoldás. Használjuk fel a Dirichlet-tételt!

Ezt azért tehetjük meg, mert $(10000,4321)=1$. Tehát a Dirichlet-tétel azt mondja, hogy a $10000k+4321$ sorozatban végtelen sok prím található, ezért végtelen sok olyan prím lesz, amelynek az utolsó négy számjegye 4321.

Észrevétel. A feladat szólhatna 4321 helyett bármilyen más olyan számmal is, amely 2-vel és 5-tel nem osztható:
Hány olyan prímszám létezik, amelynek tízes számrendszerben az utolsó k számjegye $\overline{n_1n_2\dots n_k}$?
Erre is az lenne a válasz, hogy végtelen sok, amennyiben $(10,\overline{n_1n_2\dots n_k})=1$.

2.2 Feladat. Mely a, b, c pozitív egészek esetén lesz végtelen sok prím az $a+bk+cn$ alakú számok között, ahol $k = 0, 1, 2, \ldots$, $n = 0, 1, 2, \ldots$?

Megoldás.

Az biztosan szükséges feltétel, hogy $(a, b, c) = 1$, hiszen, ha $(a, b, c) = d$ akkor az $a + bk + cn$ alakú számok közül mindegyik osztható lesz d-vel, ami nem jó. Nézzük meg, hogy ez elégséges feltétel-e.
Ha $(a, b) = s$, akkor az $a + bk + cn$ számokat át tudjuk alakítani $s\left(\frac{a}{s} + \frac{b}{s}k\right) + cn$ alakba. Dirichlet tétele miatt az $\frac{a}{s}+\frac{b}{s}k$ alakú számok között végtelen sok prím van, hiszen $\left(\frac{a}{s}, \frac{b}{s}\right) = 1$. A c-nél nagyobb minden ilyen p_i-re az $sp_i + cn$ $(n = 0, 1, 2, ...)$ sorozatban megint végtelen sok prím található, hiszen $(sp_i, c) = 1$, mivel $(s, c) = (p_i, c) = 1$.
Azaz az $(a, b, c) = 1$ feltétel elégséges feltétel is.

3. Speciális alakú prímek: Fermat- és Mersenne-prímek

Ebben a fejezetben a $2^k + 1$ alakú prímeket, azaz a Fermat-prímeket, illetve a $2^k - 1$ alakú prímeket, azaz a Mersenne-prímeket fogjuk vizsgálni. Az első fejezetben már említettük, megoldatlan, hogy létezik-e végtelen sok ilyen alakú prím. Szintén az első fejezetben beláttuk, hogy végtelen sok összetett szám szerepel az ilyen alakúak között, hiszen $2^k + 1$ csak akkor lehet prím, ha k kettőhatvány, illetve, hogy $2^k - 1$ csak akkor lehet prím, ha k maga is prím. Tehát az $F_n = 2^{2^n} + 1$ Fermat-számokkal és az $M_p = 2^p - 1$ (ahol p prím) Mersenne-számokkal fogunk részletesebben foglalkozni. Ezen belül is, a prímeket fogjuk vizsgálni.

3.1. Fermat-számok

Először a Fermat-számokat nézzük meg. Jelenleg összesen 5 Fermat-prímet ismerünk, ezek a következők:

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

Fermat egyébként azt hitte, hogy minden Fermat-szám prímszám lesz, később Euler mutatta meg, hogy F_5 összetett.
Jelenleg amit tudunk a Fermat-számokról:

- $0 \leq n \leq 4$ esetén F_n prím
- $5 \leq n \leq 32$ esetén tudjuk, hogy F_n összetett, különböző mértékig ismerjük a prímtényezős felbontásukat, például $n = 5, 6, 7, 8, 9, 10, 11$ esetén a teljes faktorizációját ismerjük F_n-nek, F_{12}-nek a prímtényezős felbontásából hat tényezőt, F_{13}-nak négy tényezőjét ismerjük. Viszont például $n = 20$, 24 esetén semmit sem tudunk a felbontásukról, csak annyit, hogy összetett számok.
- nem tudjuk, hogy F_n összetett-e vagy prím a következő esetekben:
  $n = 33$, 34, 35, 40, 41, 44, ...

A Fermat-számok vizsgálatánál a következő két tétel ad hasznos segítséget annak eldöntésében, hogy egy adott Fermat-szám prím-e vagy összetett.

3.1.1 Tétel. *F_n bármely (pozitív) osztója $k2^{n+1} + 1$, sőt $n \geq 2$ esetén $r2^{n+2} + 1$ alakú.* ♣

Valószínűleg maga Euler is ezt a tételt használta F_5 összetettségének a megmutatására: F_5 prímosztói csak a $128r + 1$ alakú prímek között lehetnek. Ezek közül az első kettő a 257 és a 641, utóbbi osztója az F_5-nek.

