

*A matematika a tudományok királynője.  
A számelmélet a matematika királynője.*

Carl Friedrich Gauss (1777-1855)

## Számelméleti alapfogalmak

### Oszthatóság a racionális egészek körében

Racionális egészek között fogunk az oszthatóságról beszélni a továbbiakban, ha a megfogalmazásaink a kedves olvasó számára első pillanatra körülményesnek v. fölöslegesen komplikáltak tűnnek annak egyik oka az is lehet, hogy igyekszünk minél általánosabban fogalmazni. Nevezetesen oszthatóságról tetszőleges integritás tartományban is szokás beszélni, s az alább következő fogalmak nem triviálisak már test feletti polinom gyűrűk esetén sem, amelyekről remélhetőleg lesz módunk még e félévben szót ejteni.

**Definíció:** A  $b$  osztója  $a$ -nak, ha van olyan  $c$  egész, hogy  $a=bc$ . Jele:  $b|a$ .

Jegyezzük meg, hogy a  $0$  bármely  $b$  számmal osztható, mivel  $0=b0$  mindig teljesedik.

**Tétel:** Ha  $b|a$  és  $b|d$ , akkor  $b|a±d$ .

**Bizonyítás:** Valóban  $b|a$  és  $b|d$  definíció szerint azt jelenti, hogy van olyan  $c_1, c_2$  melyekre  $a=bc_1, d=bc_2$  s a két egyenlet összeadásával ill. kivonásával  $a±d=bc_1±bc_2=b(c_1±c_2)$ , amiből már következik, hogy  $b|a±d$ .

**Definíció:** Az  $I$  osztóit egységeknek nevezzük.

**Definíció:** Az  $a$ -t ill.  $b$ -t asszociáltaknak mondjuk, ha csak egység szorzóban különböznek egymástól, azaz  $a=bε$ , ahol  $ε|I$ .

Itt említjük meg, hogy a racionális egészek gyűrűjében két egység van a  $+1$  és a  $-1$ , ezért egy a számnak két asszociáltja van  $a$  és  $-a$ . Találkozni fogunk olyan gyűrűkkel is amelyekben végtelen sok egység van. Az egységek halmazát jelöljük  $U$ -val az angol *unit* szóra utalva. Az  $ε$  egység definíciójából ( $ε|I \Rightarrow I=εε^{-1}=εε^{-1}$ ) rögtön adódik, hogy van multiplikatív inverze  $ε^{-1}$ , s ha  $ε_1$  is egység ( $ε_1|I \Rightarrow I=ε_1ε_1^{-1}$ ) akkor a szorzatuk  $εε_1$  is az (szorozza össze  $I=εε^{-1}$  és  $I=ε_1ε_1^{-1}$ -t, akkor rendezés után  $I=(εε_1)(ε^{-1}ε_1^{-1})$  látható, hogy  $εε_1$  is egység), mivel integritástartomány elemei között a szorzás asszociatív és kommutatív adódott, hogy az egységek Abel-csoportot alkotnak a gyűrűbeli szorzásra nézve, ezt a csoportot az  $R$  gyűrű  $U$  egység csoportjának nevezzük. Ajánljuk a Kedves Olvasónak, hogy mutassa meg, hogy  $Z(\sqrt{2}), Z(\sqrt{11})$ -ben végtelen sok egység van, de  $Z(\sqrt{-1})$  pontosan 4 egység van  $\{1, -1, \sqrt{-1}, -\sqrt{-1}\}$ . Legyen „ $d$ ” olyan racionális egész szám, amely nem négyzetszám, (sőt, legyen „ $d$ ” négyzetmentes azaz ne ossza egyetlen egy „ $p$ ” prímszám négyzete sem) azaz ne teljesedjék semmilyen „ $x$ ” racionális egész számra sem, hogy  $d = x^2$ . Nem nehéz megmutatni, ekkor hogy a  $Z(d) = \{a + b\sqrt{d} | \forall a, b \in Z\}$  alakú komplex számok (ha  $d > 1$ , akkor valós számok) a szokásos összeadásra és szorzásra nézve integritás tartományt alkotnak. S a  $Q(d) = \{a + b\sqrt{d} | \forall a, b \in Q\}$  alakú számok testet alkotnak. Valóban például legyen  $d=17$ . Ekkor annak a belátása, hogy az  $a + b\sqrt{17}$  alakú valós számok ( ahol  $\forall a, b \in Z$  ) a valós számok között szokásos összeadásra, szorzásra nézve integritás tartományt alkotnak alkotnak, mindössze annyi indoklás kíván:

**1. Az összeadásra nézve:**

i, bármely  $\alpha = a_\alpha + b_\alpha \sqrt{17}$  és  $\beta = a_\beta + b_\beta \sqrt{17}$  valós számok összege ugyancsak  $\gamma = a_\gamma + b_\gamma \sqrt{17}$  alakú, mert  $a_\gamma = a_\alpha + a_\beta, b_\gamma = b_\alpha + b_\beta$  racionális egészek, mert  $a_\alpha, a_\beta, b_\alpha, b_\beta$  is racionális egész volt.

ii,  $0 \in Z(\sqrt{17})$ , mert  $0 = 0 + 0\sqrt{17}$ ,

iii, továbbá, ha  $a + b\sqrt{17} \in Z(\sqrt{17}) \Rightarrow (-a - b\sqrt{17} \in Z(\sqrt{17}))$

iv, másrészt, ha bármely három ",\$( valós szám összeadására igaz az asszociativitás, akkor igaz marad az asszociativitás akkor is ha speciel  $a + b\sqrt{17}$  alakú valós számokat adunk össze

v, s ha bármely kettő ",\$ valós szám összeadására igaz a kommutativitás, akkor igaz marad, akkor is ha speciel  $a + b\sqrt{17}$  alakú valós számokat adunk össze.

## 2. A szorzásra nézve:

i bármely  $\alpha = a_\alpha + b_\alpha\sqrt{17}$  és  $\beta = a_\beta + b_\beta\sqrt{17}$  valós számok szorzata ugyancsak  $\gamma = a_\gamma + b_\gamma\sqrt{17}$  alakú, mert  $a_\gamma = a_\alpha a_\beta + 17b_\alpha b_\beta$ ,  $b_\gamma = (a_\alpha b_\beta + b_\alpha a_\beta)$  racionális egészek, mert  $a_\alpha, a_\beta, b_\alpha, b_\beta$  is racionális egészek, s racionális egészek szorzata és összege, egész számszorosa is racionális egész.

ii.  $1 \in Z(\sqrt{17})$ , mert  $1 = 1 + 0\sqrt{17}$

iii, másrészt, ha bármely három valós szám szorzatára igaz az asszociativitás, akkor igaz marad az asszociativitás akkor is, ha speciel  $a + b\sqrt{17}$  alakú valós számokat szorzunk össze

iv. s ha bármely kettő valós szám szorzatára igaz a kommutativitás, akkor igaz marad, akkor is ha speciel  $a + b\sqrt{17}$  alakú valós számokat szorzunk össze.

