$\mathbb{Z}_{/(m)} = \{\bar{0}, \bar{1}, \dots \overline{m-1}\}$

↓

maradékosztály

$(\mathbb{Z}_{/m}; +; \cdot) \Rightarrow \bar{a}+\bar{b} = \overline{a+b}$

$\bar{a}\cdot\bar{b} = \overline{a\cdot b}$

⇓

GYŰRŰ

pl.: $m = 6$

$\bar{2}\cdot\bar{3} = \bar{6} = \bar{0}$

⇓

pl.: $(\mathbb{Z}_{/6}; +; \cdot)$ nem integritástartomány, mert van benne zérusosztó

pl.: $(\mathbb{Z}_{/(p)}; +; \cdot)$ TEST

↓

prím

Ha a modulus prímszám ⇒ TESTET kapunk.

Bármelyik = végtelen sok test van ⇒ prímmel elkészítve a maradékosztályt, végtelen sok test lesz. (Eddig: racionális, valós, komplex)

$(\{\bar{0}; \bar{1}\}; +; \cdot)$ $\mathbb{Z}_{(2)}$ test

XXIV

Def.: Ha $a \in \bar{a} \Rightarrow$ az „a" egész számot az $\bar{a}$ osztály reprezentánsának nevezzük.
Ha minden maradékosztályból pontosan egy reprezentánst választunk $\Rightarrow$ reprezentánsok halmazát modulo m teljes reprezentáns rendszernek (maradékrendszernek) nevezzük.

Tétel: Az $a_1 \dots a_k$ egész számok akkor és csak akkor alkotnak modulo m-teljes reprezentáns rendszert, ha $k = m$ és $a_i \not\equiv a_j$ (modulo m) minden $1 \leq i \leq j \leq m$-re.

?

Biz.: az előző def.-ból közvetlenül adódik.

Pl.: modulo m teljes reprezentáns rendszere:

A legkisebb nem negatív maradékok rendszere: $\{0; 1; \dots m-1\}$

A —"— pozitív —"— : $\{1; 2; \dots m\}$

A —"— abszolút értékű —"— : $\{0; \pm 1; \dots \pm \frac{m-1}{2}\}$ ha $2 \nmid m$

ha m páros $\{0, \pm 1; \dots \pm(\frac{m}{2}-1); \frac{m}{2}\}$ ha $2 | m$

Tétel: Legyen $\{a_1, a_2 \dots a_m\}$ egy teljes reprezentáns rendszer modulo m.
Ha $c, b \in \mathbb{Z}$ és $(c; b) = 1 \Rightarrow \{ca_1 + b, ca_2 + b; \dots c \cdot a_m + b\}$ szintén teljes reprezentáns rendszer modulo m.

Biz.: $ca_i + b$ $(i = 1, 2 \dots n)$ számok száma m így elegendő a páronkénti inkongruenciát bizonyítani:
Indirekt úton:
Tfh.: $ca_i + b \equiv ca_j + b \pmod{m} \Rightarrow m | c(a_i, a_j)$ így
$(m; c) = 1$ miatt
$m | a_i - a_j \Rightarrow a_i \equiv a_j \pmod{m}$ ellentmondás

Tétel: Legyen $\bar{a} \in \mathbb{Z}/(m)$ $\forall$ $a_1, a_2 \in \bar{a}$ egészre teljesül, hogy $(a_1; m) = (a_2; m)$

Biz.: Mivel (a_1 és a_2 is az $\bar{a}$ osztályából való) $a_1, a_2 \in \bar{a}$ ezért $\exists\ q_1, q_2 \in \mathbb{Z}$: $a_1 = m \cdot q_1 + a$, $a_2 = m q_2 + a$,

$(a_1, m) = (m \cdot q_1 + a; m) = (a_1; m) = (m \cdot q_2 + a; m) =$

$= (a_2, m)$

Speciálisan $a_1; a_2 \in \bar{a}$ és $(a_1; m) = 1 \Rightarrow (a_2; m) = 1$

Def.: Azokat a modulo m maradékosztályokat, amelyek elemei m-hez relatív prímeket reprezentálnak (vagy prímek) maradékosztályoknak nevezzük.

