Diszkrét matematika II. – Definíciók és tételek

B szakirány – 2023/2024/1. őszi félév

Mérai László előadásai alapján

Legutóbbi frissítés: 2024. január 17.

Felhasznált források:

- Mérai László előadás-prezentációi
- Gyarmati Edit, Turán Pál: Számelmélet (Tankönyvkiadó, 1989)

1. Számelmélet

1.1. előadás

1.1. Definíció. Oszthatóság

Legyen $a, b \in \mathbb{Z}$. *Azt mondjuk, hogy az* a ***osztja a*** b***-t***, *ha*

$$\exists c \in \mathbb{Z} : a \cdot c = b$$

Jelölése: $a|b$

Megjegyzés. A definíció más megközelítésből: $a \neq 0$ esetén $\frac{b}{a} \in \mathbb{Z}$

1.1. Tétel. Oszthatóság tulajdonságai

$\forall a, b, c, \ldots \in \mathbb{Z}$:

1. $a|a$;
2. $a|b \ \wedge \ b|c \implies a|c$;
3. $a|b \ \wedge \ b|a \implies a = \pm b$;
4. $a|b \ \wedge \ a'|b' \implies aa'|bb'$;
5. $a|b \implies ac|bc$;
6. $ac|bc \ \wedge \ c \neq 0 \implies a|b$;
7. $a|b_1, \ldots b_k \implies a|c_1b_1 + \ldots + c_kb_k$;
8. $a|0$, *ugyanis* $a \cdot 0 = 0$;
9. $0|a \ \Leftrightarrow \ a = 0$;
10. $1|a \ \wedge \ (-1)|a$;

Bizonyítás. Házi feladat. ■

1.2. Tétel. Maradékos osztás

$$\forall a, b \in \mathbb{Z},\ b \neq 0,\ \exists! q, r \in \mathbb{Z}\ :\ a = bq + r\ \wedge\ 0 \leq r < |b|$$

Jelölése: $r = \boxed{a \mod q}$ *(kiejtése: „a modulo q”). Az operáció neve* ***modulo****.*
A $\boxed{q}$ *számot* ***hányados****nak nevezzük, az* $\boxed{r}$ *szám pedig az* ***osztási maradék****.*

Bizonyítás. A tételt csak nemnegatív számok esetében bizonyítjuk.

I. Létezés bebizonyítása ($\exists$): a szerinti indukcióval

Megkülönböztetünk két esetet.

A) $\boxed{a < b} \implies a = b \cdot 0 + a \quad (q = 0,\ r = a)$

B) $\boxed{a \geq b}$: tegyük fel, hogy az a-nál kisebb számok már felírhatók ilyen alakban.
Elevenítsük fel a tételben szereplő egyenletet: $a = bq + r\ \ (0 \leq r < |b|)$
Vegyük az alábbi egyenletet:

$$a - b = bq^* + r^* \iff a = b(q^* + 1) + r^*$$

ami akkor teljesül, ha $q = q^* + 1$ és $r = r^*$.

II. Egyértelműség bebizonyítása ($\exists!$): indirekt módon.

Tegyük fel, hogy a-hoz és b-hez két $q_1, q_2 \in \mathbb{Z}$ $(q_1 \neq q_2)$, illetve $r_1, r_2 \in \mathbb{Z}$ számok tartoznak. Ekkor

$$\begin{aligned} a &= bq_1 + r_1 \qquad (0 \leq r_1 < |b|) \\ a &= bq_2 + r_2 \qquad (0 \leq r_2 < |b|) \end{aligned}$$

aminek az átrendezésével azt kapjuk, hogy

$$b(\underbrace{q_1 - q_2}_{0}) = \underbrace{r_2 - r_1}_{0}.$$

Ez akkor teljesül, ha $q_1 = q_2$ $(\leftrightarrow q_1 \neq q_2$, itt ellentmondásra jutottunk) és $r_1 = r_2$.