3. A **disztributivitás is teljesül**. Ha bármely három ",\$( valós számra igaz a disztributivitás, akkor igaz marad akkor is ha  $a + b\sqrt{17}$  alakú valós számokat tekintünk.

4. Ha a valós számok között nincs zérus osztó akkor a valós számoknak abban a valódi részhalmozában sincs, amely csupán  $a + b\sqrt{17}$  alakú valós számokból áll (még most is  $\forall a, b \in Z$ ).

S elegendő meglátni azt, hogy  $(\sqrt{17} - 4) \cdot (\sqrt{17} + 4) = 1$ , s mindkettő oldalt  $n$ . hatványozva  $(\sqrt{17} - 4)^n \cdot (\sqrt{17} + 4)^n = 1^n = 1$ , miatt  $(\sqrt{17} - 4)^n$ , és  $(\sqrt{17} + 4)^n$  is egység bármely  $n \in N$  esetén.

Ha a Szorgalmas Olvasónk, az óhajtja megmutatni, hogy  $Q(\mathbf{17}) = \{a + b\sqrt{17} \mid \forall a, b \in Q\}$  test, akkor könnyedén beláthatja, hogy elegendő a  $Z(\mathbf{17}) = \{a + b\sqrt{17} \mid \forall a, b \in Z\}$  kapcsolatban leírtakat kiegészítenie azzal, hogy  $a + b\sqrt{17}, \forall a, b \in Q$  alakú valós számok multiplikatív inverze

$$\frac{1}{a + b\sqrt{17}} = \frac{a - b\sqrt{17}}{(a + b\sqrt{17}) \cdot (a - b\sqrt{17})} = \frac{a}{a^2 - 17 \cdot b^2} - \frac{b}{a^2 - 17 \cdot b^2} \sqrt{17} \text{ is } a + b\sqrt{17}, \forall a, b \in Q \text{ alakú. Miért}$$

is nem nulla  $a^2 - 17 \cdot b^2$  ?!

Oszthatóság szempontjából egy szám és asszociáltjai között úgy látszik nem érdemes különbséget tenni, azaz az egymáshoz asszociált elemeket azonos osztályba sorolhatjuk és mindegyik osztályt egy-egy kitüntetett elemmel reprezentálunk. A racionális egészek esetében minden  $0$ -tól különböző osztályba két elem van pozitív  $a$  és  $-a$  s a tanító nénijeinknek is köszönhetően hagyományosan a pozitív egészekkel reprezentáljuk az előbb említett osztályokat. Formálisan az  $R$  gyűrű multiplikatív félcsoportján értelmezzünk egy  $\rho$  relációt.  $r, s \in R$  esetén  $r \rho$ -ra nézve relációban van  $s$ -el, ha  $\exists \varepsilon \in U$ , melyre teljesül, hogy  $r = s\varepsilon$ . Meg lehet mutatni, hogy  $\rho$  ekvivalencia reláció  $R$ -en, s a  $\rho$  által indukált osztályozás az  $R$  multiplikatív félcsoportjának egy kompatibilis osztályozása, s oszthatóság kapcsán pont ezen osztályok érdekesekek számunkra.

**Tétel (a maradékos osztás tétele):** Bármely  $a$  és  $b \neq 0$  eleme  $Z$  esetén egyértelműen létezik olyan  $q, r \in Z$ , hogy  $a = bq + r$  és  $0 < r < |b|$  vagy  $r = 0$ .

**Bizonyítás:** Az általánosság megszorítása nélkül feltehetjük, hogy  $a$  is,  $b$  is pozitív és  $b < a$ . Tekintsük  $b$  többszöröseit  $nb$ -t valamely  $n_0$ -ra  $bn_0 \leq a < b(n_0 + 1)$ , ekkor  $n_0 = q$  és  $r = a - bn_0$  választással adódik a tétel egzisztenciára vonatkozó állítása. Az unicitást indirekt bizonyítsuk azaz tegyük fel, hogy  $a = bq + r$  és  $a = bq' + r'$  is teljesedik. A két egyenletet kivonva egymásból és rendezve  $b(q' - q) = r - r'$  adódik. Figyelembe véve, hogy a tétel feltétele szerint  $0 \leq r, r' < |b|$ , ekkor  $0 \leq |r - r'| < |b| - b$   $r - r' = 0$  adódik és így  $q' - q = 0$ , ami ellentmond a feltevésünknek.

**Definíció:** Az  $a$  és  $b$  egész számok legnagyobb közös osztójának nevezzük a  $d$  egész számot, ha rendelkezik az alábbi két tulajdonsággal:

(i)  $d|a$  és  $d|b$

(ii) ha  $d_1|a$  és  $d_1|b$ , akkor  $d_1|d$ .

Jele:  $d=(a,b)$  vagy  $lnko(a,b)$ .

**Tétel:** A legnagyobb közös osztó egység szorzó erejéig egyértelműen meghatározott.

A legnagyobb közös osztó hagyományos iskolai definíciója, mely szerint a és b közös osztói közül a legnagyobb, a racionális egészek körében teljesen megfelel, s ott az előbbi tétel, úgy módosulna, hogy az  $lnko(a,b)$  egyértelműen meghatározott. Vegye észre, hogy  $lnko(0,a)=|a|$  és  $lnko(0,0)=0$ .

**Bizonyítás:** Valóban ha  $d_1$  és  $d_2$  is egyenlő a  $lnko(a,b)$ , akkor a (ii) tulajdonság miatt  $d_1|d_2$  és  $d_2|d_1$  is teljesül vagyis van olyan  $c_1, c_2$  melyekre  $d_1=d_2c_1$  és  $d_2=d_1c_2$ . Az utolsó egyenlet jobb oldalát az azt megelőző egyenletbe helyettesítve és rendezve  $d_1=d_1c_2c_1$ , s mivel a szorzásra érvényes a kancellatív szabály ezért  $1=c_1c_2$ , azaz  $c_1$  és  $c_2$  is egység.

Tegyük fel hogy  $b \neq 0$ . Az alábbi algoritmus még Euklidesztől származik.

$$a = bq_0 + r_0, 0 < r_0 < |b|,$$

$$b = r_0q_1 + r_1, 0 < r_1 < r_0$$

$$r_0 = r_1q_2 + r_2, 0 < r_2 < r_1$$

.....

.....

$$r_{k-2} = r_{k-1}q_k + r_k, 0 < r_k < r_{k-1},$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1} + 0, (\text{azaz } r_{n+1} = 0)$$

**Tétel:** Az euklideszi algoritmus utolsó nem nulla maradéka  $r_n$  az a és b legnagyobb közös osztója.

**Bizonyítás:** Mutassuk meg először fentről lefelé haladva, hogy  $r_n$  - t osztja, bármely  $d$  közös osztóját  $a$ -nak ill.  $b$ -nek. A fenti egyenletek közül az elsőből következik, hogy  $d|r_0$ , a másodikból  $d|r_0$  és  $d|b$  miatt  $d|r_1$  adódik, ..., az  $n-2$  egyenletből, mivel  $d|r_{n-2}$  és  $d|r_{n-1}$  következik végül, hogy  $d|r_n$ .

