1.6. Feladat. Számítsuk ki a tanult képlet alapján φ néhány értékét:

(a) $\varphi(1000) = \varphi(2^3 \cdot 5^3) =$ $\varphi(2^3)\cdot\varphi(5^3) = (2^3-2^2)\cdot(5^3-5^2) = 4\cdot 100 = 400$

(b) $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) =$ $(2^3-2^2)\cdot(3^2-3^1)\cdot(5^1-5^0) = 4\cdot 6\cdot 4 = 96$

(c) $\varphi(2025) = \varphi(3^4 \cdot 5^2) =$ $(3^4-3^3)\cdot(5^2-5^1) = 54\cdot 20 = 1080$

1.7. Tétel. A primitív n-edik egységgyökök száma $\varphi(n)$ minden n pozitív egész szám esetén.

Bizonyítás. Tudjuk, hogy az n-edik egységgyökök csoportja ciklikus:

$$E_n = \{\varepsilon_0, \varepsilon_1 \ldots, \varepsilon_{n-1}\} = [\varepsilon_1], \qquad \text{ahol } \varepsilon_k = \varepsilon_1^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}.$$

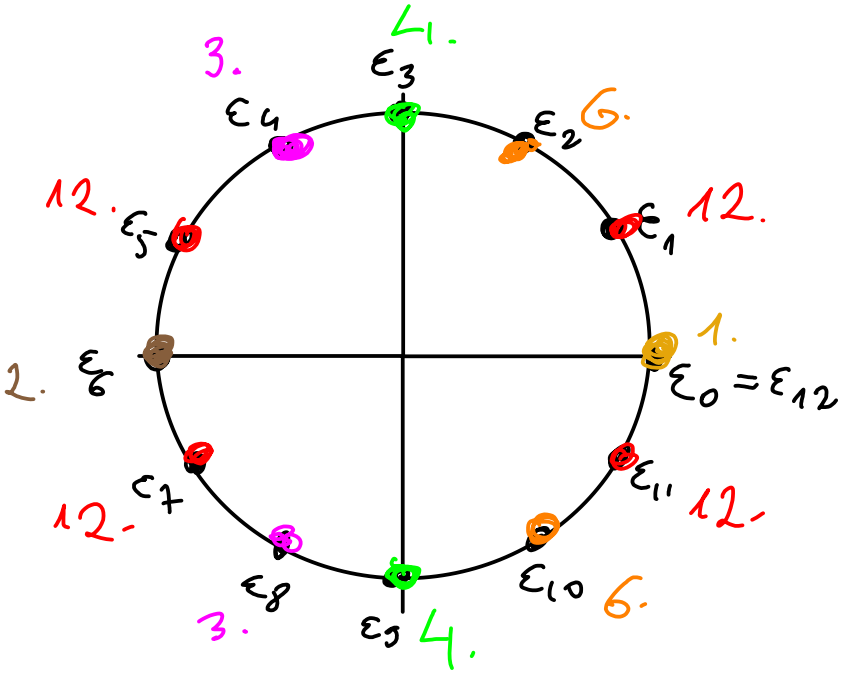
Az ε_k egységgyök akkor és csak akkor primitiv n-edik egységgyök, ha rendje n. Alkalmazzuk a hatvány rendjére vonatkozó képletet:

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{o(\varepsilon_1)}{\mathrm{lnko}(o(\varepsilon_1), k)} = \frac{n}{\mathrm{lnko}(n,k)} = n \iff \mathrm{lnko}(n,k) = 1$$

Tehát a primitív n-edik egységgyökök halmaza

$$P_n = \{\varepsilon_k : 0 \le k \le n-1 \text{ és } \mathrm{lnko}(k,n) = 1\},$$

ennek a halmaznak pedig éppen $\varphi(n)$ eleme van (ugye?). □



$|P_{12}| = 4 = \varphi(12)$

$|P_6| = 2 = \varphi(6)$

$|P_4| = 2 = \varphi(4)$

$|P_3| = 2 = \varphi(3)$

$|P_2| = 1 = \varphi(2)$

$|P_1| = 1 = \varphi(1)$

$12 = \sum_{d \mid 12} \varphi(d)$

1.8. Tétel. Minden n pozitív egész számra $\sum_{d|n} \varphi(d) = n$.

Bizonyítás. Jelölje E_n az n-edik egységgyökök halmazát, P_n pedig a primitiv n-edik egységgyökök halmazát:

$$E_n = \{z \in \mathbb{C}^* : z^n = 1\}, \qquad P_n = \{z \in \mathbb{C}^* : o(z) = n\}.$$

$|E_n| = n$ $\qquad$ $|P_n| = \varphi(n)$

A bizonyítás kulcsa az alábbi megfigyelés:

$$z \in E_n \iff o(z) \mid n$$

$z \in E_n \Leftrightarrow z^n = 1 = z^0 \Leftarrow n \equiv 0 \pmod{o(z)} \Leftrightarrow o(z) \mid n$, $o(z) = d$

