

## Kvadratikus maradékok

**Definíció:** Legyen  $p$  egy páratlan prímszám és  $a$  egy nem nulla maradékosztály a  $Z_p$  maradékosztálygyűrűben, azaz  $a \in Z_p$  és  $a \not\equiv 0 \pmod{p}$ . Az  $a \in Z_p$  kvadratikus maradékknak mondjuk, ha létezik olyan  $x_0 \in Z_p$  melyre teljesül, hogy  $x_0^2 \equiv a \pmod{p}$ . Ha az  $x^2 \equiv a \pmod{p}$  másodfokú kongruencia nem oldható meg, akkor  $a \in Z_p$  kvadratikus nem-maradéknak mondjuk  $\pmod{p}$ .

**Példa:** Az 1, 4, 9, 3, 12, 10 kvadratikus maradékok  $Z_{13}$ -ban, mivel

$$\begin{aligned} 1 &\equiv 1^2 \pmod{13}, & 2^2 &\equiv 4 \pmod{13}, & 3^2 &\equiv 9 \pmod{13}, \\ 4^2 &\equiv 16 \equiv 3 \pmod{13}, & 5^2 &\equiv 25 \equiv 12 \pmod{13}, & 6^2 &\equiv 36 \equiv 10 \pmod{13}. \end{aligned}$$

S a 2, 5, 6, 7, 8, 11 maradékosztályok nem kvadratikus maradékok  $Z_{13}$ -ban.

**Tétel:** A  $0$ -tól különböző kvadratikus maradékok a  $Z_p$  maradékosztálygyűrű multiplikatív félcsoportjának egy részcsoportját alkotják.

**Bizonyítás:** Elegendő a zártságot, s az inverz létezését igazolni, mivel  $Z_p$ -ben a szorzás asszociatív és az egységelem  $Z_p$ -ben bármely  $p$  esetén kvadratikus maradék. Ha  $a \in Z_p$  és  $b \in Z_p$  is kvadratikus maradék, akkor létezik olyan  $x_0 \in Z_p$  és olyan  $y_0 \in Z_p$ , melyekre teljesül, hogy  $x_0^2 \equiv a \pmod{p}$  és  $y_0^2 \equiv b \pmod{p}$ , ekkor viszont teljesül, hogy  $x_0^2 \cdot y_0^2 \equiv (x_0 y_0)^2 \equiv a \cdot b \pmod{p}$ . Azaz kvadratikus maradékok szorzata is kvadratikus maradék. Ha  $a \in Z_p$  nem nulla és kvadratikus maradék, akkor alkalmas  $x_0 \in Z_p$ -re teljesül, hogy  $x_0^2 \equiv a \pmod{p}$  és  $x_0 \not\equiv 0 \pmod{p}$ . Ezért létezik  $x_0$  multiplikatív inverze  $x_0^{-1} \in Z_p$ -ben, melyre teljesül, hogy  $(x_0^{-1})^2 \equiv a^{-1} \pmod{p}$  azaz  $a^{-1}$  is kvadratikus maradék a  $Z_p$  maradékosztály gyűrűben.

**Megjegyzés:** I. A kvadratikus maradék fogalmával könnyű megmutatni, hogy azok a  $p$  prímszámok, melyek  $4k+3$  alakúak nem írhatók fel két egész szám négyzetének az összegeként. Valóban egy egész szám négyzete  $4$ -el osztva  $0$  vagy  $1$  maradékot adhat, ezért két egész szám négyzetének az összege  $\pmod{4}$ , csak  $0+0 \equiv 0 \pmod{4}$ ,  $0+1 \equiv 1 \pmod{4}$ ,  $1+1 \equiv 2 \pmod{4}$  lehet. Azt is mondhatjuk az előzőek alapján, hogy az  $n = x^2 + y^2$  diofantoszi egyenletnek nincs megoldása, ha  $n \equiv 3 \pmod{4}$ .