Ha alulról jövünk felfelé, akkor azt lehet könnyen, látni, hogy  $r_n$  közös osztója  $a$ -nak ill.  $b$ -nek. Valóban az utolsó egyenlet azt jelenti, hogy  $r_n$  osztja  $r_{n-1}$ -t, az utolsó előttiből  $r_n|r_n$ -t és  $r_n|r_{n-1}$ -ből adódik, hogy  $r_n$  osztja  $r_{n-2}$ , és így tovább végül az első egyenletből következik,  $r_n|b$  és  $r_n|r_0$  miatt  $r_n|a$ -t.

**Következmény:** Bármely két racionális egész számnak létezik legnagyobb közös osztója.

Ha  $b$  nem nulla, akkor az euklideszi algoritmust alkalmazva a tételből közvetlenül adódik az állítás, ha  $b=0$ , akkor  $lnko(a,0)=|a|$ .

Annak a ténynek, hogy bármely két racionális egész számnak létezik legnagyobb közös osztója egy sereg fontos következménye van, melyek közül az alábbiakban felsorolunk és bizonyítunk is néhányat.

**Tétel:** Ha  $d=(a,b)$ , akkor létezik olyan  $x_0$  ill.  $y_0$  egész számok melyekre  $d=ax_0+by_0$ .

**Bizonyítás:** Az euklideszi algoritmus segítségével történhet a bizonyítás. Az első egyenletből  $r_0=a-bq_0=au_0+bv_0$  ( ,ahol  $u_0=1$  és  $v_0=-q_0$  ), a másodikból ( felhasználva az előbbit ),

$$b-r_0q_1=r_1 \Rightarrow b-r_0q_1=b-(a-bq_0)q_1=b(1+q_0q_1)-aq_1=r_1,$$

$$\text{azaz } r_1=au_1+bv_1, (\text{ahol } v_1=1+q_0q_1 \text{ ill. } u_1=-q_1).$$

Tételezzük fel, hogy

$$r_{k-2} = au_{k-2} + bv_{k-2} \text{ és } r_{k-1} = au_{k-1} + bv_{k-1},$$

akkor az euklideszi algoritmus  $k-2$ . lépésében szereplő  $r_{k-2} = r_{k-1}q_k + r_k$  egyenlőségből következik, hogy

$$r_k = au_k + bv_k \text{ ( ahol } u_k = u_{k-2} - u_{k-1}q_k, v_k = v_{k-2} - v_{k-1}q_k \text{ ) .}$$

Végül is  $k$  helyébe  $(n-2)$ -t, s  $u_n$  ill.  $v_n$  helyett  $x_0, y_0$ -t írva adódik a tétel állítása.

Az euklideszi algoritmust beépítik a legtöbb komputer algebrai rendszerbe is. A Maple-ben például a következő módon is meg lehet oldani:

```
> euclid:= proc(a,b)
  local i;
  global a1,b1,r,q;
  a1:=a;b1:=b;
  while(evalb(b1>0)) do
    r:=irem(a1,b1); q:=iquo(a1,b1);
    lprint(cat(a1,"=",b1,"*",q,"+",r));
    a1:=b1; b1:=r;
  end do;
end;
> euclid(2004,1456);
2004=1456*1+548
1456=548*2+360
548=360*1+188
360=188*1+172
188=172*1+16
172=16*10+12
16=12*1+4
12=4*3+0
> with(numtheory);
> print(cat(2004/1456,`=`,cfraction(2004/1456)));
```

$$\left\| \begin{pmatrix} 501 \\ 364 \end{pmatrix} \right\| = \left\| \begin{pmatrix} 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{10 + \frac{1}{1 + \frac{1}{3}}}}} \end{pmatrix} \right.$$

**Tétel(Lamé<sup>1</sup>):** Az  $a, b$  ( $a > b$ ) számok legnagyobb közös osztójának az euklideszi algoritmussal történő kiszámításához legfeljebb  $5 \log_{10}(b)$ -szer kell a maradékos osztást végrehajtani.

---

<sup>1</sup> Lamé, Gabriel (1795-1870) az École Polytechnique-n tanult. Vasút mérnök volt. Matematikában a fő területe a matematikai fizika volt. A számelméletben is jelentős eredményeket ért el. Be bizonyította a nagy Fermat tétel  $n=7$  esetét. Azaz azt, hogy az  $x^7 + y^7 = z^7$  egyenletnek nincs az egészek körében triviálistól különböző megoldása. Triviális például az  $x = z = 2009, y = 0$  megoldás. Meglepő, hogy Gauss Lamét tartotta kora legjelentősebb francia matematikusának. (Lehet, hogy neki volt igaza?!)

**Megjegyzés:** A legnagyobb közös osztót lehet egy további mondjuk harmadik módon is definiálni:

$$d = (a, b) \stackrel{\text{def.}}{=} \min_{ax+by \neq 0} (|ax+by|),$$

és  $a=b=0$ , akkor  $(0,0)=0$ . Az előbbi definíció valóban bármely  $a, b$  számpárhoz hozzá rendel egy nem negatív egészet, mivel a természetes számok a szokásos rendezésre jól rendezett halmazt alkotnak, azaz a természetes számok bármely nem üres részhalmazának van legkisebb eleme így speciel az  $S = \{s \mid s = |ax+by|, |ax+by| \neq 0, \forall x, y \in \mathbb{Z}\}$

halmaznak is. Legyen most  $d_0 = \min_{ax+by \neq 0} (|ax+by|)$ , azaz valamely  $x_0, y_0$  egészekre  $d_0 = ax_0 + by_0$ . Mutassuk meg pl., hogy  $d_0 \mid$ .

Bizonyítsunk indirekt, mivel  $d_0$  nem nulla  $a$ -t maradékosan oszthatjuk  $d_0$ -lal, azaz legyen  $a = d_0q + r$ ,  $0 < r < d_0$ . Az  $a = d_0q + r$  egyenletbe  $d_0$ -t helyettesítve  $ax_0 + by_0$  -lal, rendezés után adódik, hogy  $r = a(1 - x_0q) + b(-y_0q)$ , s mivel  $0 < r < d_0$ , ez ellentmond  $d_0$  minimalitásának. A *lnko.* (ii) tulajdonsága, hogy ha  $d \mid a$ -t és  $d \mid b$ -t, akkor triviális, hogy  $d \mid d_0$ , mert  $d_0 = ax_0 + by_0$ .

