# Kongruenciák

A kongruenciák megértése és használata nem kis próbatétel elé állítja azt, aki a velük kapcsolatos ismeretek birtokba vételére adja a fejét. Valójában azonban inkább az a meglep, hogy mért is van ez így? Életünk ugyanis telis-tele van ciklikus strukturákkal. Gondoljunk csak a napok változására, ahol hét naponként újra kezdjük a hetet, a hónapok változására, ahol 12-enként indul újra számolás, vagy évszakok változására, melyeket ugyan nem számozunk meg, de az aktuális évszaktól számított ötödik évszakot ugyanúgy nevezzük, mint amelyikrl kezdtük a számolást.

## A kongruencia bevezetése

### 15.1.1. Definíció

Legyen $1 < m$ természetes szám. Azt mondjuk, hogy az $a$ és $b$ egész számok **kongruensek modulo *m***, ha $m \mid a - b$. Azt a tényt, hogy $a$ kongruens $b$ modulo $m$ az

$$a \equiv b \ \mathbf{mod}\ m\,,$$

vagy alternatív módon az

$$a \equiv_m b$$

jelsorozattal jelöljük.

Az els jelölést Gauss vezette be, akit a matematikusok fejedelmének szokás nevezni. Mi magyarok kissé neheztelünk rá, mert bár nem kétséges, hogy felismerte Bolyai János munkásságának jelentségét, mégsem karolta fel. Elintézte az ügyet egy "magam is foglalkoztam hasonló gondolatokkal" megjegyzéssel. Hátránya a Gauss féle jelölésnek, hogy szétválasztja a kongruencia jelét a modulus értékétl. Ezen a jelenségen segít ugyan a második jelölés, ami viszont akkor válik nehezen olvashatóvá, ha a modulus valamilyen összetett kifejés. Például az. $a \equiv_{m_1 \cdot m_2 \cdot \ldots \cdot m_k} b$ lényegesen nehezebben olvasható, mint a jobban áttekinthet $a \equiv b \ \mathbf{mod}\ (m_1 \cdot m_2 \cdot \ldots \cdot m_k)$ kifejezés. Ezért a két jelölést egyenrangúnak tekintjük és felváltva használjuk.

**Példák**

1. $5 \equiv 20 \ \mathbf{mod}\ 3$, mert $20 - 5 = 15$ osztható 3-mal. A másik jelöléssel $5 \equiv_3 20$.

2. $-8 \equiv 16 \ \mathbf{mod}\ 4$, mert $16 - (-8) = 24$ osztható néggyel. Ezt így is írhatjuk $-8 \equiv_4 16$.

Vegyük észre, hogy a kongruencia teljesülésének ellenrzésekor mindegy, hogy $a$-ból vonjuk ki $b$-t, vagy fordítva. Ugyanis $a - b$ akkor és csak akkor osztható $m$-mel, ha $b - a$ is. Tehát $-8 \equiv 16 \ \mathbf{mod}\ 4$ ellenrzésekor eljárhattunk volna úgy is, hogy $-8 - 16 = -24$ 4-gyel való oszthatóságát ellenrizzük.

3. $3 \not\equiv 10 \ \mathbf{mod}\ 5$, mert $10 - 3 = 7$ nem osztható 5-tel. A kongruencia nem teljesülését a $3 \not\equiv_5 10$ jelsorozattal is jelölhetjük.

Kezdjük a kongruenciák vizsgálatát annak a tételnek az igazolásával, ami rámutat az egymással kongruens számok közös tulajdonságára.

### 15.1.2. Tétel

Az $a$ és $b$ egészek akkor és csak akkor kongruensek modulo $m$, ha $m$-mel osztva mindkett ugyanazt a maradékot adja,. Más szóval

$$a \equiv_m b \text{ akkor és csak akkor, ha } a \textbf{ mod } m = b \textbf{ mod } m.$$

## Bizonyítás

Tekintsük a $a$ és $b$ egész számokat. Ha $a \equiv_m b$, akkor a kongruencia definíciójának megfelelen $m \mid (b-a)$ vagyis alkalmas $q$ egészre $b-a = m \cdot q$, amibl $b = a + m \cdot q$. Osszuk el maradékosan $a$-t $m$-mel! Legyen $a = m \cdot p + r \ (0 \le r < m)$. Ezt az elz egyenlségbe helyettesítve kapjuk, hogy

$$b = m \cdot p + r + m \cdot q = m \cdot (p + q) + r,$$

ami az $0 \le r < m$ egyenlségeket is figyelembe véve azt mutatja, hogy $b$ is $r$ maradékot ad $m$-mel osztva.

Fordítva tegyük fel, hogy $a$ és $b$ mindegyike $m$-mel osztva $r$ maradékot ad, vagyis $a = m \cdot q_1 + r$ és $b = m \cdot q_2 + r$. Képezve a két egyenlség különbségét kapjuk, hogy $b-a = m \cdot q$. Tehát $m$ osztója és különbségének, ez pedig a kongruencia definíciója szerint pontosan azt jelenti, hogy $a \equiv_m b$.

## Példák

1. $5 \equiv_3 20$, ugyanakkor $5 \textbf{ mod } 3 = 20 \textbf{ mod } 3 = 2$.

2. $-8 \equiv_4 16$, ugyanakkor $-8 \textbf{ mod } 4 = 16 \textbf{ mod } 4 = 0$.

Kicsit zavarbaejt a kongruencia Gauss féle jelölése, valamint az osztási maradék megjelölése, ugyanis mindkett a **mod** jelsorozatot használja. A

$$22 \equiv 43 \textbf{ mod } 7$$

egy kapcsolatot, idegen szóval relációt fejez ki a 22 és a 43 számok között. Ez a kapcsolat azt mondja, hogy 7 osztja a 43-22 különbséget. Ezzel szemben a

$$22 \textbf{ mod } 7 = 43 \textbf{ mod } 7$$

egyenlség mindkét oldalán egy-egy mvelet eredménye látható. A bal oldali mvelet eredménye a 22-nek 7-tel való osztásának maradéka, míg a jobb oldalon ugyanezt a mveletet a 43 és 7 számokon végeztük el.

