5/

3. a) Legyen f (x) = 2x3 + 3x2 + 1 ∈ Z7 [x]. Írjuk fel az f (x + 6) polinomot.
b) Legyen R kommutatív, egységelemes, nullosztómentes gyűrű, f ∈ R[x], c ∈ R. Mutassuk meg, hogy f pontosan akkor irreducibilis R fölött, ha az f (x + c) polinom irreducibilis.

1) $f(x)$ irr. $\Rightarrow$ $f(x+c)$ irr.
2) $f(x+c)$ irr. $\Rightarrow$ $f(x)$ irr.

($k(x) = f(x+c)$-vel, $f(x) = k(x-c)$)

⇕

2') $f(x)$ reducibilis $\Rightarrow$ $f(x+c)$ reducibilis
1') $f(x+c)$ reducibilis $\Rightarrow$ $f(x)$ reducibilis

Elég: csak 2')-t bizonyítani (1)' ua.)

$f(x)$ red. : $f(x) = g(x)\,h(x)$, (R test esetén)
$gr\, g,\ gr\, h < gr\, f$

$f(x+c) = g(x+c) \cdot h(x+c)$
$gr\, f(x+c) = gr\, f(x)$; $gr\, g(x+c) = gr\, g(x)$, $gr\, h(x+c) = gr\, h(x)$
$\Rightarrow$ $f(x+c)$-t nem triv. felbontottuk

$f(x) = a_n x^n + \dots + a_0$
$\Rightarrow f(x+c) = a_n (x+c)^n + \dots + a_1(x+c) + a_0$ $\Longrightarrow$ $f(x+c)$ red
↓
$a_n x^n + a_n \cdot \binom{n}{1} x^{n-1} + \dots$
(főtag)

R nem test: lehet egy olyan felbontás is, hogy:

f nem egység, nem 0: $f(x) = g(x) \cdot h(x)$
$gr\, g = gr\, f$; $gr\, h = 0$
↳ konstans

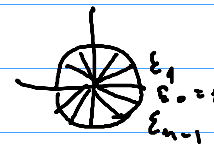
Nem triv. felbontás $\Rightarrow$ g nem irr., h sem invertálható
↑
n-edfokú

$f(x+c) = g(x+c) \cdot h(x+c) = g(x+c) \cdot h$
↑ n-edfokú ↑ nem egység $\Rightarrow$ nem egység

5/8. Számítsuk ki a Φ45 és a Φ168 körosztási polinomok fokszámát.

$$\Phi_n(x) = \prod_{o(\varepsilon_j)=n} (x - \varepsilon_j)$$

↑ pr. n. egységgyökök



$$\text{gr}\,\Phi_n(x) = \#\{\text{pr. n. egységgyökök}\}$$

$\varepsilon_0, \dots, \varepsilon_{n-1}$ n. egységgyökök : $\varepsilon_k = \cos\frac{2\pi}{n}\cdot k + i\sin\frac{2\pi}{n}\cdot k$

ε_k pr. n. egységgyök $\Longleftrightarrow$ $(k, n) = 1$

Ezek száma: $\varphi(n)$ Euler-féle fv.

Pl.: $\varphi(1) = 1$; $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(p) = p - 1$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Ez: φ multiplikatív, azaz:

$\varphi(k \cdot l) = \varphi(k) \cdot \varphi(l)$, ha $(k, l) = 1$

$45 = 5 \cdot 9 = 5 \cdot 3^2$ $\quad \varphi(45) = \text{gr}\,\Phi_{45} = \varphi(5) \cdot \varphi(3^2) = 4 \cdot 6 = 24$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$\neq (p-1)^\alpha$

168	2
84	2
42	2
21	3
7	7

$168 = 2^3 \cdot 3 \cdot 7$

$$\text{gr}\,\Phi_{168}(x) = \varphi(168) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(7)$$
$$= (2^3 - 2^2)(3 - 1)(7 - 1)$$
$$= 4 \cdot 2 \cdot 6 = \underline{\underline{48}}$$

5/10

. Írjuk fel a Φ9 és a Φ27 polinomokat, majd igazoljuk, hogy ezek irreducibilisek Q fölött. Mely körosztási polinomok irreducibilitását lehetne még belátni az általad talált módszerrel?

