FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. március 9.

k	0	1	2	3	4	5	6	7	...
$10^k \bmod 7$	1	3	2	6	4	5	1	3	...

$\cdot 10$ $\cdot 10$ $\cdot 10$ $\cdot 10$ $\cdot 10$ $\cdot 10$ $\cdot 10$

$1:7 = 0,\underbrace{142857}_{6}1\ldots$

10
30
20
60
40
50
10

$6 = \sigma_7(10)$

$0,\underline{12137}\,\underline{12137}\ldots$

$\frac{1}{a} = 0,\overbrace{027}^{3}\,027\,027\ldots$

$\frac{10^3}{a} = 27,027\,027\,027$

$\Rightarrow \frac{999}{a} = 27 \Rightarrow a = \frac{999}{27} = \frac{111}{3} = 37$

$10^k \equiv 1 \pmod{37} \Leftrightarrow \frac{10^k - 1}{37} \in \mathbb{Z} \Leftrightarrow 3 \mid k$

$\Rightarrow \sigma_{37}(10) = 3$

HF 10 $\frac{1}{a} = 0,\underbrace{\_\_}_{7}\_\_\_\_\_\ldots \quad a = ?$

---

a, b, c pr. mód $m \overset{?}{\Rightarrow} a^{\operatorname{ind}_a c}$ is pr. mód m

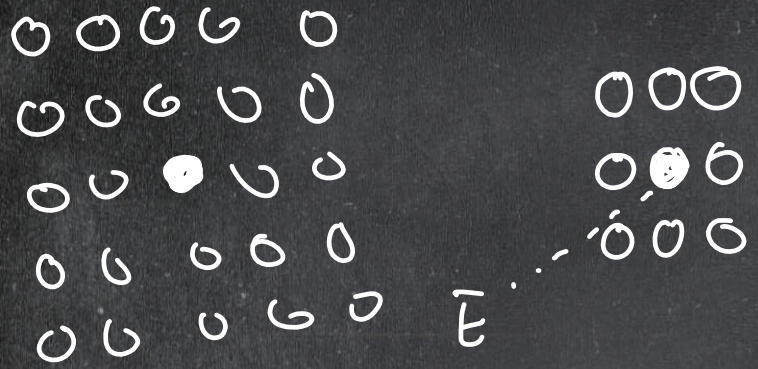
$X = a^{\operatorname{ind}_a c} = \operatorname{ind}_a X \overset{?}{\perp} \varphi(m)$

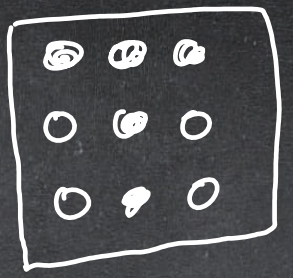
↑ OK, mert c pr. mód m

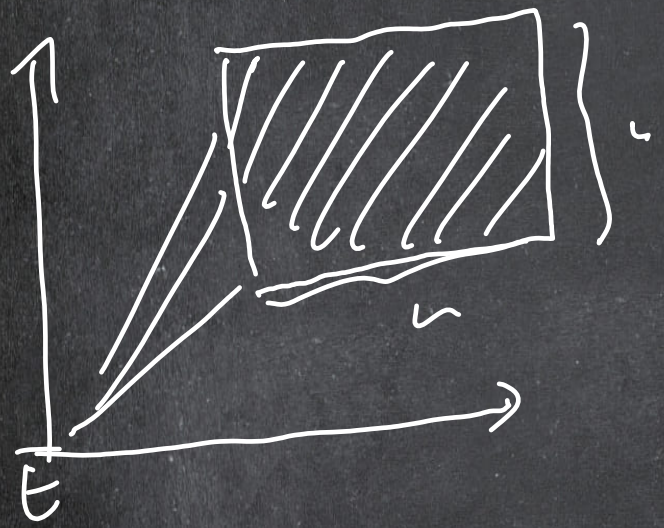
1276	2	11	2
1275	3	17	5
1274	2	7	2
	⋮		
	1308	1309	1310

$y+2$	p_7	p_8	p_9
$y+1$	p_4	p_5	p_6
y	p_1	p_2	p_3
	x	$x+1$	$x+2$

$x \equiv 0 \pmod{p_1 \cdot p_4 \cdot p_7}$
$x \equiv -1 \pmod{p_2 \cdot p_5 \cdot p_8}$
$x \equiv -2 \pmod{p_3 \cdot p_6 \cdot p_9}$
} van-e m.