Ha a 11.2 tételt $m$-nél kisebb nemnegatív $a$ és $b$ számokra alkalmazzuk, akkor azt kapjuk, hogy

$$a \equiv_m b \text{ akkor és csak akkor, ha } a = b,$$

ugyanis ha $0 \le a, b < m$, akkor $a \textbf{ mod } m = a$ és $b \textbf{ mod } m = b$. Ez pedig szemléletesen azt fejezi ki, hogy a $\{0, 1, ..., m-1\}$ halmazon a modulo $m$ kongruencia nem különbözik az egyenlségtl, vagyis

a $0, 1, ..., m-1$ számok páronként inkongruensek egymással modulo $m$.

Kezdjünk el most egy számlálást modulo 7. Nullától indulva egy darabig inkongruens értékeket kapunk, hiszen mint láttuk, a 0, 1, 2, 3, 4, 5, 6 számok páronként inkongruensek. Ám tovább folytatva a számlálást azt látjuk, hogy

$$7 \equiv_7 0 \text{ , mert } 7 - 0 = 7 \text{ osztható 7-tel,}$$

$$8 \equiv_7 1 \text{ , mert } 8 - 1 = 7 \text{ osztható 7-tel,}$$

és így tovább

$$13 \equiv_7 6 \text{ , mert } 13 - 6 = 7 \text{ osztható 7-tel.}$$

Válasszunk most találomra nagyobb értékeket. Pl. $86 \equiv_7 2$ , mert $86 - 2 = 84$ osztható 7-tel. Ugyanígy $-118 \equiv_7 1$, mert $-118 - 1 = -119$ osztható 7-tel. Úgy tnik, hogy a modulo 7 számlálás során mindösszesen 7 "különböz", egészen pontosan 7 inkongruens értéket kapunk. Ezt támasztja alá a következ tétel.

## 15.1.3. Tétel

Bármely *n* egész számra

$$n \equiv_m n \textbf{ mod } m \text{ ,}$$

vagyis minden *n* egész kongruens az *m*-mel való osztási maradékával modulo *m.*

### Bizonyítás

Csak annyit észrevennünk, hogy $(n \textbf{ mod } m) < m$ miatt

$$(n \textbf{ mod } m) \textbf{ mod } m = n \textbf{ mod } m \text{ .}$$

Így *n* és *n* **mod** *m* az *m*-mel osztva ugyanazt a maradékot adja és ekkor a 11.2 tétel szerint kongruensek egymással.

A 0, 1,..., $m-1$ számok tehát páronként inkongruensek modulo *m.* Ugyanakkor azt is láttuk, hogy bármely egész szám ezek közül valamelyikkel kongruens. Soroljuk osztályokba az egész számokat aszerint, hogy a 0, 1,..., $m-1$ értékek közül melyikkel kongruensek modulo *m.*

| | | |
|---|---|---|
| 0-*val* **mod** *m* kongruens egészek | **0**, $0 \pm m$, $0 \pm 2 \cdot m$, $0 \pm 3 \cdot m$,... | $0 + k \cdot m$ |
| 1-*gyel* **mod** *m* kongruens egészek | **1**, $1 \pm m$, $1 \pm 2 \cdot m$, $1 \pm 3 \cdot m$,... | $1 + k \cdot m$ |
| 2-*vel* **mod** *m* kongruens egészek | **2**, $2 \pm m$, $2 \pm 2 \cdot m$, $2 \pm 3 \cdot m$,... | $2 + k \cdot m$ |
| | ... | |
| $(m-1)$-*gyel* **mod** *m* kongruens egészek | $\boldsymbol{m-1}$, $(m-1) \pm m$, $(m-1) \pm 2 \cdot m$, $(m-1) \pm 3 \cdot m$ , ... | $(m-1) + k \cdot m$ |

A táblázat soraiban szerepl számok összességét **modulo *m* maradékosztályoknak** nevezzük. Mint jól látható, azonos maradékosztályba tartozó számok egymástól *m* többszöröseiben különböznek. A maradékosztály elnevezést az indokolja, hogy a maradékosztályba es számok *m*-mel osztva ugyanazt a maradékot adját. Az ilyen tulajdonságú számok mindegyike elfordul az adott maradékosztályban. Mivel az összes egész szám a 0, 1, 2,..., $m-1$ számok valamelyikével kongruens modulo *m* ezért

a 0, 1, 2,..., $m-1$ számok összességét **teljes maradékrendszernek** nevezzük.

Algebrai szempontból nézve a kongruencia kapcsolatot, u.n. relációt létesít két egész szám között. Ennek a relációnak a tulajdonságai ersen emlékeztetnek a jól megszokott egyenlségi reláció tulajdonságaihoz.

## 15.1.4. Tétel

Minden *a*, *b* és *c* egész számra és $1 < m$ modulusra igazak a következ állítások.

1. $a \equiv_m b$ és $a \not\equiv_m b$ közül pontosan az egyik teljesül.

2. $a \equiv_m a$ . A kongruencia reláció **reflexív** .

3. Ha $a \equiv_m b$ , akkor $b \equiv_m a$ . A kongruencia reláció **szimmetrikus**.

4. Ha $a \equiv_m b$ és $b \equiv_m c$ , akkor $a \equiv_m c$ . A kongruencia reláció **tranzitív**.

### Bizonyítás

Az 1. állítás abból következik, hogy tetszleges *a* és *b* egészre $a - b$ vagy osztható *m*-mel vagy nem. A 2. állítás azért igaz, mert $a - a = 0$, ennek pedig minden *m* osztója. A 3. állítással kapcsolatban már tettünk korábban megjegyzést, miszerint $a - b$ akkor és csak akkor osztható *m*-mel, ha $b - a$ is.

Végül ha $a \equiv_m b$ és $b \equiv_m c$ egyidejleg teljesül, akkor $m \mid a-b$ és $m \mid b-c$. Ekkor viszont *m* osztója a két szám összegének is, tehát $m \mid (a-b) + (b-c) = a-c$. Ez pedig pontosan azt fejezi ki, hogy $a \equiv_m c$ .

