FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. március 23.

Ha $m = p_1 \cdot \ldots \cdot p_t$ (Zerl. prim!), $f \equiv 1 \pmod{\varphi(m)}$,
also $\forall a \in \mathbb{Z}: a^f \equiv a \pmod m$. $\quad \varphi(m) = (p_1-1) \cdot \ldots \cdot (p_t-1)$

Bew. $a^f \equiv a \pmod m \iff \forall i: a^f \equiv a \pmod{p_i}$

1) $p_i \nmid a \Rightarrow p_i \perp a \Rightarrow a^{p_i-1} \equiv 1 \pmod{p_i}$

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

$f = 1 + s \cdot \varphi(m)$

$\Rightarrow a^f \equiv a \pmod{p_i}$

2) $p_i \mid a \Rightarrow a \equiv 0 \pmod{p_i}$.

$\Rightarrow a^f \equiv 0 \pmod{p_i}$

$\Rightarrow a^f \equiv a \pmod{p_i}$ $\square$

Ha $m = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$, $\exists i: \alpha_i \geq 2$, also $a = p_i$ ergibt ein Gegenbsp.,
hier $a^f \equiv a \pmod m$.

$a^f \equiv a \pmod m \Rightarrow a^f \equiv a \pmod{p_i^2}$

$p_i^f \equiv p_i \pmod{p_i^2}$ nem igaz, ha $f > 1$.

$\parallel \quad \not\parallel$

$0 \quad 0$

PRÍMTESZTEK

$n = 91$ prím-e?

$10^{90} \equiv 1 \pmod{91}$

$2^{90} \equiv 64 \not\equiv 1 \pmod{91}$

$\Downarrow$ k.F. $\quad$ P

91 összetett szám

$\parallel$

$7 \cdot 13$

$90 = 64 + 16 + 8 + 2$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv -17$

$2^{16} \equiv 16$

$2^{32} \equiv -17$

$2^{64} \equiv 16$

$2^{90} \equiv 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2$

$\equiv \underbrace{16 \cdot 16}_{16 \cdot 4 \,=\, 64} \underbrace{(-17) \cdot 4}_{(-17 + (-17)) \cdot 4}$

n pl., $a \perp n$, $1 < a < n$

↑ Ha nem, akkor n összetett.

Ha n prím, akkor $\boxed{a^{n-1} \equiv 1 \pmod{n}}$. ← $A'(a,n)$

Ha n prím, akkor $A(a,n)$ igaz.

Ha $A'(a,n)$ hamis, akkor n összetett - a tanú

Ha $A'(a,n)$ igaz, akkor n vagy prím, vagy álprím. a csalás

PÉLDA: 2 alapú Fermat-álprím: 341, 561, 645, 1105, ...

$341 = 11 \cdot 31$

10^6-ig: 245 db 2-alapú Fermat-álprím, 78498 db prím.

TÉTEL A Fermat-tételnek megoldható alkotta $\mathbb{Z}_n^*$-ban.

Biz $C = \{\bar{a} \in \mathbb{Z}_n^* \mid \bar{a}^{n-1} = \bar{1}\}$

$\bar{a}, \bar{b} \in C \Rightarrow \overline{ab}^{n-1} = \bar{a}^{n-1} \cdot \bar{b}^{n-1} = \bar{1} \cdot \bar{1} = \bar{1}$ ✓ □

KÖV $|C| \leq \frac{\varphi(n)}{2}$ ha $C = \mathbb{Z}_n^*$.

↑
n univerzális Fermat-álpr.
CARMICHAEL szám

PÉLDA: CARMICHAEL-számok: 561, 1105, 1729, 2465, ...
10^6-ig: 43 db

HF 15 Keressünk Fermat-tanút $n = 341$-hez!

TÉTEL (KORSELT, 1899) n Carmichael-szám $\iff$

($\Rightarrow$) n négyzetmentes: $n = p_1 \cdot \ldots \cdot p_r$ (különböző prímek) és

$$\forall i: p_i - 1 \mid n-1.$$

Biz: n Carmichael-szám $\iff \forall a \in \mathbb{Z}: a \perp n \Rightarrow a^{n-1} \equiv 1 \pmod{n}$.

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$

$a^{n-1} \equiv 1 \pmod{n} \iff \forall i: a^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}$

$\iff \sigma_{p_i^{\alpha_i}}(a) \mid n-1$

$\iff \varphi(p_i^{\alpha_i}) \mid n-1$

$\iff p_i^{\alpha_i - 1} \cdot (p_i - 1) \mid n-1$

$\iff \alpha_i = 1$ és $p_i - 1 \mid n-1$ $\forall i$ $\square$

TÉTEL (CARMICHAEL, 1910) 561 Carmichael-szám.

Biz. $561 = 3 \cdot 187 = 3 \cdot 11 \cdot 17$
$p_1\ p_2\ p_3$

$3-1 = 2 \mid 560$ ✓ $\quad 11-1 = 10 \mid 560$ ✓ $\quad 17-1 = 16 \mid 560$ ✓ □

TÉTEL (CHERNICK, 1939) Ha $6k+1$, $12k+1$, $18k+1$ prím,
akkor $(6k+1)\cdot(12k+1)\cdot(18k+1)$ Carmichael-szám.
pl. $k=1$: $7 \cdot 13 \cdot 19 = 1729$

TÉTEL (ALFORD, GRANVILLE, POMERANCE, 1994)
∞ sok Carmichael-szám van ($n > n^{2/7}$ db)

$A'(a,n)$	a alpi ...-alpri	$\forall a$	test
$a^{n-1} \equiv 1 \pmod n$	(Fermat)	CARMICHAEL-nbre	FERMAT
$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$	EULER-JACOBI	X	SOLOVAY-STRASSEN (77)

PÉLDA $n = 341$, $a = 2$

$$a^{\frac{n-1}{2}} = 2^{170} \equiv 1 \pmod{341}$$

$$\left(\frac{2}{341}\right) = -1 \quad \not\equiv \quad \Longrightarrow n \text{ összetett szám}$$

$$341 \equiv 21 \equiv 5 \pmod{8}$$

HF16 Találjon Euler-Jacobi-tanút $n = 561$-hez

PÉLDA 2-alapú Euler-Jacobi-álprímek: 561, 1105, 1729, 1905

10^6-ig: 114 db van

Tétel (SOLOVAY, STRASSEN, 1977)

Ha n összetett, akkor $\exists a \in \mathbb{Z}$: $a \perp n$ és $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$.

Biz. Ha n nem Carmichael-szám, akkor. ✓

Ha n Carmichael-szám, akkor $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ $(k \geq 2)$.

Vezessük be a következőt, azaz $\left(\frac{h}{p_1}\right) = -1$

$$\left.\begin{array}{l} a \equiv h \pmod{p_1} \\ a \equiv 1 \pmod{p_2} \\ \vdots \\ a \equiv 1 \pmod{p_k} \end{array}\right\} \text{van ilyen (KMT)}$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right) = \underbrace{\left(\frac{h}{p_1}\right)}_{-1} \cdot \underbrace{\left(\frac{1}{p_2}\right)}_{1} \cdot \ldots \cdot \underbrace{\left(\frac{1}{p_k}\right)}_{1} = -1$$

$a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \Rightarrow a^{\frac{n-1}{2}} \equiv -1 \pmod{p_2}$ $\not\Rightarrow a \equiv 1 \pmod{p_2}$. □

HF 19 CHERNICK-Test bis -