II. Az is könnyen megmutatható, hogy végtelen sok  $p = 4k-1$  alakú prímszám van-, a kvadratikus maradékok azon tulajdonságának a felhasználásával, hogy csoportot alkotnak. Indirekt bizonyítsunk! Tegyük fel, véges sok  $4k-1$  alakú prímszám van. Jelölje azokat rendre  $p_1, p_2, \dots, p_{k-1}, p_k \equiv -1 \pmod{4}$  g. A  $N = 4 \cdot p_1 p_2 \dots p_{k-1} p_k^2 - 1$  számnak a prím osztói között kell lennie legalább egy  $q = 4k-1$  alakú prímszámnak. ugyanis, ha mindegyik prímosztója  $N$ -nek  $4k+1$  alakú, akkor azok szorzata is kongruens volna  $1$ -gyel modulo  $4$ , de ez lehetetlen, mivel  $N \equiv -1 \pmod{4}$ . A  $q = 4k-1$  prím nem egyezhet meg a  $p_1, p_2, \dots, p_{k-1}, p_k$  prímekek egyikével, sem mivel azok közül bármelyikkel is osztjuk  $N$ -t maradékul  $-1$ -t, s nem  $0$ -t kapunk.



(i) ha  $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii)  $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(iii)  $\left(\frac{a^2}{p}\right) = 1$ .

A bizonyítás az olvasóra marad.

**Tétel:** Ha  $a$   $p$  egy páratlan prímszám, akkor  $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \\ -1, & \text{ha } p \equiv -1 \pmod{4} \end{cases}$

**Bizonyítás:** Az Euler-kritérium felhasználásával adódik a  $p \equiv 1 \pmod{4}$  esetben, hogy  $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1^{4k+1-1/2} \equiv -1^{4k/2} \equiv -1^{2k} \equiv (-1)^{2k} \equiv 1 \pmod{p}$ . S a  $p \equiv -1 \pmod{4}$  esetben, hogy  $\left(\frac{-1}{p}\right) \equiv -1^{p-1/2} \equiv -1^{4k+3-1/2} \equiv -1^{4k+2/2} \equiv -1^{2k+1} \equiv (-1)^{2k+1} \equiv (-1) \pmod{p}$ .

**Tétel(Gauss<sup>2</sup>-Lemma):** Legyen  $p$  egy páratlan prímszám és  $\left(\frac{a}{p}\right) = 1$ . Jelölje

sz az  $a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$  maradékosztályok közül azoknak a számát, amelyeknek a legkisebb nem negatív reprezentánsa nagyobb, mint  $\frac{p}{2}$ , ekkor  $\left(\frac{a}{p}\right) = (-1)^s$ .

**Bizonyítás:** Jelölje  $u_1, u_2, \dots, u_s$  az  $a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$  maradékosztályok közül azokat, melyeknek legkisebb pozitív reprezentánsa nagyobb, mint  $\frac{p}{2}$ ,  $v_1, v_2, \dots, v_t$  jelölje azokat amelyeknek legkisebb pozitív



3. <sup>2</sup> Carl Friedrich Gauss (1777-1855) Sokan minden idők legnagyobb matematikusának tartják. 1801 nyarán jelent meg *Disquisitiones Arithmeticae* c. könyve. Több adatot talál a következő könyvekben: W K Bühler, *Gauss: A Biographical Study* (Berlin, 1981).; G W Dunnington, *Carl Friedrich Gauss : Titan of Science* (New York, 1955). ; T Hall, *Carl Friedrich Gauss : A Biography* (1970). ; G M Rassias (ed.), *The mathematical heritage of C F Gauss* (Singapore, 1991).

reprezentánsai kisebbek, mint  $\frac{p}{2}$ . A  $p-u_1, p-u_2, \dots, p-u_s, v_1, v_2, \dots, v_t$  maradékosztályok száma pontosan  $\left(\frac{p-1}{2}\right)$ . Továbbá bármely  $p-u_i$  maradékosztály inkongruens bármely másik  $p-u_j$  maradékosztállyal, ha  $i \neq j$  -vel. Az sem fordulhat elő, hogy valamely  $i, j$  -re  $p-u_i \equiv v_j \pmod{\left(\frac{p}{2}\right)}$  ugyanis, akkor  $0 \equiv v_j + u_i \pmod{\left(\frac{p}{2}\right)}$ , s ez ellentmond annak, hogy a  $p-u_i, v_j$  maradékosztályok legkisebb pozitív reprezentánsai kisebbek, mint  $\frac{p}{2}$ . Ez viszont azt jelenti, hogy a  $p-u_1, p-u_2, \dots, p-u_s, v_1, v_2, \dots, v_t$

maradékosztályok sorrendtől eltekintve megegyeznek az  $1, 2, \dots, \left(\frac{p-1}{2}\right)$  maradékosztályokkal, ezért

$$\left(\frac{p}{2}\right) \cdot \left(\frac{p}{2}\right) \cdot \dots \cdot \left(\frac{p}{2}\right) \cdot v_1 \cdot v_2 \cdot \dots \cdot v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{\left(\frac{p}{2}\right)}$$