■

Megjegyzés. $q = \left\lfloor \dfrac{a}{b} \right\rfloor$, ha $a, b > 0$

1.2. Definíció. Legnagyobb közös osztó

Legyenek $a, b \in \mathbb{Z}$ *és* $d \in \mathbb{N}$. *A* d ***az*** a ***és*** b ***legnagyobb közös osztója****, ha*

- $d|a\ \wedge\ d|b$
- $\forall k \in \mathbb{Z}\ :\ (k|a\ \wedge\ k|b) \implies k|d$

Jelölése: $d = (a, b) = \text{lnko}(a, b) = \gcd(a, b)$. *Definíció szerint* $(0, 0) = 0$

1.3. Tétel. Euklideszi algoritmus

$$\forall a, b \in \mathbb{Z} \ : \ \exists \operatorname{lnko}(a, b)$$

Bizonyítás. A tétel bizonyítása algoritmikus (**euklideszi algoritmus**).
Feltehetjük, hogy $(a, b) \neq (0, 0)$. Végezzük el a következő osztásokat:

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < |b|, \\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1}. && (r_{n+1} = 0)
\end{aligned}$$

Az algoritmus véges sok lépésben véget ér maximum b darab lépésben:

$$|b| > r_1 > r_2 > \cdots > r_n (\geq 0)$$

Megmutatjuk, hogy az utolsó nem 0 maradék (r_n) lesz a kitüntetett legnagyobb közös osztó:

- r_n közös osztó: $r_n | r_{n-1} \implies r_n | r_{n-1} \cdot q$. Kérdés, hogy $r_n | r_{n-2}$? Mivel

$$r_{n-2} = \overbrace{r_{n-1}}^{r_n \cdot q_{n+1}} \cdot q_n + r_n = r_n \cdot q_{n+1} \cdot q_n + r_n = r_n (q_{n+1} \cdot q_n + 1) \implies r_n | r_{n-2}$$

  Hasonlóan haladva visszafelé

$$r_n | r_{n-1} \implies r_n | r_{n-2} \implies r_n | r_{n-3} \implies \ldots \implies \boxed{r_n | b} \implies \boxed{r_n | a}$$

- r_n legnagyobb közös osztó: legyen $c \in \mathbb{Z}$ tetszőleges. Ha

$$\left.\begin{aligned} &c|a \ \wedge \ c|b \\ &a = b \cdot q_1 + r_1 \\ &c | b \cdot q_1 \end{aligned}\right\} \implies c | \underbrace{a - bq_1}_{=r_1} \implies c | r_1$$

  Hasonlóan haladva lefelé: $c|a, \ c|b \implies c|r_1 \implies c|r_2 \implies \ldots \implies \boxed{c|r_n}$

Ekkor a legnagyobb közös osztó az utolsó nem-nulla maradék: $\boxed{(a, b) = r_n}$.
(Itt $a = r_{-1}, b = r_0$) ■

Megjegyzés.

- A tétel szerint egész számok körében az oszthatóság egy nagyon speciális *részben rendezés*.
- Az euklidészi algoritmus **hatékony**:
  - futási idő: $\simeq 2 \log a \ \ (|b| < a)$. Bizonyítás: $r_i < \frac{1}{2} r_{i-2}$
  - Prímtényezős felbontással: $\simeq e^{\sqrt{\log a \log \log a}}$

1.3. Definíció. Dionfantikus / diofantoszi egyenlet

Legyen $a, b, c, x, y \in \mathbb{Z}$. Az

$$ax+by = c$$

egyenleteket ***lineáris diofantoszi egyenlet****nek hívjuk.*

1.4. Tétel. Bővített euklideszi algoritmus

Minden $a, b, c \in \mathbb{Z}$ esetén ***pontosan*** *akkor léteznek $x, y \in \mathbb{Z}$, hogy $ax + by = c$, ha $(a, b)|c$.*

$$\forall a, b, c \in \mathbb{Z},\ (a, b)|c,\ \exists x, y \in \mathbb{Z}\ :\ ax + by = c$$

