Diszkrét Matematika1.(közép)
Tételek, bizonyítások

A tételek Kovács Attila könyvéből lettek kivágva (nem hivatalos)

http://compalg.inf.elte.hu/~attila/materials/dm.djvu

Készítette: Faludi Péter

Tartalom

Moivre-azonosság komplex szorzásra

4.5.9. tétel (De Moivre-azonosság). *Legyen* $z, w \in \mathbb{C}$, $0 \leq \varphi, \psi < 2\pi$, $\varphi, \psi \in \mathbb{R}$, $z = |z|(\cos\varphi + i\sin\varphi)$, $w = |w|(\cos\psi + i\sin\psi)$. *Ekkor*

$$z \cdot w = |zw|\big(\cos(\varphi+\psi) + i\sin(\varphi+\psi)\big),$$

továbbá $w \neq 0$ *esetben*

$$\frac{z}{w} = \frac{|z|}{|w|}\big(\cos(\varphi-\psi) + i\sin(\varphi-\psi)\big).$$

Bizonyítás. A sin és cos függvények addíciós képleteiből

$$\begin{aligned} zw &= |z|\cdot|w|(\cos\varphi + i\sin\varphi)\cdot(\cos\psi + i\sin\psi) \\ &= |zw|(\cos\varphi\cos\psi - \sin\varphi\sin\psi + i(\cos\varphi\sin\psi + \cos\psi\sin\varphi)) \\ &= |zw|(\cos(\varphi+\psi) + i\sin(\varphi+\psi)), \end{aligned}$$

a második állítás pedig a 4.5.7. tétel (7) tulajdonságából következik. ■

Komplex n-edik gyökvonás(hiányos) Láng Csabáné

Gyökvonás. $z \in \mathbb{C}$, $n \in \mathbb{N}$ esetén a $w \in \mathbb{C}$ számot a z szám *n-edik gyökének* nevezzük, ha $w^n = z$.

Legyen $z \in \mathbb{C}, n \in \mathbb{N}$. A $z = 0$ szám egyetlen n-edik gyöke 0. Ha $z \neq 0$ és $z = r(\cos\varphi + i\sin\varphi)$, akkor z-nek n különböző n-edik gyöke van, melyek trigonometrikus alakja

$$w_k = \sqrt[n]{r}\left(\cos\frac{\varphi+k2\pi}{n} + i\sin\frac{\varphi+k2\pi}{n}\right), \quad 0 \leq k \leq n-1.$$

Valamely $z \neq 0$ komplex szám n-edik gyökei a számsíkon ábrázolva n oldalú szabályos sokszög csúcsai. A csúcsoknak az origótól való távolsága $\sqrt[n]{r}$, az egyik csúcsnak a valós tengellyel bezárt szöge $\frac{\varphi}{n}$.

$n \in \mathbb{N}\setminus\{1\}$ esetén a $z \in \mathbb{C}$ szám n-edik gyökeinek összege 0.

Relációszorzás asszociativitása

TB

2.2.9. tétel (relációszorzat asszociativitása). *Legyen* $\varrho \subseteq A \times B, \sigma \subseteq B \times C$ *és* $\tau \subseteq C \times D$. *Ekkor a relációszorzat asszociatív, vagyis* $(\tau \circ \sigma) \circ \varrho = \tau \circ (\sigma \circ \varrho)$.

Bizonyítás. A két halmaz egyenlőségét kölcsönös tartalmazással bizonyítjuk. Először a $(\tau \circ \sigma) \circ \varrho \subseteq \tau \circ (\sigma \circ \varrho)$ tartalmazást látjuk be. Ha $(a,d) \in (\tau \circ \sigma) \circ \varrho$, akkor létezik olyan $b \in B$, amelyre $(a,b) \in \varrho$ és $(b,d) \in \tau \circ \sigma$. A második összefüggésből következik, hogy létezik olyan $c \in C$, amelyre $(b,c) \in \sigma$ és $(c,d) \in \tau$. Ekkor viszont erre a c-re $(a,c) \in \sigma \circ \varrho$ és $(c,d) \in \tau$. Így pedig $(a,d) \in \tau \circ (\sigma \circ \varrho)$ is teljesül. Hasonlóképpen bizonyítható a $\tau \circ (\sigma \circ \varrho) \subseteq (\tau \circ \sigma) \circ \varrho$ összefüggés is, amiből a két reláció egyenlősége következik. ■