Térjünk vissza egy gondolat erejéig induló példánkhoz, a hét napjaihoz! Gyakran elfordul, hogy meg kell határoznunk, hogy néhány nap elteltével melyik napja lesz a hétnek. Ezt bizony leginkább az ujjainkon szoktuk eladni, ami kicsit nehézkes, ha mondjuk arra vagyunk kivácsiak, hogy "ha ma szerda van, akkor 40 nap elteltével milyen nap lesz?". Számozzuk meg gondolatban a hét napjait. Legyen vasárnap sorszáma 0, hétf sorszáma 1, és így tovább 6-ig, ami a szombatra fog jutni. Feltételünk szerint ma szerda van, az a hét 3-dik napja. Negyven nap elteltével a hét 43 napján lennénk, ha folyamatosan sorszámoznánk a napokat. Ám mi modulo 7 sorszámozzuk azokat. Így annak megállapításához, hogy 40 nap elteltével milyen nap lesz, csak annyit kell tenni, hogy megnézzük, hogy 43 mivel kongruens modulo 7. Mivel $43 \equiv_7 1$, így azt mondhatjuk, hogy 40 nap elteltével hétf lesz.

"A halál 50 órája" c. filmben a német vezérkar egy olyan órát csináltatott a fhadiszállás vezérl termébe, ami 50 óra alatt fordul egyszer körbe, és mint ilyen, körülfordulásának aránya a hadmvelet abszolut arányait mutatta. A német tábornokokat bizonyára nem izgatta a most általunk feltett kérdés: ha a hadmvelet éjfélkor, vagyis 0 órakor indul, akkor hány órakor ér véget?. A válasz a kongruenciák ismeretében egyszer: éjjel kettkor, mert $0 + 50 = 50 \equiv_{24} 2$.

## Mveletek kongruenciákon

Korábbi tanulmányaink során éppen eleget gyakoroltuk a mérlegelvet. Az egyenlet mindkét oldalát növelhetjük és csökkenthejük ugyanazzal a számmal, anélkül, hogy elrontanánk az egyenlséget. Ugyanígy az egyenlet mindkét oldala tetszleges számmal szorozható és nullától különböz számmal osztható. Ezek a tulajdonságok nagy része a konguenciákkal való számolás során is megmarad.

### 15.2.1. Tétel

Ha $a_1 \equiv_m b_1$ és $a_2 \equiv_m b_2$, akkor

$$a_1 + a_2 \equiv_m b_1 + b_2,$$

és

$$a_1 - a_2 \equiv_m b_1 - b_2 .$$

#### Bizonyítás

A tétel feltételei azt jelentik, hogy $m \mid a_1 - b_1$ és $m \mid a_2 - b_2$. Ekkor $m$ osztható az $a_1 - b_1$ és az $a_2 - b_2$ összegével és különbségével is. Tehát

$$m \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2),$$

ez pedig definíció szerint azt jelenti, hogy $a_1 + a_2 \equiv_m b_1 + b_2$.

Ugyanígy

$$m \mid (a_1 - b_1) - (a_2 - b_2) = (a_1 - a_2) - (b_1 - b_2),$$

vagyis $a_1 - a_2 \equiv_m b_1 - b_2$.

Lássunk illusztrációként néhány példát.

| Mvelet | Ellenrzés |
|---|---|
| $2 \equiv_7 16$ | $2 - 16 = -14$ osztható 7-tel |
| $25 \equiv_7 4$ | $25 - 4 = 21$osztható 7-tel |
| $27 = 2 + 25 \equiv_7 16 + 4 = 20$ | $27 - 20 = 7$ osztható 7-tel |

Tételünk következménye, hogy a kongruencia minkét oldalához ugyanazt a számot hozzáadhatjuk, illetve mindkét oldalból levonhatjuk. Ezt azért tehetjük meg, mert bármely egész önmagával kongruens. Így például a $2 \equiv_7 16$ kongruenciából
$10 = 2 + 8 \equiv_7 16 + 8 = 24$ következik. Ugyanakkor egy kongruenciát önmagához is hozzáadhatunk, amivel azt érjük el, hogy a kongrencia mindkét oldalát 2-vel megszorozzuk. Ismét

csak a $2 \equiv_7 16$ kongruenciát használva

$$4 = 2 + 2 \equiv_7 16 + 16 = 32 .$$

Ehhez a kongruenciához ismét hozzáadhatjuk a kiindulásit, megkapva ezzel annak háromszorosát.

$$6 = 2 + 2 + 2 \equiv_7 16 + 16 + 16 = 48.$$

Ezt a gondolatmenetet követve azt kapjuk, hogy a kongruancia mindkét oldala ugyanazzal a számmal szorozható.

## 15.2.2. Tétel

Ha $a \equiv_m b$ , akkor minden $n$ egészre

$$a \cdot n \equiv_m b \cdot n .$$

Bizonyítás

A természetes számokra $n$ szerinti teljes indukcióval bizonyítunk. Állításunk $n = 1$-re nem más, mint a tétel feltétele. Ha pedig az állítás $n$-re már teljesül, vagyis ha $a \cdot n \equiv_m b \cdot n,$ akkor ehhez az $a \equiv_m b$ kongruenciát hozzáadva kapjuk, hogy $a \cdot (n + 1) = a \cdot n + a \equiv_m b \cdot n + b = b \cdot (n + 1)$ .

A tétel állítása $n = 0$-ra nyilvánvaló. Ha pedig $n < 0$, akkor az eddigiek alapján mondhatjuk, hogy $a \equiv_m b$ -bl $a \cdot (-n) \equiv_m b \cdot (-n)$ következik. Ez pedig azt jelenti, hogy $m \mid a \cdot (-n) - b \cdot (-n) = b \cdot n - a \cdot n$, ami definíció szerint azt fejezi ki, hogy $a \cdot n \equiv_m b \cdot n$.

Ennél az észrevételnél azonban általánosabb állítást ad a következ tétel, mely szerint azonos modulusu kongruenciák megfelel oldalai összeszorozhatók.

## 15.2.3.Tétel

Ha $a_1 \equiv_m b_1$ és $a_2 \equiv_m b_2$, akkor

$$a_1 \cdot a_2 \equiv_m b_1 \cdot b_2 .$$

### Bizonyítás

Az $a_1 \equiv_m b_1$ kongruencia mindkét oldala beszorozható $a_2$-vel:

$$a_1 \cdot a_2 \equiv_m b_1 \cdot a_2 .$$

Most az $a_2 \equiv_m b_2$ kongruenciát szorozzuk be $b_1$-gyel:

$$b_1 \cdot a_2 \equiv_m b_1 \cdot b_2 .$$

A kapott két kongruenciából a tranzitív tulajdonság miatt

$$a_1 \cdot a_2 \equiv_m b_1 \cdot b_2$$

következik.