Ez utóbbi azonosságból viszont az adódik,

hogy  $\left(\frac{p}{2}\right) \cdot u_1 \cdot u_2 \cdot \dots \cdot u_s \cdot v_1 \cdot v_2 \cdot \dots \cdot v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{\left(\frac{p}{2}\right)}$  Figyelembe véve, hogy

$$u_1 \cdot u_2 \cdot \dots \cdot u_s \cdot v_1 \cdot v_2 \cdot \dots \cdot v_t \equiv a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a \pmod{\left(\frac{p}{2}\right)}$$

következik, hogy

$$\left(\frac{p}{2}\right) \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{\left(\frac{p}{2}\right)}$$

S mivel  $\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$ , azért  $\left(\frac{p}{2}\right) \equiv a^{\frac{p-1}{2}} \pmod{\left(\frac{p}{2}\right)}$ , s az Euler-

kritérium felhasználásával adódik, hogy  $\left(\frac{a}{p}\right) = \left(\frac{p-1}{2}\right) \equiv \left(\frac{p}{2}\right)$ .

**Tétel:** Ha a  $p$  egy páratlan prímszám, akkor  $\left(\frac{2}{p}\right) = -1^{\frac{p^2-1}{8}}$ .

**Bizonyítás:** A Gauss-lemmában szereplő  $s$  szimbólum most azt mondja meg, hogy az  $1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \dots, \left(\frac{p-1}{2}\right) \cdot 2$  számok között, hány olyan van, melynek a legkisebb pozitív maradéka nagyobb mint

$\frac{p}{2}$ . Figyelembe véve azt, hogy az  $1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \dots, 2 \cdot j, \dots, \left(\frac{p-1}{2}\right) \cdot 2$  számok mindegyike kisebb, mint  $p$

elegendő összeszámolni azokat, melyek kisebbek, mint  $\frac{p}{2}$ . Azon pozitív egész  $j$ -k száma, melyekre teljesül,

hogy  $2j \leq \frac{p}{2}$  nyilván megegyezik  $\frac{p}{4}$  egész részével azaz  $\left\lfloor \frac{p}{4} \right\rfloor$ -gyel. Az előbbieket alapján  $s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$  és

most már elegendő azt megmutatni, hogy  $s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod{2}$ . Könnyű látni, hogy  $p$  páratlan

volta miatt  $ha \ p = 8k \pm 1 \Rightarrow \frac{p^2-1}{8} \equiv 0 \pmod{2}$  . Továbbá annak az igazolása, hogy  $ha$   
 $ha \ p = 8k \pm 3 \Rightarrow \frac{p^2-1}{8} \equiv 1 \pmod{2}$

$p = 8k + 1$  vagy  $p = 8k + 7$  akkor  $s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+1-1}{2} - \left\lfloor 2k + \frac{1}{4} \right\rfloor = 4k - 2k \equiv 0 \pmod{2}$  illetve

2009. XI. 16.

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+7-1}{2} - \left\lfloor 2k + \frac{3}{2} \right\rfloor = 4k+3 - 2k+1 \equiv 0 \pmod{2} \quad \text{nem t\u00fcnik nehéz sz\u00e1mol\u00e1snak. Ha}$$

$$p = 8k+3 \text{ vagy } p = 8k+5 \quad \text{akkor} \quad s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+3-1}{2} - \left\lfloor 2k + \frac{3}{4} \right\rfloor = 4k+1 - 2k \equiv 1 \pmod{2}$$

illetve  $s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+5-1}{2} - \left\lfloor 2k + \frac{5}{4} \right\rfloor = 4k+2 - 2k+1 \equiv 1 \pmod{2}$  is teljesen hasonl\u00f3 sz\u00e1mol\u00e1ssal megkaphat\u00f3. S ezzel a bizony\u00edt\u00e1s k\u00e9sz.