Nehezebb **Tétel** (NB) $\Phi_n(x)$ irreducibilis $\mathbb{Z}[x]$-ben ($\mathbb{Q}[x]$-ben) $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}$

(Kiss Emil könyve)

Tétel $\Phi_p(x)$ irr. $\mathbb{Z}[x]$-ben ($\mathbb{Q}[x]$-ben)

Előadáson volt.

Biz.: $\Phi_p(x) = \frac{x^p - 1}{x - 1} =$ (a rekurzív képlet alapján)

$= x^{p-1} + x^{p-2} + \dots + x + 1$

5/3.b): $f(x)$ irr. $\Leftrightarrow$ $f(x+c)$ irr.

All.: $\Phi_p(x+1)$ irr. ($\Rightarrow \Phi_p(x)$ irr.)

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x + 1 - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}\cdot 1$$

Alk. a Sch. Eis. p-vel a) $p \nmid 1$

$1 \le k \le p-1$ $\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{1\cdot 2 \cdots k} = p \cdot a$, $a \in \mathbb{Z}$

b) $p \mid \binom{p}{1}, \dots \binom{p}{p-1}$

c) $\binom{p}{p-1} = p$; $p^2 \nmid p$

a)–c) ✓ $\Rightarrow$ $\Phi_p(x+1)$ irred.

---

9 mire műk.;

$$\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\cdot\Phi_3(x)} = x^6 + x^3 + 1$$

($\Phi_1(x)\cdot\Phi_3(x) = x^3 - 1$)

$1 \le k \le 8$ $\binom{9}{3}$

(mod 3) $0 \equiv \binom{9}{k} = \frac{9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}$

$$\Phi_9(x+1) = \frac{(x+1)^9 - 1}{(x+1)^3 - 1} =$$

$(x+1)^9 - 1$ $\mathbb{Z}_3$ fölött

$x^9 + \binom{9}{1}x^8 + \binom{9}{2}x^7 + \dots \binom{9}{8}x + 1 - 1$

$= x$

$(x+1)^3 - 1 = x^3 + \binom{3}{1}x^2 + \binom{3}{2}x + 1 - 1$

$\mathbb{Z}_3[x]$-ben: $\frac{x^9}{x} = x^8$ $\overline{\Phi_9(x+1)} \in \mathbb{Z}_3[x]$

$\mathbb{Z}[x]$-ben: Vel. osztható 3-mal, kivéve a főeh.-t.

Sch. Eis. $\Rightarrow$ $\Phi_9(x+1)$ irr. $\Rightarrow$ $\Phi_9(x)$ irr.

A módszer működik p^2

5/ 5. Igazoljuk, hogy az x4 + x2 + x + 1 polinom irreducibilis Q fölött.

Sch. Eis. ⟶ nem működik

Puszta kézzel: $f(x) = x^4 + x^2 + x + 1 = g(x) \cdot h(x)$, $g, h \in \mathbb{Q}[x]$, $\text{gr}\, g, \text{gr}\, h < 4$

1+3, 2+2 formájú

↳ ∃ 1. fokú tényező ⇒ ∃ gyök ∈ Q

de racionális gyök lehet: ±1 lehetne ↯

1+3 felbontás ∄

2+2: 2. Gauss-lemma ⇒ $f(x) = g(x) \cdot h(x) = q_1 \cdot \bar{g}(x) \cdot q_2 \cdot \bar{h}(x)$

($f(x) \in \mathbb{Z}[x]$, $g(x) \in \mathbb{Q}[x]$, $q_1, q_2 \in \mathbb{Q}$, $\bar{g}, \bar{h}$ primitív, $\in \mathbb{Z}[x]$)