Példaként szorozzuk össze a korábban használt két kongruenciát.

| Mvelet | Ellenrzés |
|---|---|
| $2 \equiv_7 16$ | $2-16=-14$ osztható 7 -tel |
| $25 \equiv_7 4$ | $25-4=21$ osztható 7-tel |
| $50=2\cdot 25 \equiv_7 16\cdot 4 = 64$ | $50-64=-14$ osztható 7-tel |

Ha ugyanannak kongruenciának a megfelel oldalait szorozzuk össze, akkor a kongruencia oldalainak négyzetéhez jutunk, és így azt mondhatjuk, hogy kongruencia oldalai négyzetre emelhetk anélkül, hogy elrontanánk magát a kongruenciát. Lássuk a $2 \equiv_7 16$ esetét. A négyzetre emelés után

$$4=2^2 \equiv_7 16^2=256.$$

Ezt az eredeti kongruenciával szorozva megkapjuk annak köbét.

$$8=4\cdot 2=2^3 \equiv_7 16^3=256\cdot 16=4096.$$

Ezt a gondolatmenetet folytatva megállapíthatjuk, hogy kongruencia mindkét oldala ugyarra a természetes szám kitevj hatványra emelhet.

## 15.2.4. Tétel

Ha $a \equiv_m b$, akkor minden $n$ természetes számra

$$a^n \equiv_m b^n.$$

### Bizonyítás

$n$ szerinti teljes indukcióval. Az állítás $n = 1$-re nem más, mint maga a tétel feltétele. Ha pedig feltesszük, hogy $n$-re teljesül, vagyis ha $a^n \equiv_m b^n$ már igaz, akkor ezt a kongruenciát az $a \equiv_m b$ kongruenciával összeszorozva kapjuk, hogy $a^{n+1} \equiv_m b^{n+1}$.

## Számolás modulo m

Vegyük el még egyszer az azonos modulusú kongruenciák összeadhatóságáról szóló tételünket. Ez azt állítja, hogy ha

$$a_1 \equiv_m b_1$$

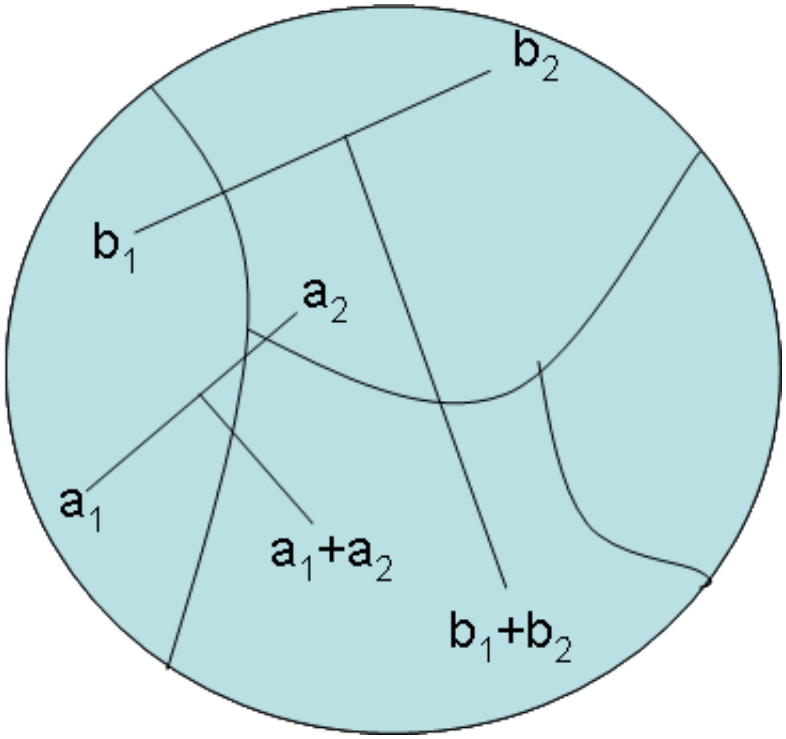
és

$$a_2 \equiv_m b_2,$$

akkor

$$a_1 + a_2 \equiv_m b_1 + b_2.$$

Mit is jelent az, hogy $a_1 \equiv_m b_1$? Azt, hogy az $a_1$ és $b_1$ egészek ugyanabba a modulo $m$ maradékosztályba tartoznak. Ehhez hasonlóan $a_2 \equiv_m b_2$ teljesülése $a_2$-t és $b_2$-t sorolja egyazon modulo $m$ maradékosztályba. Eszerint a tétel állítása úgy is megfogalmazható, hogy ha $a_1$ és $b_1$ ugyanabba a modulo $m$ maradékosztályba esik, valamint $a_2$ és az $b_2$ is egyazon maradékosztályból való, akkor az $a_1 + a_2$ összeg is azonos modulo $m$ maradékosztályba esik $b_1 + b_2$-vel.




És most tegyük fel, hogy feladatunk az $a_1 + a_2$ összeg kiszámítása, ám az eredményre csak modulo $m$ vagyunk kíváncsiak, másszóval az érdekel bennünket, hogy az $a_1 + a_2$ összeg melyik modulo $m$ maradékosztályba esik. A legegyszerbb, amit tehetünk, hogy egyszeren összeadjuk a két egész számot, az összegük kijelöli a megfelel maradékosztályt. Ám az ábra szemléletesen mutatja, hogy úgy is eljárhatunk, hogy $a_1$ helyett választunk egy vele kongruens, vagyis azonos maradékosztályba es $b_1$ számot, és $a_2$ maradékosztályából is választunk egy másik $b_2$ számot. Tételünk szerint az így kiválasztott két másik szám összege, vagyis $b_1 + b_2$ kongruens lesz

$a_1 + a_2$-vel, tehát ugyanazt a mellékosztályt határozza meg.