Ekvivalenciareláció és osztályozás kapcsolata

2.2.13. tétel (ekvivalenciareláció és osztályfelbontás kapcsolata)**.** *Valamely A halmazon értelmezett ϱ ekvivalenciareláció az A-nak egy osztályfelbontását határozza meg. Megfordítva, az A halmaz egy osztályfelbontása ekvivalenciarelációt definiál ϱ elemei között.*

Bizonyítás. Legyen adott az A halmazon egy ϱ ekvivalenciareláció. Megmutatjuk, hogy $\{[a] \mid a \in A\}$ egy osztályozása A-nak. Nyilván

$$\bigcup_{a \in A} [a] = A\,,$$

továbbá ϱ reflexivitása miatt $a \in [a]$, így az osztályok nem-üresek. Azt kell csak belátnunk, hogy a különböző osztályok metszete üres. Legyen $c \in [a] \cap [b]$. Ekkor $a \varrho c$ és $b \varrho c$, amiből a tranzitivitás és a szimmetria miatt $a \varrho b$ és $b \varrho a$. Ha most $d \in [a]$, akkor a szimmetria és a tranzitivitás miatt $d \in [b]$. Ugyanígy, ha $d \in [b]$, akkor $d \in [a]$. Végeredményben tehát $[a] = [b]$, azaz ha két ekvivalenciaosztálynak van közös eleme, akkor azonosak. Eszerint A minden eleme pontosan egy ekvivalenciaosztályban fordul elő, és az osztályok páronként diszjunktak.

Megfordítva, ha adott az A halmaz egy osztályfelbontása, akkor a

$$\varrho = \{(a, b) \in A \times A \mid a \text{ és } b \text{ egyazon osztály elemei}\}$$

reláció reflexív, szimmetrikus és tranzitív, vagyis ekvivalenciareláció. ■

Permutációk száma

TB

5.2.2. tétel. $P_n = n!$.

Bizonyítás. Teljes indukcióval bizonyítunk. $n = 1$ esetén $P_1 = 1 = 1!$, tehát az állítás igaz. Legyen $n > 1$ és tegyük fel, hogy $n - 1$-ig igaz az állítás. Létesítsünk relációt az n-elemű permutációk halmazán. Legyen két permutáció relációban, ha az elrendezésben az első elemük megegyezik. Ez a reláció ekvivalenciareláció, tehát osztályoz. Az osztályok száma n, hiszen ennyi különböző elem állhat az első helyen. Egy-egy osztályba P_{n-1} elem kerül, így az összes permutáció száma $P_n = n \cdot P_{n-1}$. Az indukciós feltevés szerint $P_n = n \cdot (n-1)! = n!$. ■

Variációk száma

5.2.4. tétel. $V_n^k = P_n / P_{n-k} = n(n-1)\cdots(n-k+1)$.

Bizonyítás. Tekintsük ismét az n elem összes permutációját, és létesítsünk a permutációk között relációt az alábbi módon: két permutáció akkor legyen relációban, ha az első k elemük megegyezik. Könnyű belátni, hogy ekvivalenciarelációt kapunk. Az összes permutációt megkapjuk, ha megnézzük, hogy egy osztályban hány elem található, és hány osztály van. Az egy osztályba kerülő elemek száma P_{n-k}, vagyis annyi, ahányféleképpen a többi $n-k$ elem felsorolható. Különböző osztályokba pedig akkor kerül két permutáció, ha az első k helyen valahol van köztük eltérés. Így tehát annyi osztály van, ahányféleképpen n elemből k-tagú sorozatot képezhetünk, vagyis V_n^k. Ezek szerint $P_n = V_n^k \cdot P_{n-k}$, amiből a tétel állítása következik. ■

Ismétléses variációk száma

TB

Jelölje az ilyen sorozatok számát $V_n^{k,i}$.

5.2.8. tétel. $V_n^{k,i} = n^k$.