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

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

Megjegyzés. A Pepin-tesztben a 3 helyére írhatnánk 5-öt vagy 10-et is, ha $n \geq 2$. Azaz ha $n \geq 2$, akkor F_n akkor és csak akkor prím, ha

$$5^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$ ♣

Bizonyítás. Először az odafele irányt bizonyítjuk, azaz tegyük fel, hogy F_n prím. Ekkor a tétel pontosan azt jelenti, hogy az 5 kvadratikus nemmaradék modulo F_n, azaz

$$\left(\frac{5}{F_n}\right) = -1$$

Ennek bizonyításához felhasználjuk, hogy mivel ($n \geq 1$ esetén) $2^{2^n} = 4^t$ (egész pontosan $t = 2^{n-1}$), így $F_n \equiv 1 \pmod 4$.
Ezen kívül $F_n = 4^t + 1 \equiv 2 \pmod 5$, mivel t páros.
Most alkalmazni fogjuk a kvadratikus reciprocitási tételt.

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Tehát az 5 kvadratikus nemmaradék modulo F_n. Ezzel az odafele irányt beláttuk.

A megfordításhoz azt tesszük fel, hogy

$$5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

Azt szeretnénk, hogy ebből valamilyen módon következzen, hogy F_n prím.
A fenti összefüggést négyzetre emelve kapjuk, hogy

$$5^{F_n-1} \equiv 1 \pmod{F_n}$$

Ebből, illetve az eredeti összefüggésből következik, hogy

$$O_{F_n}(5) \mid F_n - 1 \qquad \text{és} \qquad O_{F_n}(5) \nmid \frac{F_n - 1}{2}$$

Viszont azt is tudjuk, hogy $F_n = 2^{2^n} + 1$ tehát $F_n - 1$ kettőhatvány, amiből az következik, hogy $O_{F_n}(5) = F_n - 1$.
Mivel $O_{F_n}(5) \mid \varphi(F_n)$, így $F_n - 1 \mid \varphi(F_n)$.
Már majdnem készen vagyunk, csak azt kell még hozzávenni, hogy

$$\varphi(F_n) \leq F_n - 1$$

Így csak az lehetséges, hogy

$$F_n - 1 = \varphi(F_n) \Longleftrightarrow F_n \text{ prím.}$$

□

A megjegyzés elején említettük, hogy akár 10-et is írhatnánk 3 vagy 5 helyére. Ha ezt is be szeretnénk bizonyítani, akkor a fenti bizonyítás gondolatmenetét kell követnünk, annyiban változik csak, hogy azt kell belátnunk amikor az odafele irányt bizonyítjuk, hogy

$$\left(\frac{10}{F_n}\right) = -1$$

$$\left(\frac{10}{F_n}\right) = \left(\frac{2}{F_n}\right) \cdot \left(\frac{5}{F_n}\right)$$

Azt már tudjuk, hogy $\left(\frac{5}{F_n}\right) = -1$, már csak azt kellene igazolnunk, hogy

$$\left(\frac{2}{F_n}\right) = 1$$

Ez akkor teljesül, ha $F_n \equiv \pm 1 \pmod 8$.
Mivel $F_n = 2^{2^n} + 1 = 8s + 1$ (egész pontosan $s = 2^{2^n-3}$, ha $n \geq 2$), ezért

$$F_n \equiv 1 \pmod 8$$

Ez jó nekünk, mert ebből már következik, hogy

$$\left(\frac{10}{F_n}\right) = -1.$$

Az állítás megfordításának bizonyítása, azaz a visszafele irány ugyanúgy működik, mint az 5 esetében.

Észrevétel. A bizonyítás azon az egy dolgon múlik, hogy az odafele irány bizonyításánál be tudjuk-e bizonyítani, hogy

$$\left(\frac{k}{F_n}\right) = -1 \qquad \text{ahol } k \text{ az a szám, amit a 3 helyére szeretnénk írni}$$

Azt már tudjuk, hogy $\left(\frac{3}{F_n}\right) = \left(\frac{5}{F_n}\right) = \left(\frac{10}{F_n}\right) = -1$, illetve, hogy $\left(\frac{2}{F_n}\right) = 1$.

Ez azt jelenti, hogy például ha $k = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 10^{\alpha_4}$, ahol $\alpha_2 + \alpha_3 + \alpha_4$ páratlan, akkor a Pepin-teszt erre a k-ra is jó lesz. Nyilván a tesztnek gyakorlati szempontból nagyobb számokra nincs sok értelme, hiszen nehezebb ellenőrizni.

3.1.1 Feladat

a) Igazoljuk, hogy $F_{n+1} = F_0 F_1 \dots F_n + 2$.

Bizonyítás. Azt látjuk, hogy az $F_{n+1} - 2$-t kell felírnunk egy elég speciális szorzatalakban. Próbáljuk meg egyáltalán valamilyen szorzatalakba átírni $F_{n+1} - 2$-t!

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

Ez már elég jól néz ki, ugyanis tudjuk alkalmazni rá az $a^2 - b^2 = (a+b)(a-b)$ azonosságot:

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

Ha ezt az összefüggést most alkalmazzuk $F_n - 2$-re:

$$F_{n+1} - 2 = F_n(F_n - 2) = F_n F_{n-1}(F_{n-1} - 2)$$

$$\Rightarrow F_{n+1} - 2 = F_n F_{n-1} F_{n-2} \dots F_1 F_0 (F_0 - 2) = F_n F_{n-1} F_{n-2} \dots F_1 F_0$$

Innen átrendezéssel kapjuk a bizonyítandó állítást. □

b) Igazoljuk, hogy a Fermat-számok páronként relatív prímek.