Bizonyítás. Elég $c = (a, b)$ esetet vizsgálni.
Legyenek $q_i, r_i \in \mathbb{Z}$ az *euklideszi algoritmus*sal megkapott hányadosok, maradékok:

$$r_{i-2} = r_{i-1} \cdot q_i + r_i.$$

Legyen $x_{-1} := 1,\ x_0 := 0$ és

$$x_i = x_{i-2} - q_i \cdot x_{i-1} \qquad (i \geq 1).$$

Hasonlóan legyen $y_{-1} := 0,\ y_0 := 1$ és

$$y_i = y_{i-2} - q_i \cdot y_{i-1} \qquad (i \geq 1).$$

Ekkor $i \geq 1$ esetén: $x_i \cdot a + y_i \cdot b = r_i$, ami speciálisan $x_n a + y_n b = r_n = (a, b)$:

- $i = -1, 0$ esetében: $r_{-1} = 1 \cdot a + 0 \cdot b,\ r_0 = 0 \cdot a + 1 \cdot b$
- más esetben:

$$\begin{aligned} r_{i-2} &= x_{i-2} \cdot a + y_{i-2} \cdot b \\ r_{i-1} &= x_{i-1} \cdot a + y_{i-1} \cdot b \\ r_i &= r_{i-2} - r_{i-1} \cdot q_i \end{aligned} \iff \begin{aligned} r_i &= (x_{i-2} \cdot a + y_{i-2} \cdot b) - (x_{i-1} \cdot a + y_{i-1} \cdot b) \cdot q_i \\ &= (x_{i-2} - q_i \cdot x_{i-1}) \cdot a + (y_{i-2} - q_i \cdot y_{i-1}) \cdot b \end{aligned}$$

■

1.2. előadás

1.4. Definíció. Prímszámok

Egy $p \neq 0, \pm 1$ szám ***prímszám****, ha*

$$p = a \cdot b \implies p = \pm a \ \vee\ p = \pm b$$

Megjegyzés.

1. Ekvivalens definíció: $p|a \cdot b \implies p|a \ \vee\ p|b$.
2. Nagy matematikai áttörés lenne nagy számok **prímfaktorizációja**, azaz megtalálni nagy számok prímosztóit.
   Precízen: adott két prímszám p, q, a szorzatból $p \cdot q$ számoljuk ki p-t.

1.5. Definíció.

Adott $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ $(n \in \mathbb{N}^+)$ számok.

- ***Relatív prímek**nek nevezzük őket, ha $(a_1, a_2, \ldots, a_n) = 1$*
- ***Páronként relatív prímek**nek nevezzük őket, ha $(a_i, a_j) = 1 \quad (i, j \in [1..n] \ \wedge \ i \neq j)$*

1.5. Tétel. Számelmélet alaptétele

$\forall n \in \mathbb{Z}\backslash\{0, \pm 1\}$ sorrendtől és előjeltől eltekintve egyértelműen felírható prímszámok szorzataként:

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$$

ahol $p_1, p_2, \ldots, p_\ell$ pozitív prímek és $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ pozitív egészek.

1.6. Tétel. Számelmélet alaptételének következménye

Legyenek $n, m > 1$ pozitív egészek, melyekre teljesül, hogy

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell} \qquad (\forall i \in [1..\ell] : \alpha_i, \beta_i \geq 0)$$

Ekkor:

- $(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell, \beta_\ell\}}$
- $[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_\ell^{\max\{\alpha_\ell, \beta_\ell\}}$
- $(a, b) \cdot [a, b] = a \cdot b$

Bizonyítás. Házi feladat. ■

1.7. Tétel. Euklidesz tétele

Végtelen sok prímszám létezik.