Ezen osztályok halmazát $P(m)$-el jelöljük

Def.: Ha minden modulo m redukált maradékosztályból pontosan egy representánst választunk, akkor a representánsok halmazát redukált representáns rendszernek ill. redukált maradékrendszernek nevezzük. modulo m.

XXV

Def.: Euler-féle f függvény: $f: \mathbb{N} \setminus \{0\} \to f(m) = \begin{cases} 1, \text{ha } m = 1 \\ k, \text{ha } m \geq 2 \end{cases}$

ahol k jelöli a mod m redukált maradékosztályok számát, azaz a $0, 1, \ldots, m-1$ teljes representáns rendszerből az m modulushoz relatív prímek számát.

Tétel: Legyen $a, b \in \mathbb{N} \setminus \{0\}$, ha $(a, b) = 1 \Rightarrow f(a \cdot b) = f(a) \cdot f(b)$

$m = p_1^{\alpha_1} \ldots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i} \Rightarrow f(m) = \prod_{i=1}^{r} f(p_i^{\alpha_i})$ igaz

elegendő $f(p^{\alpha_i})$ értékét ismerni.

$\varphi(p^\alpha) = ?$ $\alpha = 1$ $\varphi(p) = p-1$, mert a $0, 1, \dots, p-1$ egészek közül csak a 0 nem relatív prím p-hez.

Ha $\alpha \geq 2 \Rightarrow \varphi(p^\alpha)$ jelöli $0, 1, \dots p, \dots 2p, \dots p^\alpha - 1$ számok közül a p^α-hoz (azaz p-hez) relatív prímek számát.

$0, p, 2p, \dots (p^{\alpha-1}-1)\,p$ számok nem relatív prímek p-hez.

csak $p^{\alpha-1}$ van $\Rightarrow \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)$

$m = \prod_{i=1}^{r} p_i^{\alpha_i} \Rightarrow \varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} \left(p^{\alpha_i} - p^{\alpha_i - 1}\right) =$

$= \prod_{i=1}^{r} p^{\alpha_i}\left(1-\frac{1}{p_i}\right) = m \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$

Pl.: $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\cdot\varphi(5^2) = (2^2-2)(5^2-5) =$

$2 \cdot 20 = 40$

Tétel: A $r_1, r_2 \dots r_k$ egész számok $\Leftrightarrow$ alkotnak modulo m redukált maradékrendszert, ha $k = \varphi(m)$, $r_i \not\equiv r_j$ inkongruensek $(\mathrm{mod}\ m)$ minden $1 \leq i \leq j \leq m$-re és $(r_i, m) = 1$ minden $1 \leq i \leq \varphi(m)$-re.

Biz: A $\{c \cdot r_1;\ c \cdot r_2;\ \dots\ c \cdot r_{\varphi(m)}\}$ $\varphi(m)$ tagból áll így az előző tétel alapján elegendő belátni, hogy a rendszer elemei páronként inkongruensek és a modulushoz relatív prímek.

Mivel $(c, m) = 1$ és $(r_i, m) = 1$ $(i = 1, 2, \dots \varphi(m))$ ezért $(c \cdot r_i, m) = 1$

Indirekt úton kk.

Tfh: $c \cdot r_i \equiv c \cdot r_j \pmod m$ valamely $1 \leq i \leq j \leq m$-re $\Rightarrow$

$\Rightarrow m \mid c(r_i - r_j)$, $(m,c) = 1 \Rightarrow m \mid r_i - r_j \Rightarrow r_i \equiv r_j \pmod m$

ellentétre jutottunk

XVI.

Tétel: (Euler – Fermat – tétel)

Ha $a \in \mathbb{Z}$ és $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Biz.: Legyen $\{r_1, r_2, \dots r_{\varphi(m)}\}$ modulo m redukált maradékrendszer.