Jogosan vetdik fel a kérdés, hogy mért van erre a mutatványra szükség? És ha már csináljuk, akkor hogyan válasszuk ki az összeadandó számok helyett a $b_1$ és $b_2$ számokat? Nos elég kézenfekv megoldásnak tnik $b_1$-et és $b_2$-t, a 0, 1, 2, ..., $m-1$ teljes maradékrendszerbl választani. Ekkor ugyanis a lehet legkisebb nemnegatív számokhoz jutunk, melyek nem mások, mint a kiindulási egészek *m*-mel vett osztási maradékai. Választásunk tehát legyen

$$b_1 = a_1 \textbf{ mod } \mathrm{m} \quad \text{és} \quad b_2 = a_2 \textbf{ mod } m.$$

Ekkor az $a_1 + a_2 \equiv_m b_1 + b_2$ kongruencia az

$$a_1 + a_2 \equiv_m (a_1 \textbf{ mod } m) + (a_2 \textbf{ mod } m)$$

alakot ölti, melyben nem rontjuk el a kongruenciát akkor, ha a bal oldali összeget a vele kongruens $(a_1 + a_2)$ **mod** *m* értékkel helyettesítjük:

$$(a_1 + a_2) \textbf{ mod } m \equiv_m (a_1 \textbf{ mod } m) + (a_2 \textbf{ mod } m).$$

Nagyon fontos egyenlséghez jutottunk, mely azt fejezi ki, hogy az összeadás mvelete modulo *m* erejéig felcserélhet a **mod** *m* maradékképzés mveletével. Még szebb lenne, ha a két kifejezés közé egyenlség jelet írhatnánk. Ez azonban nem lehetséges, mert $(a_1 + a_2)$ **mod** *m* kisebb *m*-nél, ami viszont a jobboldali összegre nem feltételenül teljesül. Ugyanis két *m*-nél kisebb egész összege lehet *m*-nél nagyobb. Megkapjuk azonban az egyenlséget, ha a jobb oldali kifejezésre is alkalmazzuk a **mod** *m* maradékképzés mveletét

$$(a_1 + a_2) \textbf{ mod } m = (a_1 \textbf{ mod } m + a_2 \textbf{ mod } m) \textbf{ mod } m.$$

Példaként számítsuk ki a $4205 + 8137$ összeget modulo 7. Természetesen eljárhatunk úgy, hogy elbb az öszeadást végezük el, és utána vesszük az összeg 7-el való osztási maradékát, ahogy ez az alábbi táblázat baloldali cellájában látható. Ám elbbi észrevételünk szerint a mveletek sorrendjét felcserélhetjük. Elször vesszük a az összeadandók 7-tel való osztási maradékait, és a maradékokat adjuk össze.

| | |
|---|---|
| $4205 + 8137 = 12342$<br>$12341$ **mod** $7 = 1$ | $4205$ **mod** $7 = 5$<br>$8136$ **mod** $7 = 3$<br>$5 + 3 = 8$<br>$8$ **mod** $7 = 1$ |
| $(4205 + 8137)$ **mod** $7 \equiv_7 (4205$ **mod** $7) + (8136$ **mod** $7)$<br><br>vagy<br>$(4205 + 8137)$ **mod** $7 = ((4205$ **mod** $7)$<br>$+ (8136$ **mod** $7))$ **mod** $7$ | |

Figyeljük meg, hogy jobboldali számolás során két 7-nél kisebb szám összegét kellett képeznünk, és az összeg modulo 7 meghatározása is könnyedén ment, hiszen mindössze a modulus értékét kellett kivonni a kapott eredménybl.

Még jobban mutatja a modulo *m* aritmetika használatának elnyeit a szorzás mvelete. A szorzás

is felcserélhet az *m*-el való osztási maradékok kiszámításával, hiszen $a_1 \equiv_m b_1$ és $a_2 \equiv_m b_2$ maga után vonja az $a_1 \cdot a_2 \equiv_m b_1 \cdot b_2$ kongruencia teljesülését is. Tehát az összeadáshoz hasonlóan

$$(a_1 \cdot a_2) \bmod m = \left( (a_1 \bmod m) \cdot (a_2 \bmod m) \right) \bmod m .$$

Szorozzuk most össze elbbi két számunkat, vagyis számítsuk ki a $4205 \cdot 8137$ szorzatot. A táblázat bal oldali cellájában a számítást a szorzással kezdjük, majd vesszük az eredményt modulo 7. A jobboldali cellában elször vettük a szorzó-t és a szorzandót modulo 7 és ezeket az értékeket szoroztuk össze.

| | |
|---|---|
| $4205 \cdot 8137 = 34216085$<br>$34216085 \bmod 7 = 1$ | $4205 \bmod 7 = 5$<br>$8136 \bmod 7 = 3$<br>$5 \cdot 3 \equiv_7 15$<br>$15 \bmod 7 = 1$ |
| $(4205 \cdot 8137) \bmod 7 \equiv_7 (4205 \bmod 7) \cdot (8136 \bmod 7)$<br><br>vagy<br>$(4205 \cdot 8137) \bmod 7 = ((4205 \bmod 7) \cdot (8136 \bmod 7)) \bmod 7$ | |

Ez utóbbi számítás már markánsabban mutat rá módszerünk jelentségére. Ugyanis itt két négyjegy szám helyett az 5-öt kellett 3-mal szorozni, ami lényegesen egyszerbb feladat. És mivel a modulo 7 maradékok mindíg a 0, 1, 2, ..., 6 számok közül kerülnek ki, ez a kellemes tulajdonság megmarad, akármilyen nagy számokkal való mveletek elvégzése esetén is.

Végül megjegyezzük, hogy több mvelet egymás utáni elvégzése esetén a most felfedett felcserélhetségi tulajdonságokat többször egymás után alkalmazhatjuk. Érvényes tehát az alábbi

## 15.3.1. Számolási szabály

Egész számokon végzett tetszleges összeadás, kivonást és szorzást tartalmazó kifejezés modulo *m* kiszámítható oly módon, hogy a kifejezésben szerepl számokat és a számítás során keletkez bármely részeredményt modulo *m* veszünk, vagyis helyettesítjük az *m*-mel való osztási maradékával.