Bizonyítás. Indirekt bizonyítással. Tegyük fel, hogy csak véges sok prím van.
Legyenek ezek $p_1, p_2, \ldots, p_k$. Tekintsük az $n := p_1 \cdots p_k + 1$ számot. Ez nem osztható egyetlen $p_1, \ldots, p_k$ prímmel sem, így n prímtényezős felbontásában kell szerepelnie egy újabb prímszámnak. ■

Megjegyzés.

- **Figyelem**: $p_1 \cdots p_k + 1$ nem feltétlen prím: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$
- **Prímszámtétel**: x-ig a prímek száma: $\sim \dfrac{x}{\ln x}$.

1.6. Definíció. Kongruencia

*Adott $n \neq 0$ és $a, b \in \mathbb{Z}$ esetén, a **kongruens** b**-vel modulo** n;*

$$a \equiv b \mod n, \quad \text{ha } n|(a - b).$$

1.8. Tétel.

A kongruencia ***ekvivalencia reláció****.*

Bizonyítás. Ellenőrizzük az ekvivalencia reláció tulajdonságait.

I. Reflexivitás: $a \equiv a \mod n$, ugyanis $n|a-a=0$

II. Tranzitivitás: $a \equiv b \mod n \ \wedge \ b \equiv c \mod n \implies a \equiv c \mod n$,
ugyanis $n|a-b,\ n|b-c \implies n|(a-b)+(b-c)=a-c$

III. Szimmetria: $a \equiv b \mod n \implies b \equiv a \mod n$,
ugyanis $n|a-b \implies n|(-1)\cdot(a-b)=b-a$

■

1.9. Tétel. A kongruencia kompatibilitása az összeadással és a szorzással

Legyenek $a,b,c,d,n \in \mathbb{Z}, n \neq 0$. *Ekkor:*

- $a \equiv b \mod n \ \wedge \ c \equiv d \mod n$ *esetén* $a+c \equiv b+d \mod n$
- $a \equiv b \mod n \ \wedge \ c \equiv d \mod n$ *esetén* $a \cdot c \equiv b \cdot d \mod n$

Bizonyítás. Házi feladat. ■

1.10. Tétel. Osztás művelete kongruenciákkal

Legyenek $a,b,c,n \in \mathbb{Z}, n \neq 0$. *Ekkor:*

$$ab \equiv ac \mod n \iff b \equiv c \mod \frac{n}{(a,n)}\ .$$

Bizonyítás. Ekvivalenciánál mindkét irányt meg kell vizsgálni.

I. $\boxed{\implies}$: Legyen $d := (a,n)$ és tegyük fel, hogy $n|ab-ac=a(b-c)$. Ekkor

$$\frac{n}{d}\cdot d \ \Big| \ \frac{a}{d}\cdot d\cdot(b-c)\ ,$$

azaz

$$\exists k \in \mathbb{Z} \ : \ k\cdot\frac{n}{d}\cdot d = \frac{a}{d}\cdot d\cdot(b-c)\ .$$

Egyszerűsítve d-vel meghapjuk, hogy

$$\frac{n}{d} \ \Big| \ \frac{a}{d}\cdot(b-c)\ .$$

Azonban $\frac{n}{d}$ és $\frac{a}{d}$ *relatív prímek*, így $\frac{n}{d} \ \Big| \ (b-c)$.

II. $\boxed{\impliedby}$: A másik irány triviális.

■

1.11. Tétel. Lineáris kongruenciák

Legyenek $a, b, n \in \mathbb{Z},\ n > 1$. *Azt mondjuk, hogy*

$$ax \equiv b \mod n \text{ megoldható} \iff (a,b)|b$$

és pontosan (a,n) *darab inkongruens megoldása van* $\mod n$.