Az előző tétel alapján $(a, m) = 1$ miatt $\{a \cdot r_1, \dots a \cdot r_{\varphi(m)}\}$ is modulo m redukált maradékrendszer.

Így minden redukált maradékosztályból pontosan egy reprezentánsunk van. Az egyik $\{r_1, r_2 \dots r_{\varphi(m)}\}$ a másik $\{a \cdot r_1, a \cdot r_2, \dots a \cdot r_{\varphi(m)}\}$-ből való

ezek a párok kongruensek modulo m. Ezért $a \cdot r_1 \cdot a \cdot r_2 \dots \cdot a \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \dots r_{\varphi(m)} \pmod m$, amiből $(r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Def.: Ha $m \equiv p$ prímszám $\Rightarrow$ Euler – Fermat tétel speciális esetét a kis Fermat tételt kapjuk.

Tétel: Legyen p prímszám, ha $(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

Tétel: Bármely „a" egész és prímszámra $a^p \equiv a \pmod p$

Biz.: H $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p \Rightarrow$ szorozva mindkét oldalt „a"-val.

$\Rightarrow a^p \equiv a \pmod p$

Ha $(a,p) \neq 1$, $p \mid a \Rightarrow a \equiv 0 \pmod p \Rightarrow a^p \equiv 0 \pmod p \Rightarrow$

$\Rightarrow a^p \equiv a \pmod p$

XXVII

Algebrai egyenletek

Def.: Legyen $(T; +, \cdot)$ test

$f(x) \in T_{[x]}$ $\quad f^\circ \geq 1$

(test feletti min. elsőfokú polinom)

$f(x) = 0$ - t alg. egyenletnek nevezzük.

pl.: $3x^2 + 2x - 1 = 0$

legyen $\alpha \in T$ $\quad f(\alpha) \rightarrow f(x)$ polinom α helyen vett helyettesítési értéke

ha $f(\alpha) = 0$, akkor α gyöke az $f(x) = 0$ egyenletnek.

Algebrai megoldás:

$f(x) = 0$ alg.-i egyenlet algebrai megoldása:

ha $+, -, \cdot, :$, pozitív egész kitevőjű gyökvonás véges sok-

szori alkalmazásával állítjuk elő a gyököt (=megoldást)

$f(x) = 0$ megoldóképlete: az algebrai eljárás során (együtthatóiból) nyert olyan képlet, amelynek az értékei a gyökök.

1., $ax + b = 0$ $\quad a \neq 0$

$$x = -\frac{b}{a}$$

2., $ax^2 + bx + c = 0$ $\quad a \neq 0$ $\quad (a, b, c \in \mathbb{R})$

$b^2 - 4ac \geq 0$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

3., $f^\circ = 3$ ✓ (harmadfokú)

4., $f^\circ = 4$ ✓ (negyedfokú)

———— o ————

Ruffini - Abel tétel: $f^\circ \geq 5$ esetén nem létezik általános megoldóképlet.

pl.: $x^5 - 32 = 0 \rightarrow$ binom egyenletek

$x = \sqrt[5]{32}$

Algebra alaptétele: (egyenletekre vonatkozik, és azt mutatja, hogy megoldható-e)

$\mathbb{C}$: $x^2 + 2 = 0$ $\quad x = \sqrt{2} = \pm i\sqrt{2}$

$\mathbb{R}$: $x^2 + 2 = 0$ $\quad \nexists$ megoldás

$f(x) = 0 \quad (f^\circ \geq 1) \quad (f(x) \in \mathbb{C}[x])$

↓

komplex együtthatós esetben

(Bármely legalább elsőfokú komplex együtthatós egyenletnek)

$\exists$ megoldása $\mathbb{C}$-ben.

BIZ. NEM KELL!!!

