A klasszikus számelmélet néhány kérdése feladatokban.

Klukovits Lajos

TTIK Bolyai Intézet

2020. október 16.

Maradékos osztás $\mathbb{Z}[i]$-ben.

1. Legyen $\alpha, \beta \in \mathbb{Z}[i], \alpha\beta \neq 0$. Létezik olyan $\gamma, \varrho \in \mathbb{Z}[i]$, amelyre $\alpha = \beta\gamma + \varrho$, és $|\varrho| < |\beta|$.
2. Az α/β számnak megfelelő pont benne van egy 1 oldalélű egész koordinátájú rácsnégyzetben, vagy annak a határán.
3. A négyzet csúcspontjai közül legalább egy 1-nél kisebb távolságra van e ponttól. Legyen γ egy ilyen pontnak megfelelő Gauss-egész.
4. Ekkor
$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1$$
$$|\alpha - \beta\gamma| < |\beta|$$
5. A $\varrho = \alpha - \beta\gamma$ választással igazoltuk állításunkat.

Legnagyobb közös osztó $\mathbb{Z}[i]$-ben.

1. Az előbbi maradékos osztás alapján bármely két nemzéró Gauss-egészen Euklideszi-algoritmus hajtható végre: a megfelelő osztás-sorozat véges sok lépés után megáll.
2. Az, hogy az osztás-sorozat utolsó nemzéró maradéka éppen egy legnagyobb közös osztó, formálisan ugyanúgy látható be, mint a racionális egész számok esetén.
3. Illusztrációként meghatározzuk az $\alpha = 8 + i$ és a $\beta = 4 - 2i$ Gauss-egészek egy legnagyobb közös osztóját.

A számolás.

- $\frac{8+i}{4-2i} = \frac{(8+i)(4+2i)}{20} = \frac{30+20i}{20} = \frac{3}{2} + i$.
- Két választási lehetőségünk van: $2 + i$, $1 + i$.
- Válasszuk a $(2 + i)$-t, legyen $\gamma_1 = 2 + i$.
- Ekkor $\alpha = \beta\gamma_1 + (-2 + i)$. Legyen $\varrho_1 = -2 + i$.
- Látható, hogy $\beta = 4 - 2i = \gamma_1(-2) + 0$, tehát az utolsó nemzéró maradék a $\varrho_1 = -2 + i$.
- Kaptuk, hogy ln. k. o.(α, β) egy lehetséges értéke a $2 - i$.
- $\gamma_1 = 1 + i$ választás is lehetséges, ekkor is csupán két lépés kell a legnagyobb közös osztó meghatározásához.

Ismétlés: alapvető definíciók, néhány tétel.

1. A *modulo m* kongruencia a $\mathbb{Z}$ gyűrűben.
2. Alapvető tulajdonságai:
   1. ekvivalencia-reláció,
   2. művelettartások.
3. Lineáris kongruenciák megoldhatósága, a lényegesen különböző megoldások száma.:

Theorem

Legyen $a, b, m \in \mathbb{Z},\ m > 1$. Az $ax \equiv b \pmod{m}$ lineáris kongruencia pontosan akkor oldható meg, ha $\text{ln. k. o.}(a, m) | b$. A modulo m inkongruens megoldások száma $\frac{m}{\text{ln.k.o.}(a,m)}$.

Ismétlés: További tételek.

Theorem

Legyen $a, b, c \in \mathbb{Z}$. Az $ax + by = c$ lineáris egyenletnek pontosan akkor van egész megoldása, ha $\text{ln. k. o.}(a, b) | c$. Ha x_0, y_0 megoldások, akkor

$$x_t = x_0 + t\frac{b}{\text{ln. k. o.}(a,b)} \quad y_t = y_0 - t\frac{a}{\text{ln. k. o.}(a,b)} \qquad t \in \mathbb{Z}$$

szintén megoldások, és az összes megoldás ilyen alakú.