E




L
E

① m-nek van két pl. prímosztója NINCS

② $m = p^\alpha$ $(p > 2)$

2a) $m = p$ VAN

2b) $m = p^2$ VAN

2c) $m = p^\alpha$ $(\alpha \geq 3)$ VAN

③ $m = 2^\beta \cdot p^\alpha$ $(p > 2)$

3a) $m = 2p^\alpha$ VAN

3b) $m = 2^\beta \cdot p^\alpha$ $(\beta \geq 2)$ NINCS

④ $m = 2^\alpha$

4a) $m = 2$ VAN

4b) $m = 2^2$ VAN

4c) $m = 2^\alpha$ $(\alpha \geq 3)$ NINCS

DEF. p prím, $q \in \mathbb{N}$, $a \in \mathbb{Z}$

$$p^q \| a \iff p^q \mid a \text{ de } p^{q+1} \nmid a.$$

(pouze onehdy)

LEMMA. $p^q \| a-1 \Rightarrow p^{q+1} \| a^p - 1$, KIVÉVE, HA $q=1$ a $p=2$.

Biz. $p^q \| a-1 \Rightarrow a = 1 + t \cdot p^q$, ale $p \nmid t$

$$a^p - 1 = (1+tp^q)^p - 1 = 1^p + p \cdot tp^q + \binom{p}{2}(tp^q)^2 + \dots - 1 =$$

$$= tp^{q+1} + \binom{p}{2} t^2 p^{2q} + \dots = p^{q+1}\left(t + \binom{p}{2} t^2 \cdot p^{q-1} + \dots\right) =$$

$$= p^{q+1}\left(\underbrace{t}_{p\nmid} + \underbrace{t^2 \frac{p(p-1)}{2} \cdot p^{q-1}}_{p\mid} + \underbrace{\dots}_{p\mid}\right)$$

$p \nmid$

$p \mid t^2 \frac{p(p-1)}{2} \cdot p^{q-1}$?

$q > 1 \Rightarrow$ OK

$q = 1, p > 2 \Rightarrow$ OK

$q = 1, p = 2 \Rightarrow$ nem OK ☠

MEGJ. $p = 2, q = 1$ esetén $a = 1 + 2t$, ahol t pt.

$a^2 - 1 = 4t^2 + 4t + 1 - 1 = 4t(t+1)$

$8 \mid a^2 - 1 \qquad 2^{\geq 3} \| a^2 - 1$

ÁLL. $\alpha \geq 3$ és $a \perp 2^\alpha \Rightarrow \sigma_{2^\alpha}(a) \leq 2^{\alpha-2} = \frac{\varphi(2^\alpha)}{2} < \varphi(2^\alpha) = 2^{\alpha-1}$.

Biz $2^{\geq 3} \| a^2 - 1 \Rightarrow 2^{\geq 4} \| a^4 - 1 \Rightarrow 2^{\geq 5} \| a^8 - 1 \Rightarrow \ldots \Rightarrow 2^{\geq \alpha} \| a^{2^{\alpha-2}} - 1$

$\Downarrow$

$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$

$\Downarrow$

$\sigma_{2^\alpha}(a) \mid 2^{\alpha-2}$ ☑

PÉLDA $\alpha \geq 5$

$2^3 \| 5^2-1 \Rightarrow 2^4 \| 5^{2^2}-1 \Rightarrow \dots \Rightarrow 2^{\alpha-1} \| 5^{2^{\alpha-3}}-1 \Rightarrow 2^\alpha \| 5^{2^{\alpha-2}}-1$

$\Downarrow$

$5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$

$\Downarrow$

$\sigma_{2^\alpha}(5) = 2^{\alpha-2}$

$$\mathbb{Z}_{2^\alpha}^* = \{\bar{5}^0, \bar{5}^1, \dots, \bar{5}^{2^{\alpha-2}}, -\bar{5}^0, -\bar{5}^1, \dots, -\bar{5}^{2^{\alpha-2}}\} = [\bar{5}, \bar{-1}]$$

Van pr. mód $m \Leftrightarrow \mathbb{Z}_m^* \cong \mathbb{Z}_{\varphi(m)}$

$$(\alpha \geq 3) \quad \mathbb{Z}_{2^\alpha}^* \cong [\bar{5}] \times [\bar{-1}] \cong \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_2$$

Mostantól p ptl. prím.

Áll. g pr. gyök mod p $\Rightarrow$ g vagy g+p pr. gyök mod p^2.