Látjuk tehát, hogy E_n felbontható a P_d $(d \mid n)$ halmazok egyesítésére, és ezek a halmazok páronként diszjunktak (miért?):

$$E_n = \dot{\bigcup_{d|n}} P_d.$$

Diszjunkt halmazok egyesítésénél az elemszámok összeadódnak, tehát

$$n = |E_n| = \left|\bigcup_{d|n} P_d\right| = \sum_{d|n} |P_d|.$$

$|P_d| = \varphi(d)$

Az előző tételből tudjuk, hogy $|P_d| = \varphi(d)$, tehát a fenti egyenlőség igazolja, hogy $n = \sum_{d|n} \varphi(d)$. □

2. Az Euler–Fermat-tétel

2.1. Definíció. Ha $a \in \mathbb{Z}$ és $m \geq 2$ relatív prímek, akkor az a szám **modulo** m **rendjén** a $\mathbb{Z}_m^*$ csoport $\overline{a}$ elemének rendjét értjük:

$$o_m(a) = o_{\mathbb{Z}_m^*}(\overline{a}) := \min\left\{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\right\}.$$

Ha a nem relatív prím m-hez, akkor $o_m(a)$ nem értelmezett.

2.2. Példa. Határozzuk meg $o_{18}(7)$ értékét. Ehhez kezdjük el hatványozni a $\overline{7} \in \mathbb{Z}_{18}^*$ elemet:

k	1	2	3	4	5	6	7	8	$\cdots$	1001
$\overline{7}^k$	$\overline{7}$	$\overline{13}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\cdots$	$\overline{13}$

A harmadik hatványra jött ki először $\overline{1}$, ezért $o(\overline{7}) = 3 = o_{18}(7)$.

2.3. Példa. Mit ad 18-cal osztva maradékul 7^{1001}?

Fent megállapítottuk, hogy $o_{18}(7) = 3$, és ez azt jelenti, hogy $\mathbb{Z}_{18}^* \geq [\overline{7}] \cong \mathbb{Z}_3$, vagyis 7 modulo 18 hatványozásakor a kitevő modulo 3 „számít”:

$$1001 \equiv 2 \pmod{3} \implies \overline{7}^{1001} = \overline{7}^2 = \overline{13}.$$

Tehát $7^{1001} \equiv 13 \pmod{18}$.

2.4. Tétel (**Euler–Fermat-tétel**)**.** Ha az a egész szám relatív prím az m modulushoz, akkor

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

Bizonyítás.

- Ha a és m relatív prímek, akkor $\overline{a}$ eleme a $G := (\mathbb{Z}_m^*, \cdot)$ csoportnak.
- LAGRANGE tételének egyik következménye szerint $\overline{a}^{|G|} = \overline{1}$.
- Definíció szerint $|G| = \varphi(m)$.

Tehát $\overline{a}^{\varphi(m)} = \overline{1}$, és épp ezt kellett bizonyítani. □

2.5. Következmény (**kis Fermat-tétel**)**.** Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Más (ekvivalens) megfogalmazásban: Ha p prímszám, akkor minden a egész számra $a^p \equiv a \pmod{p}$.

Bizonyítás.

- Ha p prímszám, akkor $\varphi(p) = p - 1$.
- Ha p prímszám, akkor $\operatorname{lnko}(a, p) = 1 \iff p \nmid a$.

Tehát az Euler–Fermat-tételt az $m = p$ esetben ezt adja:

$$p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}.$$

Ha beszorozzuk mindkét oldalt a-val, akkor az $a^p \equiv a \pmod{p}$ kongruenciát kapjuk, ami még akkor is igaz, ha $p \mid a$ (miért?). □

2.6. Példa. Mit ad 18-cal osztva maradékul 7^{1001}?

Ezt a feladatot már egyszer megoldottuk, de most az Euler–Fermat-tétel segítségével úgy is meg tudjuk oldani, hogy nem készítünk táblázatot 7 hatványaiból.

Osszuk el a kitevőt maradékosan $\varphi(18) = 6$-tal: $1001 = 166 \cdot 6 + 5$. A hatványt átalakítva és az Euler-Fermat-tételt használva a következőképpen számolhatunk:

$$7^{1001} \equiv 7^{166 \cdot 6 + 5} \equiv (7^6)^{166} \cdot 7^5 \equiv 1^{166} \cdot 7^5 \equiv 7^5 \equiv 13 \pmod{18}.$$

2.7. Következmény. Ha $a \in \mathbb{Z}$ relatív prím az $m \geq 2$ modulushoz, akkor tetszőleges $k, \ell \in \mathbb{Z}$ kitevők esetén

(1) $o_m(a) \mid \varphi(m)$;

(2) $k \equiv \ell \pmod{\varphi(m)} \implies a^k \equiv a^\ell \pmod{m}$.

Bizonyítás.

(1) Ez rögtön következik Lagrange tételéből, ha a $G = \mathbb{Z}_m^*$ csoport $H = [\overline{a}]$ részcsoportjára alkalmazzuk.

(2) $k \equiv \ell \pmod{\varphi(m)} \implies k \equiv \ell \pmod{o_m(a)} \iff \overline{a}^k = \overline{a}^\ell$.