**Definíció:** Ha  $(a, b) = 1$ , akkor azt mondom, hogy  $a$  és  $b$  relatív prímek.

**Tétel:** Ha  $(a, b) = 1$  és  $(a, c) = 1$ , akkor  $(a, bc) = 1$ .

**Bizonyítás:** Legyen  $1 = (a, b) = ax_0 + by_0$  és  $1 = (a, c) = au_0 + cv_0$ . Nyilván elegendő megmutatni, hogy van olyan  $z_0, w_0$  egészek, melyekre teljesül, hogy  $1 = az_0 + bcw_0$ . Ha az  $1 = ax_0 + by_0$  és  $1 = au_0 + cv_0$  egyenleteket összeszorozzuk és rendezzük, akkor

$$1 = (ax_0 + by_0)(au_0 + cv_0) = a[x_0(au_0 + cv_0) + by_0u_0] + bc[y_0v_0],$$

miatt  $z_0$  választható  $[x_0(au_0 + cv_0) + by_0u_0]$ -nek és  $w_0 y_0v_0$  -nek, s ezzel a bizonyítás kész.

**Tétel:** Ha  $(a, b) = 1$  és  $a \mid bc$  akkor  $a \mid c$ .

**Bizonyítás:** Legyen  $1 = (a, b) = ax_0 + by_0$  és  $bc = za$ , ekkor az első egyenletet  $c$ -vel végig szorozva  $c = acx_0 + bcy_0 = a(cx_0 + zy_0)$  adódik amiből már valóban látszik, hogy  $a$  osztója  $c$ -nek.

**Definíció:** A  $p$ -t prím számnak nevezzük, ha  $p \mid ab$ -t, akkor  $p \mid a$  vagy  $p \mid b$ , (és  $p$  nem 0 és különbözik az egységtől).

Prím számok, a 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... stb. Az alábbi módszerrel meghatározhatjuk azon  $p$  prímeket melyek  $1$  és  $n$  között, helyezkednek el. Írjuk fel  $1$ -től  $n$ -ig a számokat. Tudjuk, hogy 2 az prím, húzzuk át 2 összes többszörösét, a 2-nél nagyobb legkisebb át nem húzott szám a 3 prím lesz a 3 kivételével 3 összes többszörösét húzzuk át, ismét a 3-nál nagyobb számok közül a legkisebb prím lesz, ...  $n$ -ig folytatva az eljárást az át nem húzott számok megadják az összes prímet  $1$  és  $n$  között. Legyen most  $n=34$ , ekkor az alábbi táblázat adódik:

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.

Ezt az eljárást eratosthenészi szitának nevezik. Nyilván elegendő csupán az  $1$  és  $\sqrt{n}$  közötti  $p$  prímeikkel elvégezni a szitálást, mivel ha valamely  $a$  szám  $n$ -nél kisebb és összetett, akkor van  $\sqrt{n}$ -nél kisebb prím osztója.

**Tétel ( a számelmélet alap tétele ):** Bármely 0-tól és egységtől különböző egész szám felírható prímszámok szorzataként, s ez a felírás sorrendtől egység szorzóktól és asszociáltaktól eltekintve egyértelmű.

Szeretnénk itt megjegyezni, hogy azt a közkedvelt megfogalmazást, mely szerint "bármely  $1$ -nél nagyobb pozitív egész sorrendtől eltekintve egyértelműen írható fel prímszámok szorzataként", nem szabad sommásan elítélni. Gondoljunk arra, hogy ez bővebb magyarázat után teljesen korrekté tehető ( lásd az egységscsoporttal kapcsolatos osztályozást ).

**Bizonyítás:** A tétel egzisztenciára vonatkozó részét teljes indukcióval bizonyítjuk.  $n=2$ -re az állítás igaz, tételezzük fel, hogy  $n$ -nél kisebbekre igaz és bizonyítsuk, hogy akkor  $n$ -re is teljesül. Ha  $n$  prím szám, akkor kész vagyunk, ha  $n$  összetett azaz  $n=ab$ , ahol  $1 < a, b < n$  és az indukciós feltevés miatt  $a, b$  már prímszámok szorzata és ezért  $n$  is az.

Az unicitást indirekt bizonyítjuk tegyük fel, hogy  $n$  kétféleképpen bomlik fel prímelek szorzatára.

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_r \quad (I)$$

Ha a  $p_1$  a  $q_1, q_2, \dots, q_r$  mindegyikéhez relatív prím volna, akkor korábbi tételünk szerint a szorzatukhoz is ami nyilván nem igaz, ezért feltehetjük, hogy  $p_1 = \varepsilon q_1$ , (I)-t osztva  $q_1$ -gyel majd megismételve az eljárást  $r$ -szer adódik az egyértelműség.

**Tétel:** Végtelen sok prímszám van.

**Bizonyítás:** Még Euklidesztől származik a következő indirekt bizonyítás. Tételezzük fel hogy csak véges sok van. Legyenek azok rendre  $p_1 p_2 \dots p_k$ , s legyen  $N = p_1 p_2 \dots p_k + 1$ . A számelmélet alaptétele szerint  $N$  is prímek szorzatára bomlik, például  $N = q_1 q_2 \dots q_r$ , de ezek között nem fordulhat elő a  $p_1, p_2, \dots, p_k$  egyike sem, tehát a feltevés szemben legalább  $k+1$  prím van, s ez ellentmondás, s így a bizonyítás kész.

*Az elemi igazságok túlságosan érthetőek számunkra.*

Blaise Pascal, (1623-1662)<sup>2</sup>

## Maradékosztály gyűrűk, kongruenciák

**Definíció:** Az  $a$  kongruens  $b$ -vel moduló  $m$ , ha  $m|(a-b)$ . Jele:  $a \equiv b \pmod{m}$ .

**Definíció:**  $a \equiv b \pmod{m}$ , ha  $a$  is és  $b$  is  $m$ -mel osztva ugyan azt a maradékot adja, azaz  $a = mq_a + r_a, b = mq_b + r_b$  és  $r_a = r_b$ .

Nyilvánvaló, hogy a két definíció ekvivalens.

**Tétel:** Az  $a \equiv b \pmod{m}$  reláció ekvivalencia reláció.

**Bizonyítás:** A reflexivitás  $a \equiv a \pmod{m}$  teljesül, mert  $m|(a-a)=0$ -t. Szimmetrikus is a reláció, mivel ha  $a \equiv b \pmod{m}$ , akkor  $m|(a-b) \Rightarrow m|(b-a)$  és ez azt jelenti, hogy  $b \equiv a \pmod{m}$ . Végül a tranzitivitás is teljesedik, mert a  $a \equiv b \pmod{m}$  és  $b \equiv c \pmod{m}$  feltételekből következik, hogy  $r_a = r_b = r_c$  és adódik, hogy  $a \equiv c \pmod{m}$ .

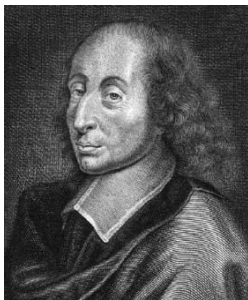
**Megjegyzés:** Az ekvivalencia reláció definíciójánál megemlítettük (sőt bizonyítottuk is), hogy az  $A$  halmazon adott  $D$  ekvivalencia reláció mindig indukál egy osztályozást is az  $A$  halmazon, s az osztályokból álló faktorhalmazt  $A/(D)$ -val jelöltük. Jelen esetben a  $Z$  egész számok halmazán a  $\pmod{m}$  reláció indukál egy osztályozást. Két egész szám  $\pmod{m}$  ugyanabba a maradékosztályba fog tartozni, ha ugyan azt a maradékot adják  $m$ -mel osztva. Ha valamely egész számot maradékosan osztunk  $m$ -mel, akkor  $m$  darab különböző maradékunk lehet, nevezetesen  $0, 1, 2, \dots, m-2, m-1$ . Az  $A/(D)$  faktorhalmaznak most értelemszerűen a  $Z(m)$  jelölés lesz a megfelelője.