Bizonyítás. A bizonyítást rögzített n-re k szerinti indukcióval végezzük. Legyen $k = 1$. Ekkor $V_n^{1,i} = n$, tehát az állítás igaz. Legyen $k > 1$, és tegyük fel, hogy $k-1$-ig igaz az állítás. k-ad osztályú ismétléses variációkat úgy is képezhetünk, hogy sorban vesszük a $k-1$ osztályúakat, és a k-adik helyre elhelyezünk még egy elemet. Ezt n-féleképpen tehetjük meg, így $V_n^{k,i} = V_n^{k-1,i} \cdot n = n^{k-1} \cdot n = n^k$. ■

Kombinációk száma

TB

5.2.6. tétel. *Ha $n \geq k$, akkor*

$$C_n^k = \frac{V_n^k}{P_k} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Bizonyítás. n elem k-ad osztályú variációinak száma V_n^k. Ezeket a variációkat úgy is előállíthatjuk, hogy képezzük az n-elemű halmaz k-elemű részhalmazait, majd a kapott k elemet az összes lehetséges módon sorba rakjuk. Ez a sorba rendezés P_k-féleképpen történhet. Ily módon minden variációt pontosan egyszer kapunk meg, ezért $V_n^k = C_n^k P_k$, amiből a tétel állítása következik. ■

Ismétléses kombinációk száma

5.2.10. tétel. $C_n^{k,i} = C_{n+k-1}^k$.

Bizonyítás. Az $\{1, 2, \ldots, n\}$ halmaz valamely k-ad osztályú ismétléses kombinációja úgy is megadható, hogy a k elemet tetszőleges sorrendben felsoroljuk, például növekvően, vagyis az ismétléses kombinációk száma az n elemből képezhető k-elemű monoton növekvő sorozatok számával egyezik meg. Hasonló gondolattal, az $\{1, 2, \ldots, n+k-1\}$ halmaz k-ad osztályú ismétlés nélküli kombinációi száma az $n+k-1$ elemből képezhető k elemű szigorúan monoton sorozatok számával egyezik meg. Ennek megfelelően definiáljunk két halmazt:

$$\begin{aligned} A &= \{(a_1, a_2, \ldots, a_k) \mid a_j \in \mathbb{N},\ 1 \leq a_1 \leq a_2 \leq \ldots \leq a_k \leq n\}, \\ B &= \{(b_1, b_2, \ldots, b_k) \mid b_j \in \mathbb{N},\ 1 \leq b_1 < b_2 < \ldots < b_k \leq n+k-1\}. \end{aligned}$$

Mivel $|A| = C_n^{k,i}$ és $|B| = C_{n+k-1}^k$, a tétel bizonyításához elegendő egy bijekciót létesíteni a két halmaz között. Legyen $f : A \to B$ az alábbi: $a = (a_1, a_2, \ldots a_k)$ és $b = (b_1, b_2, \ldots, b_k)$ esetén $f(a) = b$, ahol

$$\begin{aligned} b_1 &= a_1\,, \\ b_2 &= a_2 + 1\,, \\ &\ldots \\ b_k &= a_k + (k-1). \end{aligned}$$

f nyilvánvalóan függvény. Mivel adott $b = (b_1, b_2, \ldots, b_k) \in B$ ponthoz az f függvény képzési szabálya miatt egyetlen $a = (a_1, a_2, \ldots, a_k)$ pont tartozik, ezért f injektív. De

Ismétléses permutációk száma

5.2.12. tétel.

$$P_n^{n_1,n_2,\ldots,n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$

Bizonyítás. A bizonyítást k szerinti indukcióval végezzük. $k = 1$ esetén $P_n^n = 1 = n!/n!$. Legyen $k > 1$, és tegyük fel, hogy $k-1$ számú különböző elem esetén igaz az állítás. Legyen ezek után adott k különböző elem $n_1, n_2, \ldots, n_k$ előfordulási gyakoriságokkal. Az ismétléses permutációk között készítsünk relációt: két permutáció akkor legyen relációban, ha elhagyva belőlük az n_k-szor előforduló elemeket, azonos permutációhoz jutunk. Könnyű belátni, hogy ez a reláció ekvivalenciareláció, az osztályok száma $P_{n-n_k}^{n_1,n_2,\ldots,n_{k-1}}$. Most számoljuk össze az osztályok elemszámát. A $k-1$ különböző elemből álló permutációból annyiféleképpen tudunk k-eleműt készíteni, ahányféleképpen az $n - n_k + 1$ lehetséges hely közül (s darab sorba rakott tárgy között $s-1$ darab helyre, valamint az első elé és az utolsó mögé lehet rakni) n_k darab kiválasztható, megengedve egy hely többszöri kiválasztását is. Egy osztályban tehát $C_{n-n_k+1}^{n_k,i} = C_n^{n_k}$ elem lesz. Ezért az ismétléses permutációk száma

$$P_n^{n_1,n_2,\ldots,n_k} = P_{n-n_k}^{n_1,\ldots,n_{k-1}} C_n^{n_k} = \frac{(n-n_k)!}{n_1!n_2!\cdots n_{k-1}!}\frac{n!}{n_k!(n-n_k)!} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$