Bizonyítás. A bizonyítás algoritmikus.

$$ax \equiv b \mod n \iff ax + ny = b$$

I. Szükséges feltétel ($\Longrightarrow$): mivel (a,n) osztja a bal oldalt, osztja a jobb oldalt is, azaz

$$(a,n)|b \implies (a,n)|ax+ny.$$

II. Elégséges feltétel ($\Longleftarrow$): a **bővített euklideszi algoritmus** szerint

$$\exists x_0, y_0 \in \mathbb{Z} \ : \ x_0 a + y_0 n = (a,b).$$

Beszorozva $\dfrac{b}{(a,n)}$-nel megkapjuk a megoldást.

III. Megoldások száma: Legyen $a' := \dfrac{a}{(a,n)}$, $b' := \dfrac{b}{(a,n)}$, $n' := \dfrac{n}{(a,n)}$. Ekkor $(a',b') = 1$.

Ha (x_0, y_0) és (x_1, y_1) két megoldása az $a'x + n'y = b'$ egyenletnek, akkor

$$a'(x_0 - x_1) + n'(y_0 - y_1) = 0.$$

Ekkor $x_0 \equiv x_1 \mod n'$.

További megoldások: $\boxed{\dfrac{b}{(a,n)} \cdot x + k \cdot n' \quad (k = 0, \ldots, (a,n) - 1)}$.

■

1.3. előadás

1.7. Definíció. Szimultán kongruencia

Egy ismeretlenre vonatkozó különböző modulusú lineáris kongruenciákat szimultán (egyidejű) kongruenciáknak nevezünk.

$$\left.\begin{aligned} a_1 x &\equiv b_1 \mod n_1 \\ a_2 x &\equiv b_2 \mod n_2 \\ &\vdots \\ a_k x &\equiv b_k \mod n_k \end{aligned}\right\}$$

ahol $k \in \mathbb{N}^+$, $(n_1, n_2, \ldots, n_k) = 1$ *és* $a_1, a_2, \ldots a_k, b_1, b_2, \ldots, b_k, x \in \mathbb{Z}$

Megjegyzés. [a] Mivel a szimultán kongruenciák megoldhatóságához nyilvánvalóan szükséges, hogy a fenti definícióbeli kongruenciák külön-kölün megoldhatók legyenek, tehát ezen kongru-

enciák helyett rögtön a megoldásokat tekintve az

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

alakú szimultán kongruenciák megoldására szorítkozhatunk, ahol c_i az i-edik kongruencia valamelyik megoldása ($i \in [1..k]$).
Ha az összes ilyen rendszer megoldását megadjuk, ezáltal már a kongruenciarendszer összes megoldását előállítottuk.

[a]Forrás: Gyarmati Edit, Turán Pál – Számelmélet (Tankönyvkiadó, 1989), 70. oldal

1.12. Tétel. Kínai maradék tétel

Legyenek $k \in \mathbb{N}^+$, $n_1, n_2, \ldots, n_k \in \mathbb{N}\backslash\{0,1\}$ páronként relatív prímszámok és $c_1, c_2, \ldots, c_k \in \mathbb{Z}$. Ekkor a

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

***kongruenciarendszer megoldható** és bármely két megoldása kongruens egymással modulo $n_1 \cdot n_2 \cdots n_k$.*

Bizonyítás. A bizonyítás algoritmikus.

I. Legyen $k := 2$:

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \end{aligned}\right\}$$

A **bővített euklideszi algoritmus**sal oldjuk meg az alábbi egyenletet:

$$n_1 x_1 + n_2 x_2 = 1.$$

Legyen $c_{1,2} := n_1 x_1 \cdot c_2 + n_2 x_2 \cdot c_1$. Ekkor[a]

$$c_{1,2} = n_1 x_1 \cdot c_2 + n_2 x_2 \cdot c_1 = c_2 \cdot \overbrace{(1 - n_2 x_2)}^{n_1 x_1 + n_2 x_2 = 1} + n_2 x_2 \cdot c_1 = c_2 + (c_1 - c_2) n_2 x_2$$