**Tétel:** Legyen  $a \equiv b \pmod{m}$  és  $a = a'd, b = b'd$  és  $m = m'd$ , akkor

$$a' \equiv b' \pmod{m'}.$$

**Bizonyítás:** A feltételekből  $a-b=mc$ , és  $(a'-b')d=m'dc$  ez utóbbi egyenletet  $d$ -vel osztva a tétel állítását kapjuk.

**Tétel:** Ha  $a \equiv b \pmod{m}$  és  $c \equiv d \pmod{m}$ , akkor



2

(1623-1662) Pascal, Blaise fia volt Pascal, Etienne-nek aki levelezésben állt Mersenne-nel, (Mersenne Marin (1588-1648)). 16 évesen felfedezte a kúpszeletekbe írt hatszögekre vonatkozó „Pascal-tétel”-t, s tizennyolc évesen tervezett egy számológépet, melyet később megépített. Huszonötévesen a janzenisták Port Royali kolostorába vonult. 1654-től lényegében már csak teológiával foglalkozott.

$$\underline{a \pm c \equiv b \pm d \pmod{m} \text{ és}}$$

$$\underline{ac \equiv bd \pmod{m}}.$$

**Bizonyítás:** A feltételek definíció szerint azt jelentik, hogy  $r_a = r_b$  és  $r_c = r_d$ , ha az  $a = mq_a + r_a$ ,  $c = mq_c + r_c$  egyenleteket ill.  $b = mq_b + r_b$ ,  $d = mq_d + r_d$ -t összeszorozzuk, akkor

$$ac = m(mq_a q_c + q_a r_c + q_c r_a) + r_a r_c \text{ ill.}$$

$$bd = m(mq_b q_d + q_b r_d + q_d r_b) + r_b r_d$$

miatt látható, hogy  $r_a r_c = mq' + r_{ac}$  ill.  $r_b r_d = mq'' + r_{bd}$ . Valóban teljesedik  $ac \equiv bd \pmod{m}$ . Az  $a \pm c \equiv b \pm d \pmod{m}$  igazolását az olvasóra bízuk.

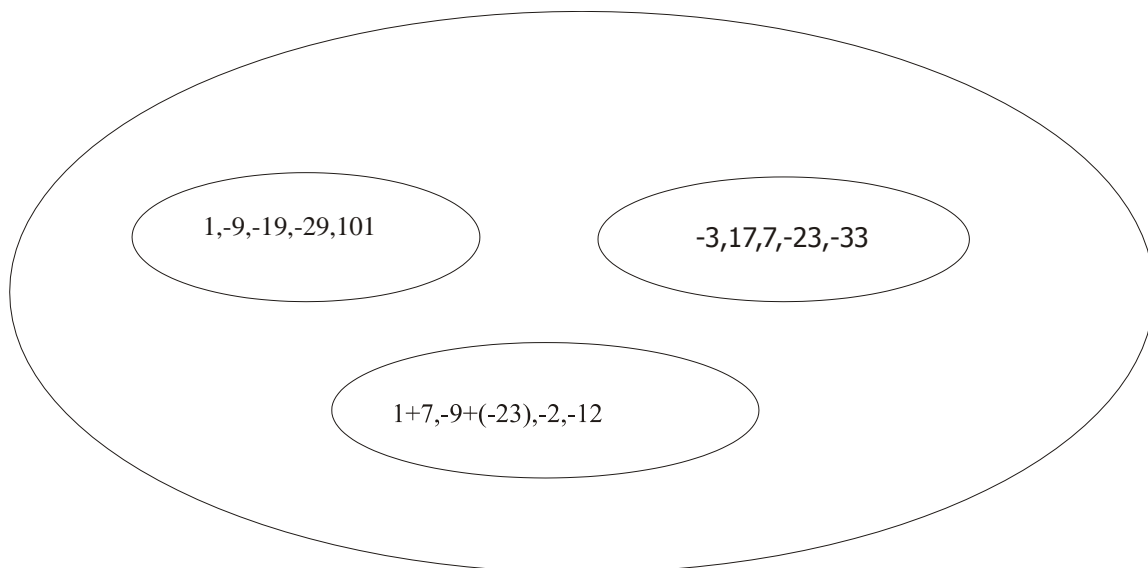
A  $\pmod{m}$  kongruencia reláció, mint ekvivalencia reláció létrehoz egy osztályozást  $Z$ -n. Ez az osztályozás kompatibilis a fenti tétel szerint a  $Z$ -n értelmezett összeadásra és a szorzásra nézve. A  $Z$ -n a  $\pmod{m}$  reláció által létrehozott osztályokat maradékosztályoknak nevezzük, a faktorhalmazt maradékosztály gyűrűnek. Jele:  $Z(m)$  vagy még tömörebben csak  $Z_m$ . A  $\pmod{m}$  vett maradékosztályokat szokás reprezentálni pl. a legkisebb nem negatív számokkal azaz  $0, 1, 2, \dots, (m-1)$ , vagy a legkisebb abszolút értékűekkel ha  $m=2k$  alakú, akkor

$$(-k), (-k+1), \dots, -1, 0, 1, \dots, k-2, k-1, \text{ vagy}$$

$$(-k+1), \dots, -1, 0, 1, \dots, k-2, k-1, k \text{ és } m=2k+1, \text{ akkor}$$

$$-k, (-k+1), \dots, -1, 0, 1, \dots, k-2, k-1, k.$$

Legutolsó tételünk lényegében azt mondja ki hogy az osztályok közötti összeadást ill. szorzást megadhatjuk a "kedvünk szerint választott" reprezentánsaikkal is. E tényt úgy is kiszokták fejezni, hogy a  $(Z(+, *))$  egész számok gyűrűjének műveletei az  $+, *$  kompatibilis a  $\pmod{m}$  osztályozással. Másképpen mondva, ha  $a$  és  $b$  az egyik osztályba tartozik, továbbá  $c$  és  $d$  valamely másik osztályba, akkor  $a+c$  ill.  $b+d$  is valamely harmadik osztályba tartozik. Például  $\pmod{10}$  esetén  $1$  és  $-9$  egy osztályba tartoznak  $7$  és  $-23$  egy másik osztályba, de ekkor  $1+7$ -nek és  $-9+(-23)$ -nak is egy osztályba kell tartoznia  $\pmod{10}$ .