**P\u00e9lda:**  $\left(\frac{2}{7}\right) = 1; \left(\frac{2}{17}\right) = 1; \left(\frac{2}{23}\right) = 1; \left(\frac{2}{31}\right) = 1; \left(\frac{2}{41}\right) = 1; \left(\frac{2}{5}\right) = -1; \left(\frac{2}{19}\right) = -1; \left(\frac{2}{101}\right) = -1$

**Lemma (Ferdinand Gotthold Max Eisenstein (1823-1852)):** Legyen  $p$  egy p\u00e1ratlan pr\u00edsz\u00e1m \u00e9s legyen  $a$  is egy

olyan p\u00e1ratlan sz\u00e1m, amelyre m\u00e9g az is teljes\u00fcl, hogy  $\left(\frac{a}{p}\right) = 1$ . Jel\u00f6lje  $T\left(\frac{a}{p}\right) = \sum_{j=1}^{\left(\frac{p-1}{2}\right)} \left\lfloor \frac{ja}{p} \right\rfloor$ , ekkor

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^{T\left(\frac{a}{p}\right)}$$

**Bizony\u00edt\u00e1s:** Jel\u00f6lje  $u_1, u_2, \dots, u_s$  az  $a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$  marad\u00e9koszt\u00e1lyok k\u00f6z\u00fcl azokat, melyeknek legkisebb

pozit\u00edv reprezent\u00e1nsai nagyobbak, mint  $\frac{p}{2}$ . A  $v_1, v_2, \dots, v_t$  jel\u00f6lje azokat, amelyeknek legkisebb pozit\u00edv

reprezent\u00e1nsai kisebbek, mint  $\frac{p}{2}$ . A marad\u00e9kos oszt\u00e1s t\u00e9tele alapj\u00e1n  $ja = p \left\lfloor \frac{ja}{p} \right\rfloor + \text{marad\u00e9k}$ , s itt a *marad\u00e9k*

term\u00e9szetesen  $u_i$ -t vagy valamelyik  $v_j$ -t jel\u00f6li. Az el\u00f6bbi  $\left(\frac{p-1}{2}\right)$  egyenletet \u00f6sszeadva az ad\u00f3dik, hogy

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^s u_i + \sum_{j=1}^t v_j. \quad \text{A Gauss-lemma bizony\u00edt\u00e1s\u00e1n\u00e1l bel\u00e1ttuk, hogy}$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^s p - u_i + \sum_{j=1}^t v_j = ps - \sum_{i=1}^s u_i + \sum_{j=1}^t v_j. \quad \text{Ez ut\u00f3bbi egyenletet kivonva az \u00f3t megel\u00f3z\u00f3b\u0151l a k\u00f6vetkez\u0151 ad\u00f3dik:}$$

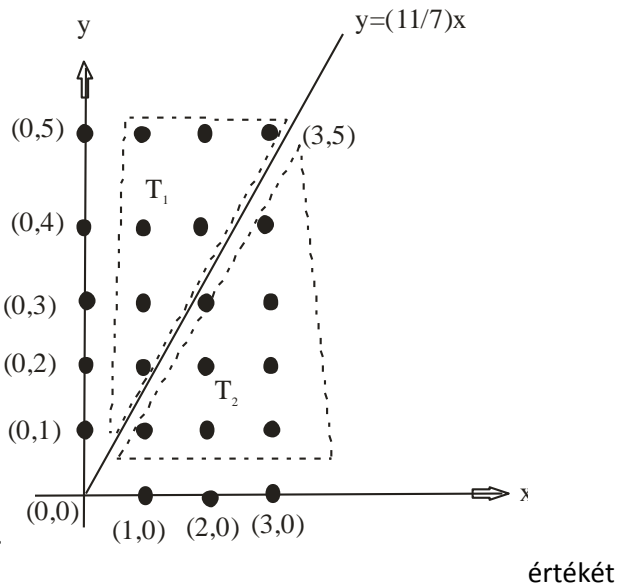
$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor - ps + 2 \sum_{i=1}^s u_i, \quad \text{amib\u0151l} \quad \left(\frac{a}{p}\right) \sum_{j=1}^{\frac{p-1}{2}} j = p T\left(\frac{a}{p}\right) - ps + 2 \sum_{i=1}^s u_i \quad \text{ad\u00f3dik. Figyelembe}$$

v\u00e9ge, hogy  $a$  is \u00e9s  $p$  is p\u00e1ratlan sz\u00e1m  $0 \equiv T\left(\frac{a}{p}\right) - s \pmod{p}$ , s a Gauss-lemm\u00e1b\u0151l kapjuk a k\u00edv\u00e1nt eredm\u00e9nyt