Corollary

Legyen $a, b, c, m \in \mathbb{Z},\ m > 1$. Az $ax + by = c$ lineáris egyenletnek pontosan akkor van egész megoldása, ha megoldható az $ax \equiv c \pmod{m}$ lineáris kongruencia.

Ismétlés: A kínai maradéktétel..

Theorem

Legyenek $a_1, \ldots, a_k \in \mathbb{Z}$ és $m_1, \ldots, m_k \in \mathbb{N}$. Az

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

ún. lineáris kongruenciarendszer megoldható, ha a modulusok páronként relatív prímek.

Megjegyzés. Hangsúlyozzuk, hogy a tételbeli föltétel csak elegendő, de nem szükséges.

1. Feladat.

Bontsuk föl a 367-et két természetes szám összegére úgy, hogy az egyik szám osztható legyen 17-tel, míg a másik 21-gyel.

A $17x + 21y = 367$ egyenlet pozitív egész gyökeit kell megkeresni. Először a $17u + 21v = 1$ egyenletet oldjuk meg.

$$21 = 17 \cdot 1 + 4$$
$$17 = 4 \cdot 4 + 1$$

Visszafelé helyettesítve: $17 \cdot 5 + 21(-4) = 1$, amiből

$$367 = 17(5 \cdot 367) + 21(-4 \cdot 367) = 17 \cdot 1835 + 21 \cdot (-1468)$$
$$17 \cdot 87 = 1479 > 1468$$
$$367 = 17 \cdot (1835 - 87 \cdot 21) + 21 \cdot (-1468 + 87 \cdot 17)$$
$$367 = 17 \cdot 8 + 21 \cdot 11 = \mathbf{136} + \mathbf{231}$$

Ismétlés: Néhány klasszikus feladat.

Sun-ce az i.sz. III.-IV. század.

Adott ismeretlen számú tárgy. Ha hármasával leszámoljuk, a maradék 2 lesz, ha ötösével, úgy a maradék 3, míg ha hetesével, akkor a maradék 2. Hány tárgy van?

Ókori v. kora középkori kínai feladat.

Egy 17 tagú kalózcsapat egy zsák aranypénzt rabolt. Amikor megpróbálták egyenlő arányban elosztani a zsákmányt 3 érme kimaradt. E maradékon összevesztek, aminek során egy kalózt társai megöltek. Újraosztották egyenlő arányban a zsákmányt, de most 10 érme maradt ki. Ezen ismét összecsaptak, aminek végén ismét megölték egy társukat. Ekkor azonban már a hátramaradottak el tudták osztani a zsákmányt egyenlő arányban egymás között. Mennyi lehetett a zsákmányolt aranypénzek legkisebb száma?

Megoldások: Sun ce feladata

- Megoldandó a

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

  lineáris kongruenciarendszer.
- Az első kongruenciából $x = 2 + 3t,\ t \in \mathbb{Z}$, a másodikba helyettesítve $t = 2 + 5u$, így $x = 8 + 3 \cdot 5u$, ahol $u \in \mathbb{Z}$.
- Ezt a harmadikba helyettesítve $8 + 15u \equiv 2 \pmod 7$, amiből $u \equiv 1 \pmod 7$, így $x = 8 + 15(1 + 7v) = 23 + 105v,\ v \in \mathbb{Z}$.
- A megoldás tehát $x \equiv 23 \pmod{105}$.

Megoldások: a kalózok problémája.

- Megoldandó az

$$x \equiv 3 \pmod{17}$$
$$x \equiv 10 \pmod{16}$$
$$x \equiv 0 \pmod{15}$$

  lineáris kongruenciarendszer.
- Az előbbihez hasonlóan számolva: $t, u, v \in \mathbb{Z}$, $x = 3 + 17t,\ 3 + 17t \equiv 10 \pmod{16}$.
- Ebből $t \equiv 7 \pmod{16}$, azaz $x = 3 + 17(7 + 16u) = 122 + 272u$.
- $122 + 272u \equiv 0 \pmod{15}$, miből $u \equiv 14 \pmod{15}$.
- Végül: $x \equiv 3930 \pmod{4080}$, azaz az aranyak minimális száma 3930.