■

Binomiális tétel

TB

5.4.1. tétel (binomiális tétel). *Legyen $(R;+,\cdot)$ egy kommutatív, egységelemes gyűrű, $x,y\in R$ és legyen $n\in\mathbb{N}^+$. Ekkor*

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}.$$

Bizonyítás. Az n tényezős $(x+y)^n$ szorzatot kifejtve $x^k y^{n-k}$ alakú tagokat kapunk $(0\le k\le n)$. Egy ilyen tag úgy keletkezik, hogy az n tényező közül k-ból az x-et, $n-k$-ból az y-t választjuk. Rögzített k-ra az $x^k y^{n-k}$ tag annyiszor fog előállni, ahányszor az n tényezőből a k darab x-et kiválaszthatjuk, vagyis $\binom{n}{k}$-szor. k-ra összegezve kapjuk a tétel állítását. ■

Az $\binom{n}{k}$ alakú számok innen kapták a ***binomiális együttható*** elnevezést.

5.4.2. Következmény. *Legyen $n\in\mathbb{N}^+$. Az $x=y=1$, illetve $x=1, y=-1$ helyettesítéssel azt kapjuk, hogy*

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n,$$

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0.$$

Szita formula

5.6. A logikai szita formula

Legyen adott N objektum, amelyek közül bizonyosak rendelkeznek az előre megadott $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül egyesekkel. Az N objektum bármelyikének lehet több tulajdonsága is, vagy akár egy sem. Jelölje $N(\alpha_i, \alpha_j, \ldots, \alpha_k)$ azon objektumok számát, amelyek az $\alpha_i, \alpha_j, \ldots, \alpha_k$ tulajdonságok mindegyikével (esetleg továbbiakkal is) rendelkeznek. Ha hangsúlyozni akarjuk, hogy olyan objektumot választunk ki, amelyik valamelyik tulajdonsággal nem rendelkezik, akkor azt fölülvonással jelöljük. Például $N(\alpha_1, \alpha_3, \overline{\alpha}_4)$ jelenti azon objektumok számát, amelyek az α_1 és α_3 tulajdonságokkal rendelkeznek, az α_4 tulajdonsággal azonban nem. Az egyik tulajdonsággal sem rendelkező objektumok számát így $N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n)$ jelöli. Vezessük be az alábbi jelöléseket.

$$\begin{aligned}
S_0 &= N, \\
S_1 &= N(\alpha_1) + N(\alpha_2) + \cdots + N(\alpha_n), \\
S_2 &= N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + \cdots + N(\alpha_1, \alpha_n) + \cdots + N(\alpha_{n-1}, \alpha_n), \\
S_3 &= N(\alpha_1, \alpha_2, \alpha_3) + \cdots + N(\alpha_{n-2}, \alpha_{n-1}, \alpha_n), \\
&\vdots \\
S_n &= N(\alpha_1, \alpha_2, \ldots, \alpha_n).
\end{aligned}$$

Az összegzés az $\alpha_1, \ldots, \alpha_n$ tulajdonságok minden lehetséges kombinációjára értendő a sorrend figyelembevétele nélkül.