$f(x) = 0$ ekvivalens $g(x) = 0$ -val T-fölött, ha gyökeik azonosak.

pl.: $x - 1 = 0$ és $x^3 - 1 = 0$

$x_1 = 1$ $\quad x_{1;2;3} = \sqrt[3]{1} = 1 \; ; \; -\frac{1}{2} + i\frac{\sqrt{3}}{2} \; , \; -\frac{1}{2} - \frac{i\sqrt{3}}{2}$ $\mathbb{C}$-ben

$\mathbb{C}$ fölött nem ekvivalensek

$\mathbb{R}$ fölött ekvivalensek.

☠ Ekvivalens átalakítás: amely ekvivalens ~~át~~ egyenletet eredményez.

pl.: $\mathbb{R}$ feletti

$$x^3 - 1 = 0$$

$$(x-1)(x^2+x+1) = 0$$

↳ csak komplex gyökök voltak (az egyenlet csak tényezőjében)

@ feletti $x^2 - 1 = (x-1)(x^2+x+1) = 0$

nem egyszerűsíthető, mert gyököt vesztünk.

Kövtkezményegyenlet:

$f(x) = 0$ -nak köv.egyg.-e a $g(x) = 0$, ha

$g(x) = 0$ gyökei közül $f(x) = 0$ minden gyöke megtalálható.

ellenőrzés!

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

$|x^2 + 2x - 1| = \sqrt{3}$

Olyan eljárás, mely gyökvesztést eredményez, nem alkalmazható. (Ha kezdőgyök lép fel, az ellenőrzéssel kiválogatható.)

$f(x) = 0$; $f^\circ = n \geq 1$; $f(x) \in \mathbb{C}[x]$

Alg. alaptétel $\Rightarrow \exists\, \alpha_1 \in \mathbb{C}$, hogy $f(\alpha_1) = 0$

Segédtétel: $x - \alpha \mid f(x) \Leftrightarrow f(\alpha) = 0$

$\alpha \in \mathbb{C}$:

Biz.: $f(x) = (x-\alpha) f_1(x) + C$ → konstans (1. 0-fokú, vagy nincs foka)

ha $f(\alpha) = 0$: $f(\alpha) = (\alpha - \alpha) \cdot f_1(\alpha) + C \Rightarrow C = 0$

ha $C = 0 \Rightarrow x - \alpha \mid f(x)$

$f(x) = a_n x^n + \dots a_1 x + a_0 = 0$

$a_n \neq 0 \qquad a_i \in \mathbb{C}$

$f(x) = (x - \alpha_1) \cdot f_1(x)$

ha $f_1^\circ \geq 1$, akkor az alg. alaptétele biztosít neki gyököt $\Rightarrow$

$\exists\, \alpha_2 \in \mathbb{C} \quad f_1(\alpha_2) = 0$

$f(x) = (x - \alpha_1)(x - \alpha_2) \cdot f_2(x)$

ha $f_2^\circ \geq 1$

$$\boxed{f(x) = a_n (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) = 0}$$

$f(x)$ polinom gyöktényezős alakja

? van-e n-nél több gyök: NINCS

Biz.: indirekt módon! triv.

$\Rightarrow$ alg. alaptétele a $\mathbb{C}$-ben biztosítja a gyököket!

XXVIII.

Következmény: $\mathbb{C}[x]$-ben pontosan az elsőfokú polinomok, az irreducibilis, avagy prímpolinomok.

Polinomokra alaptétele $\mathbb{C}[x]$-ben!

$f(x) = ax^2 + bx + c = 0 \qquad a, b, c \in \mathbb{R} \;;\; a \neq 0$

$b^2 - 4ac \geq 0$

$f(x) = a(x - x_1)(x - x_2)$

$$\boxed{\begin{aligned} x_1 + x_2 &= -\frac{b}{a} \\ x_1 \cdot x_2 &= \frac{c}{a} \end{aligned}}$$

Általánosan gyökök és együtthatók összefüggése:

$$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = a_n (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

összetett — szorzat

Két polinom egyenlő, ha a megfelelő fokszámú együtthatója megegyezik.

x^n $\quad a_n = a_n$

x^{n-1} $\quad a_{n-1} = -a(\alpha_1 + \alpha_2 + \dots + \alpha_n)$

x^{n-2} $\quad a_{n-2} = a_n(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n)$

A gyökök összes lehetséges kéttényezős szorzatának összege.

x^0 $\quad a_0 = a_n (-1)^n \alpha_1\alpha_2 \cdot \dots \cdot \alpha_n$

a gyökök és együtthatók közötti összefüggés.