Ismétlés: Még egy klasszikus feladat.

Brahmagupta i.sz. VII.sz.

Ha egy kosárból a tojásokat kettesével, hármasával, négyesével, ötösével, vagy hatosával szedjük ki mindig marad egy tojás a kosárban. Ha azonban hetesével szedjük ki, egy sem marad benne. Keressük meg a kosárban levő tojások legkisebb számát.

Feladat: kongruenciák alkalmazásai.

Egy hatvány maradéka.

1. Feladat.
Mi a maradék, ha a 247^{244}-et elosztjuk 23-mal?

$247 \equiv 17 \equiv -6 \pmod{23}$, $247^{244} \equiv (-6)^{244} = 6^{244} \pmod{23}$.

Euler tétele alapján: $247^{22} \equiv 1 \pmod{23}$, $244 = 22 \cdot 11 + 2$,

$247^{244} = (247^{22})^{11} \cdot 247^2 \equiv 247^2 \equiv 6^2 = 36 \pmod{23}$.

$36 \equiv 13 \pmod{23}$, ez a keresett maradék.

Számelméleti függvények.

Definíció.

Az $\mathbb{N} \to \mathbb{C}$ leképezéseket **számelméleti függvényeknek** nevezzük.
Megjegyzés. E kurzusban csak olyan számelméleti függvényekkel foglalkozunk, amelyek értékkészlete az egész számok halmazának egy részhalmaza.

Példák.

(1) $\sigma(n) = n$ pozitív osztói száma,
(2) $\tau(n) = n$ pozitív osztói összege.
(3) $\varphi(n) =$ az n-nél nem nagyobb n-hez relatív prím természetes számok száma. **Euler-féle φ függvény**.

Állítás.

Legyen $m > 1$ egész. A $\mathbb{Z}_m$ maradékosztálygyűrű egységeinek (invertálható elemeinek) száma éppen $\varphi(m)$.

Egy fontos tulajdonság.

Definíció.

Azt mondjuk, hogy az f számelméleti függvény **gyengén multiplikatív**, ha tetszőleges $a, b \in \mathbb{N}$-re $f(ab) = f(a)f(b)$, valahányszor ln. k. o.$(a, b) = 1$.

Tétel.

Az Euler-féle φ függvény gyengén multiplikatív.

Fontos észrevétel.

A gyengén multiplikatív számelméleti függvények értékét elég prímhatványokra tudni/meghatározni.

Egy feladat.

Egy természetes számról annyit tudunk, hogy két prímosztója van, osztóinak száma 6 és osztóinak összege 39. Melyik ez a szám?

- Legyen $n = p^k \cdot q^l$, p, q prímek.
- $$(k+1)(l+1) = 6$$
$$\frac{p^{k+1}-1}{p-1} \cdot \frac{q^{l+1}-1}{q-1} = 39$$
- Az első egyenletből $k = 1$, $l = 2$, a másodikból $(p+1)(q^2+q+1) = 39$.
- Mivel $p > 1$, csak $p = 2$, $q = 3$ lehetséges,
- így a keresett szám a 18.
- Ezek alapján miért nem oldható meg a 49. feladat?

Maradékrendszerek.

Definíció.

Legyen $m > 1$ egész. Azt mondjuk, hogy az $a_1, \ldots, a_m$ egészek **modulo** m **teljes maradékrendszert** alkotnak, ha páronként inkongruensek modulo m. Az $a_1, \ldots, a_{\varphi(m)}$ egészek **modulo** m **redukált maradékrendszert** alkotnak, ha páronként inkongruensek modulo m, és mindegyikük relatív prím m-hez.

Tétel.

