# FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

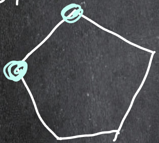
2021. március 2.

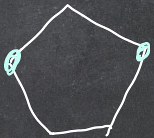
$p$ prím $0<q<p \Rightarrow p \mid \binom{p}{q}$

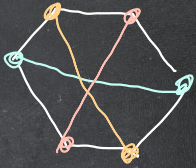
$$\binom{p}{q} = \frac{p!}{q!(p-q)!} \Rightarrow \underbrace{1\cdot\ldots\cdot q}_{p\nmid \ldots p\nmid\ p\nmid}\cdot \underbrace{1\cdot\ldots\cdot(p-q)}_{p\nmid}\cdot\underbrace{\binom{p}{q}}_{p\mid} = \underbrace{p!}_{\Leftarrow p\mid}$$

$$\frac{p!}{q!(p-q)!} \in \mathbb{Z}$$

$p=5,\ q=2$ $\binom{5}{2}$







$5$ db $+$ $5$ db $= \binom{5}{2}$

$p + \ldots + p = \binom{p}{q}$

# PRIMITÍV GYÖKÖK

DEF $m \geq 2$, $a \perp m$ $(\bar{a} \in \mathbb{Z}_m^*)$

$$\sigma(\bar{a}) = \min\{k \in \mathbb{N} \mid \bar{a}^k = \bar{1}\}$$

$$\sigma_m(a) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{m}\}$$

$\boxed{\text{HF7.}}$ $a \perp 10 \Rightarrow \frac{1}{a} = \_\,,\underbrace{\_\_}\underbrace{\_\_}\underbrace{\_\_}\dots$

$\sigma_?(?)$

ÁLL $\bar{a} \in \mathbb{Z}_m^*$, $k, l \in \mathbb{Z}$

(1) $\bar{a}^k = \bar{a}^l \iff k \equiv l \pmod{\sigma(\bar{a})}$

(2) $\bar{a}^k = \bar{1} \iff \sigma(\bar{a}) \mid k$ $\quad [\Rightarrow \sigma(\bar{a}) \mid \varphi(m)]$

(3) $\{\bar{a}^k \mid k \in \mathbb{Z}\} = \{\bar{a}^0, \dots, \bar{a}^{\sigma(a)-1}\} \underset{[\bar{a}]}{\cong} \mathbb{Z}_{\sigma(\bar{a})}$

(4) $\sigma(\bar{a}^k) = \dfrac{\sigma(\bar{a})}{(\sigma(\bar{a}), k)}$. $\quad$ Spec. $\sigma(\bar{a}^k) = \sigma(\bar{a}) \iff k \perp \sigma(\bar{a})$

Biz. (4) $\sigma(\bar{a}) = d$

$$(\bar{a}^k)^l = \bar{1} \iff \bar{a}^{kl} = \bar{1} \overset{(2)}{\iff} d \mid kl \underset{\text{t.l.}}{\iff} \frac{d}{(d,k)} \mid l$$

A legkisebb ilyen poz. $l$: $\dfrac{d}{(d,k)} = \sigma(\bar{a}^k)$. ■

PÉLDA $\varphi(100) = 40 \Rightarrow \sigma_{100}(a) \mid 40$

$$\left.\begin{array}{l} a \perp 100 \Rightarrow a \perp 4 \overset{\text{E.F.}}{\Rightarrow} a^{20} \equiv 1 \pmod 4 \\ \phantom{a \perp 100} \Rightarrow a \perp 25 \underset{\text{E.-F.}}{\Rightarrow} a^{20} \equiv 1 \pmod{25} \end{array}\right\} \Rightarrow \boxed{a^{20} \equiv 1 \pmod{100}}$$

$$\Downarrow$$

$$\sigma_{100}(a) \mid 20.$$

DEF $g$ pr. gyök mod $m$ $\iff \sigma_m(g) = \varphi(m)$

$$\iff \underset{\text{ciklikus csop.}}{[\bar{g}]} = \mathbb{Z}_m^*$$

**ÁLL.** Van pr. gyök mod m $\iff$ $\mathbb{Z}_m^*$ ciklikus csoport-

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{\varphi(m)}$$

**DEF.** $a \perp m$ és $g$ pr. gyök mod $m$ $\Rightarrow \exists\, i \in \mathbb{Z}:\ g^i \equiv a \pmod m$.

$$i \equiv \operatorname{ind}_g^{(m)} a \pmod{\varphi(m)}$$

**HF8** Készítsük indextáblázatot $p=13$, $g=2$-höz, és oldjuk segítségével az $x^9 \equiv 8 \pmod{13}$ kongruenciát.

**ÁLL.** $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha ind } a \text{ ps} \\ -1, & \text{ha ind } a \text{ ptl.} \end{cases}$

**Biz.** $x^2 \equiv a \pmod p$ Legyen $g$ pr. gyök mod $p$. $x \equiv g^i \pmod p$

$g^{2i} \equiv g^{\operatorname{ind} a} \pmod p \iff 2i \equiv \operatorname{ind} a \pmod{p-1}$

Van mo $\iff$ lnko$(2, p-1) \mid \operatorname{ind} a \iff 2 \mid \operatorname{ind} a$ ▨