5.6.1. tétel. *Az iménti jelölésekkel*

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n) = S_0 - S_1 + S_2 - S_3 + \ldots + (-1)^n S_n .$$

Bizonyítás. Legyen P egy olyan objektum, amelyre az $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül pontosan k darab teljesül. Ekkor P k-szor fordul elő a legalább egy tulajdonsággal rendelkező objektumok számának felsorolásában, $\binom{k}{2}$-ször a legalább két tulajdonsággal rendelkező objektumok számának felsorolásában, $\binom{k}{3}$-szor a legalább három tulajdonsággal rendelkező objektumok számának felsorolásában, és így tovább, $\binom{k}{k}$-szor a legalább k tulajdonsággal rendelkező objektumok számának felsorolásában. Így, ha $k \geq 1$, akkor a 5.4.2. következmény szerint a P objektum előfordulásainak száma az egyenlet jobb oldalán

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^k \binom{k}{k} = (1-1)^k = 0.$$

Ha $k = 0$, akkor P egy olyan objektum, amely az $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül egyikkel sem rendelkezik, így pontosan egyszer fordul elő az egyenlet jobb oldalán. Ezzel a tételt bebizonyítottuk. ■

Euklideszi algoritmus és helyessége

7.2.8. tétel (két egész szám legnagyobb közös osztójának létezése)**.** *Bármely két egész számnak létezik legnagyobb közös osztója.*

Bizonyítás. A legnagyobb közös osztó létezését a matematika egyik legősibb eljárásával, az ***euklideszi algoritmussal*** bizonyítjuk (EUKLIDÉSZ i.e. 300 körül élt görög matematikus). Az algoritmus alapgondolata az, hogy az egyik számot maradékosan elosztjuk a másikkal, majd a másik számot a maradékkal, és így tovább mindaddig, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó osztó ($b \nmid a$ esetén az utolsó nem-nulla maradék) lesz a két szám (egyik) legnagyobb közös osztója.

Tegyük fel, hogy $a, b \in \mathbb{Z}$, $b \neq 0$. Ha $b \mid a$, akkor b nyilván legnagyobb közös osztó. Ha $b \nmid a$, akkor a maradékos osztás tételét alkalmazva alkalmas q_i, r_i egészekkel

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

Az eljárás véges sok lépésben befejeződik, hiszen a maradékok nemnegatív egészek szigorúan monoton csökkenő sorozatát alkotják. Be kell még látnunk, hogy r_n valóban az a és b számok (egyik) legnagyobb közös osztója.

Az algoritmus során visszafelé haladva először azt igazoljuk, hogy r_n közös osztója a-nak és b-nek. Az utolsó egyenlőségből $r_n \mid r_{n-1}$. Az utolsó előtti egyenlőségből a 7.1.2. tétel lineáris kombinációs tulajdonsága miatt

$$r_n \mid r_{n-1} \text{ és } r_n \mid r_n \Rightarrow r_n \mid r_{n-1} q_n + r_n = r_{n-2}.$$

Az eljárást folytatva végül $r_n \mid b$, majd (az első egyenlőségből) $r_n \mid a$ adódik. A legnagyobb közös osztó tulajdonság bizonyításához felülről lefelé haladunk. Legyen $c \in \mathbb{Z}$ olyan, hogy $c \mid a$ és $c \mid b$. Ekkor az első egyenlőségből $c \mid a - bq_1 = r_1$, majd a másodikból $c \mid b \wedge c \mid r_1 \Rightarrow c \mid b - r_1 q_2 = r_2$. Ugyanígy folytatva végül az utolsó előtti egyenlőségből azt kapjuk, hogy $c \mid r_n$. ■

Prím és felbonthatatlan tulajdonság ekvilenciája az egészek körében

7.1.8. tétel. *Minden prímelem felbonthatatlan.*

Bizonyítás. Legyen p prím és $p = xy$. Mivel egységelemes integritási tartományban dolgozunk, ezért $p \mid xy$. A 7.1.7. definíció szerint ekkor $p \mid x$ vagy $p \mid y$. Feltehető, hogy $p \mid x$. Így $x = pz = x(yz)$ miatt $yz = 1$, amiből következik, hogy y és z egységek, x és p pedig asszociáltak. ■

Számelmélet alaptétele (prímfelbontás létezése és egyértelműsége)

7.2.18. tétel (a számelmélet alaptétele)**.** *Minden, a 0-tól és egységektől különböző egész szám véges sok felbonthatatlan szám szorzatára bontható, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű.*

