34. tétel

A φ függvény. Euler-Fermat-tétel. A kis Fermat-tétel. Pszeudoprímszámok.

Tétel: (Euler-féle φ függvény)

$$\varphi : \mathbb{N}\setminus\{0\} \to \mathbb{N}, \quad \varphi(m) = \begin{cases} 1, & \text{ha } m = 1 \\ \varepsilon, & \text{ha } m \geq 2 \end{cases}$$

ahol ε jelöli a modulo m redukált maradékrendszerének számát, azaz a $0, 1 \dots m-1$ teljes reprezentánsrendszerből az m modulushoz relatív prímek számát.

Tétel: Legyen $a, b \in \mathbb{N}\setminus\{0\}$. Ha $(a,b) = 1 \Rightarrow$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

BIZ: Az $a = 1, b \geq 1$ esetekben igaz, mert

$$\varphi(1b) = \varphi(b) = \varphi(1)\varphi(b)$$

Legyen $a > 1$, $b > 1$ és

$$A := \{ax + by \mid x = 0, 1 \dots b-1,\ y = 0, 1 \dots a-1\}$$

$\Rightarrow$ Megmutatjuk, hogy A teljes maradékrendszer modulo ab.

Mivel $|A| = ab \Rightarrow$ csak az A elemeinek páronkénti inkongruenciáját kell bizonyítani.

$\rightarrow$ Tfh.: A def-ban x, y értékei között $\exists\ x_1, x_2, y_1, y_2 \in \mathbb{Z}$, amelyekre: $ax_1 + by_1 \equiv ax_2 + by_2 \pmod{ab}$

Így a Euklid. tul. miatt:

$$ax_1 + by_1 \equiv ax_2 + by_2 \pmod{a}$$

$$ax_1 + by_1 \equiv ax_2 + by_2 \pmod{b}$$

34. tétel

$(a,b)=1$ miatt: $y_1 \equiv y_2 \pmod a \wedge x_1 \equiv x_2 \pmod b$

→ x_1 és x_2 lehetséges értékei miatt csak $x_1 = x_2$ esetben teljesülhet, ami ellentmondás ↯ A elemei inkongruensek modulo ab.

→ Így A-ban az ab-hez relatív prímek száma $f(ab)$.

$$(ax+by, ab) = 1 \Leftrightarrow (ax+by, a) = 1 \wedge (ax+by, b) = 1.$$

$$\Downarrow$$

$(a,b)=1$ és Euler tulajdonságai miatt

$$(ax+by, a) = (by, a) = (y, a) = 1 \wedge (ax+by, b) = (ax, b) = (x, b) = 1.$$

→ És utóbbiakat kielégítő y-ok száma $f(a)$, az x-ek száma $f(b)$ ezért a lehetséges (y,x) számpárok száma $f(a)f(b)$. Így igaz az állítás: $f(ab) = f(a)f(b)$

Tétel: Ha $a_1, a_2 \dots a_\varepsilon$ páronként relatív prím pozitív egész számok $(\varepsilon \geq 2)$, $\Rightarrow$

$$f(a_1, a_2 \dots a_\varepsilon) = f(a_1) f(a_2) \dots f(a_\varepsilon)$$

Tétel: Az $r_1, r_2 \dots r_\varepsilon$ egész számok $\Leftrightarrow$ akkorak modulo m redukált reprezentánsrendszert, ha $\varepsilon = f(m)$, $r_i \not\equiv r_j \pmod m$ minden $1 \leq i < j \leq f(m)$-re és $(r_i, m) = 1$ minden $1 \leq i \leq f(m)$-re.

Tétel: Ha $\{r_1, r_2 \dots r_{f(m)}\}$ modulo m redukált reprezentánsrendszer és $(c,m) = 1 \Rightarrow \{cr_1, cr_2 \dots cr_{f(m)}\}$ szintén redukált reprezentánsrendszer modulo m.

Tétel: (Euler-Fermat-tétel)

Ha $a \in \mathbb{Z}$ és $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

Biz.: ! $\{r_1, r_2 \dots r_{\varphi(m)}\}$ modulo m redukált maradékrendszer

előző tétel miatt: $(a,m)=1$ miatt: $\{ar_1, ar_2 \dots ar_{\varphi(m)}\}$ is

modulo m redukált reprezentánsrendszer.