Bizonyítás. Ennek bizonyításához felhasználjuk, hogy $F_k \mid F_n - 2$, ha $k < n$. (Ez az előző részfeladatból azonnal következik.)
Most tegyük fel indirekt, hogy $(F_k, F_n) = d$. Ekkor

$$F_k \mid F_n - 2 \quad \Rightarrow \quad d \mid F_n - 2$$

Viszont ebből következik:

$$d \mid F_n - (F_n - 2) = 2$$

$$\Rightarrow\ d = \pm 1 \text{ vagy } \pm 2$$

Azonban, figyelembe véve, hogy F_n páratlan, arra jutunk, hogy $d = \pm 1$. Ez pontosan azt jelenti, hogy a Fermat-számok páronként relatív prímek. □

Megjegyzés. Ennek felhasználával új bizonyítást adhatunk arra, hogy végtelen sok prím létezik.

Ha ugyanis egy q prímosztója F_n-nek, akkor semelyik másik F_k-nak ($k \neq n$) nem lehet osztója, hiszen relatív prímek. Mivel végtelen sok (különböző) Fermat-szám létezik, és mindegyiknek bármely prímosztója egyik másik Fermat-számnak sem osztója, így végtelen sok különböző ilyen q létezik.

3.1.2 Feladat. Legyen n pozitív egész. Mutassuk meg, hogy az $A_n = 2^{2^n} + 2^{2^{n-1}} + 1$ számnak legalább n különböző prímosztója van. (Arany Dániel, 13/14 haladó, II. kategória, döntő)

Megoldás. Bizonyítsunk teljes indukcióval!

1. Nézzük meg, hogy $n = 1$ - re illetve $n = 2$ - re igaz az állítás!
   $n = 1$ esetén $A_1 = 2^2 + 2^1 + 1 = 7$, de ez igazából nem is kell, hiszen minden egynél nagyobb számnak van legalább 1 prímosztója. Ez az eset tehát triviális.
   $n = 2$ esetén $A_2 = 2^{2^2} + 2^{2^1} + 1 = 2^4 + 4 + 1 = 21 = 3 \cdot 7$, tehát az állítás igaz.

2. Most tegyük fel, hogy $n > 2$ - re igaz az állítás!

3. Nézzük meg, mit mondhatunk el A_{n+1} - ről!
   $A_{n+1} = 2^{2^{n+1}} + 2^{2^n} + 1$.
   Legyen $2^{2^{n-1}} = a$. Ekkor $A_n = a^2 + a + 1$, illetve $A_{n+1} = a^4 + a^2 + 1$.
   Bontsuk szorzattá A_{n+1} - et! $A_{n+1} = a^4 + a^2 + 1 = (a^2 + a + 1)(a^2 - a + 1)$. Az indukciós feltevés azt állítja, hogy $a^2 + a + 1$ - nek legalább n különböző prímosztója van. Ha belátjuk, hogy az $a^2 - a + 1 = 2^{2^n} - 2^{2^{n-1}} + 1$ számnak létezik legalább 1 különböző prímosztója az előbb említett A_n szám prímosztóitól, akkor készen vagyunk. Ehhez nézzük meg A_{n+1} szorzattá alakítását:

$$A_{n+1} = (a^2 + a + 1)(a^2 - a + 1) = (2^{2^n} + 2^{2^{n-1}} + 1)(2^{2^n} - 2^{2^{n-1}} + 1)$$

Észrevehetjük, hogy a zárójelben szereplő tényezők különbsége: $2a = 2 \cdot 2^{2^{n-1}}$. Ha van olyan d, amely mindkét tényezőt osztja, akkor annak osztania kell a különbségüket is, azaz $2 \cdot 2^{2^{n-1}}$-t. Ebből az következik, hogy d kettőhatvány. De ez nem lehetséges, hiszen mindkét zárójelben szereplő tényező páratlan.
Tehát a két tényező egymáshoz képest relatív prím. Ez azt jelenti, hogy az $a^2 - a + 1 = 2^{2^n} - 2^{2^{n-1}} + 1 > 1$ számnak létezik legalább 1 különböző prímosztója A_n-től.

Azaz az $A_{n+1} = 2^{2^{n+1}} + 2^{2^n} + 1$ számnak létezik legalább $n + 1$ darab, különböző prímosztója. Tehát $n + 1$ - re is igaz az állítás.

A Fermat-prímeknek egyébként a szabályos sokszögek szerkesztésénél játszanak nagyon fontos szerepet, de ezzel most bővebben nem foglalkozunk.

3.2. Mersenne-számok

Most az $M_p = 2^p - 1$ (ahol p prím) Mersenne-számokat fogjuk megvizsgálni. Máig nem tudjuk általában, hogy mely M_p számok prímek vagy melyek összetettek.
Mersenne 1644-ben adott egy listát az M_p Mersenne-prímekről, ahol $p \leq 257$. Szerinte $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ esetén kapunk prímeket. De ez $p = 67, 257$ esetén nem igaz, másrészt a $p = 61, 89, 107$ prímek kimaradtak, amelyekre M_p prímszám.