□

2.8. Példa. Mit ad 18-cal osztva maradékul 7^{1001}?

A második megoldásunk tömörebb leírása (vegyük észre, hogy a 166-os számnak semmi szerepe nem volt):

$$1001 \equiv 5 \pmod{6} \implies 7^{1001} \equiv 7^5 \equiv 13 \pmod{18}.$$

2.9. Feladat. Mit ad 11-gyel osztva maradékul 123^{765}?

- $123 \equiv 2 \pmod{11} \implies 123^{765} \equiv 2^{765} \pmod{11}$
- $\varphi(11) = 10$
- $\text{lnko}(2, 11) = 1$ ✓
- $765 \equiv 5 \pmod{10} \implies 2^{765} \equiv 2^5 \equiv 10 \pmod{11}$

Összefoglalva:

$$123^{765} \equiv 2^{765} \equiv 2^5 \equiv 10 \pmod{11}.$$

Mit felejtettünk el?

2.10. Feladat. Mit ad 44-gyel osztva maradékul 4447^{2018}?

1. $4447 \equiv 3 \pmod{44}$
2. $\varphi(44) = \varphi(2^2 \cdot 11) = (2^2 - 2^1) \cdot (11 - 1) = 2 \cdot 10 = 20$
3. $\text{lnko}(3, 44) = 1$ ✓
4. $2018 \equiv 18 \pmod{20}$

A fentiekből következik, hogy

$$4447^{2018} \equiv 3^{2018} \equiv 3^{18} \equiv 3^{-2} \equiv 9^{-1} \equiv x \equiv 5 \pmod{44}.$$

$9x \equiv 1 \pmod{44}$

$9x = 45 \pmod{44} \quad / : 9 \quad \text{lnko}(9, 44) = 1$

$x \equiv 5 \pmod{44}$

$3^{18} \equiv 3^9 \cdot 3^9 \cdot 3^9 \cdot 3^9 \cdot 3^2 \equiv (-7)(-7)(-7)(-7) \cdot 9 \equiv 49 \cdot 49 \cdot 9 \equiv 5 \cdot 5 \cdot 9 = 5 \cdot 1 \equiv 5$

3. Primitív gyök, index

3.1. Definíció. Azt mondjuk, hogy a g egész szám **primitív gyök** modulo m, ha rendje éppen $\varphi(m)$.

3.2. Tétel. A g egész szám akkor és csak akkor primitív gyök modulo m, ha az összes mod$m$ redukált maradékosztály megkapható $\overline{g}$ hatványaként.

Bizonyítás. A $\mathbb{Z}_m^*$ csoportban $\overline{g}$ hatványai a $[\overline{g}]$ részcsoportot alkotják, melynek $o_m(g)$ eleme van. Ez akkor és csak akkor teszi ki a teljes $\mathbb{Z}_m^*$ csoportot, ha $o_m(g) = \varphi(m)$. □

3.3. Példa.

$m=5 \quad \mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = [\overline{g}]$ (pr. mód ö.)

$\varphi(5)$

g	1	2	3	4
$\overline{2}^4$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$

$o(\overline{2}) = 4 = \varphi(5) \iff [\overline{2}] = \mathbb{Z}_5^*$

$\overleftarrow{\text{E-F}}$

g	1	2	3	4
$\overline{3}^q$	$\overline{3}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

$o(\overline{3}) = 4 = \varphi(5) \iff [\overline{3}] = \mathbb{Z}_5^*$

q	1	2	3	4
$\overline{4}^q$	$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{1}$

$o(\overline{4}) = 2$

$\overleftarrow{\text{E-F}} \quad [\overline{4}] = \{\overline{1}, \overline{4}\} \neq \mathbb{Z}_5^*$

3.4. Tétel. Akkor és csak akkor létezik primitív gyök, ha a modulus $2, 4$, páratlan prímhatvány vagy páratlan prímhatvány kétszerese:

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha \qquad (p \text{ páratlan prím}, \alpha \in \mathbb{N}).$$

$\overline{5}$

$\text{ind}_2 3 = 7$

$a^k = b \qquad k = \log_a b \qquad \overline{3} = \overline{2}^? \in \mathbb{Z}_5^* \qquad ? = \log_{\overline{2}} \overline{3} = 3$

3.5. Definíció. Tegyük fel, hogy g primitív gyök az m modulushoz. Az a egész szám **indexén** (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{m}$.

~~$\text{ind}_4 3$ nem ért-~~

Jelölés. A modulust az egyszerűség kedvéért nem írjuk ki (ez többnyire amúgy is világos a szövegkörnyezetből), tehát a indexét röviden $\text{ind}_g a$ jelöli.

3.6. Megjegyzés. Világos, hogy ha a és m nem relatív prím, akkor $\text{ind}_g a$ nem értelmezett (ugyanis g^i mindig relatív prím m-hez). Ha viszont a és m relatív prím, akkor a 3.2. Tétel szerint a előáll g hatványaként modulo m, tehát ekkor $\text{ind}_g a$ értelmezett.

3.7. Megjegyzés. Az index nem egyértelmű, csak modulo $\varphi(m)$ van meghatározva.

$g^i \equiv g^{i'} \pmod{m} \iff i \equiv i' \pmod{\varphi(m)}$

3.8. Tétel. Legyen g primitív gyök modulo m, legyen k tetszőleges egész szám, a és b pedig relatív prímek m-hez. Ekkor érvényesek az alábbi azonosságok:

(1) $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;

(2) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;

(3) $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(4) $\operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

Bizonyítás.

(1) $g^0 \equiv 1 \pmod{m} \implies \operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.