Legyen $m > 1$ egész. Ha $a_1, \ldots, a_m$ teljes maradékrendszer modulo m, akkor
(1) $a_1 + b, \ldots, a_m + b$ is teljes maradékrendszer modulo m tetszőleges $b \in \mathbb{Z}$-re,
(2) $ca_1, \ldots, ca_m$ szintén teljes maradékrendszer modulo m minden olyan c egészre, amelyre $\ln.\,k.\,o.(c, m) = 1$.

Maradékrendszerek és alkalmazásaik.

Tétel.

Legyen $m > 1$ egész, és $r_1, \ldots, r_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Ha az a egész relatív prím m-hez, akkor $ar_1, \ldots, ar_{\varphi(m)}$ szintén egy redukált maradékrendszer modulo m.

Euler-Fermat tétel.

Legyen $a, m \in \mathbb{Z},\ m > 1$. Ha $\ln.\,k.\,o.(a, m) = 1$, akkor

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Következmény, Fermat tétele.

Legyen p prímszám. Ha az $a \in \mathbb{Z}$ nem osztható p-vel. akkor

$$a^{p-1} \equiv 1 \pmod{p}.$$

Továbbá, bármely $a \in \mathbb{Z}$-re $a^p \equiv a \pmod{p}$.

Feladat.

Határozza meg 3^{279} utolsó két számjegyét a tizes számrendszerben.

Azt a kétjegyű x számot kell meghatározni, amelyre $x \equiv 3^{279} \pmod{100}$.

Az Euler-Fermat tételt alkalmazzuk.

$\varphi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$, és így $3^{40 \cdot 7} \equiv 1 \pmod{100}$

Így a $3x \equiv 1 \pmod{100}$ kongruencia legkisebb megoldása adja a keresett kétjegyű számot: $\mathbf{x = 67}$.

Fermat tételének egy egyszerű általánosítása.

Legyen p prímszám. Tetszőleges $a \in \mathbb{Z}$-re $a^p \equiv a \pmod{p}$.

Természetes kérdések.

Igaz-e az előbbi tétel megfordítása. Nevezetesen, ha valamely $a \in \mathbb{Z}$-re $a^{m-1} \equiv 1 \pmod{m}$ valamely $m > 1$ egészre, akkor m prímszám? Illetve, ha az előbbi kongruencia nem teljesül valamely $a \in \mathbb{Z}$-re, akkor m összetett?

Egy számpélda a második kérdésre.

Legyen $a = 2,\ m = 117$.

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} 2^5$$
$$2^7 = 128 \equiv 11 \pmod{117}$$

További számolások.

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$
$$2^{21} = (2^7)^3$$
$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 = 44 \pmod{117}$$
$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

A 117 valóban összetett,

$$117 = 13 \cdot 9.$$

Válasz a kérdésekre 1.

Egy technikai lemma.

Ha a p, q különböző prímszámokra teljesül, hogy $a^p \equiv a \pmod{q}$ és $a^q \equiv a \pmod{p}$, akkor $a^{pq} \equiv a \pmod{pq}$.

Bizonyítás.

Egyrészt Fermat tétele szerint $(a^q)^p \equiv a^q \pmod{p}$, másrészt $a^q \equiv a \pmod{p}$ föltételünk szerint. A két kongruenciából $a^{pq} \equiv a \pmod{p}$, azaz $p | a^{pq} - a$. A $q | a^{pq} - a$ reláció is ugyanígy kapható. Mivel p, q különböző prímek, ezért $pq | a^{pq} - a$, amit igazolni kellett.

Válasz a kérdésekre 2.

Az előbbi lemma alapján $2^{340} \equiv 1 \pmod{341}$, ugyanis egyrészt
$321 = 11 \cdot 31$, másrészt
$2^{11} \equiv 2 \pmod{31}$ és $2^{31} \equiv 2 \pmod{11}$.
E kettőből $2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$, és így
$2^{340} \equiv 1 \pmod{341}$,
azaz a Fermat tétel megfordítása nem igaz.

Egy történeti érdekesség.