Jelenleg összesen 48 Mersenne-prímet ismerünk, 2008-ban találták meg a 46-odik Mersenne-prímet, ez a $2^{43112609} - 1$ szám, amely 12 978 189 számjegyű, 2009-ben találták meg a (nála kisebb) 47-edik Mersenne-prímet, ez a $2^{42643801} - 1$ szám, amely 12 837 064 számjegyű, és 2013-ban találták meg a 48-adik Mersenne-prímet, ez a $2^{57885161} - 1$ szám, amely 17 425 170 számjegyből áll. Jelenleg ez a legnagyobb ismert prímszám.

A Mersenne-számok esetében is léteznek a Fermat-számokra érvényes tételekhez hasonló öszefüggések, ezeket fogjuk most megnézni.

3.2.1 Tétel. Legyen $p > 2$ prím. Ekkor M_p brámely (pozitív) osztója egyszerre $2kp + 1$ és $8r \pm 1$ alakú. ♣

Ezt a tételt nem bizonyítjuk be, de megnézzük néhány példán keresztül, hogyan tudjuk alkalmazni.

3.2.1 Feladat. Keressük meg az alábbi Mersenne-számok legkisebb prímosztóját:

a) $2^{23} - 1$

Megoldás. Az előbbi tételt alkalmazva: $2^{23} - 1 = M_{23}$ tetszőleges q prímosztója $46k + 1$ és $8r \pm 1$ alakú.

Szeretnénk megkeresni ezt a prímosztót (ha létezik ilyen viszonylag kis q). Ehhez a két feltételt kell egyszerre megnéznünk. Így adódik két szimultán kongruenciarendszer:

$$\begin{aligned} x &\equiv 1 \pmod{46} \\ x &\equiv \pm 1 \pmod{8} \end{aligned}$$

Ezt kell megoldanunk:

$$\begin{aligned} 46k+1 &\equiv \pm 1 \pmod{8} \\ 6k+1 &\equiv \pm 1 \pmod{8} \end{aligned}$$

$$\begin{aligned} 6k &\equiv 0 \pmod{8} \quad \text{vagy} \quad 6k \equiv -2 \pmod{8} \\ k &\equiv 0 \pmod{4} \quad \text{vagy} \quad k \equiv 1 \pmod{4} \end{aligned}$$

$$k = 4s \quad \text{vagy} \quad k = 4s+1$$

Innen már adódik a megoldás:

$$x = 184s+1 \quad \text{vagy} \quad x = 184s+47$$

azaz

$$x \equiv 1 \text{ és } 47 \pmod{184}$$

Az ilyen alakú prímek

$$q = 47,\ 599,\ 967, \ldots$$

Ezek után ellenőrizni kell, hogy ezek közül melyik osztja $2^{23}-1 = M_{23}$-at. Először a 47-tel próbálkozunk. Ezt úgy csináljuk, hogy 23-szor kétszerezve és az eredményt mindig modulo 47 redukálva ki tudjuk számolni 2^{23} modulo 47 vett maradékát, és kiderül, hogy ez a maradék 1, tehát $47 \mid 2^{23}-1$, és ez a legkisebb.

b) $2^{37}-1$

Megoldás. Tudjuk, hogy $2^{37}-1 = M_{37}$ tetszőleges q prímosztója $74k+1$ és $8r \pm 1$ alakú.
Az így adódó szimultán kongruenciarendszerek:

$$\begin{aligned} x &\equiv 1 \pmod{74} \\ x &\equiv \pm 1 \pmod{8} \end{aligned}$$

Azaz:

$$\begin{aligned} 74k+1 &\equiv \pm 1 \pmod{8} \\ 2k+1 &\equiv \pm 1 \pmod{8} \end{aligned}$$

$$\begin{aligned} 2k &\equiv 0 \pmod{8} \quad \text{vagy} \quad 2k \equiv -2 \pmod{8} \\ k &\equiv 0 \pmod{4} \quad \text{vagy} \quad k \equiv -1 \pmod{4} \end{aligned}$$

$$k = 4s \qquad \text{vagy} \qquad k = 4s - 1$$

Ezt visszahelyettesítve kapjuk:

$$x = 296s + 1 \qquad \text{vagy} \qquad x = 296s - 73$$

azaz

$$x \equiv 1 \text{ és } -73 \pmod{296}$$

Ilyen alakú prímek:

$$q = 223,\ 593,\ 1481,\ 1777, \ldots$$

Ezeket ugyanúgy tudjuk ellenőrizni, mint az előbb, és kiderül, hogy $223 \mid 2^{37} - 1$, és megintcsak ez a legkisebb.

Végül kimondjuk a Pepin-teszt Mersenne-számokra vonatkozó megfelelőjét.

3.2.2 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 akkor és csak akkor prím, ha

$$M_p \mid a_p - 1. \ \clubsuit$$

A Mersenne-prímeknek a páros tökéletes számoknál van nagy jelentőségük, ezzel a következő fejezetben foglalkozunk részletesebben.