Biz. Tudjuk, hogy $o_p(g)=\varphi(p)=p-1$, $o_{p^2}(g)\mid\varphi(p^2)=p(p-1)$.

$$g^{o_{p^2}(g)}\equiv 1 \pmod{p^2} \Rightarrow g^{o_{p^2}(g)}\equiv 1 \pmod{p} \Rightarrow \underbrace{o_p(g)}_{p-1}\mid o_{p^2}(g)$$

$$\overbrace{p-1}^{o_p(g)}\mid o_{p^2}(g)\mid p(p-1) \Rightarrow o_{p^2}(g)=p-1 \text{ vagy } o_{p^2}(g)=p(p-1)=\varphi(p^2)$$

TFH. $o_{p^2}(g)=p-1$ és $o_{p^2}(g+p)=p-1$ vagy $o_{p^2}(g+p)=p(p-1)=\varphi(p^2)$

TFH. $g^{p-1}\equiv 1\equiv(g+p)^{p-1} \pmod{p^2}$

$$\underset{\sim}{1} \equiv (g+p)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} \cdot g^{p-2} \cdot p + \binom{p-1}{2} \cdot g^{p-3} \cdot p^2 + \dots$$

$$\equiv 1 + (p-1) \cdot g^{p-2} \cdot p + 0 + \dots \equiv \underline{1 - g^{p-2} \cdot p \pmod{p^2}}$$

$$\Rightarrow 0 \equiv -g^{p-2} \cdot p \pmod{p^2} \Rightarrow p^2 \mid g^{p-2} \cdot p \Rightarrow p \mid g^{p-2} \quad \lightning \quad \square$$

Def. $\sigma_{p^\alpha}(g) =: r(\alpha)$

LEMMA: $r(1) \mid r(2) \mid r(3) \mid \dots \mid r(\alpha-1) \mid r(\alpha) \mid \dots$

Bez.: $g^{r(\alpha)} \equiv 1 \pmod{p^\alpha} \Rightarrow g^{r(\alpha)} \equiv 1 \pmod{p^{\alpha-1}} \Rightarrow r(\alpha-1) \mid r(\alpha) \quad \square$

ALL. g prim. mod p, $p^2 \Rightarrow \forall \alpha \geq 3$: g prim. mod p^α.

Bez.:

$$p \,\|\, g^{p-1} - 1 \Rightarrow p^2 \,\|\, g^{p(p-1)} - 1 \Rightarrow p^3 \,\|\, g^{p^2(p-1)} - 1 \Rightarrow \dots \Rightarrow p^{\alpha-1} \,\|\, g^{p^{\alpha-2}(p-1)} - 1$$

$$\Uparrow \qquad \Downarrow \qquad \Downarrow \qquad \Downarrow$$

$$g^{p-1} \not\equiv 1 \pmod{p^2} \quad g^{p(p-1)} \not\equiv 1 \pmod{p^3} \quad g^{p^2(p-1)} \not\equiv 1 \pmod{p^4} \quad \dots \quad g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$$

$$\Uparrow \qquad \Downarrow \qquad \Downarrow \qquad \Downarrow$$

$$r(2) = p(p-1) \quad r(3) \neq p(p-1) \quad r(4) \neq p^2(p-1) \quad r(\alpha) \neq p^{\alpha-2}(p-1)$$

$$\underbrace{r(1)}_{p-1} \mid \underbrace{r(2)}_{p(p-1)} \mid \underbrace{r(3)}_{p^2(p-1)} \mid \underbrace{r(4)}_{p^3(p-1)} \mid \dots \mid \underbrace{r(\alpha-1)}_{p^{\alpha-2}(p-1)} \mid \underbrace{r(\alpha)}_{p^{\alpha-1}(p-1)} \mid \dots$$

$$\| \qquad \| \qquad \| \qquad \| \qquad\qquad \| \qquad \|$$

$$\varphi(p) \quad \varphi(p^2) \quad \varphi(p^3) \quad \varphi(p^4) \qquad \varphi(p^{\alpha-1}) \quad \varphi(p^\alpha)$$

□

ÁLL g pr. mód $p^\alpha \Rightarrow g$ és $g+p^\alpha$ közül a pk. pr. mód $2p^\alpha$.

Biz: h a pk. g és $g+p^\alpha$ közül

$$h \equiv g \pmod{p^\alpha} \Rightarrow \sigma_{p^\alpha}(h) = \varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

$$h^k \equiv 1 \pmod{2p^\alpha} \iff 2p^\alpha \mid h^k - 1$$

$$\iff p^\alpha \mid h^k - 1$$

$$\iff h^k \equiv 1 \pmod{p^\alpha}$$

Tehát $\sigma_{2p^\alpha}(h) = \sigma_{p^\alpha}(h) = \varphi(p^\alpha) \overset{?}{=} \varphi(2p^\alpha)$

$$\| \quad \varphi(2)\cdot\varphi(p^\alpha) \quad \blacksquare$$

$$1$$

HF11 Kerensúl pr. nyílót mod 13^d, $2 \cdot 13^d$.

HF12 $\{$pr. nyílst mod $p\} = \{\square$-es nemm. mod $p\}$

↑

miért?