### Példák

1. $(39 \cdot 22) \bmod 9 \equiv_9 (39 \bmod 9) \cdot (22 \bmod 9) = 3 \cdot 4 = 12 \equiv_9 3$ .

2.
$(19 \cdot (22 + 43)) \bmod 3 \equiv_3 (19 \bmod 3) \cdot ((22 + 43) \bmod 9) \equiv_3 1 \cdot ((22 \bmod 3) + (43 \bmod 3))$
$= 1 + 1 = 2$
.

3.

$$57^3 \bmod 6 = (57\cdot 57)\cdot 57 \bmod 6 \equiv_6 (57\cdot 57 \bmod 6)\cdot(57 \bmod 6) \equiv_6 (57 \bmod 6)\cdot(57 \bmod 6)\cdot(57 \bmod 6) = (57 \bmod 6)^3 = 3^3 = 27 \equiv_6 3$$

4.

$$(10^5 + 24\cdot 51^3 + 42\cdot 10 + 7) \bmod 8 \equiv_8 (10^5 \bmod 8) + (24\cdot 51^3 \bmod 8) + (42\cdot 10 \bmod 8) + (7 \bmod 8) \equiv_8$$

$$\equiv_8 (10 \bmod 8)^5 + (24 \bmod 8)\cdot(51 \bmod 8)^3 + (42 \bmod 8)\cdot(10 \bmod 8) + 7 \equiv_8$$

$$\equiv_8 2^5 + 0\cdot 3^3 + 2\cdot 2 + 7 = 32 + 4 + 7 = 43 \equiv_8 3\,.$$

Persze, ha már van kell gyakorlatunk a modulo *m* számolásban, akkor nem írunk ennyit, hanem különösebb magyarázkodás nélkül alkalmazzuk számolási szabályunkat

$$(10^5 + 24\cdot 51^3 + 42\cdot 10 + 7) \bmod 8 \equiv_8 2^5 + 0\cdot 3^3 + 8\cdot 2 + 7 = 43 \equiv_8 3.$$

Ejtsünk a végén néhány szót a hatványozásról. Nem nehéz belátni, hogy pozitív egész kitevs hatványokra

$$n^k \bmod m \equiv_m (n \bmod m)^k.$$

A bizonyítás *k* szerinti teljes indukcióval végezhet el. Ebben a kongruenciában a hatvány alapját helyettesítettük *m*-mel való osztási maradékával. Vajon megtehet-e ez a kitevre is? Sajnos nem, ugyanis a

$$k_1 \equiv_m k_2 \text{ kongruenciából NEM következik az } n^{k_1} \equiv_m n^{k_2} \text{ kongruencia.}$$

Legyen például $k_1 = 1$ és $k_2 = 4$. Ekkor

$$k_1 = 1 \equiv_3 4 = k_2,$$

ugyanakkor $n = 2$ esetén

$$n^{k_1} = 2^1 = 2 \not\equiv_3 16 = 2^4 = n^{k_2}.$$

Mindezt lefordítva a gyakorlat nyelvére a következt mondhatjuk. Olyan kifejezések kiszámítása során, melyben hatványok is szerepelnek, a hatvány alapja helyettesíthet, a kitev azonban nem helyettesíthet *m*-mel való osztási maradékával.

## Gyorshatványozás modulo m

Az eddig elmondottak alkalmazásaként határozzuk meg, hogy $23^{19}$ milyen maradékot ad 7-tel osztva. A feladat elvégezhet, hiszen mind a hatványozásra, mind a maradékos osztásra van algoritmusunk. Elrettentésül felírjuk a $23^{19}$ gyors hatványozással való kiszámítását, és a végén egy lépésben vesszük a 17-tel való osztási maradékot.

| $k = 19$ | $n = 23$ | $n^k$ |
|---|---|---|
| 19 | * | 7461547092759071056190\<br>8487 |

| | | |
|---|---|---|
| 18 | ^ | 3244150909895248285300\<br>369 |
| 9 | * | 1801152661463 |
| 8 | ^ | 78310985281 |
| 4 | ^ | 279841 |
| 2 | ^ | 529 |
| 1 | | 23 |
| 746154709275907105619084 87 **mod** 17 = 12 | | |

Vegyük azonban észre, hogy számolási szabályunk szerint a számítás során minden lépést elvégezhetünk modulo 17 az alábbi módon.

| $k = 19$ | $n = 23$ | $n^k$ **mod** 17 | Magyarázat |
|---|---|---|---|
| 19 | * | 12 | $2 \cdot 23$ **mod** $17 = 46$ **mod** $17 = 12$ |
| 18 | ^ | 2 | $11^2$ **mod** $17 = 121$ **mod** $17 = 2$ |
| 9 | * | 11 | $16 \cdot 23$ **mod** $17 = 368$ **mod** $17 = 11$ |
| 8 | ^ | 16 | $4^2$ **mod** $17 = 16$ **mod** $17 = 16$ |
| 4 | ^ | 4 | $2^2$ **mod** $17 = 4$ **mod** $17 = 4$ |
| 2 | ^ | 2 | $6^2$ **mod** $17 = 36$ **mod** $17 = 2$ |
| 1 | | 6 | $6 = 23$ **mod** 17 |

A táblázat második oszlopát alulról felfelé töltöttük ki, de minden lépésnél modulo 17 számoltunk. A legalsó cellába 23 helyett $6 = 23$ **mod** 17 -et írtunk. A felette lév cella úgy keletkezett, hogy 6-ot négyzetre emeltük, a gyors hatványozás algoritmusának megfelelen majd vettük a $2 = 36$ **mod** 17 értéket. Így jutottunk a $6^2 \equiv_{17} 2$ kongruenciához. Ahol a gyorshatványozás algoritmusa 23-mal való szorzást követel, ott értelemszeren az alatta lév kongruencia mindkét oldalát 6-tal szoroztuk, majd vettük az eredményt modulo 17.