4. Tökéletes számok

Ebben a fejezetben a tökéletes számokkal foglalkozunk. A definíciót követően néhány tulajdonságot fogunk megvizsgálni velük kapcsolatban. Az eddig tárgyaltakhoz szorosan kapcsolódik ez a téma, hiszen, ahogy majd a későbbiekben részletezzük, a Mersenne-prímeknek rendkívül sok közük van a páros tökéletes számokhoz.

Tökéletes számokkal már az ókori görögök is foglalkoztak. Tökéletesnek nevezték azokat a számokat, amelyek előállnak, mint a „részeik", azaz magát a számot kivéve, az osztóik összege. Ilyen szám például a $6 = 1 + 2 + 3$ vagy a $28 = 1 + 2 + 4 + 7 + 14$. A görögök ezen kívül még két tökéletes számot ismertek, ezek a 496 és a 8128. Azt, hogy mi köze van a Mersenne-prímeknek a tökéletes számokhoz, már Euklidész is felfedezte, amikor az Elemek című könyvében a következőket írta, majd be is bizonyította:
„Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk az utolsó tagot, akkor a szorzat tökéletes szám lesz."
E szerint a tétel szerint az

$$(1 + 2 + 2^2 + \ldots + 2^k)2^k = (2^{k+1} - 1)2^k$$

szám tökéletes, ha $2^{k+1} - 1$ prím, azaz $2^{k+1} - 1$ egy Mersenne-prím. Ezen túlmenően, Euler bebizonyította, hogy ez a konstrukció megadja az összes páros tökéletes számot. Ez azt jelenti, hogy minden Mersenne-prímhez találunk páros tökéletes számot, sőt, a két halmaz között létezik bijekció, azaz ekvivalensek. Mivel máig megoldatlan, hogy létezik-e végtelen sok Mersenne-prím, így azt sem tudjuk, hogy végtelen sok páros tökéletes szám van-e. Ezen kívül az is megoldatlan, hogy létezik-e páratlan tökéletes szám.
Most kimondjuk a tökéletes szám definícióját a mai terminológiával élve, illetve megnézünk néhány tételt a páros, illetve a páratlan tökéletes számokra nézve.

4.1 Definíció Az n pozitív egész *tökéletes szám*, ha $\sigma(n) = 2n$. ♣

4.1. Páros tökéletes számok

Mielőtt bármiféle tételt vagy általános összefüggést megállapítanánk a páros tökéletes számokkal kapcsolatban, ismerkedésképpen álljon itt egy bevezető feladat.

4.1.1 Feladat. Melyek azok a k pozitív egész számok, amelyekre $2 \cdot 3^k$ tökéletes szám? (KöMal, 2013, szeptember. B.4553.)

Megoldás. Az $n = 2 \cdot 3^k$ tökéletes szám, ha a pozitív osztóinak az összege éppen $2 \cdot 2 \cdot 3^k$, azaz, ha $\sigma(n) = 2^2 \cdot 3^k = 4 \cdot 3^k$.

Tudjuk: $\sigma(n) = (1 + 2)(1 + 3 + 3^2 + ... + 3^k) = 3 \cdot \frac{3^{k+1}-1}{3-1} = \frac{3}{2} \cdot (3^{k+1} - 1)$. Ennek kell egyenlőnek lennie $4 \cdot 3^k$ - nal.
Azaz:

$$\frac{3}{2} \cdot (3^{k+1} - 1) = 4 \cdot 3^k$$

Rendezve:

$$(\frac{1}{2} \cdot 3^2 - 4)3^{k-1} = \frac{1}{2}$$

Innen: $3^{k-1} = 1$, azaz $k = 1$. Csak ez az egy megoldás létezik.

4.1.1 Tétel. Egy n páros szám akkor és csak akkor tökéletes, ha $n = 2^{p-1}(2^p - 1)$ alakú, ahol $2^{p-1} - 1$ Mersenne-prím (azaz, ekkor p szükségszerûen prím). ♣

Ezt a tételt most nem bizonyítjuk be, viszont ennek felhasználásával bebizonyítjuk a következő tételt:

4.1.2 Tétel. Minden páros tökéletes szám utolsó számjegye 6 vagy 8 (a tízes számrendszerben). ♣

Bizonyítás. A 4.1.1 Tétel szerint n páros tökéletes szám $\Leftrightarrow n = 2^{p-1}(2^p - 1)$, ahol $2^p - 1$ prím.
Induljunk ki abból, hogy megnézzük, a kettőhatványok mire végződnek.
A megfigyeléseket egy táblázatba összegeztük, azaz, hogy k függvényében 2^k milyen maradékot ad modulo 10.

$k =?$	$2^k \equiv ?\pmod{10}$
1	2
2	4
3	8
4	6
5	2
6	4
7	8
8	6

stb.