$= \underbrace{q_1 \cdot q_2}_{\in \mathbb{Z}} \cdot \bar{g}(x) \cdot \bar{h}(x)$ primitív

$f(x) = \underbrace{q_1 \cdot q_2 \cdot \bar{g}(x)}_{\in \mathbb{Z}[x]} \cdot \bar{h}(x)$, $\bar{h}(x) \in \mathbb{Z}[x]$

$x^4 + x^2 + x + 1 = g(x) \cdot h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $\text{gr}\, g = 2$, $\text{gr}\, h = 2$

$= (ax^2 + bx + c)(dx^2 + ex + f) = ad \cdot x^4 + (ae + bd)x^3 + (af + be + cd)x^2 + (bf + ce)x + cf$

$a \cdot d = 1$ $\quad b \cdot f + ce = 1$ $\quad a, b, c, d, e, f \in \mathbb{Z}$

$ae + bd = 0$ $\quad cf = 1$

$af + b \cdot e + c \cdot d = 1$

Feltehető: $a = d = 1$ (másik lehetőség: $a = d = -1$)

$cf = 1 \Rightarrow c = f = 1$ v. $c = f = -1$

1. eset: $x^4+x^2+x+1 = (x^2+bx+1)(x^2+ex+1)$

2. eset: $x^4+x^2+x+1 = (x^2+bx-1)(x^2+ex-1)$

1. eset: $a=d=1,\ c=f=1 \qquad 1\cdot e + 1\cdot b = 0 \Rightarrow e = -b$

$x^4+x^2+x+1 = (x^2+bx+1)(x^2-bx+1) = x^4 + (1\cdot1 + b\cdot(-b) + 1\cdot1)x^2 + (b\cdot1 - 1\cdot b)x + 1$

$\hookrightarrow 1 \longrightarrow \overset{\shortparallel}{0}$ ↯

2. eset: hasonlóan.

Másik módszer: mod p számolás.

$f \in \mathbb{Z}[x] \rightsquigarrow \bar{f}(x) \in \mathbb{Z}_p[x]$ együtthatókat mod p nézzük

$x^3+6x^2-3x+2 \qquad \mathbb{Z}_5$ fölött: x^3+x^2+2x+2

$\mathbb{Z}_3$ fölött: x^3+2

T. föl: $f(x) = g(x)\cdot h(x)$

$\bar{f}(x) = \bar{g}(x)\cdot\bar{h}(x) \qquad f$ főegyütthatója: $1 \neq 0$ mod p

$\Rightarrow \operatorname{gr} f = \operatorname{gr}\bar{f},\ \operatorname{gr} g = \operatorname{gr}\bar{g},\ \operatorname{gr} h = \operatorname{gr}\bar{h}$.

Nézzük ezt a polinomot $\mathbb{Z}_2$ fölött:

$\bar{f}(x) = x^4+x^2+x+1 \qquad \mathbb{Z}_2[x]$-ben a SzAT.

$\bar{g}\cdot\bar{h}$ ''

$\mathbb{Z}_2$ fölött: $x^4+x^2+x+1 = x^2(x^2+1) + (x+1) = (x+1)(x^2(x+1)+1)$

$\overset{\shortparallel}{(x+1)^2} \qquad = (x+1)(x^3+x^2+1)$

$(\exists$ 0-fokú osztó$)$ $\qquad \hookrightarrow \nexists$ gyöke $\overset{\text{fok: } 3}{\Rightarrow}$ irr.

$\mathbb{Z}_2[x]$-ben: $\exists$ 1 fokú osztója

$\exists$ 3-fokú osztója $\quad < \nexists$ 2 fokú

$\exists$ 4-fokú osztója

Ha $\mathbb{Z}$ fölött $\exists$ felbont. $\Rightarrow$ 1 + 3 fokú $\rightsquigarrow$ $\mathbb{Z}_2$ fölött is o.k.

2 + 2 fokú $\rightsquigarrow$ $\mathbb{Z}_2$ fölött is $\nexists$ ↯