(2) $ab \equiv g^{\operatorname{ind}_g(a)} g^{\operatorname{ind}_g(b)} \equiv g^{\operatorname{ind}_g(a)+\operatorname{ind}_g(b)} \pmod{m} \implies$
$\implies \operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$.

(3) $a^k \equiv (g^{\operatorname{ind}_g(a)})^k \equiv g^{k \operatorname{ind}_g(a)} \pmod{m} \implies \operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(4) $ab^{-1} \equiv g^{\operatorname{ind}_g(a)} (g^{\operatorname{ind}_g(b)})^{-1} \equiv g^{\operatorname{ind}_g(a)-\operatorname{ind}_g(b)} \pmod{m} \implies$
$\implies \operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

□

3.9. Feladat. Ellenőrizzük, hogy $g = 2$ primitív gyök a $p = 11$ modulushoz. Ehhez számítsuk ki 2 hatványainak modulo 11 maradékait:

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \pmod{11}$	1	2	4	8	5	10	9	7	3	6	1

A táblázatból látható, hogy $o_{11}(2) = 10 = \varphi(11)$, tehát 2 valóban primitív gyök modulo 11. Az is látszik a táblázatból, hogy minden modulo 11 redukált maradékosztály megkapható $\overline{2}$ hatványaként. A táblázatban minden szám fölött az indexe található. Ha megcseréljük a két sort, és a fölső számok szerint rendezzük az oszlopokat, akkor kapjuk az alábbi **indextáblázatot**:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_g a$	0	1	8	2	4	9	7	3	6	5

3.10. Feladat. Oldjuk meg a fenti példában konstruált indextáblázat segítségével az $x^6 \equiv 5 \pmod{11}$ kongruenciát.

A megoldást kereshetjük $x \equiv 2^i \pmod{11}$ alakban (miért?), és a jobb oldali 5-öst is felírhatjuk 2 hatványaként. Így az $i = \operatorname{ind}_2 x$ ismeretlenre egy lineáris kongruenciát kapunk, amit könnyen meg tudunk oldani:

$\text{lnko}(x, 11) = 1 \Rightarrow \exists\, i : x \equiv 2^i \pmod{11}$

$i = \operatorname{ind}_2 x$

$\operatorname{ind}_2 5$

$\overline{5} \equiv 2^4 \pmod{11}$

$x^6 \equiv 5 \pmod{11}$

$2^{6i} \equiv 2^4 \pmod{11}$

$\varphi(11) = \sigma(2)$

$6i \equiv 4 \pmod{10}$

$6i \equiv 24 \pmod{10}$

$i \equiv 4 \pmod{5}$

$i = 4, 9 \pmod{10}$

$x \equiv 2^4, 2^9 \pmod{11}$

$\overline{5}$ $\overline{6}$

Eredményünk így is megfogalmazható: a $\mathbb{Z}_{11}$ testben $\overline{5}$-nak két hatodik gyöke van, mégpedig $\overline{5}$ és $\overline{6}$.

3.11. Definíció. Azt mondjuk, hogy az a egész szám **n-edik hatványmaradék** modulo m, ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.

3.12. Tétel. Legyen g primitív gyök modulo m, és legyen a relatív prím m-hez. Ekkor a pontosan akkor n-edik hatványmaradék modulo m, ha

$$\text{lnko}(n, \varphi(m)) \mid \text{ind}_g a.$$

Bizonyítás.

$x \equiv g^i \pmod{m}$ $\quad i = \text{ind}_g x$

$a \equiv g^{\text{ind}_g a} \pmod{m}$

$x^n \equiv a \pmod{m}$

$g^{ni} \equiv g^{\text{ind}\, a} \pmod{m}$

$\Updownarrow$

$ni \equiv \text{ind}\, a \pmod{\varphi(m)}$

van $\iff$ $\text{lnko}(n, \varphi(m)) \mid \text{ind}\, a$

$100\ldots001 = x^2 \equiv 2 \pmod{3}$

$x^2 \equiv 0^2 \equiv 0$

$x^2 \equiv 1^2 \equiv 1 \pmod{3}$

$x^2 \equiv 2^2 \equiv 1$

□

4. Négyzetes maradékok, Legendre-szimbólum

4.1. Definíció. Az a egész számot **négyzetes maradéknak** nevezzük modulo m, ha az $x^2 \equiv a \pmod m$ kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy a **négyzetes nemmaradék** modulo m.

4.2. Tétel. Legyen p páratlan prímszám, g primitív gyök modulo p. Ekkor $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p, ha $p \mid a$ vagy $\operatorname{ind}_g a$ páros.

Bizonyítás.

- Ha $p \mid a$, akkor $a \equiv 0 \pmod p$, és a 0 nyilván négyzetes maradék.
- Ha $p \nmid a$, akkor $\operatorname{lnko}(a, p) = 1$, így alkalmazható a 3.12. Tétel:

$$a \text{ négyzetes maradék} \iff \operatorname{lnko}(2, \underbrace{\varphi(p)}_{p-1}) \mid \operatorname{ind}_g a.$$

$$\underbrace{\operatorname{lnko}(2, p-1)}_{2}$$

□

4.3. Definíció. Tetszőleges p páratlan prímszám és p-vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ **Legendre-szimbólumot** a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék } \bmod p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék } \bmod p. \end{cases}$$

4.4. Tétel (**Euler-kritérium**)**.** Ha p páratlan prímszám és $p \nmid a$, akkor

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

Bizonyítás. Legyen g primitív gyök modulo p és $i := \operatorname{ind}_g a$.

