

Számelmélet lesz.

a) $-\frac{\sqrt{3}}{2} + \frac{i}{2}$, $|z|=1$, rendszer van. 4 osztója 360° -nak.

$-\frac{1}{2} + \frac{\sqrt{2}}{2}i$ nem melyik egységgyök.

$\cos \frac{6\pi}{7} + i \sin \frac{6\pi}{7}$ igen

b) $\sqrt[6]{-27} = \sqrt[6]{(-1) \cdot 3^3} = -1 \cdot \sqrt{3}$

hatodik egységgyökkel kell szorozni: ± 1
 $\pm \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$.
 végig kell szorozni.

$\sqrt{-1} = i$ $i^3 = (\sqrt{-1})^3 = -i$

$\sqrt{-1} = -i$

PÉLDA AZ ELLENTMONDÁSRA.

Gyűrűs példa.

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ $\mathbb{R}$ reálalgebra.

$\mathbb{Z}(\omega) = \{a + b\omega : \omega^3 = 1, \omega \neq 1\}$ EZ mi?

ill. egyszerűen $\mathbb{Q}$ -val: $\mathbb{Z} \subset \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}(\omega)$
 $\uparrow$ test.

$\{a + bi : a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}$

Zértekg: $\frac{1}{a+b\sqrt{2}} = x + y\sqrt{2}$ adható-e?
 $a, b \in \mathbb{Q}$.

$1 = (x + y\sqrt{2})(a + b\sqrt{2})$

$1 = (ax + 2by) + (bx + ay)\sqrt{2}$

①

$\left. \begin{array}{l} ax + 2by = 1 \\ bx + ay = 0 \end{array} \right\}$ $\downarrow$ a és b van lehet ilyenek.
 $D = a^2 - 2b^2 \neq 0$
 $- a^2 = 2b^2$

$\mathbb{Z}(\omega)$ - el mi a helyet?

Zártság-e?

$$(a+b\omega)(c+d\omega) \Rightarrow \omega^2 \text{ lesz}$$

X^3-1 gyökei lesznek a 3. egységgyökök

$\downarrow X \neq 1$ ezt kioldósuk

$$X^3-1 = (X-1)(X^2+X+1)$$

$\underbrace{\hspace{1cm}}$

$$\omega^2 + \omega + 1 = 0$$

$$\boxed{\omega^2 = -1 - \omega} \quad \checkmark$$

az inverz mindig van-e? $\mathbb{H} =$ lehet

ennyi volt a gyökök

$$\mathbb{Z}_m \quad \bar{a} = \{a + km : k \in \mathbb{Z}\}$$

$$\text{lukc}(a+km, m) = \text{lukc}(a, m).$$

gyenge multiplikatívitas.

$$c \mid ab, \quad \text{lukc}(a, 6) = 1.$$

$\uparrow$ nincs közös prímosztója.

$$p^2 \mid c \quad \text{lukc}(p, 6) = 1.$$

$C = C_1 C_2$ relatív prímtényező.

Euler-függvény: $\varphi(p^2) =$

$\uparrow$ p prim. $1, 2, 3, \dots, p, \dots, 2p, \dots, (p-1)p, \dots, p^{p-1} \cdot p$

Nem relatív prímtényező: $1, p, 2p, 3p, \dots, p^{p-1} \cdot p$

ezeket kell kivenni, a
restet ezeken.

$a > 1$ esetén $\varphi(a)$ páros.

$\varphi(1) = 1$, mert φ gyenge multiplikatív.

p^{p-1} db van.

φ értéke 1 vagy páros szám.

$p_i^{m_i} - p_{i-1}^{m_{i-1}}$ mindig páros

$\text{lnko}(a, m) = 1$ és legyen $b_1, b_2, \dots, b_{\varphi(m)}$ redukált maradékosztályok.

$ab_1, ab_2, \dots, ab_{\varphi(m)}$ és a_2 .

$$(ab_1)(ab_2) \dots (ab_{\varphi(m)}) \equiv b_1 b_2 \dots b_{\varphi(m)} \pmod{m}$$

$$a^{\varphi(m)} (b_1 b_2 \dots b_{\varphi(m)}) \equiv b_1 b_2 \dots b_{\varphi(m)} \pmod{m}$$

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

Wilson-tétel. Nem prímszámoknál $(p-1)!$ nagy!

Tökéletes számok kérdése. 6-ra vagy 8-ra végződő tökéletes számok.

(HF)

$$a_0 + a_1 10 + a_2 10^2 + \dots + a_k 10^k \equiv 0 \pmod{p}$$

$$0 \leq a_i < 10$$

$$p=3: 10 \equiv 1 \pmod{3}$$

és a 3-al oszthatóság szabálya

$$10^m \equiv 1 \pmod{p} \quad p \nmid 10$$

$$10^{p-1} \equiv 1 \pmod{p} \quad p \text{ prím.}$$

$$10^{p-1} - 1 \equiv 0 \pmod{p}$$

$$p \mid 10^{p-1} - 1 = \left(10^{\frac{p-1}{2}} - 1\right) \left(10^{\frac{p-1}{2}} + 1\right)$$

p valamelyik osztója lesz

csúszó számszorzás

Kriterien: $\gamma: R[x] \rightarrow R$

$$f \rightarrow f(\alpha)$$