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^s = \left(\frac{a}{p}\right)^{T\left(\frac{a}{p}\right)}$$

**Példa:** Számoljuk ki a lemma segítségével  $\left(\frac{11}{7}\right), \left(\frac{7}{11}\right)$ -t. Határozzuk meg a  $T_{11,7}$  és a  $T_{7,11}$  értékét!

$T_{11,7} = \sum_{j=1}^{\binom{7-1}{2}} \left[\frac{j11}{7}\right] = \left[\frac{11}{7}\right] + \left[\frac{22}{7}\right] + \left[\frac{33}{7}\right] = 1+3+4=8$ . Látható, hogy a mellékelt ábra  $T_2$  háromszögébe eső egész koordinátájú pontokat számoltuk össze. Oly módon, hogy az egy oszlopba esőket összeszámoltuk, majd összeadtuk. Illetve a  $T_{7,11} = \sum_{j=1}^{\binom{11-1}{2}} \left[\frac{j7}{11}\right] = \left[\frac{7}{11}\right] + \left[\frac{14}{11}\right] + \left[\frac{21}{11}\right] + \left[\frac{28}{11}\right] + \left[\frac{35}{11}\right] = 0+1+1+2+3=7$  esetében a  $T_1$  háromszög egy-egy sorában lévő egész koordinátájú pontokat számoltuk össze, s a kapott számokat összeadtuk. Az is világos, hogy azon  $T$  téglalapon elhelyezkedő egész koordinátájú pontok számával egyezik meg a  $T_1, T_2$  háromszögek belsejében lévő egész koordinátájú pontok száma, amely  $T$  téglalap tetszőleges  $x, y \in T$  pontjára teljesül, hogy  $0 < x < \frac{7}{2}, 0 < y < \frac{11}{2}$ . Az is látható, hogy az  $y = \frac{11}{7}x$  egyenesnek a  $T$  téglalap belsejébe eső szakaszán nincs egész koordinátájú pont.



**Tétel (Kvadrátikus Reciprocitás Tétele):** Legyenek  $p, q$  páratlan prímszámok, ekkor

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

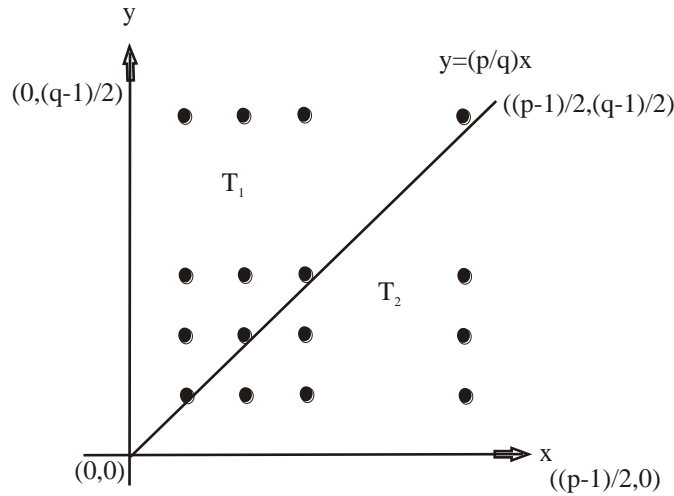
**Megjegyzés:** Az első teljesen hibátlan, részletes bizonyítást a kvadrátikus reciprocitás tételének Gauss adta.