**Tétel:** A moduló  $m$  maradékosztályok az összeadásra és a szorzásra nézve egységelemes kommutatív gyűrűt alkotnak.

**Bizonyítás:** Vázlatosan a következőket mondhatjuk: A maradékosztályok között az összeadás és a szorzás a reprezentánsok közötti összeadással és szorzással definiálva van, mivel az osztályozás kompatibilis volt mindkét művelettel. Az asszociativitása és a kommutativitása is mind két műveletnek az egész számok közötti asszociativitásából ill. kommutativitásából adódik, hasonlóan a disztributivitás is. Létezik zéruselem a  $0$  és additív inverze  $a$ -nak  $m-a$  és az  $1$  egységelem a szorzásra nézve.

$$\left( \begin{array}{c|cccccc} + & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 5 & 0 & 1 & 2 & 3 & 4 \end{array} \right), \left( \begin{array}{c|cccccc} \bullet & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 2 & 4 & 0 & 2 & 4 \\ 3 & 0 & 3 & 0 & 3 & 0 & 3 \\ 4 & 0 & 4 & 2 & 0 & 4 & 2 \\ 5 & 0 & 5 & 4 & 3 & 2 & 1 \end{array} \right)$$

Tekintsük például a  $Z(6)$  összeadási ill. szorzó tábláját. Néhány dolog a táblázatra vetett első pillantás után szembe ötlök. Az összeadási és a szorzási táblázat is szimmetrikus a fő átlójukra, ez a kommutativitás következménye. A  $2 \cdot 3 \equiv 0 \pmod{6}$  azt mutatja hogy a  $Z(6)$  maradékosztály gyűrűben vannak zérus osztók.

**Definíció:** Az  $a$ -val reprezentált maradékosztályt redukált maradékosztálynak mondjuk  $\pmod{m}$ , ha  $(a,m)=1$ .

**Definíció:** A pozitív egészek halmazán értelmezett valós, vagy komplex értékű függvényt számelméleti függvénynek mondjuk.

**Definíció:** Az  $f(n)$  számelméleti függvényt multiplikatívnek mondjuk, ha  $(a,b)=1 \Rightarrow f(ab)=f(a)f(b)$ .

**Definíció:** Jelölje a  $1,2,\dots,n-2,n-1,n$  számok közül az  $n$ -hez relatív prímekek számát  $\varphi(n)$ . A  $\varphi(n)$  függvényt Euler-féle  $\varphi$  függvénynek nevezzük.

Ha az  $n=p$  prímszám, akkor  $\varphi(p)=p-1$ , s különösebb nehézség nélkül látható az is, hogy prímszám helyeken

$$\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right). \text{ A következő tétel megadja } \varphi(n) \text{ explicit alakját.}$$

**Tétel:** Ha  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , akkor

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

**Bizonyítás:** Az  $1,2,3,\dots,n-1,n$  számok között  $n/p_i$  darab van amely  $p_i$  többszöröse vonjuk le ezeket  $n$ -ből. Azokat a számokat amelyek  $p_i p_j$ -vel is oszthatók kétszer vontuk le, ezért az  $n/p_i p_j$ -t adjuk hozzá  $n - \sum_{i=1}^k \frac{n}{p_i}$ -hez, kapjuk  $n -$

$\sum_{i=1}^k \frac{n}{p_i} + \sum_{1 \leq i < j \leq k} \frac{n}{p_i p_j}$ . A  $p_i p_j p_k$ -val osztható számokat a kellelénél eggyel többször vettük figyelembe ezért az  $n/(p_i p_j p_k)$ -kat vonjuk le, az előbbi összegből. Folytatva az eljárást a következő összefüggés adódik:

$$\varphi(n) = n - \sum_{i=1}^k \frac{n}{p_i} + \sum_{1 \leq i < j \leq k} \frac{n}{p_i p_j} - \sum_{1 \leq i < j < k \leq k} \frac{n}{p_i p_j p_k} + \dots + (-1)^k \frac{n}{p_1 p_2 \dots p_k}.$$

A fenti egyenlet jobboldalán szereplő összeg pontosan megegyezik a  $n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  szorzattal. Ha a Kedves

Olvasónak túl sok volt a jelölés, tudjuk javasolni, hogy a fenti algoritmust ami nem más, mint az eratoszthenészi-szita, abban az esetben, mikor a  $p_1, p_2, \dots, p_k$  számokkal szitáltunk, számolja végig az  $n=2 \cdot 3 \cdot 5=30$  esetén. A fenti tételből adódik, hogy az Euler-féle  $\varphi(n)$  függvény multiplikatív.

**Tétel(Euler-Fermat):** Ha  $(a,m)=1$ , akkor  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**Bizonyítás:** Jelölje rendre  $r_1, r_2, \dots, r_{\varphi(m)}$  a redukált maradékosztályokat  $\pmod{m}$ . Szorozzuk ezeket rendre végig  $a$ -val kapjuk, hogy  $ar_1, ar_2, \dots, ar_{\varphi(m)}$ . Állítjuk, hogy a kapott maradékosztályok páronként különbözőek. Ha valamely  $i, j$ -re  $ar_i \equiv ar_j \pmod{m}$ , akkor

$a(r_i - r_j) \equiv 0 \pmod{m}$ , s mivel  $a$  relatív prím  $m$ -hez, ekkor  $m \mid (r_i - r_j)$ , s ez ellentmond annak, hogy  $r_i, r_j$  különbözők  $\pmod{m}$ . Ezek szerint az  $ar_1, ar_2, \dots, ar_{\varphi(m)}$  maradékosztályok sorrendtől eltekintve megegyeznek  $r_1, r_2, \dots, r_{\varphi(m)}$ -vel, ekkor szorzataik is megegyezik  $\pmod{m}$  azaz  $r_1 r_2 \dots r_{\varphi(m)} \equiv ar_1 ar_2 \dots ar_{\varphi(m)} \pmod{m}$  rendezés után  $r_1 r_2 \dots r_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m}$ , s itt az  $r_1 r_2 \dots r_{\varphi(m)}$  szorzat relatív prím az  $m$ -hez ezért  $m \mid (a^{\varphi(m)} - 1)$ , ez pedig ténylegesen a tétel állítását adja.

**I. Következmény:** A  $Z(m)$  maradékosztály gyűrűben bármely  $a$  redukált maradékosztálynak van multiplikatív inverze. Ha

$$((a, m) = 1) \Rightarrow (\exists a^{-1} \in Z_m, \text{ é. s. } a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}).$$

**II. Következmény:** Ha  $p$  prím, akkor a  $Z(p)$  maradékosztály gyűrű test.

Az  $F$  és az  $F'$  testet izomorfnek mondjuk, ha  $F$ -nek van olyan  $F'$ -re való  $\varphi$  bijektív leképezése, mely művelet tartó azaz  $\forall a, b \in F \Rightarrow ((\varphi(a+b) \equiv \varphi(a) + \varphi(b)) \text{ é. s. } (\varphi(ab) \equiv \varphi(a)\varphi(b)))$ . Meg lehet mutatni, hogy bármely test prímteste vagy a racionális számok testével vagy a  $Z(p)$  ( $p$  prím) testtel izomorf. A II. következmény is nyilvánvaló, ha arra gondolunk, hogy  $Z(p)$ -nek a  $0$  maradék osztály kivételével mindegyik maradék osztálya redukált maradékosztály és így van inverze.