Így minden redukált maradékosztályból 1 et reprezentáns

van: $\{r_1, r_2 \dots r_{\varphi(m)}\}$; $\{ar_1, ar_2 \dots ar_{\varphi(m)}\}$. Ezek kongruensek

modulo m, így:

$$ar_1 ar_2 \dots ar_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m}$$

$$\Downarrow$$

$(r_1 r_2 \dots r_{\varphi(m)}, m) = 1$ miatt

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Tétel: (kis Fermat-tétel)

Legyen p prímszám. Ha $(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$\Downarrow$

$\forall a \in \mathbb{Z}$ p prímszám: $a^p \equiv a \pmod{p}$

↳ nem kell feltétel hozzá.

A k.F.t megfordítása nem igaz.

Def.: n összetett pozitív egész szám, $(2,n)=1$ (páratlan).

Ha $2^{n-1} \equiv 1 \pmod{n} \Rightarrow$ pszeudoprímnek nevezzük.

A legkisebb pszeudoprím: 341. (Sarrus 1819)

$11 \cdot 31$

Tétel: (Sierpinski 1947)

Ha n egy pszeudoprím szám $\Rightarrow 2^n - 1$ is pszeudoprím.

BIZ.: 1; $N = 2^n - 1$ összetett

Mivel n pszeudoprím $\Rightarrow n$ összetett $(n = n_1 \cdot n_2)$ $(n_1, n_2 \geq 2)$

n páratlan

$$N = 2^n - 1 = 2^{n_1 \cdot n_2} - 1 = \left(2^{n_1}\right)^{n_2} - 1 = \underbrace{\left(2^{n_1} - 1\right)}_{\geq 7} \cdot A$$

n legkisebb osztója 3.

Összetett · felírható 2 szám szorzataként.

2., $N \mid 2^{N-1} - 1$
?

$$2^n - 1 = 2^{2^n - 1 - 1} - 1 = 2^{2(2^{n-1} - 1)} - 1 = *$$

De.: $n \mid 2^{n-1} - 1 \Rightarrow$ felírható $n \cdot q$, mivel n az osztója

$$* \quad 2^{2nq} - 1 = \left(2^n\right)^q - 1^q = \underbrace{\left(2^n - 1\right)}_{N} B$$

A tétel igaz! (A következmény is!)

LEHMER:

Többet bizonyít. Megmutatja, hogy x-nél nem nagyobb pszeudoprímek száma nagyobb, mint $c \log x$, ahol $c > 0$ $c \in \mathbb{R}$.

$P_1(x) := \{ n \mid n$ pszeudoprím $\wedge\ n < x \}$ $x \in \mathbb{R}^+$
→ x-nél kisebb pszeudoprímek halmaza.

$\exists\, x_0 \in \mathbb{R}^+,\ c \in \mathbb{R}$, h. $|P_1(x)| > c \cdot \log x$, ha $x > x_0$

[100000-ig mennyi prím van? → $c \log 100000$

FERMAT-FÉLE SZÁMOK:

$F_n = 2^{2^n} + 1$ alakú számok Fermat-számok, prímszámok $\forall\, n \geq 0$ esetén.

F_0, F_1, F_2, F_3, F_4 → ellenőrizhető könnyen, n · prímek
Euler belizonyította: F_5 összetett. (F. sejtés nem igaz)

Ha több F-prím nem ismert, de az sem bizonyított, h. nem létezik.

Fermat állítása igaz:

Tétel: Ha $n \geq 0$ $n \in \mathbb{N}$ $\wedge$ $F_n = 2^{2^n}+1$ nem prím, $\Rightarrow$ prendoprím

MERSENNE-SZÁMOK:

$M_n = 2^n - 1$ alakú

M_n csak akkor prím, ha n prímszám.

Fordítva nem igaz, de a következő tétel igaz:

Tétel: Legyen $p > 2$ egy prímszám. Ekkor $M_p = 2^p - 1$ vagy prím, vagy prendoprím.

Tétel: Végtelen sok olyan prendoprímszám létezik, mely pontosan két különböző páratlan prímszám szorzata.

Def.: n abszolút prendoprím, ha $\forall$ a-ra $(a,n) = 1$ „a^n"-ra vonatkozóan prendoprím.

$n = 561 = 3 \cdot 11 \cdot 17$

CARMICHAEL-FÉLE SZÁMOK = ABSZOLÚT PSZEUDOPRÍMEK.

$P_2(x) := \{ n \mid n$ abszolút prendoprím, $n < x \}$ $x \in \mathbb{R}^+$

Ha x elég nagy (megadható olyan korlát, amitől nagyobb) $\Rightarrow$ $|P_2(x)| > x^{\frac{2}{7}}$

Tétel: (Lippold 1904) Ha $a \geq 2$ pozitív egész és $p > 2$ egy prím, melyre $p \nmid (a^2-1) \Rightarrow$

$$n = \frac{a^{2p}-1}{a^2-1}$$

prendoprím, a^1 vonatkozásában.