## 15.4.1. Algoritmus: Gyorshatványozás mod m

| Szöveges leírás | Maple metakód |
|---|---|

1. *Input*: $n$, $k$ és $m$ természetes számok, $n$ az alap, $k$ a kitev, $m$ a modulus
2. Legyen $s$ az üres sorozat ($s$ kezdetben üres)
3. Amíg $1 < m$ hajtsuk végre az alábbi utasításokat
   Ha $m$ páros Akkor
      Legyen $m := \frac{m}{2}$ és $s := s, 0$ ( Ha $m$ páros, akkor $s$-hez hozzáfzzük a 0-t)
   Különben
      Legyen $m := m - 1$ és $s := s, 1$ ( Ha $m$ páratlan, akkor $s$-hez hozzáfzzük az 1-t)
4. Legyen *hatvány* := $n$ **mod** $m$ (A *hatvány* változó kezdértéke $n$ **mod** $m$)
5. Az $x$ haladjon végi az s utolsó elemétl az elsig, és hajtsuk végre az alábbi utasításokat
   Ha $x$=0 Akkor
      Legyen *hatvány* := *hatvány*$^2$ **mod** $m$ (Az elz hatványt négyzetre emeljük)
   Különben
      Legyen *hatvány* := *hatvány*$\cdot n$ **mod** $m$ (Az elz hatványt szorozzuk $n$ **mod** $m$-mel)
6. *Output*: *hatvány* az $n$ szám $k$-adik hatványa modulo $m$.

```
Input : n és m természetes számok,
        n az alap, m a kitevő
s := NULL
while 1 < n do
  if irem(m, 2) = 0 then
    m := iquo(m, 2) : s := s, 0
  else
    m := m-1 : s := s, 1
  fi
od:
hatvány := n mod m :
for i from nops(s) to 1 by -1 do
  if s[i] = 0 then
    hatvány := hatvány^2 mod m
  else
    hatvány := hatvány·n mod m
  fi
od:
Output : hatvány az n szám k
       -adik hatványa modulo m.
```

## 15.4.2. Maple implementáció

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!" **(1.4.2.1)**

A **gyorshatványmodm** eljárás lépései megegyeznek a **gyorshatványozás** algoritmusának lépéseivel, ám most minden egyes mveletet (négyzetre emelést, illetve szorzást) modul $m$ végzünk el. Ennek megfelelen az eljárás paraméterei kiegészülnek egy harmadik paraméterrel, ami a modulust adja meg.

```
> gyorshatványmodm(23,19,17);
```

12 **(1.4.2.2)**

```
> gyorshatványmodm(23,19,17,ini,cal);
Inicializálás(gyorshatványmodm):
```

$$\begin{bmatrix} k & Művelet & 23^k \\ 19 & & \end{bmatrix}$$

```
Részletek megjelenítése(gyorshatványmodm):
```

$$\begin{bmatrix} k & \textit{Művelet} & 23^k \\ 19 & 23\,x \bmod 17 & \\ 18 & x^2 \bmod 17 & \\ 9 & 23\,x \bmod 17 & \\ 8 & x^2 \bmod 17 & \\ 4 & x^2 \bmod 17 & \\ 2 & x^2 \bmod 17 & \\ 1 & & 6 \end{bmatrix}, \begin{bmatrix} k & \textit{Művelet} & 23^k \\ 19 & 23\,x \bmod 17 & 12 \\ 18 & x^2 \bmod 17 & 2 \\ 9 & 23\,x \bmod 17 & 11 \\ 8 & x^2 \bmod 17 & 16 \\ 4 & x^2 \bmod 17 & 4 \\ 2 & x^2 \bmod 17 & 2 \\ 1 & & 6 \end{bmatrix}$$

```
Eredmény(gyorshatványmodm):
```

$$12 \qquad \textbf{(1.4.2.3)}$$

```
>
```

## Kongruenciák egyszersítése

Az eddigiekben megismerkedtünk a kongruenciák mindazon tulajdonságaival, amelyek emlékeztettek az egyenlség tulajdonságaira, megismertük azokat a mveleteket, amelyeket kongruenciákra ugyanúgy kell elvégezni, mint az egyenletekre. Megtanultuk azt, hogy a kongruenciák mindkét oldalát ugyanazzal a számmal növelhetjük, csökkenthetjük, st szorozhatjuk is. Az osztással kapcsolatban azonban már óvatosabban kell eljárnunk. Nézzük csak meg a következ példákat!

$$12 \equiv_5 22$$

Kettvel való osztás után

$$6 \equiv_5 11.$$

Eddig minden rendben, hiszen 6 és 11 is öttel osztva 1 maradékot ad. Ugyanakkor a

$$6 \equiv_4 2$$

kongruencia esetén a kettvel való osztás már nem lehetséges. Ugyanis ha ennek a kongruenciának mindkét oldalát kettvel osztanánk, akkor $3 \equiv_4 1$ eredményre jutnánk, ami sajnos nem teljesül. Vajon mi okozza azt, hogy az egyik példában az osztás után helyes eredményt, a másikban pedig hibás eredményt kaptunk?

Alkalmazzuk a definíciót! Az els példában $5 \mid 22-12 = 2\cdot(11-6)$. Mivel 5 és 2 relatív prímek, ezért az osztási lemma miatt az 5 osztója lesz a szorzat másik tényezjének, (11-6)-nak. Ez pedig pontosan azt fejezi ki, hogy $6 \equiv_5 11$. A második példában $4 \mid 6-2 = 2\cdot(3-1)$, ám most 4 nem relatív prím 2-vel, és így nem következtethetünk arra, hogy osztója (3-1)-nek, mint ahogy ez nem is következik be. Tehát az els példában olyan számmal osztottunk, ami a modulushoz relatív prím és ekkor helyes eredményt kaptunk.

A következ tétel választ ad arra is, hogyan lehet a második példában hibásan elvégzett egyszersítést helyesen elvégezni.

### 15.5.1. Tétel

Ha $a \cdot k \equiv_m b \cdot k$, akkor

$$a \equiv b \bmod \frac{m}{lnko(m, k)}. \square$$

## Bizonyítás

Tegyük fel, hogy $a \cdot k \equiv b \cdot k \bmod m$. Ekkor $m \mid (a \cdot k - b \cdot k) = (a - b) \cdot k$. Alkalmas $q$ egészre

$$m \cdot q = (a - b) \cdot k.$$

Ez az egyenlség eloszthető $lnko(m, k)$-val. Kapjuk, hogy

$$\frac{m}{lnko(m, k)} \cdot q = (a - b) \cdot \left( \frac{k}{lnko(m, k)} \right),$$

amibl

$$\frac{m}{lnko(m, k)} \mid (a - b) \cdot \left( \frac{k}{lnko(m, k)} \right)$$

adódik. Ám $\frac{m}{lnko(m, k)}$ és $\frac{k}{lnko(m, k)}$ relatív prímek, így szükségképpen (lásd osztási lemma) $\frac{m}{lnko(m, k)} \mid (a - b)$, ami pedig azt jelenti, hogy

$$a \equiv b \bmod \frac{m}{lnko(m, k)}.$$

És éppen ez az, amit bizonyítani akartunk.