Bizonyítás. (1) A felbonthatóság bizonyítása. Legyen $a \in \mathbb{Z}$ nem-nulla és nem-egység. Ha a felbonthatatlan, akkor készen vagyunk. Ha a nem felbonthatatlan, akkor létezik nem-triviális osztója. Ezek közül a legkisebb pozitív szükségképpen felbonthatatlan. Ekkor $a = p_1 a_1$, ahol p_1 felbonthatatlan és a_1 nem egység. Ha a_1 felbonthatatlan, akkor készen vagyunk; ha nem, akkor létezik olyan p_2 felbonthatatlan, hogy $a_1 = p_2 a_2$, ahol a_2 nem egység. Hasonlóan járunk el a_2-vel, stb. Eljárásunk véges sok lépésben véget ér, mert az $|a_i|$ számok pozitív egészek szigorúan monoton csökkenő sorozatát alkotják, így eljutunk egy olyan a_k-hoz, amely már felbonthatatlan. Ekkor az $a = p_1 p_2 \cdots p_{k+1}$ előállítást nyerjük.

(2) Az egyértelműség bizonyítása. Tegyük fel indirekt, hogy a-nak (legalább) két lényegesen különböző felbontása létezik, vagyis

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \tag{7.3}$$

Ha itt valamelyik p_i egységszerese valamelyik q_j-nek, például $p_1 = \varepsilon q_1$, akkor q_1-gyel egyszerűsítve

$$a' = \frac{a}{q_1} = \varepsilon p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s,$$

vagyis a'-nek két lényegesen különböző felbontását kapjuk. Az eljárást folytatva végül egy olyan számhoz jutunk, amelynek kétféle felbontásában már nincsenek egységszeres tényezők. Feltehető, hogy az indirekt feltevésben szereplő (7.3) előállítás ilyen. Ekkor $p_1 \mid q_1 q_2 \cdots q_s$. Mivel p_1 felbonthatatlan, ezért prím is, vagyis p_1 szükségképpen osztja legalább az egyik q_j tényezőt. Ha azonban $p_1 \mid q_j$, akkor q_j felbonthatatlansága miatt p_1 vagy egység vagy q_j egységszerese, de mindkettő ellentmondás. ■

Lineáris kongruencia megoldása

7.3.21. tétel. *Az* $ax \equiv b \pmod{m}$ *kongruenciának pontosan akkor létezik megoldása, ha* $(a, m) \mid b$. *Ha létezik megoldás, akkor a megoldásszám* (a, m).

Bizonyítás. Az $ax \equiv b \pmod{m}$ kongruencia megoldhatósága azt jelenti, hogy létezik olyan x_1 egész, amelyre $ax_1 \equiv b \pmod{m}$. A kongruencia definíciója miatt ekkor létezik olyan x_2 egész, amelyre $mx_2 = b - ax_1$, vagyis $ax_1 + mx_2 = b$. Így az $ax \equiv b \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha az $ax_1 + mx_2 = b$ diofantikus egyenlet megoldható, aminek a szükséges és elégséges feltétele az $(a, m) \mid b$ oszthatóság teljesülése (7.2.13. tétel).

Most vizsgáljuk meg a megoldásszámot, amennyiben létezik megoldás. Legyen $d = (a, m)$, $m_1 = m/d$, $a_1 = a/d$, $b_1 = b/d$. Ha $d = 1$, akkor amennyiben $\{c_1, c_2, \ldots, c_m\}$ teljes maradékrendszer, akkor a 7.3.13. tétel miatt $\{c_1a, c_2a, \ldots, c_ma\}$ is teljes maradékrendszer modulo m, így pontosan egy elem van köztük, amelyik b-vel kongruens. Ezen elem által reprezentált maradékosztály az egyetlen megoldás. Ha $d > 1$, akkor, mivel az $ax \equiv b \pmod{m}$ és az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciákat ugyanazok az egész számok elégítik ki, elég azt megvizsgálni, hogy a modulo m_1 egyetlen maradékosztályt alkotó megoldások hány inkongruens maradékosztályt jelentenek modulo m. Ha x_0 megoldása az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciának, akkor pontosan az

$$x_0, x_0 + m_1, x_0 + 2m_1, \ldots, x_0 + (d-1)m_1$$

elemek esnek különböző maradékosztályokba modulo m. Ez pedig d darab inkongruens megoldást jelent modulo m. Vagyis a teljes megoldást az