1. lépés: $g^{\frac{p-1}{2}} \equiv x \equiv -1 \pmod p$

$x^2 = g^{p-1} \equiv 1 \pmod p \Rightarrow p \mid x^2 - 1 = (x-1)(x+1) \overset{p \text{ prím}}{\Rightarrow} p \mid x-1 \vee p \mid x+1$

$\Rightarrow$ ~~$x \equiv 1\ (p)$~~ $\vee\ x \equiv -1\ (p)$

$o(g) \le \frac{p-1}{2}$ ↯ g prim. gy.

2. lépés: $a^{\frac{p-1}{2}} \equiv (g^i)^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^i \equiv (-1)^i \equiv \left(\frac{a}{p}\right) \pmod p$ □

4.5. Tétel. Tetszőleges p páratlan prímszám és p-vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:

(1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Bizonyítás.

(1) Triviális.

(2) $\left(\frac{ab}{p}\right) \overset{\text{E-K}}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \overset{\text{E-K}}{\equiv} \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}$.

□

4.6. Tétel (**a négyzetes reciprocitási tétel első kiegészítő tétele**)**.** Tetszőleges p páratlan prímszám esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4}. \end{cases}$$

4.7. Feladat. Számítsuk ki az alábbi Legendre-szimbólumokat.

(a) $\left(\frac{8}{79}\right) = \left(\frac{2\cdot 2\cdot 2}{79}\right) \overset{\text{M}}{=} \left(\frac{2}{79}\right)\cdot\left(\frac{2}{79}\right)\cdot\left(\frac{2}{79}\right) = \left(\frac{2}{79}\right)^3 \overset{\text{T}}{=} \left(\frac{81}{79}\right)^3 = 1^3 = 1$

Tehát $\exists x : x^2 \equiv 8 \pmod{79}$.

(b) $\left(\frac{19}{23}\right) \overset{\text{T}}{=} \left(\frac{-4}{23}\right) \overset{\text{M}}{=} \left(\frac{-1}{23}\right)\cdot\left(\frac{4}{23}\right) = (-1)\cdot 1 = -1$

$\left(\frac{-1}{23}\right) = -1$, $\left(\frac{4}{23}\right) = 1$

Tehát $\nexists x : x^2 \equiv 19 \pmod{23}$

4.8. Tétel (**négyzetes reciprocitási tétel**).
Tetszőleges p, q különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod 4 \text{ vagy } q \equiv 1 \pmod 4; \\ -1, & \text{ha } p \equiv 3 \pmod 4 \text{ és } q \equiv 3 \pmod 4. \end{cases}$$

4.9. Tétel (**a négyzetes reciprocitási tétel második kiegészítő tétele**).
Tetszőleges p páratlan prímszám esetén

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod 8; \\ -1, & \text{ha } p \equiv 3, 5 \pmod 8. \end{cases}$$

4.10. Feladat. Számítsuk ki az alábbi Legendre-szimbólumokat.

(a) $\left(\frac{7}{17}\right) \overset{R}{=} \left(\frac{17}{7}\right) \overset{T}{=} \left(\frac{3}{7}\right) \overset{R}{=} -\left(\frac{7}{3}\right) \overset{T}{=} -\left(\frac{1}{3}\right) = -(-1)\cdot 1 = -1$

(b) $\left(\frac{77}{101}\right) = \left(\frac{101}{77}\right) \overset{M}{=} \left(\frac{7}{101}\right)\cdot\left(\frac{11}{101}\right) \overset{R}{=} \left(\frac{101}{7}\right)\cdot\left(\frac{101}{11}\right) \overset{T}{=} \left(\frac{3}{7}\right)\cdot\left(\frac{2}{11}\right) =$

$= -\left(\frac{7}{3}\right)\cdot\left(\frac{7}{2}\right) = -\left(\frac{7}{3}\right)(-1) \overset{T}{=} +\left(\frac{1}{3}\right) = +1$

(c) $\left(\frac{69}{83}\right) \overset{M}{=} \left(\frac{3}{83}\right)\cdot\left(\frac{23}{83}\right) \overset{R}{=} -\left(\frac{83}{3}\right)(-1)\left(\frac{83}{23}\right) \overset{T}{=} \left(\frac{2}{3}\right)\cdot\left(\frac{14}{23}\right) = -\left(\frac{2}{23}\right)\cdot\left(\frac{7}{23}\right) =$

$= -\left(\frac{7}{23}\right) \overset{R}{=} +\left(\frac{23}{7}\right) \overset{T}{=} \left(\frac{2}{7}\right) = 1$

$\left(\frac{69}{83}\right) \overset{T}{=} \left(\frac{-14}{83}\right) = \left(\frac{-1}{83}\right)\cdot\left(\frac{2}{83}\right)\cdot\left(\frac{7}{83}\right) = -\left(\frac{83}{7}\right) = -\left(\frac{-1}{7}\right) = 1$

TÉTEL Végtelen sok $4k+1$ alakú prím van.