Tételünk szerint tehát a bevezet példában helyesen úgy kellett volna eljárnunk, hogy a $6 \equiv_4 2$ kongruenciát a

$$3 \equiv 1 \bmod \frac{4}{lnko(4, 2)}$$

kongruenciára egyszersítjük, és mivel $lnko(4, 2) = 2$, az egyszersítés helyes eredménye $3 \equiv_2 1$.

Természetesen, ha $lnko(m, k) = 1$, vagyis, ha a modulus és a szám, amivel egyszersíteni akarunk relatív prímek, akkor az egyszersítés a modulus megváltoztatása nélkül elvégezhet, mert ekkor $\frac{m}{lnko(m, k)} = m$. Érvényes tehát a

## 15.5.2. Tétel

Ha $a \cdot k \equiv_m b \cdot k$, és $lnko(m, k) = 1$, akkor $a \equiv_m b$.

Ez a tétel biztosítja például, hogy a

$$65 \equiv_6 125$$

kongruencia 5-tel egyszersíthet a modulus megváltoztatása nélkül, ugyanis 5 és 6 relatív prímek. Tehát

$$13 \equiv_6 25.$$

Speciálisan, ha a modulus prím, akkor a kongruencia a modulus többszöröseinek kivételével bármely számmal egyszerűsíthet. A

$$24 \equiv_7 66$$

kongruencia egyszerűsíthet 2-vel, 3-mal, és 6-tal, ugyanis ezek mindegyike relatív prím 7-tel. Érvényesek tehát a

$$12 \equiv_7 33,\ 8 \equiv_7 22,\ 4 \equiv_7 11$$

kongruenciák. Ugyanakkor

$$7 \equiv_7 14$$

ám a 7-tel való osztás inkongruenciát eredményez, hiszen $1 \not\equiv_7 2$ . Ez az egyszerűsítés tehát nem végezhet el.

A következ tétel, mely az elzhöz hasonlóan a 12.1 tétel következménye, hasznos eszközt kínál a gyakorlati számítások során.

## 15.5.3. Tétel

Ha $a \equiv_m b$, és $k$ közös osztója $a$-nak, $b$-nek és $m$-nek, akkor

$$\frac{a}{k} \equiv \frac{b}{k} \ \mathbf{mod}\ \frac{m}{k}. \ \square$$

### Bizonyítás

A tétel feltételei mellett az $a \equiv b \ \mathbf{mod}\ m$ kongruencia $\frac{a}{k} \cdot k \equiv \frac{b}{k} \cdot k \ \mathbf{mod}\ m$ alakba írható. Mivel $k \mid m$ így $lnko(k, m) = k$, és ekkor a 12.1 Tétel felhasználásával

$$\frac{a}{k} \equiv \frac{b}{k} \ \mathbf{mod}\ \frac{m}{lnko(k, m)},$$

ahol a modulus egyenl $\frac{m}{k}$-val.

Példaként tekintsük a

$$6 \equiv_4 30$$

kongruenciát. Mivel 2 osztója a kongruenciában szerepl mindhárom számnak, egyszerűsítés után azt írhatjuk, hogy

$$3 \equiv_2 15.$$

## Ellenrz kérdések

1. Mikor mondjuk, hogy az $a$ és $b$ egészek számok kongruensek modulo $m$?
2. Hogyan jelöljük azt, hogy az $a$ és $b$ egészek számok kongruensek modulo $m$ ?

3. Mi jellemzi az egymással kongruens egészeket? Miben különbözhet két egymással modulo $m$ kongruens egész?

4. Van-e olyan egész szám, ami nem kongruens modulo m az m-mel való osztási maradékával?

5. Van-e a 0, 1, 2, 3, 4, 5, 6, 7 számok között két olyan, amelyek kongruensek egymással modulo 8?

6. Van-e olyan egész, ami a 0, 1, 2, 3, 4 számok egyikével sem kongruens modulo 4?

7. Mi az a két tulajdonsága a 0, 1, 2,..., $m-1$ egészeknek, ami miatt ket teljes maradékrendszernek hívjuk?

8. Mit jelent a kongruencia tranzitív tulajdonága? Fel tudunk-e sorolni további tulajdonságokat?

9. Összeadhatók-e az $a_1 \equiv_m b_1$ és $a_2 \equiv_m b_2$ kongruenciák megfelel oldalai? És az $a_1 \equiv_m b_1$ és $a_2 \equiv_n b_2$ kongruenciáké? Adjunk számpéldákat!

10. Összeszorozhatók-e az $a_1 \equiv_m b_1$ és $a_2 \equiv_m b_2$ kongruenciák megfelel oldalai? És az $a_1 \equiv_m b_1$ és $a_2 \equiv_n b_2$ kongruenciáké? Adjunk számpéldákat!

11. Mit jelent az, hogy a modulo $m$ összeadás felcserélhet az $m$-mel való maradékképzés mveletével?

12. Mit jelent az, hogy a modulo $m$ szorzás felcserélhet az $m$-mel való maradékképzés mveletével?

13. Mondjuk ki (legalább háromszor) a modulo $m$ számolás szabályát!

14. Ha modulo $m$ számolunk, akkor az $a^k$ kiszámítása során helyettesíthet-e az $a$ szám $a$ **mod** $m$-mel? És a kitev?

15 Számítsuk ki az alábbi hatványokat!

a) $2^{2000}$ **mod** 4; $b)$ $3^{3000}$ **mod** 7 $c)$ $4^{4000}$ **mod**

16. Számítsuk ki az alábbiakat!

2! mod 3, 3! mod 4, 4! mod 5, 5! mod 6, 6! mod 7, 7!mod 8, 8! mod 9