# Kongruenciák, számrendszerek

**Maradékos osztás:** $a,b$, $a \geq b$ pozitív egész számokhoz egyértelműen találhatunk olyan $q$ és $r$ egész számokat melyekre $a = b \cdot q + r$, ahol $0 \leq r < b$. Ilyenkor $q$-t $a$-nak $b$-vel való osztásakor keletkező hányadosnak, $r$-t pedig maradéknak nevezzük.

**Def:** Az $a,b$ 0-tól különböző természetes számok legnagyobb közös osztóján azt a $d$ természetes számot értjük, mely $a$-nak és $b$-nek is osztója, és a közös osztók közül a legnagyobb.

Jelölés: $(a;b)$

Pl. $(960;1056) = (2^6 \cdot 3 \cdot 5; 2^5 \cdot 3 \cdot 11) = 2^5 \cdot 3 = 96$

**Euklideszi algoritmus:** $a,b$ természetes számok

Elosztjuk az $a$ számot $b$-vel maradékosan, majd $b$-t a maradékkal stb.., mindig az osztót a maradékkal. Addig folytatjuk ezt, amíg 0 maradékra nem jutunk.

$a = bq_1 + r_1$, ahol $0 < r_1 < b$

$b = r_1 q_2 + r_2$, ahol $0 < r_2 < r_1$

…

$r_{n-2} = r_{n-1} q_n + r_n$, ahol $0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1}$, ahol a maradék már 0

Mivel a maradékok egyre csökkennek így az eljárás biztosan véget ér véges sok lépésben.

**Tétel:** Az $a,b$ természetes számokon végrehajtott euklideszi algoritmus utolsó nem 0 maradéka a két szám legnagyobb közös osztója.

**Biz:** Az utolsó sor alapján $d = r_n$ osztója $r_{n-1}$-nek. $d \mid r_n$ és $d \mid r_{n-1} \Rightarrow d \mid r_{n-1} q_n + r_n = r_{n-2}$-nek, stb… Soronként visszafelé haladva $d \mid b$ és $d \mid a$-t kapjuk, tehát valóban közös osztó. Ha egy másik közös osztót választunk és lefelé haladunk az algoritmusban azt kapjuk, hogy ez a közös osztó *d*-nek is osztója, ezért *d* a közös osztók közül csak a legnagyobb lehet.

Pl. $(1972;1852) = ?$

$1972 : 1852 = 1$ $\quad$ $1852 : 120 = 15$ $\quad$ $120 : 52 = 2$ $\quad$ $52 : 16 = 3$ $\quad$ $16 : 4 = 4$

120 $\quad$ 52 $\quad$ 16 $\quad$ 4 $\quad$ 0

A fentiek alapján: $(1972;1852) = 4$

Felírás: *a*-val *r* maradékot adó számok általános alakja: $a \cdot k + r$

Oszthatóság illetve maradékok vizsgálatánál elég csak a maradékokkal elvégeznünk a műveleteket vagyis összeg, különbség, szorzat maradéka a maradékok összege, különbsége, szorzata.

Pl. vizsgáljuk a négyzetszámok 4-gyel vett maradékát!

Biz:Tetszőleges egész szám felírható $4k + r$ alakban, ahol *r=0,1,2,3* lehet. $(4k + r)^2 = 16k^2 + 8kr + r^2$ kifejezés 4-es maradéka csak $r^2$-ből származhat, s mivel $r^2 = 0,1,4,9$ ezért a négyzetszámok 4-gyel osztva 0 vagy 1 maradékot adnak.

Műveleti táblák: $(\text{mod}5)$

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | 3 |

| * | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 |
| **2** | 0 | 2 | 4 | 1 | 3 |
| **3** | 0 | 3 | 1 | 4 | 2 |
| **4** | 0 | 4 | 3 | 2 | 1 |

**Def1:** Az *a* és *b* egész számokat az $m \neq 0$ egész számra nézve kongruensnek nevezzük, ha *a* és *b* az *m*-mel való osztáskor azonos maradékot adnak. Jelölés: $a \equiv b \pmod{m}$

**Def2:** $a \equiv b \pmod{m}$ ha $m \mid b - a$, ahol $a,b,m \neq 0 \in Z$ A két definíció egymással ekvivalens.

A kongruencia tulajdonságai: $a,b,c,d,m \neq 0 \in Z$

1. $a \equiv a \pmod{m}$ reflexív
2. $a \equiv b \Rightarrow b \equiv a \pmod{m}$ szimmetrikus
3. $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c \pmod{m}$ tranzitív
4. $a \equiv b \Rightarrow a^k \equiv b^k \pmod{m}$, ahol $k \in N$ a kongruencia hatványozható
5. $a \equiv b \Rightarrow a \pm c \equiv b \pm c \pmod{m}$ kongruenciához hozzáadhatunk egész számot
6. $a \equiv b \Rightarrow a \cdot c \equiv b \cdot c \pmod{m}$ kongruenciát megszorozhatjuk egész számmal
7. $a \equiv b \wedge c \equiv d \Rightarrow a \pm c \equiv b \pm d \pmod{m}$ két kongruencia összeadható, kivonható
8. $a \equiv b \wedge c \equiv d \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$ két kongruencia összeszorozható
9. $a \cdot c \equiv b \cdot c \pmod{m} \Rightarrow a \equiv b \left( \text{mod} \frac{m}{(m;c)} \right)$ oszthatunk, de ekkor a modulus is változik!

**Kis Fermat-tétel:** Ha *p* prímszám és $(a;p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$

A tételből következően: $a^p \equiv a \pmod{p}$ minden *a*-ra.

**Euler-tétel:** Ha $(a;m) = 1$ akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$, ahol $\varphi(m)$ az *m*-nél kisebb, hozzá relatív prím pozitív számok darabszámát jelenti.

**Wilson-tétel:** Ha *p* prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$

**Számrendszerek:**

Az *a* alapú számrendszerben a *0,1,2,...a-1* számjegyeket használhatjuk, s a helyiértékek az *a* alapszám hatványai.

Pl. $1234_5 = 1 \cdot 5^3 + 2 \cdot 5^2 + 3 \cdot 5^1 + 4 \cdot 5^0 = 194_{10}$

Műveleti táblák 5-ös számrendszerben:

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 10 |
| **2** | 2 | 3 | 4 | 10 | 11 |
| **3** | 3 | 4 | 10 | 11 | 12 |
| **4** | 4 | 10 | 11 | 12 | 13 |

| * | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 |
| **2** | 0 | 2 | 4 | 11 | 13 |
| **3** | 0 | 3 | 11 | 14 | 22 |
| **4** | 0 | 4 | 13 | 22 | 31 |

Átváltás 10-ből 5-ös számrendszerbe: A számot, majd a hányadost 5-tel osztjuk maradékosan addig, amíg a hányados 0 nem lesz. Ezután a maradékokat fordított sorrendben leírjuk.

| | |
|---|---|
| Pl. 346 | 1 |
| 69 | 4 |
| 13 | 3 |
| 2 | 2 |
| 0 | |

$346_{10} = 2341_5$

Átváltás 5-ös számrendszerből tízesbe: Az első helyiértéket, illetve a továbbiakban az eredményt 5-tel szorozzuk, majd hozzáadjuk a következő helyiértéket. Ezt ismételjük az összes számjegyre.

Pl. $1234_5 = ((1 \cdot 5 + 2) \cdot 5 + 3) \cdot 5 + 4 = 194_{10}$