Bizt. Indirekt tfh. $p_1, p_2, \dots p_n$ az összes $4k+1$ alakú prím

$$N = 4 \cdot p_1^2 \cdot \dots \cdot p_n^2 + 1$$

$p_1 \nmid N, \dots, p_n \nmid N \Rightarrow N$-nek csak $4k+3$ alakú prímosztói vannak.

Lm q prím $q \mid N$. $q \equiv 3 \pmod 4$

$\Downarrow$

$N \equiv 0 \pmod q$

$4 \cdot p_1^2 \cdot \dots \cdot p_n^2 + 1 \equiv 0 \pmod q$

$(2 \cdot p_1 \cdots p_n)^2 \equiv -1 \pmod q$

$\Downarrow$

$\left(\frac{-1}{q}\right) = 1$ $\quad$ $\left(\frac{-1}{p}\right) = -1$

$\square$

POLINÓMOK

1. Gyűrűk és testek

1.1. Definíció. Legyenek $\circ$ és $*$ kétváltozós műveletek a nemüres A halmazon. Azt mondjuk, hogy $\circ$ **disztributív** a $*$ műveletre, ha minden $a, b, c \in A$ esetén

$$a \circ (b * c) = (a \circ b) * (a \circ c) \quad \text{és} \quad (b * c) \circ a = (b \circ a) * (c \circ a).$$

1.2. Definíció. Legyen R egy nemüres halmaz, amelyen kettő kétváltozós művelet is értelmezve van, nevezzük az egyiket összeadásnak, a másikat szorzásnak. Azt mondjuk, hogy az $(R; +, \cdot)$ struktúra **gyűrű**, ha

1. $(R; +)$ Abel-csoport,

2. $(R; \cdot)$ félcsoport,

3. a szorzás disztributív az összeadásra.

$\forall a \in R: a + 0 = a$

1.3. Tétel. Ha $(R; +, \cdot)$ gyűrű, akkor minden $a \in R$ esetén $a \cdot 0 = 0 \cdot a = 0$.

Bizonyítás. $a \cdot 0 = b$

$b + b = a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = b \quad / + (-b)$

$b = 0$ ✓ $\qquad 0$

□

1.4. Definíció.

- **Kommutatív gyűrű**: olyan R gyűrű, amelyben nemcsak az összeadás, hanem a szorzás is kommutatív:

$$\forall a, b \in R: a \cdot b = b \cdot a.$$

- **Egységelemes gyűrű**: olyan R gyűrű, amelyben nemcsak additív, de **multiplikatív egységelem** is létezik (jelölése: 1):

$$\forall a \in R: a \cdot 1 = 1 \cdot a = a.$$

- **Zérusosztómentes gyűrű**: olyan R gyűrű, amelyben

$$\forall a, b \in R: ab = 0 \implies a = 0 \text{ vagy } b = 0.$$

1.5. Definíció. A kommutatív, egységelemes, zérusosztómentes gyűrűket **integritástartományoknak** nevezzük.

1.6. Tétel. Integritástartományban lehet nemzéró elemmel egyszerűsíteni:

$$\forall a, b, c \in R\colon \text{ ha } c \neq 0, \text{ akkor } a \cdot c = b \cdot c \implies a = b.$$

Bizonyítás. $a \cdot c = b \cdot c \Rightarrow a \cdot c - b \cdot c = 0$

$\Rightarrow (a-b) \cdot c = 0$

$c \neq 0$

$\Rightarrow a - b = 0 \Rightarrow a = b$ □

1.7. Definíció. **Testnek** nevezünk egy $(T; +, \cdot)$ gyűrűt, ha $(T \setminus \{0\}; \cdot)$ Abel-csoport (ebből következik, hogy T integritástartomány és $|T| \geq 2$).

Checklist. Számok esetén

0. $+$ és $\cdot$ műveletek a nemüres R halmazon — R zárt $+, \cdot$-ra
1. ~~$+$ asszociatív~~
2. van additív egységelem (jelölés: 0) $0 \in R$
3. mindenkinek van additív inverze (jelölés: $-a$) — R zárt $-$-ra
4. ~~$+$ kommutatív~~
5. ~~$\cdot$ asszociatív~~
6. ~~$\cdot$ disztributív $+$-ra~~