**Bizonyítás:** Lényegében azt használjuk fel, hogy  $\left(\frac{p}{q}\right) = -1^{T_{p,q}}, \left(\frac{q}{p}\right) = -1^{T_{q,p}}$ , ahol  $T_{p,q}$  megegyezik e szöveg után szereplő ábra  $T_2$  háromszögébe eső egész koordinátájú pontok számával, illetve  $T_{q,p}$  megegyezik e szöveg után szereplő ábra  $T_1$  háromszögében szereplő egész koordinátájú pontok számával. Figyelembe véve, hogy  $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = -1^{T_{p,q}} \cdot -1^{T_{q,p}} = -1^{T_{p,q} + T_{q,p}} = -1^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ , mivel a két háromszögben szereplő egész koordinátájú pontok száma pontosan kiadja a  $T$  téglalapon elhelyezkedő

2009. XI. 16.

egész koordinátájú pontok számát. Értelmszerűen a  $T$  téglalap tetszőleges  $x, y \in T$  pontjára, most

$$0 < x < \frac{p-1}{2}, \quad 0 < y < \frac{q-1}{2}. \text{ S ezzel a bizonyítás kész.}$$



Euler a kvadratikus reciprocitás tételének a következő átfogalmazását adta, amely nagyon hasznos konkrét kvadratikus maradékok kiszámítására..

**Tétel:** Legyenek  $p, q$  páratlan prímszámok és  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$  továbbá tegyük fel, hogy

$$p \equiv \pm q \pmod{4}, \text{ ekkor } \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

**Példa:** Számoljuk ki  $\left(\frac{713}{1009}\right)$  tudván, hogy  $713 = 23 \cdot 31$ , s  $1009$ -ról pedig tudjuk, hogy prím. Ekkor

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right). \text{ Felhasználva, hogy } 1009 = 4k + 1 \text{ alakú egész írhatjuk, hogy } \left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right),$$

$$\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right). \text{ A kvadratikus maradékok, illetve a Legendre-szimbólum tulajdonságai miatt}$$

$$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2 \cdot 5}{23}\right) = \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1. \text{ Hasonló módon, egyszerű számolással}$$

$$\text{megkapjuk, hogy } \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right) \cdot \left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) =$$

$$= \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = \left(\frac{2^2}{3}\right) = -1. \text{ Visszatérve a kezdetekhez } \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right) = -1 \cdot -1 = 1. \text{ Az}$$

adódik, hogy  $\left(\frac{713}{1009}\right) = 1$  azaz  $713$  kvadratikus maradék a  $Z_p$  maradékosztály gyűrűben, azaz léteznek olyan racionális

egész  $x_i$  számok, melyek négyzetét maradékosan  $1009$ -cel osztva  $713$ -t kapunk maradék gyanánt,  $x_i^2 = 1009k + 713$ .

### Pepin teszt

Jelölje  $F_m = 2^{2^m} + 1$  az  $m$ . Fermat féle számot, mivel  $F_m$  az  $m$  növekedésével nagyon gyorsan nő, már kicsi  $m$  esetén is sok számolást igényel annak az eldöntése, hogy  $F_m$  prím szám-é vagy sem. Emlékeztetjük a

2009. XI. 16.

Tisztelt Olvasót, hogy egy szabályos  $n$  oldalú sok szög, akkor és csakakkor szerkeszthető körzővel és vonalzóval, euklideszi értelemben, ha az  $n$  prímtényezőss felbontása a következő alakú  $n = 2^k p_1 p_2 \dots p_{t-1} p_t$ , ahol  $k$  nem negatív egész, s a  $p_1, p_2, \dots, p_{t-1}, p_t$  különböző Fermat-féle prímekek. Fermat azt hitte, hogy  $F_m$  mindig

prím, ha  $m$  egész és  $0 \leq m$ . Valóban kicsi  $m$ -re:  $F_0 = 2^{2^0} + 1 = 3$ ,  $F_1 = 2^{2^1} + 1 = 5$ ,  $F_2 = 2^{2^2} + 1 = 17$ ,  $F_3 = 2^{2^3} + 1 = 257$ ,  $F_4 = 2^{2^4} + 1 = 65537$  rendre prím. Eulernek azonban sikerült megmutatnia, hogy 641 osztja  $F_5$ -t felhasználva azt a tényt, hogy  $641 = 2^4 + 5^4$ . Némi töprengés árán belátható a következő számolás korrekt volta

$$F_5 = 2^{32} + 1 = 2^4 2^{28} + 1 = 641 - 5^4 2^{28} + 1 = 641 \cdot 2^{28} - 5 \cdot 2^{7 \cdot 4} + 1 =$$

$$= 641 \cdot 2^{28} - 641 - 1^4 + 1 = 641 \cdot 2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4$$