Ebből az következik, hogy

$$c_{1,2} \equiv c_1 \mod n_1 \quad (1)$$
$$c_{1,2} \equiv c_2 \mod n_2 \quad (2)$$

A (2) egyenletet megkapjuk a fentiekhez hasonló átalakításokkal. Összegezve,

$$c_{1,2} \equiv c_j \mod n_j \quad (j = 1, 2).$$

Ha $x \equiv c_{1,2} \mod n_1 n_2$, akkor x megoldása a két kongruenciának. Megfordítva: ha x megoldása a két kongruenciának, akkor az $(x - c_{1,2}) | n_1 \wedge (x - c_{1,2}) | n_2$, így a szorzatukkal is: $x \equiv c_{1,2} \mod n_1 n_2$ (ne feledjük, hogy $(n_1, n_2) = 1$).

II. Általános eset. Az alábbi

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

szimultán kongruencia ekvivalens a

$$\left.\begin{aligned} x &\equiv c_{1,2} \mod n_1 n_2 \\ x &\equiv c_3 \mod n_3 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

rendszerrel. Iterálva az eljárást, megkapjuk az

$$x \equiv c_{1,\dots,k} \mod n_1 n_2 \dots n_k$$

kongruenciát.

■

[a]Forrás: `https://www.wikiwand.com/en/Chinese_remainder_theorem#Existence_(constructive_proof)`

Megjegyzés. **A megjegyzés a javított dia szövege, ami nem lesz számonkérve.**
Ha a modulosok nem relatív prímek ($(n_1, n_2) \neq 1$), akkor a feladat hasonlóan kezelhető.
Például $k = 2$ esetén tekintsük a

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \end{aligned}\right\}$$

rendszert. Legyen $d := (n_1, n_2) > 1$. Megmutatható, hogy ha

$$c_1 \not\equiv c_2 \mod d,$$

akkor a rendszernek nincs megoldása.
Ellenkező esetben legyen $d := n_1 x_1 + n_2 x_2$. Ekkor

$$c_{1,2} \equiv c_1 - x_1 \cdot n_1 \cdot \frac{c_1 - c_2}{d} \mod \frac{n_1 n_2}{d}$$

lesz az összes megoldás (*bizonyítása házi feladat*).
A $k \geq 3$ esetén az eljárást iterálva oldhatjuk meg a szimultán kongruenciarendszert.

1.8. Definíció. Euler-függvény

Adott $n \in \mathbb{N}$ szám esetén legyen

$$\varphi(n) = \#\{1 \leq a < n \mid (a, n) = 1\}$$

*az **Euler-függvény** (vagy **Euler-féle φ-függvény**).*

Megjegyzés. Az Euler-függvény néhány tulajdonsága multiplikatív (gyakorlaton hangzott el):

1. Multiplikativitás: $\forall a, b \in \mathbb{N} : \ (a, b) = 1 \implies \varphi(ab) = \varphi(a) \cdot \varphi(b)$

2. Kis Fermat-tétel: $\varphi(p) = p - 1$, ha p prímszám.

1.13. Tétel. Euler-függvény értékének kiszámítása

Legyen n prímtényezős felbontása $n := p_1^{e_1} \cdot p_2^{e_2} \cdots p_\ell^{e_\ell}$. Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right)$$

Bizonyítás. Nem bizonyítjuk. ■

Pár szó az **osztahtósági szabályo**król. Vegyünk szemügyre pár példát.

1. 3-mal való oszthatóság: ha a számjegyek összege osztható 3-mal, akkor a szám is osztható 3-mal.

   Például: $\boxed{123} = 1 \cdot 100 + 2 \cdot 10 + 3 \cdot 1 \boxed{\equiv 1 + 2 + 3 \mod 3}$

   Általában:

   $$n = \sum_{i=0}^{k} n_i \cdot 10^i \equiv \sum_{i=0}^{k} n_i \cdot 1^i \equiv \sum_{i=0}^{k} n_i,$$

   ugyanis $10 \equiv 1 \mod 3$.