↓

nem helyettesítő az algebrai műveket.

(Fel lehet vele írni az egyenletet!)

$f(x) \in \mathbb{R}_{[x]}$; $f^\circ = n \geq 1$

$f(x) = 0$

Ha $\exists\, \alpha \in \mathbb{C} \setminus \mathbb{R}$ úgy, hogy $f(\alpha) = 0 \Rightarrow f(\bar{\alpha}) = 0$.

($\alpha = a + b\cdot i \quad b \neq 0$)

↓

konjugált is gyöke

Biz.: $a_n \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$

$a_n \bar{\alpha}^n + a_{n-1}\bar{\alpha}^{n-1} + \dots + a_1\bar{\alpha} + a_0 = \bar{0} = a_n \bar{\alpha}^n + a_{n-1}\bar{\alpha}^{n-1} + \dots a_1\bar{\alpha} + a_0 =$

$(\bar{a}\cdot\bar{b} = \overline{a\cdot b})$ → azonosság

$= \bar{a}_n \bar{\alpha}^n + \bar{a}_{n-1}\bar{\alpha}^{n-1} + \dots \bar{a}_1\bar{\alpha} + \bar{a}_0 = \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0} = \bar{0} = 0$ ✓

valósszám = valós szám

$$f(x) = a_n (x-\alpha_1)(x-\bar{\alpha}_1)(x-\alpha_2)(x-\bar{\alpha}_2)\dots \;\Big|\; (x-\beta_1)\dots(x-\beta_t)$$

$\alpha_1 \in \mathbb{C}\setminus\mathbb{R}$ $\quad \alpha_2 \in \mathbb{C}\setminus\mathbb{R}$ $\quad\Big|\quad \beta_i \in \mathbb{R}$

Def.: $(x-\alpha)(x-\bar{\alpha}) = x^2 - \underbrace{(\alpha+\bar{\alpha})}_{\in\mathbb{R},\ -p}\, x + \underbrace{\alpha\bar{\alpha}}_{(a+bi)^2 \in \mathbb{R},\ q} = x^2 + px + q$

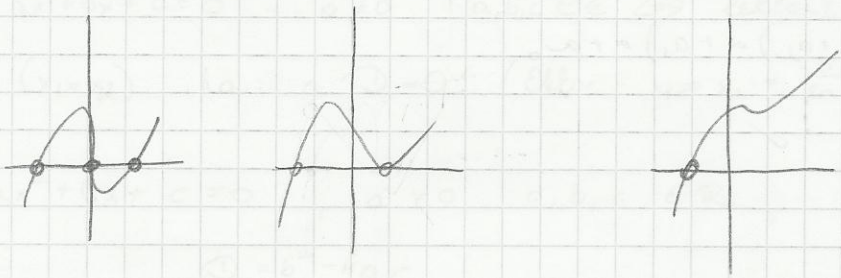
$$f(x) = a_n (x^2+p_1x+q_1)(x^2+p_2x+q_2)\dots (x-\beta_1)(x-\beta_2)\dots(x-\beta_t)$$

$(p_i^2 - 4q_i < 0)$ $\qquad \beta_i \in \mathbb{R}$ $\quad i \geq 0$

Irreducibilis az elsőfokúak és

Minden $\ominus$ diszkriminánsú polinomok.

3.-adfokú polinom



4-edfokú polinom

pl.:

$\alpha_1 = 1$

$\alpha_2 = i$

$\mathbb{C}$ fölött $(x-1)(x-i)$ ✓

$\mathbb{R}$ fölött $(x-1)(x-i)(x+i)$ figyelembe kell venni:

i, mellett mindig van $-i$!!!...