**III. Következmény:** Ha  $(a,m)=1$ , akkor az  $ax \equiv b \pmod{m}$  lineáris kongruenciának egy és csak egy  $x_0$  megoldása van  $\pmod{m}$ , és az kongruens  $a^{\varphi(m)-1} b$ -vel.

Ha az  $ax \equiv b \pmod{m}$  kongruenciába  $x$  helyére beírjuk  $a^{\varphi(m)-1} b$  látható, hogy az megoldás. Másrésztől, ha  $ax \equiv b \pmod{m}$  mindkét oldalát szorozzuk  $a^{\varphi(m)-1}$ , akkor látható, hogy tetszőleges  $x$  megoldás  $a^{\varphi(m)-1} b$  alakú.

**Megjegyzés:** Mersenne prímekeknek nevezzük azokat az  $M_k$  számokat amelyek egyrészt prímszámok másrészt  $2^n - 1$  alakba írhatók. Könnyen látható, hogy ha  $n$  összetett szám, akkor  $2^n - 1$  nem lehet prím. Ha  $p$  páratlan prímszám,  $2^p - 1$  akkor és csak akkor prím -a Lucas-Lehmer teszt szerint- ,ha  $2^p - 1$  osztója  $S(p-1)$ -nek, ahol  $S(1)=4$  és  $S(n+1)=S(n)^2 - 2$ . A bináris számítógépeken nagyon könnyen lehet „gyors” programokat írni a Lucas-Lehmer tesztre. Egy pszeudokód lehet a következő:

```

Lucas_Lehmer_Test(p): s:=4;
for i from 2 to p-1 do s := (s^2 - 2) mod (2^p - 1);
if s ≡ 0 mod (2^p - 1) then 2^p - 1 is prime
else 2^p - 1 is composite;

```

Példa: Legyen  $p=5$ , ekkor  $M_5 = 2^5 - 1 = 31$ ,  $s(1) = 4$ , továbbá  $s(2) = 4^2 - 2 = 14$ ;  $s(3) = 14^2 - 2 \equiv 8 \pmod{31}$ ;  $s(4) = 8^2 - 2 \equiv 0 \pmod{31}$ , ezért  $M_5 = 2^5 - 1 = 31$  prím. Mutassa meg, a Lucash-Lehmer teszttel, hogy  $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$  nem prím.

A Mersenne prímekek közül kerülnek ki napjainkban a legnagyobb ismert prímekek. Az következő táblázat ad némi információt a Mersenne prímekekről. A táblázat első oszlopában  $k$  jelöli, hogy hányadik Mersenne prímről van szó, a

második oszlop a  $p$  kitevőt, a harmadik a tízes számrendszerbeli számjegyeinek a számát, a negyedik oszlop a felfedezés évét az ötödik a felfedező nevét:

k	p	számjegyek száma	év	név
1	2	1	...	...
2	3	1	...	...
3	5	2	...	...
4	7	3	...	...
5	13	4	1456	anonymous
6	17	6	1588	Cataldi
8	31	10	1772	Euler
12	127	39	1876	Lucas
13	521	157	1952	Robinson
20	4423	1332	1961	Hurwitz
24	19937	6002	1971	Tuckermann
28	86243	25962	1982	Slowinski
32	756839	227832	1992	Slowinski & Gage
37	3021377	909526	1998	Clarkson, Woltman, Kurowski et. al (GIMPS, PrimeNet),
38?	6972593	2098960	1999	Hajratwala, Woltman, Kurowski et. al (GIMPS, PrimeNet)
<b>39?</b>	13466917	4053946	<b>2001</b>	
<b>40?</b>	20996011	6320430	<b>2003</b>	
<b>41?</b>	24036583	7235733	<b>2004</b>	
<b>42?</b>	<b>25964951</b>	<u>7816230</u>	2005	
<b>43?</b>	<b>30402457</b>	<b><u>9152052</u></b>	2005	
<b>44?</b>	<b>32582657</b>	<u>9808358</u>	2006	
<b>45?</b>	<b>37156667</b>	<b><u>11185272</u></b>	2008	
<b>46?</b>	<b>42643801</b>	<b><u>12837064</u></b>	2009	
<b>47?</b>	<b>43112609</b>	<b><u>12978189</u></b>	2008	

George Woltman 1995-ben megszervezte, hogy hálózatba kapcsolt gépeken futathassanak szabadon letölthető Mersenne-prím kereső programot, s biztosított egy nagy adatbázist a rész eredmények felhasználásához. A GIMPS e

rendszer rövidítése ( the Great Internet Mersenne Prime Search)<sup>3</sup>. Az utolsó előtti sor alapján elég valószínűnek látszik, hogy a 2009. esztendőben a legnagyobb ismert prímszám, amely egyben Mersenne prím is az a  $2^{43112609}-1$ , amelyet 2008.augusztus 8.-án találtak meg.

## Lineáris diofantoszi egyenletek és lineáris kongruenciák

Diofantoszi egyenletekről, akkor beszélünk, ha az egyenletnek a megoldásait az egészek körében keressük. Lineáris diofantoszi egyenleten az

$$a_1x_1+a_2x_2+\dots+a_kx_k=b$$

kifejezést értjük. A továbbiakban két ismeretlenes lineáris diofantoszi egyenletekről fogunk szót ejteni.

**Tétel:** Az  $ax+my=b$  lineáris diofantoszi egyenlet, akkor és csak akkor oldható meg, ha

$$(a,m)|b.$$

**Bizonyítás:** Tételezzük most fel, hogy  $(a,m)|b$  igaz. Legyen  $d=(a,m)$  és  $a=a'd$ ,  $b=b'd$  valamint  $m=m'd$ . Az  $ax+my=b$  egyenletet  $d$ -vel végig osztva  $a'x+m'y=b'$  adódik és  $(a',m')=1$ . Az euklideszi algoritmus tárgyalásánál megmutattuk, hogy két szám lnko.-ja előáll a két szám konstansszorosainak összegeként. Jelen esetben ez azt jelenti, hogy létezik  $x_0, y_0$  olyan, melyre teljesedik, hogy  $a'x_0+m'y_0=1$ , ez utóbbi egyenlőséget végig szorozzuk  $b'd$ -vel láthatjuk, hogy az  $x_0b', y_0b'$  számpár megoldása az eredeti egyenletünknek.

**Megjegyzés:** Vegye észre a Kedves Olvasó, hogy ha az  $ax+by=c$  lineáris diofantoszi egyenletnek  $x_0, y_0$  megoldása, akkor az  $x_t = \frac{b}{(a,b)}t + x_0, y_t = -\frac{a}{(a,b)}t + y_0$  is megoldása bármely egész  $t$  szám esetén. Azaz, ha valamely kettő vagy több ismeretlenes lineáris diofantoszi egyenlet megoldható, akkor végtelen sok megoldása van

**Tétel:** Az  $ax\equiv b \pmod{m}$  lineáris kongruencia akkor és csak akkor megoldható, ha  $(a,m)=d|b$  és ekkor pontosan  $d$  darab inkongruens megoldása van moduló  $m$ .