2. 7-tel való oszthatóság: Például:

   $$\boxed{123} = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 \equiv$$
   $$1 \cdot \overbrace{3^2}^{10 \equiv 3 \mod 7} + 2 \cdot \overbrace{3^1}^{10 \equiv 3 \mod 7} + 3 \cdot \overbrace{1^0}^{1 \equiv 1 \mod 7} \equiv$$
   $$1 \cdot \overbrace{2}^{3^2 \equiv 9 \equiv 2 \mod 7} + 1 \cdot 3 + 3 \cdot 1 \mod 7$$

   A kérdés: $10^i \equiv ? \mod 7$. Vizsgáljuk meg a hatványmaradékokat!

i	0	1	2	3	4	7	6	7	8	9	10	11	12	13	14	...
$10^i \mod 7$	1	3	2	6	4	5	1	3	2	6	4	5	1	3	2	...

   Tehát: $123 \equiv 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 1 = 11 \boxed{\equiv 4 \mod 7}$.

3. Következtetéseink:

   - Mindig van oszthatósági szabály.
   - Az $a^i \mod n$ **hatványmaradékok periodikusan ismétlődnek**.
     - Vannak olyan a alapok, amikor teljesen ciklikusan ismétlődnek az osztási maradékok, míg más esetben csak egy bizonyos ponttól. Ez utóbbiak egy aciklikus és egy ciklikus részből állnak.
     - Vannak olyan a alapok, ahol a teljes maradékosztály maradékai megjelennek, míg mások esetében csak pár jelenik meg.

1.4. előadás

Maradékosztályok.
Jelölés: legyen $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ a nem-negatív maradékok halmaza, és tekintsük a $+, \cdot$ műveleteket modulo n.

$\mathbb{Z}_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	0
3	3	0	0	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Emlékeztető: ha $(a, b) = 1$, akkor $ax \equiv b \mod n$ kongruenciának létezik *egyértelmű* megoldása modulo n.
Legyen $\mathbb{Z}_n^* := \{1 \leq a < n | (a, n) = 1\}$. Speciálisan $|\mathbb{Z}_n^*| = \varphi(n)$

1.14. Tétel. Euler–Fermat-tétel

Legyenek $a, n \in \mathbb{Z}$, $(a, n) = 1$. Ekkor

$$a^{\varphi(n)} \equiv 1 \mod n,$$

ahol φ az Euler-függvény.

Bizonyítás. Lineáris kongruenciákkal.
Tekintsük az

$$ax \equiv b \mod n$$

lineáris kongruenciát. Mivel $(a, n) = 1$, minden b-hez létezik egyértelmű (vagyis pontosan egy) x megoldás, azaz az

$$x \mapsto ax \mod n,$$

ami $\mathbb{Z}_n^*$ maradékosztálynak egy bijekciója. Így a

$$\mathbb{Z}_n^* \quad \text{és} \quad \{ax \mod n \mid x \in \mathbb{Z}_n^*\}$$

halmazok azonosak. Ekkor a halmazok elemeinek **szorzata** is megegyezik:

$$\prod_{x \in \mathbb{Z}_n^*} x \equiv \prod_{x \in \mathbb{Z}_n^*} ax \equiv a^{\varphi(n)} \cdot \prod_{x \in \mathbb{Z}_n^*} x \mod n.$$

Mivel

$$\left(n, \prod_{x \in \mathbb{Z}_n^*} x\right) = 1$$

így a szorzattal egyszerűsíthetünk: $1 \equiv a^{\varphi(n)} \mod n$. ■

Hatványok maradékai még egyszer.
Legyen p egy prímszám és $p \nmid a$. Ekkor az *Euler–Fermat-tétel* szerint $a^{\varphi(n)} \equiv 1 \mod p$ ($\varphi(p) = p - 1$). Vannak jó a alapok, melyknek $p - 1$ **különböző** hatványa van modulo p.