$$[x_0], [x_0 + m_1], [x_0 + 2m_1], \ldots, [x_0 + (d-1)m_1]$$

maradékosztályok elemei alkotják. ■

Euler-Fermat-tétel

7.3.14. tétel (Euler-tétel)**.** *Legyen* $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Ekkor* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás. Legyen $\{r_1, r_2, \dots r_{\varphi(m)}\}$ egy redukált maradékrendszer modulo m. Mivel $(a, m) = 1$, ezért $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ is redukált maradékrendszert alkot modulo m. A két redukált maradékrendszerben a megfelelő reprezentánsok párba állíthatók aszerint, hogy modulo m azonos osztályba esnek, vagyis $r_i \equiv ar_j \pmod{m}$ alkalmas $1 \leq i, j \leq \varphi(m)$ esetén. Ezeket a kongruenciákat összeszorozva kapjuk, hogy

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} r_j \pmod{m}.$$

$(r_i, m) = 1$ miatt az összes r_i-vel egyszerűsíthetünk, így $a^{\varphi(m)} \equiv 1 \pmod{m}$ adódik. ■

Polinomiális tétel

5.4.3. tétel (polinomiális tétel). *Legyenek $x_1, x_2, \ldots, x_r$ egy kommutatív egységelemes gyűrű elemei és legyen $r, n \in \mathbb{N}^+$. Ekkor*

$$(x_1 + x_2 + \ldots + x_r)^n = \sum_{i_1+i_2+\ldots+i_r=n} P_n^{i_1,i_2,\ldots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}.$$

Bizonyítás. Két különböző bizonyítást is adunk.
(1) Az n tényezős $(x_1+x_2+\cdots+x_r)(x_1+x_2+\cdots+x_r)\cdots(x_1+x_2+\cdots+x_r)$ szorzatból válasszuk ki x_1-et i_1-szer, ami $\binom{n}{i_1}$-féleképpen lehetséges, a fennmaradó $n-i_1$ tényezőből x_2-t i_2-ször, ami $\binom{n-i_1}{i_2}$-féleképpen lehetséges, és így tovább, az $n-i_1-i_2-\cdots-i_{r-1}$ tényezőből x_r-t i_r-szer, ami $\binom{n-i_1-i_2-\cdots-i_{r-1}}{i_r}$-féleképpen lehetséges. Ekkor

$$\binom{n}{i_1}\binom{n-i_1}{i_2}\cdots\binom{n-i_1-i_2-\cdots-i_{r-1}}{i_r}$$

$$= \frac{n!}{(n-i_1)!i_1!}\frac{(n-i_1)!}{(n-i_1-i_2)!i_2!}\cdots\frac{(n-i_1-i_2-\cdots-i_{r-1})!}{(n-i_1-i_2-\cdots-i_r)!i_r!}$$

$$= \frac{n!}{i_1!i_2!\cdots i_r!} = P_n^{i_1,i_2,\ldots,i_r},$$

ami éppen az $x_1^{i_1}x_2^{i_2}\cdots x_r^{i_r}$ tag együtthatója.

(2) A bizonyítást r szerinti teljes indukcióval végezzük. Az $r=1$ eset nyilvánvaló. Legyen $r>1$ és tegyük fel, hogy $r-1$-ig igaz az állítás. Végezzük el az $x_2+\ldots+x_r=u$ helyettesítést, és tekintsük a binomiális tételt. Ekkor

$$(x_1 + x_2 + \ldots + x_r)^n = (x_1+u)^n = \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}u^{n-i_1}.$$

Az indukciós feltevést u^{n-i_1}-re alkalmazva

$$\sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}\sum_{i_2+i_3+\ldots+i_r=n-i_1} P_{n-i_1}^{i_2,i_3,\ldots,i_r}x_2^{i_2}x_3^{i_3}\cdots x_r^{i_r}$$

$$= \sum_{i_1+i_2+\ldots+i_r=n}\binom{n}{i_1}P_{n-i_1}^{i_2,i_3,\ldots,i_r}x_1^{i_1}x_2^{i_2}\cdots x_r^{i_r}.$$

Felhasználva, hogy

$$\binom{n}{i_1}P_{n-i_1}^{i_2,i_3,\ldots,i_r} = \frac{n!}{i_1!(n-i_1)!}\frac{(n-i_1)!}{i_2!\cdots i_r!} = P_n^{i_1,\ldots,i_r},$$

a bizonyítás kész. ■

Kínai maradéktétel

7.3.25. tétel (kínai maradéktétel). *Ha $m_1, \dots, m_k$ páronként relatív prím modulusok, akkor az*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k}, \end{aligned} \tag{7.8}$$

kongruencia-rendszernek bármely $c_1, \dots, c_k$ egészek esetén van megoldása, s ez a megoldás modulo $M = m_1 \cdots m_k$ egyértelmű.