Azt látjuk, hogy a maradékok periodikusan ismétlődnek, mindig az első négy szám követi egymást, ugyanolyan sorrendben. Azt is észrevehetjük, hogy ha k páratlan, akkor a maradék 2, vagy 8 lesz, ha pedig k páros, akkor 2^k végződése 4 vagy 6 lesz.
Tudjuk, ha $p > 2$, akkor p páratlan, $p - 1$ pedig páros. Ez azt jelenti, hogy 2^{p-1} végződhet 4-re vagy 6-ra:

– ha $2^{p-1} \equiv 4 \pmod{10}$, akkor $2^p \equiv 8 \pmod{10}$. Ez azt jelenti, hogy $2^p - 1 \equiv 7 \pmod{10}$.

$$\Rightarrow n = 2^{p-1}(2^p - 1) \equiv 4 \cdot 7 \equiv 8 \pmod{10}$$

Azaz ekkor n 8-ra végződik.
– ha $2^{p-1} \equiv 6 \pmod{10}$, akkor $2^p \equiv 2 \pmod{10}$. Ez azt jelenti, hogy $2^p - 1 \equiv 1 \pmod{10}$.

$$\Rightarrow n = 2^{p-1}(2^p - 1) \equiv 6 \cdot 1 \equiv 6 \pmod{10}$$

Azaz, ekkor pedig n 6-ra végződik.

Meg kell még vizsgálnunk a $p = 2$ esetet, ekkor $n = 2(2^2 - 1) = 6$, tehát erre az esetre is teljesül a tétel. □

4.2. Páratlan tökéletes számok

Most a páratlan tökéletes számokat fogjuk vizsgálni. Ahogy fentebb említettük, nem tudjuk, hogy léteznek-e egyáltalán ilyen számok, viszont *ha* léteznek, akkor az alábbi tétel szerint bizonyos tulajdonságokkal mindenképpen rendelkezniük kell.

4.2.1 Tétel. Ha létezik egy páratlan n tökéletes szám, akkor $n = s^2 p$, ahol p egy $4k + 1$ alakú prím. ♣

Bizonyítás. Tegyük fel, hogy n egy páratlan tökéletes szám. Nézzük meg, hogy mit tudunk róla ekkor.

Legyen n kanonikus alakja a következő: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, n páratlan, tehát $p_i \neq 2$, és mivel tökéletes, így $\sigma(n) = 2n$.
A $\sigma(n)$ tulajdonságait kihasználva:

$$\sigma(n) = 2n = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i})$$

Ebből az következik, hogy a szorzatban van pontosan egy tényező, ami osztható kettővel, de 4-gyel már nem, hiszen n páratlan. A többi tényező pedig páratlan.
Azaz, $\exists\, i$, hogy $(1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i})$ páros, de 4-gyel nem osztható. Mivel p_i páratlan és minden hatványa páratlan, így ez az összeg csak akkor tud páros lenni, ha α_i páratlan.

Ekkor már a bizonyítás felével készen vagyunk, hiszen ha van pontosan egy páratlan α_i, akkor a hozzá tartozó p_i legyen p. Ekkor $p^{\alpha_i - 1}$-t leválasztjuk, és így kapunk két tényezőt: p-t, ami páros, valamint $s = p_2^{\alpha_2} \dots p_r^{\alpha_r} \cdot p^{\alpha_i - 1}$, ahol minden α_j páros, tehát s négyzetszám. Tehát ekkor $n = s^2 p$, ahol s páratlan. Már csak az hiányzik, hogy $p = 4k + 1$ alakú. Ezt indirekt bizonyítuk: tegyük fel, hogy

$$p \equiv -1 \pmod 4$$

Nézzük meg, hogy ekkor mi történik az $(1 + p + p^2 + \ldots + p)$ összeg esetében. Mivel

$$p \equiv -1 \pmod 4,$$

így p minden párosadik hatványa 4-gyel osztva 1 maradékot ad, míg páratlanadik hatványai -1-et adnak. Azaz

$$p^{2k} \equiv 1 \pmod 4, \text{ és}$$
$$p^{2k+1} \equiv -1 \pmod 4$$

Ez azt jelenti, hogy

$$1 + p + p^2 + \ldots + p^{\alpha_i} \equiv 1 - 1 + 1 - 1 \pm \ldots + 1 - 1 \equiv 0 \pmod 4$$

Ebből az következik, hogy $\sigma(n) \equiv 0 \pmod 4$, ami ellentmondás, hiszen tudjuk, hogy $\sigma(n)$ bár páros, de nem osztható 4-gyel. Azaz $p \equiv 1$, ezzel az állítást bebizonyítottuk. □

4.3. Bővelkedő és hiányos számok

4.3.1 Definíció Egy n számot *hiányosnak* nevezünk, ha nagyobb, mint a nála kisebb pozitív osztóinak az összege, azaz, ha $\sigma(n) < 2n$. ♣

4.3.2 Tétel. Minden prímhatvány hiányos szám. ♣

Bizonyítás. Legyen $n = p^\alpha$. Ekkor azt kell belátnunk, hogy $\sigma(n) = \sigma(p^\alpha) < 2p^\alpha$.
Ehhez írjuk fel $\sigma(n)$-nek a képletét!

$$\sigma(n) = \sigma(p^\alpha) = (1 + p + p^2 + \ldots + p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}$$

$$\sigma(p^\alpha) - p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} - p^\alpha = \frac{p^{\alpha+1} - 1 - p^{\alpha+1} + p^\alpha}{p - 1} = \frac{p^\alpha - 1}{p - 1}$$

$$\frac{p^\alpha - 1}{p - 1} < p^\alpha \quad \Longleftrightarrow \quad \sigma(p^\alpha) < 2p^\alpha.$$

□

A következőkben kiderül, hogy ha nem teszünk fel ilyen erős feltételt, n akkor is lehet hiányos. Egy olyan tételt nézünk meg, ami a páratlan „majdnem prímhatványokról" szól.