1.15. Tétel. Generátor létezéséről szóló tétel

Legyen p prímszám. Ekkor $\mathbb{Z}_p^*$-ban ***van generátor*** *(vagy* ***primitív gyök****), azaz*

$$\exists g \in \mathbb{Z},\ 1 < g < p\ :\ \{\overbrace{g^0 \mod p}^{=1}, g \mod p, g^2 \mod p, \ldots, g^{p-2} \mod p\} = \mathbb{Z}_p^* = \{1, \ldots, p-1\}$$

Bizonyítás. Nem bizonyítjuk. ■

1.9. Definíció. Diszkrét logaritmus

Legyen p prímszám, g generátor modulo p. Ekkor az $a \in \mathbb{Z} : (p \nmid a)$ g alapú ***diszkrét logaritmusa*** *(****indexe****).*

$$\log_a a = n\ :\ a \equiv g^n \mod p,\quad 0 \leq n < p-1.$$

Megjegyzés. Példa: 2 generátor modulo 11.

n	0	1	2	3	4	5	6	7	8	9
$2^n \mod 11$	1	2	4	8	5	10	9	7	3	6

$$\Downarrow$$

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

1.16. Tétel. Diszkrét logaritmus műveletei

Legyen p prímszám, g generátor modulo p, valamint $1 \leq a, b < p, n \in \mathbb{Z}$. Ekkor

$$\log_g(a \cdot b) \equiv \log_g a + \log_g b \mod (p-1)$$

$$\log_g(a^n) \equiv n \cdot \log_g a \mod (p-1)$$

Bizonyítás. Nem bizonyítjuk. ■

1.5. előadás – Titkosítási algoritmusok

I. Caesar-kód

Kidolgozni.

II. One-Time Pad

Kidolgozni.

III. RSA

Kidolgozni.

2. Polinomok

2.1. előadás

A polinomok x^2+2x+1, $x^5+\frac{3}{2}x^2-ix+i-\sqrt{2}$, ... típusú kifejezések.

Alkalmazások:

I. Numerikus módszerek: bonyolult függvények közelítése

$$\sin(x) \approx x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!}, \qquad |x|<1, \quad \text{hiba} < 10^{-7}$$

$$e^x \approx 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} + \frac{x^7}{7!}, \qquad |x|<1, \quad \text{hiba} < 10^{-3}$$

II. Hibajavító kódok: Adatátvitel során sérült jel rekonstrukciója

$$\text{kódszavak} \leftrightarrow \text{polinomok}$$

III. Komputeralgebra, szimbolikus számítások: határozott integrálok, differenciálegyenletek (pontos) megoldása

$$\int x^2 dx = \frac{x^3}{3} + C$$

IV. Robotika: Robotkarok pontos mozgásának leírása

Jelölés: legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p\}$ (p egy prímszám). Jelentése: $\mathbb{K}$ egy tetszőleges számhalmaz.

2.1. Definíció. Polinom.

*Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p\}$. A $\mathbb{K}$ fölötti **polinomok** halmaza $\mathbb{K}[x]$ az x és $\mathbb{K}$ elemei által az $+$, $-$, $\cdot$ segítségével alkotott formális kifejezések:*

$$\mathbb{K}[x] := \{c_n x^n + \ldots + c_0 \mid n \geq 0 \wedge c_n, \ldots, c_0 \in \mathbb{K}\}$$

*Adott polinom $f := c_n x^n + \ldots + c_0$ **együtthatói** a $c_n, \ldots, c_0$ számok, míg $c_n \neq 0$ esetén f **foka** $\deg f = n$ és **főegyütthatója** c_n.*

Megjegyzés. Megkülönböztetjük a polinomot a polinomfüggvénytől.

- **Polinom**: $f = c_n x^n + \ldots + c_0$
- **Polinomfüggvény**: $f(x) = c_n x^n + \ldots + c_0$