**Tétel (Pepin teszt):** Az  $F_m = 2^{2^m} + 1$  Fermat-féle szám akkor és csak akkor prímszám, ha

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

**Bizonyítás:** Mutassuk meg először azt, hogy ha a tételben szereplő kongruencia feltétel teljesül, akkor  $F_m$  prím.

A  $3^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m}$  azonosság mindkét oldalát négyzetre emelve  $3^{F_m - 1} \equiv 1 \pmod{F_m}$  adódik. Ha  $F_m$  nem prím, akkor létezik egy olyan  $p$  páratlan prím osztója, amelyre teljesül, hogy  $p \leq \sqrt{F_m}$ , ekkor nyilván az is teljesül, hogy  $3^{F_m - 1} \equiv 1 \pmod{p}$ . Ez utóbbi viszont azt jelenti, hogy 3-nak a  $p$ -re vonatkozó rendje  $\text{ord}_p 3$  osztja  $F_m - 1 = 2^{2^m} - 1$ -t, azaz 3-nak  $p$ -re vonatkozó rendje 2-nek valamely egész kitevős hatványa kell, hogy legyen. 3-nak a  $p$ -re vonatkozó rendje  $\text{ord}_p 3$  nem osztja  $2^{2^m} - 1 = \frac{F_m - 1}{2}$ -t, mivel a feltétel szerint  $3^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m}$  s így  $3^{2^{2^m - 1}} \equiv -1 \pmod{p}$  is teljesül. Ezért  $\text{ord}_p 3 = F_m - 1 \leq p - 1$ . S ez ellentmond annak, hogy  $p \leq \sqrt{F_m}$ . S ezzel a bizonyítás az egyik irányba kész.

Tegyük fel most azt, hogy  $F_m$  prím. S mutassuk meg, hogy a kongruencia feltétel teljesül. A kvadratikus reciprocitás tételéből

$$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{2}{3}\right) = -1, \text{ mivel } F_m \equiv 1 \pmod{4} \text{ és } F_m \equiv 2 \pmod{3}.$$

Az Euler-kritérium alapján viszont tudjuk azt, hogy  $\left(\frac{3}{F_m}\right) \equiv -1^{\frac{F_m - 1}{2}} \pmod{F_m}$ . E két eredményt

$$\text{összevetve } 3^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m} \text{ -t kapjuk.}$$

## Jacobi 3szimbólum

**Definíció:** Legyen  $n$  egy páratlan pozitív egész, prímfelbontása pedig a következő  $n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$  és  $a$  egy  $n$ -hez relatív prím egész, ekkor a Jacobi-szimbólumot a következő formulával definiáljuk:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \cdot \left(\frac{a}{p_2}\right)^{t_2} \cdot \dots \cdot \left(\frac{a}{p_m}\right)^{t_m}$$

**Tétel:** Legyen  $n$  egy páratlan szám és legyenek  $a$  és  $b$   $n$ -hez relatív prím egészek, ekkor

$$(i) \text{ ha } a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

$$(ii) \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$$

$$(iii) \left(\frac{-1}{n}\right) = -1^{\frac{n-1}{2}}$$

$$iv) \left(\frac{2}{n}\right) = -1^{\frac{n^2-1}{8}}$$

**Tétel (Kvadratikus Reciprocitás Tétele Jacobi szimbólumra):** Legyenek  $n, m$  páratlan relatív prímek,

$$\text{ekkor } \left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = -1^{\left(\frac{n-1}{2}\right) \cdot \left(\frac{m-1}{2}\right)}$$

---

<sup>3</sup> **Carl Gustav Jacobi** (1804-1851) egy jó módú német bankár családban született. Otthon kítűnő képzésben részesült. A berlini egyetemen tanult Euler munkáiból. 1825-ben doktorált, s 1826-ban már a Königsbergi egyetemen előadó, s 1831-ben nevezik ki egyetemi tanárnak. Alapvetően hozzá járult a számelmélet, az analízis, mechanika fejlődéséhez.