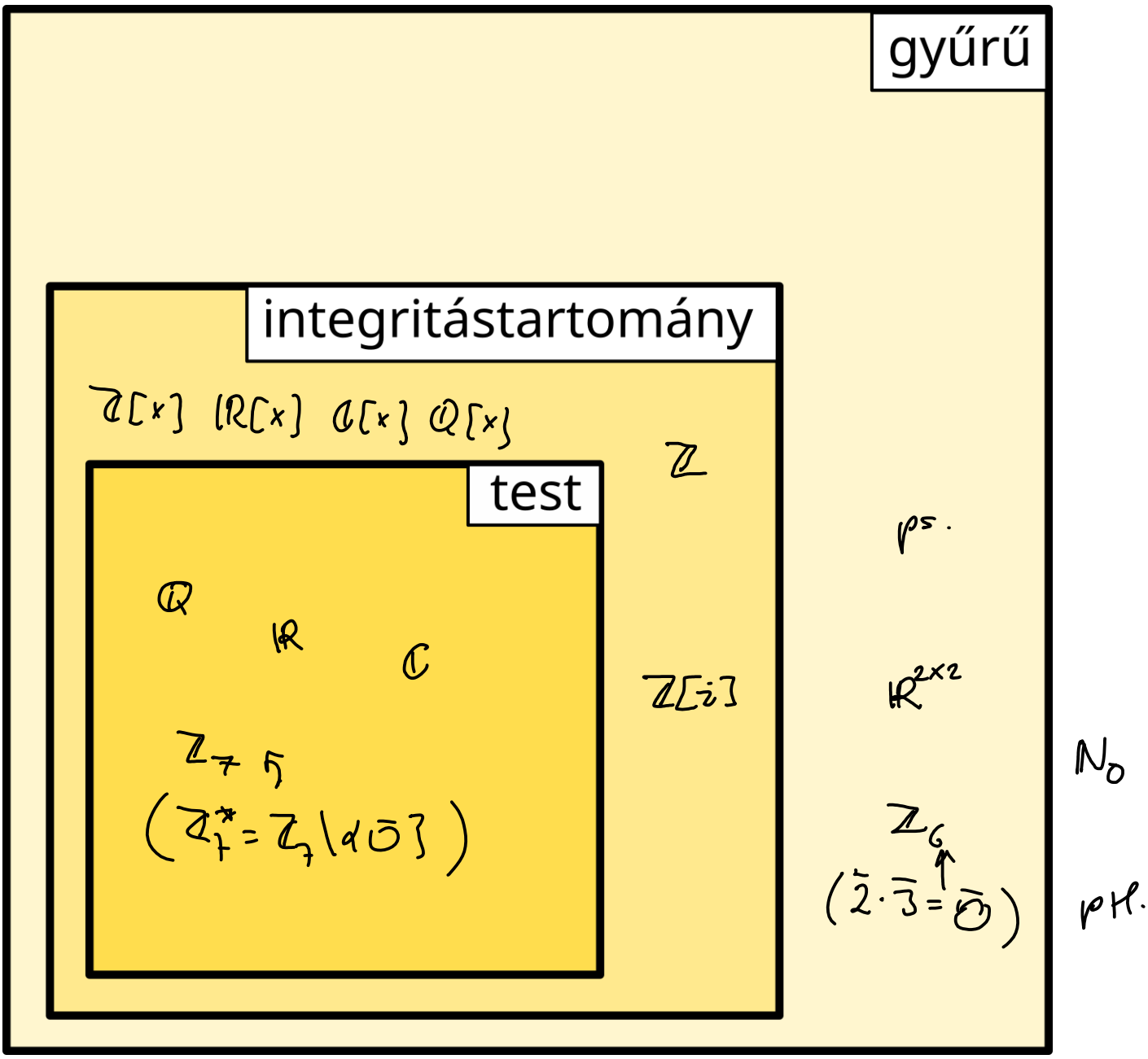
gyűrű

7. ~~$\cdot$ kommutatív~~
8. van multiplikatív egységelem (jelölés: 1) $1 \in R$
9. ~~nincsenek zérusosztók~~

int. tart.

10. minden nemnulla elemnek van multiplikatív inverze (jelölés: a^{-1}) $\forall a \in R \setminus \{0\} : a^{-1} \in R$

test



1.8. Feladat. Gyűrűt, integritástartományt, testet alkotnak-e az alábbi halmazok a szokásos összeadással és szorzással?

(a) $\mathbb{N}_0$

(b) $\mathbb{Z}$

(c) $\mathbb{Q}$

(d) $\mathbb{R}$

(e) $\mathbb{C}$

(f) $\mathbb{R}^{2\times 2}$

(g) páros számok

(h) páratlan számok

(i) $\mathbb{Z}_6$

(j) $\mathbb{Z}_7$

(k) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (**Gauss-egészek**)

1.9. Tétel.

(1) Minden $m \geq 2$ egész szám esetén $\mathbb{Z}_m$ egységelemes kommutatív gyűrű.

(2) Ha m prímszám, akkor $\mathbb{Z}_m$ test.

(3) Ha m összetett szám, akkor $\mathbb{Z}_m$ még csak nem is integritástartomány.

Bizonyítás.

(1) Világos.

(2) Tudjuk, hogy inverze pontosan a redukált maradékosztályoknak van.
Ha m prímszám, akkor $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\overline{0}\}$.

(3) Ha m összetett szám, akkor $m = ab$, ahol $1 < a, b < m$.
Ekkor $\overline{a}$ és $\overline{b}$ zérusosztók $\mathbb{Z}_m$-ben: $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, pedig $\overline{a}, \overline{b} \neq \overline{0}$.

□

Időutazás!

1.10. Tétel. Ha R integritástartomány, akkor az R feletti polinomok $R[x]$ halmaza is integritástartomány a polinomok szokásos összeadásával és szorzásával.

$5x^3 + 3x^2 - 7x + 6 \in \mathbb{R}[x]$

$x, 2, 5, 8, 7, 9, -7$

$(2 \cdot x \cdot x + 5) \cdot (8 \cdot x \cdot x \cdot x + 9) - 7 \cdot x$

2. A polinom fogalma

$R = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

A polinom receptje.