Bizonyítás. Legyen

$$M_i = M/m_i \qquad (1 \le i \le k),$$

vagyis $M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$. Tekintsük az

$$\begin{aligned} M_1 y &\equiv 1 \pmod{m_1} \\ M_2 y &\equiv 1 \pmod{m_2} \\ &\vdots \\ M_k y &\equiv 1 \pmod{m_k} \end{aligned}$$

kongruenciákat. Ezek külön-külön mind egyértelműen megoldhatók, mert M_i és m_i relatív prímek minden $1 \le i \le k$ esetén. Jelöljük megoldásaikat sorban $y_1, y_2, \dots, y_k$-val és legyen

$$g_i = M_i y_i \qquad (1 \le i \le k). \tag{7.9}$$

Legyen

$$x_0 \equiv (c_1 g_1 + c_2 g_2 + \cdots + c_k g_k) \pmod{M}. \tag{7.10}$$

Megmutatjuk, hogy ebből az egyenletből $x_0 \equiv c_i \pmod{m_i}$ $(1 \le i \le k)$ következik. Ha $i \ne j$, akkor $M_j \equiv 0 \pmod{m_i}$, amiből (7.9) miatt $g_j = M_j y_j \equiv 0 \pmod{m_i}$. Azt is észrevehetjük, hogy $g_i \equiv 1 \pmod{m_i}$ minden $1 \le i \le k$ esetén, így

$$\begin{aligned} x_0 &\equiv c_i g_i \pmod{m_i} \\ &\equiv c_i \pmod{m_i} \end{aligned}$$

minden i-re teljesül. A (7.10) szerint kiszámolt x_0 tehát valóban megoldás.

Tegyük fel, hogy a (7.8) kongruencia-rendszernek több inkongruens megoldása is van modulo M, vagyis tegyük fel, hogy $x_0 \not\equiv x_1 \pmod{M}$ a kongruencia-rendszer megoldásai. Mivel $x_0 \equiv x_1 \pmod{m_i}$ minden $1 \le i \le k$ esetén, ezért $m_i \mid x_0 - x_1$. De $(m_i, m_j) = 1$ $(i \ne j)$, ezért $M \mid x_0 - x_1$, s így $x_0 \equiv x_1 \pmod{M}$, ami ellentmondás.

Megmutatjuk még, hogy a (7.8) kongruencia-rendszer összes megoldását az $[x_0]_M$ maradékosztály elemei szolgáltatják. Legyen $x_1 \in [x_0]_M$, vagyis $x_0 \equiv x_1 \pmod{M}$. Ekkor $M \mid x_0 - x_1$, így $m_i \mid x_0 - x_1$ minden $1 \leq i \leq k$ esetén. Ez azt jelenti, hogy $x_0 \equiv x_1 \pmod{m_i}$, vagyis x_1 is kielégíti (7.8) minden egyenletét. ■

Diofantikus egyenletek megoldása

7.2.13. tétel. *Rögzített a, b és c egész számok esetén az $ax + by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a, b) \mid c$.*

Bizonyítás. Először tegyük fel, hogy létezik egy x_0, y_0 megoldás. Ekkor $(a, b) \mid a$ és $(a, b) \mid b$ alapján $(a, b) \mid ax_0 + by_0 = c$. Megfordítva, tegyük fel, hogy $(a, b) \mid c$, vagyis valamilyen t-re $c = (a, b)t$. Ekkor a 7.2.12. tétel miatt alkalmas u, v egészekkel $(a, b) = au + bv$. Az egyenletet t-vel szorozva azt kapjuk, hogy $c = a(ut) + b(vt)$, azaz $x = ut$ és $y = vt$ megoldása az $ax + by = c$ diofantikus egyenletnek. ■

Megoldhatóság esetén az euklideszi algoritmus egyúttal eljárást is szolgáltat a lineáris diofantikus egyenlet (egyik) megoldásának megkereséséhez.