4.3.3 Tétel. Ha egy n páratlan számnak csak két különböző prímosztója van, akkor n hiányos. ♣

Bizonyítás. Legyen n páratlan, azaz $p_i > 2$, és $n = p_1^{\alpha_1} p_2^{\alpha_2}$. Ekkor azt kell belátnunk, hogy

$$\sigma(n) < 2n \quad \Longleftrightarrow \quad \frac{\sigma(n)}{n} < 2$$

A $\sigma(n)$ multiplikativitását felhasználva:

$$\frac{\sigma(n)}{n} = \frac{\sigma(p_1^{\alpha_1} p_2^{\alpha_2})}{p_1^{\alpha_1} p_2^{\alpha_2}} = \frac{\sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})}{p_1^{\alpha_1} p_2^{\alpha_2}} = \frac{\frac{p_1^{\alpha_1+1}-1}{p_1-1}}{p_1^{\alpha_1}} \cdot \frac{\frac{p_2^{\alpha_2+1}-1}{p_2-1}}{p_2^{\alpha_2}} = \frac{p_1 - \frac{1}{p_1^{\alpha_1}}}{p_1 - 1} \cdot \frac{p_2 - \frac{1}{p_2^{\alpha_2}}}{p_2 - 1}$$

Most ezt a szorzatot felülről becsüljük, hogy közelebb jussunk a bizonyítandó állításhoz.

$$\frac{p_1 - \frac{1}{p_1^{\alpha_1}}}{p_1 - 1} \cdot \frac{p_2 - \frac{1}{p_2^{\alpha_2}}}{p_2 - 1} < \frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} = \left(1 + \frac{1}{p_1 - 1}\right)\left(1 + \frac{1}{p_2 - 1}\right)$$

Erről kell megmutatnunk, hogy kisebb, mint 2. Észrevehetjük, hogy ahogy p_i nő, úgy az $\frac{1}{p_i - 1}$ tört értéke egyre kisebb lesz, ezáltal $1 + \frac{1}{p_1 - 1}$ értéke is egyre csökken. Ezért nézzük

meg, hogy hol van a két törtnek, és ezáltal az egész szorzatnak a maximuma! Mivel mindkét prímosztó páratlan, így a maximum:

$$\frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

Ezzel az állítást bebibizonyítottuk. □

Most röviden foglalkozunk a *bővelkedő* számokkal is.

4.3.4 Definíció Egy n számot *bővelkedőnek* nevezünk, ha kisebb, mint a nála kisebb pozitív osztóinak az összege, azaz, ha $\sigma(n) > 2n$. ♣

4.3.5 Tétel. Egy bővelkedő szám minden többszöröse is bővelkedő. ♣

Bizonyítás. Legyen n egy bővelkedő szám, azaz $\sigma(n) > 2n$, és legyen n tetszőleges többszöröse kn. Ekkor ahhoz, hogy kn is bővelkedő legyen, azt kell belátni, hogy $\sigma(kn) > 2kn$. Amit tudunk: $2kn < k \cdot \sigma(n)$. Már csak azt kellene bebizonyítani, hogy $k \cdot \sigma(n) < \sigma(kn)$. Ennek igazolásához n összes osztója legyen $d_1, d_2, \ldots, d_l$. Ekkor

$$k \cdot \sigma(n) = k(d_1 + d_2 + \ldots + d_l) = kd_1 + kd_2 + \ldots + kd_l$$

Mivel $kd_i \mid kn$, így kn osztóinak az összege legalább annyi, mint n osztói összegének a k-szorosa. Ez azt jelenti, hogy

$$k \cdot \sigma(n) \leq \sigma(kn)$$

Azaz

$$2kn < k \cdot \sigma(n) \leq \sigma(kn).$$

Megjegyzés. A második egyenlőtlenségnél szerepelhetne szigorú egyenlőtlenség is. Tudniillik, kn osztói között is szerepelnek n osztói, azaz $d_1, d_2, \ldots, d_l$, viszont közülük az 1 biztosan nem áll elő n osztójának többszöröseként, ha $k > 1$. Mindezekből az következik, hogy

$$k \cdot \sigma(n) < \sigma(kn).$$

□

4.4. Egyéb érdekes számok

Végül megnézünk hasolnó tulajdonságokkal rendelkező számokat, amelyeknek mind köze van az előbbiekhez, az osztók összegéhez.