$f = x^2 \in \mathbb{Z}_2[x]$ $\quad f \overset{?}{=} g$

$g = x^2 \in \mathbb{Z}_2[x]$

$f \neq g$

$f(\bar{0}) = \bar{0} = g(\bar{0}), \quad f(\bar{1}) = \bar{1} = g(\bar{1})$

Végy

- egy **határozatlant**: x;
- **együtthatókat**: egy R integritástartományból néhány elemet,

majd jól keverd őket össze az összeadás (kivonás) és szorzás műveletével.

2.1. Definíció. Az R integritástartomány feletti **polinomnak**

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

alakú **formális kifejezést** nevezünk, ahol

- x **határozatlan**;
- az $a_0, a_1, a_2, \ldots, a_n \in R$ elemek az f polinom **együtthatói**.

Az általánosság megszorítása nélkül tfh. $a_n \neq 0$. Ekkor

- az f polinom **fokszáma**: $\deg f = n$;
- az f polinom **főegyütthatója**: a_n.

$\deg 0 = -\infty$

Speciális polinomok:

- **főpolinom**: $a_n = 1$, azaz $f = x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$;
- **konstans polinom**: $\deg f \leq 0$, azaz $f = a_0$.

Jelölés. Az R integritástartomány feletti polinomok halmazát $R[x]$ jelöli.

Polinomok összegét és szorzatát „természetes módon” definiáljuk (lásd az előadásvázlatban és a videóban).

$-\infty = -\infty + \deg g$

$\deg(0g) = \deg 0 + \deg g$

2.2. Tétel. Tetszőleges $f, g \in R[x]$ polinomokra

$$\deg(f+g) \leq \max(\deg f, \deg g) \quad \text{és} \quad \deg(fg) = \deg f + \deg g.$$

2.3. Tétel. A fent (nem) definiált összeadással és szorzással $R[x]$ integritástartomány.

2.4. Definíció. Az $R[x]$ gyűrűt az R feletti egyhatározatlanú polinomok gyűrűjének, röviden R feletti **polinomgyűrűnek** nevezzük.

3. A polinomok „számelmélete"

$T = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$

Megállapodás. Mostantól T mindig tetszőleges testet jelöl, és – hacsak mást nem mondunk – minden polinomot ezen test felett tekintünk.

3.1. Definíció. Legyenek $f, g \in T[x]$ polinomok a T test felett.

- **oszthatóság**: $f \mid g \iff \exists h \in T[x] : g = f \cdot h$.
- **asszociáltság**: $f \sim g \iff f \mid g$ és $g \mid f$.
- **legnagyobb közös osztó**: $d \sim \text{lnko}(f, g)$, ha

  KO: $d \mid f$ és $d \mid g$;

  LN: $\forall k \in T[x] : (k \mid f \text{ és } k \mid g) \implies k \mid d$.
- **legkisebb közös többszörös**: $t \sim \text{lkkt}(f, g)$, ha

  KT: $f \mid t$ és $g \mid t$;

  LN: $\forall k \in T[x] : (f \mid k \text{ és } g \mid k) \implies t \mid k$.

3.2. Tétel. A $T[x]$ polinomgyűrűn az oszthatósági reláció rendelkezik az alábbi tulajdonságokkal:

$2x^3 + 5x^2 + 4x + 2 = 2(x^3 + \frac{5}{2}x^2 + 2x + 1)$

$\sim x^3 + \frac{5}{2}x^2 + 2x + 1$

(1) reflexív;

(2) tranzitív;

(3) $\forall f, g \in T[x] : f \sim g \iff \exists c \in T \setminus \{0\} : g = cf$;

(4) $\forall f, g \in T[x] : f \mid g$ és $g \neq 0 \implies \deg f \leq \deg g$.

3.3. Tétel.

(1) Az asszociáltság ekvivalenciareláció $T[x]$-en.

(2) A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.

(3) Az lnko és az lkkt asszociáltság erejéig egyértelmű.

3.4. Tétel (**a maradékos osztás tétele**). Ha $f, g \in T[x]$ és $g \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és $r \in T[x]$ polinomok, amelyekre

$$f = qg + r \quad \text{és} \quad \deg r < \deg g.$$

Ebben a maradékos osztásban

- f az **osztandó**;
- g az **osztó**;
- q a **hányados**;
- r a **maradék**.

3.5. Feladat. Osszuk el maradékosan az f polinomot a g polinommal az $\mathbb{R}[x]$ polinomgyűrűben.

$f = x^3 - 2, \qquad g = x^2 - 2x + 1$ $\qquad \deg r \leq 1$

$(x^3 - 2) : (x^2 - 2x + 1) = x + 2$

$-\,(x^3 - 2x^2 + x)$

$2x^2 - x - 2$

$-\,(2x^2 - 4x + 2)$

$3x - 4$

r

2.1 (f): $f = 4x^4 + 2x^3 + x^2 + x + 2 \in \mathbb{Z}_5[x]$

$g = 2x^4 + 3x^2 + 1 \in \mathbb{Z}_5[x]$

$g = qf + r \qquad \deg r \leq 3$

$(2x^4 + 3x^2 + 1) : (4x^4 + 2x^3 + x^2 + x + 2) = 3$

$12x^4 + 6x^3 + 3x^2 + 3x + 6 \quad 1$

$-10x^4 \quad 4x^3 \quad +2x$

r