**Bizonyítás:** A tétel megoldhatóságra vonatkozó szükséges és elégséges feltétele adódik abból, hogy  $ax+my=b$  akkor és csak akkor oldható meg, ha az  $ax\equiv b \pmod{m}$  megoldható. Valóban legyen  $x_0$  megoldása  $ax\equiv b \pmod{m}$ -nek akkor van olyan  $y_0$ , hogy  $ax_0-b=my_0$  és az  $x_0, y_0$  megoldása,  $ax+my=b$ -nek. Fordítva is triviális.

Legyen most  $(a,m)=d|b$ , s mutassuk meg, hogy  $ax\equiv b \pmod{m}$ -nek pontosan  $d$  darab inkongruens megoldása van. Legyen  $a=a'd, m=m'd, b=b'd$ . Korábbi tételünk alapján az  $a'x\equiv b' \pmod{m'}$  kongruenciának pontosan  $1$  megoldása van, mivel az előzőek miatt  $(a',m')=1$ , s legyen az  $x_0$ . Behelyettesítéssel ellenőrizhető, hogy az  $xt=tm'+x_0$ , ahol  $t=0,1,\dots,d-1$  megoldásai az  $ax\equiv b \pmod{m}$ -nek és páronként inkongruensek  $\pmod{m}$ .

**Megjegyzés:** A tétel alkalmazásaként megmutatjuk, hogy ha  $p$  egy páratlan prím, akkor  $(p-1)! \equiv -1 \pmod{p}$ .

**Például:** Legyen  $p=7$ , ekkor  $(7-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ . Csoportosítsuk a szorzat tényezőit oly módon, hogy az elemeket a  $\pmod{7}$  vett multiplikatív inverzeikkel állítjuk párba. Jelesül  $2 \cdot 4 \equiv 1 \pmod{7}$ ;  $3 \cdot 5 \equiv 1 \pmod{7}$ , ekkor  $(7-1)! = 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod{7}$ .

**Tétel(Wilson-tétel):** Ha  $p$  egy prím, akkor  $(p-1)! \equiv -1 \pmod{p}$ .

<sup>3</sup> A következő internet címen több adatot is találnak a prímekekkel kapcsolatban <http://primes.utm.edu/largest.html>.

**Bizonyítás:** Legyen  $p = 2$ , ekkor  $(p-1)! \equiv (2-1)! \equiv 1! \equiv -1 \pmod{2}$ . Tételezzük fel most, hogy  $p \geq 3$ , ekkor bármely olyan  $a$  egész számra, amelyre teljesül, hogy  $1 \leq a \leq p-1$  teljesül az is hogy a multiplikatív inverze  $a^{-1} \in \mathbb{Z}_p$  reprezentálható olyan egésszel, melyre teljesül, hogy  $1 \leq a^{-1} \leq p-1$  (Reméljük a Tisztelt Olvasót nem zavarja, hogy a maradékosztályt, s a szóban forgó egészt ugyanazon szimbólummal jelöltük.) . Figyelembe véve, hogy  $x \equiv x^{-1} \pmod{p} \Rightarrow x^2 \equiv 1 \pmod{p}$  csak  $x \equiv 1 \pmod{p}$  illetve  $x \equiv p-1 \pmod{p}$  esetén teljesedhet, adódik hogy  $2 \cdot 3 \cdot \dots \cdot (p-3) \cdot (p-2) \equiv 1 \pmod{p}$ . Ez utóbbit megszorozva  $1 \cdot (p-1)$  a tétel állítása adódik.

Vegye észre, hogy a tétel megfordítása is igaz.

**Tétel:** Ha az  $n > 2$  egészre teljesül, hogy  $(n-1)! \equiv -1 \pmod{n}$ , akkor az  $n$  prímszám.

**Bizonyítás:** Indirekt bizonyítunk. Tegyük fel, hogy a tétel állítása nem teljesül, azaz  $n$  nem prím, hanem összetett. Az, hogy az  $n$  összetett azt jelenti, hogy valamely  $a, b \in \mathbb{Z}$ -re  $n = ab$  és  $1 < a \leq n-1, 1 < b \leq n-1$ . Ha  $a \neq b$ , tegyük fel, hogy  $a < b$ , akkor  $(n-1)! = 1 \cdot 2 \cdot \dots \cdot a \cdot \dots \cdot b \cdot \dots \cdot (n-1) \equiv 0 \pmod{n}$ , s ez ellentmond a feltevésnek. Ha  $a = b > 2$ , akkor az  $(n-1)! = 1 \cdot 2 \cdot \dots \cdot a \cdot \dots \cdot 2a \cdot \dots \cdot (n-1) \equiv 0 \pmod{n}$ , s ismét ellentmondásra jutottunk a feltevésünkkel. Az  $a = b = 2$  eset ellenőrzését a Kedves Olvasóra bízunk.

**Tétel(kínai maradék tétel):** Ha az  $m_1, m_2, \dots, m_k$  számok páronként relatív prímek és  $a_1, a_2, \dots, a_k$  tetszőleges egészek, akkor az

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

.....

.....

$$x \equiv a_k \pmod{m_k}$$

szimultán kongruencia rendszernek pontosan egy megoldása van moduló  $N$  (ahol  $N = m_1 m_2 \dots m_k$ ).

**Bizonyítás:** Legyen  $M_i = \prod_{j \neq i} m_j$ , ekkor igaz a következő:  $((M_i, m_i) = 1) \Rightarrow (\exists (M_i^{-1}) \in \mathbb{Z})$ , melyre teljesül, hogy  $(M_i M_i^{-1} \equiv 1 \pmod{m_i})$ .

Legyen  $x_0 = \sum_{i=1}^{i=k} a_i M_i M_i^{-1}$ , behelyettesítve a  $j$ . kongruenciába valóban  $x_0 \equiv a_j \pmod{m_j}$ -t kapunk, mivel a  $\sum_{i=1}^{i=k} a_i M_i M_i^{-1}$  összeg  $j$ . tagja pontosan  $a_j$  és az összes többi tag  $0$  lesz  $\pmod{m_j}$ . A megoldás  $\pmod{N}$ -re vonatkozó egyértelműségét indirekt bizonyítsuk. Tételezzük fel, hogy van egy másik  $x_0'$  megoldás, mely nem kongruens  $\pmod{N}$   $x_0$ -lal. Az

$$x_0 \equiv a_j \pmod{m_j} \text{ és az}$$

$$x_0' \equiv a_j \pmod{m_j}$$

kongruenciákat kivonva egymásból  $x_0' - x_0 \equiv 0 \pmod{m_j}$  -ből  $(m_j) | (x_0' - x_0)$  adódik bármely  $j=0, 1, \dots, k$ -ra, s mivel az  $m_j$  páronként relatív prímek voltak  $N/(x_0' - x_0)$ , ami ellentmond feltevésünknek.