4.4.1 Definíció Egy n számot *kvázitökéletes* számnak nevezünk, ha előáll, mint a nála kisebb, de 1-nél nagyobb pozitív osztók összege, azaz, ha $\sigma(n) = 2n + 1$. ♣

A tökéletes számok definíciójától nem sokban különbözik ez a definíció, mégis máig megoldatlan probléma, hogy egyáltalán létezik-e kvázitökéletes szám. Ennek ellenére a tulajdonságait tudjuk vizsgálni, és így eljuthatunk a következő tételhez:

4.4.2 Tétel. Ha létezik egy n kvázitökéletes szám, akkor egy páratlan szám négyzete, azaz $n = s^2$, ahol s páratlan. ♣

Bizonyítás. Legyen n olyan, hogy $\sigma(n) = 2n + 1$, és legyen n prímtényezős felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$.
Ekkor

$$\sigma(n) = (1 + p_1 + \ldots + p_1^{\alpha_1}) \cdot \ldots \cdot (1 + p_r + \ldots + p_r^{\alpha_r}) = 2n + 1$$

Ebből az következik, hogy a szorzatban minden tényező páratlan, hiszen máskülöben nem lehet a szorzatuk páratlan.

– ha minden p_i páratlan, akkor minden α_i páros, hiszen csak úgy lehet minden tényező páratlan, ha p_i hatványaiból páros sokat adunk össze. Ha minden α_i páros, akkor n egy páratlan szám négyzete.
– ha nem minden p_i páratlan, akkor $p_1 = 2$, viszont a többi p_i páratlan, és a hozzájuk tartozó α_i-k pedig párosak. Így n valamely páratlan szám négyzete lesz, csak meg van még szorozva egy kettőhatvánnyal. Azaz

$$n = 2^k t^2$$

$$\Rightarrow\ 2n + 1 = 2(2^k t^2) + 1 = 2^{k+1} t^2 + 1 = \sigma(n) = \sigma(2^k)\sigma(t^2) = (2^{k+1} - 1)\sigma(t^2)$$

Most mind a két oldalból kivonunk $(2^{k+1} - 1)t^2$-et:

$$t^2 + 1 = (2^{k+1} - 1)(\sigma(t^2) - t^2).$$

Itt azt látjuk, hogy t^2+1-nek van egy $4k-1$ alakú osztója. Ez pedig ellentmondás, korábban beláttuk, hogy egy $n^2 + 1$ alakú számnak nem lehet $4k - 1$ alakú prímosztója. □

4.4.3 Definíció Az $a \neq b$ pozitív egészek *barátságos* számpárt alkotnak, ha $\sigma(a) = \sigma(b) = a + b$. ♣

A barátságos számok fogalma is az ókori görögöktől származik. Ők úgy nevezték őket, hogy 2 szám barátságos, ha „az egyik szám részeiből (azaz a nála kisebb pozitív osztóiból) éppen összeáll a másik szám, és viszont." Ilyen számpár például a 220 és a 284. Szintén megoldatlan probléma, hogy létezik-e végtelen sok barátságos számpár, vagy hogy létezik-e olyan számpár, ahol a két szám relatív prím egymáshoz. Most megnézünk egy tételt a barátságos számokra vonatkozóan.

4.4.4 Tétel.

a) Egy barátságos számpár egyik tagja hiányos, a másik pedig bővelkedő szám.
b) Egy barátságos számpár egyik eleme sem lehet kettőhatvány. ♣

Bizonyítás. Legyen a és b egy barátságos számpár, azaz $\sigma(a) = \sigma(b) = a + b$.
a) Mivel $a \neq b$, így feltehetjük, hogy $a > b$.
Most nézzük meg, hogy mit tudunk elmondani külön-külön az osztók összegéről:

$$\sigma(a) = a + b < 2a$$

$$\sigma(b) = a + b > 2b$$

Ez pontosan azt jelenti, hogy a hiányos, b pedig bővelkedő szám.

b) Ha b bővelkedő szám, akkor ő nem lehet kettőhatvány, hiszen korábban bebizonyítottuk, hogy minden prímhatvány hiányos szám.
Már csak az a-ról kellene belátni, hogy ő sem kettőhatvány. Ezt indirekt bizonyítjuk:
Tegyük fel hogy $a = 2^k$. Ekkor

$$\sigma(a) = (1 + 2 + \ldots + 2^k) = 2^{k+1} - 1 = \sigma(b) = a + b$$

Innen fejezzük ki b-t!

$$b = 2^{k+1} - 1 - a = 2^{k+1} - 1 - 2^k = 2^k - 1$$

Ez azt jelenti, hogy $b \equiv -1 \pmod 4$. Mivel b és $\sigma(b)$ is páratlan, így b egy páratlan szám négyzete kell legyen. Viszont ez ellentmondás, mert egy négyzetszám nem adhat -1 maradékot 4-gyel osztva. □

Irodalomjegyzék

[1] Freud Róbert - Gyarmati Edit: Számelmélet.
Nemzeti Tankönyvkiadó Zrt., Budapest, 2006.

[2] www.komal.hu

[3] www.eszesen2010.hu

[4] www.mersenne.org