**Áll.** $g$ pr. gyök mod $m$, $a \perp m$. $\quad a$ pr. gyök mod $m \iff \mathrm{ind}_g a \perp \varphi(m)$.

**Biz.** $o_m(a) = \varphi(m) \iff o_m\left(g^{\mathrm{ind}_g a}\right) = \varphi(m)$

$$\iff \frac{o_m(g)}{(o_m(g), \mathrm{ind}_g a)} = \frac{\varphi(m)}{(\varphi(m), \mathrm{ind}_g a)} \quad < \varphi(m)$$

$$\iff (\varphi(m), \mathrm{ind}_g a) = 1. \quad \blacksquare$$

**Köv.** A mod $m$ pr. gyökök száma: $0$ vagy $\varphi\big(\overbrace{\varphi(m)}^{|\mathbb{Z}_m^*|}\big)$.

Ha $\mathbb{Z}_m^*$ ciklikus, akkor $\varphi(\varphi(m))$ db. generátoreleme van.

---

① $m$-nek van két ph. primkontója NINCS

② $m = p^\alpha$ $(p > 2)$

(2a) $m = p$
VAN

(2b) $m = p^2$

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

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

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

(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) $m = 2^\alpha$ $(\alpha \geq 3)$

TÉTEL. $m > 2 \Rightarrow \varphi(m)$ ps.

Biz. $1, \ldots, \frac{m}{2}, \ldots, m-1, \cancel{m}$

$\text{lnko}(a, m) = \text{lnko}(m-a, m)$

$\frac{m}{2} \perp m$ (ha $m > 2$) ■

ÁLL. $m = u \cdot v,\ u \perp v,\ u, v > 2 \Rightarrow \forall a:\ o_m(a) \le \frac{\varphi(m)}{2} < \varphi(m)$

Biz: $a \perp m \Rightarrow a \perp u \overset{E-F}{\Rightarrow} a^{\varphi(u)} \equiv 1 \pmod{u} \Rightarrow a^{\frac{\varphi(u)\cdot\varphi(v)}{2}} \equiv 1 \pmod{u}$

$\hookrightarrow a \perp v \underset{E-F}{\Rightarrow} a^{\varphi(v)} \equiv 1 \pmod{v} \Rightarrow a^{\frac{\varphi(u)\cdot\varphi(v)}{2}} \equiv 1 \pmod{v}$

$$\blacksquare \quad o_m(a) \mid \frac{\varphi(m)}{2} \Leftrightarrow a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$$

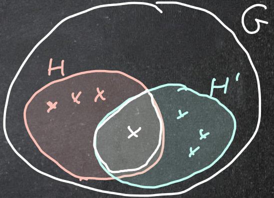
---

$G$ véges csop. $|G| = n$

$$r(d) = |\{a \in G \mid o(a) = d\}| = c(d) \cdot \varphi(d)$$

$$c(d) = |\{H \le G \mid H \cong \mathbb{Z}_d\}|$$

LAGRANGE $\Rightarrow d \nmid n \Rightarrow r(d) = 0$ és $c(d) = 0$.



ISMÉTLÉS:

$G=\mathbb{Z}_n \Rightarrow c(d)=1 \Rightarrow r(d)=1\cdot\varphi(d)=\varphi(d)$

$$\sum_{d|n} \underbrace{r(d)}_{\varphi(d)} = n \Rightarrow \sum_{d|n}\varphi(d)=n=id(n)$$

$$\underbrace{\frac{1}{n},\frac{2}{n},\dots,\frac{n}{n}}_{n\text{ db}} \longrightarrow \frac{1}{n},\dots,\frac{k}{d},\dots,\frac{1}{1}$$

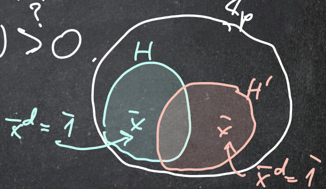
$d|n,\ \underbrace{k\perp n,\ 1\le k\le d}_{\varphi(d)}$

**TÉTEL** $p$ prím $\Rightarrow$ van pr. gyök mod $p$. ($\varphi(\varphi(p))=\varphi(p-1)$ db.)

**Biz.** $G=\mathbb{Z}_p^*$ a pr. gyökök száma: $r(p-1)\overset{?}{>}0$.

$d\nmid p-1 \Rightarrow c(d)=0$ és $r(d)=0$

$d|p-1 \Rightarrow c(d)=0$ vagy $c(d)=1$



Ha $c(d) \geq 2$, akkor az $x^d - 1 \in \mathbb{Z}_p[x]$ polinomnak több, mint $p$ gyöke lenne $\mathbb{Z}_p$-ben. ↯ $\mathbb{Z}_p$ test.

$$|\mathbb{Z}_p^*| = p-1 = \sum_{d \mid p-1} r(d) = \sum_{d \mid p-1} \underbrace{c(d)}_{\leq 1} \cdot \varphi(d) \underset{=}{\leq} \sum_{d \mid p-1} \varphi(d) = p-1$$

$\Rightarrow \forall d \mid p-1: \; c(d) = 1 \Rightarrow r(d) = \varphi(d).$

Spec. $d = p-1$ esetén. $r(p-1) = \varphi(p-1) \geq 1$ ∎

$\boxed{\text{HF 5}}$ Biz. be:

$a, b, c$ pr. gyökök mod $m$ $\Rightarrow$ $a^{\operatorname{ind}_b c}$ is pr. gyök mod $m$.