- Kb. 25 évszázaddal ezelőtt kínai matematikusok állították: $n \in \mathbb{N}$ akkor és csak akkor prímszám, ha $n | 2^n - 2$.
- Ezen állítás igaz, ha $n \leq 340$, de $n = 341$-re már nem (1819).
- Azon n összetett számokat, amelyekre $n | 2^n - 2$ *pszeudoprímeknek* nevezzük.
- Azt mondjuk, hogy az n összetett szám *abszolút pszeudoprím*, vagy *Carmichael-szám*, ha bármely $a \in \mathbb{Z}$-re $n | a^n - a$.
- A legkisebb ilyen szám az 561.
- Erdős Pál sejtése szerint végtelen sok Carmichael szám van.

Egy elvi prímteszt: Wilson tétele.

Wilson tétele

Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Megfordítás.

Ha valamely $m > 1$ egészre $(m-1)! + 1 \equiv 0 \pmod{m}$, akkor m prímszám.

Kérdés.

Miért csak elvi jelentőségű prímteszt alapul e tételen?

Feladat.

Milyen maradékot ad 2(26!), ha elosztjuk 29-cel?

- Wilson tétele alapján: $28! \equiv -1 \pmod{29}$.
- Ebből $-2 \equiv 2(26!)27 \cdot 28 \pmod{29}$,
- $27 \cdot 28 \equiv 2 \pmod{29}$,
- így $2(2(26!)) \equiv -2 \pmod{29}$,
- tehát $2(26!) \equiv 28 \pmod{29}$.

Hatványozás modulo m.

Definíció.

Legyen $a, m \in \mathbb{Z},\ m > 1,\ \text{ln. k. o.}(a, m) = 1$. Azt mondjuk, hogy az a egész szám **multiplikatív rendje modulo** m $k \in \mathbb{N}$, ha k a legkisebb olyan pozitív (egész) kitevő, amelyre $a^k \equiv 1 \pmod{m}$. Jelölése: $\text{o}_m(a) = k$.

Tétel.

Legyen $a, m \in \mathbb{Z},\ m > 1,\ \text{ln. k. o.}(a, m) = 1$, továbbá $\text{o}_m(a) = k$. Ha valamely $n \in \mathbb{N}$-re $a^n \equiv 1 \pmod{m}$, akkor $k | n$.

Állítás.

Legyen $a, m \in \mathbb{Z},\ m > 1$, és $k_1, k_2 \in \mathbb{N}$. Ekkor

$$a^{k_1} \equiv a^{k_2} \pmod{m} \quad \Leftrightarrow \quad k_1 \equiv k_2 \pmod{\text{o}_m(a)}.$$

Primitív gyök.

Definíció.

Legyen m egynél nagyobb egész szám. Azt mondjuk, hogy a $g \in \mathbb{Z}$ **primitív gyök modulo** m, ha a $g, g^2, \ldots, g^{\varphi(m)}$ egészek redukált maradékrendszert alkotnak modulo m.

Tétel.

Legyen $m > 1$ egész. A $g \in \mathbb{Z}$ egész pontosan akkor primitív gyök modulo m, ha $\text{o}_m(g) = \varphi(g)$.

Tétel.

Valamely $m \in \mathbb{Z}$-hez pontosan akkor létezik primitív gyök modulo m, ha $m = 2, 4, p^m, 2p^m$, ahol p páratlan prím, m pedig természetes szám.

Index.

Definíció

Tegyük föl, hogy g primitív gyök az m modulushoz. Az $\alpha \in \mathbb{Z}$ **indexén** (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{a}$,

Megjegyzések.

1. Világos, hogy ha $\ln.\,k.\,o.(a, m) \neq 1$, akkor $\operatorname{ind}_g a$ nem értelmezett, ugyanis g^i mindig relatív prím m-hez. Ha viszont $\ln.\,k.\,o.(a, m) = 1$, akkor a primitív gyök definíciójából következően a kongruens g valamely hatványával, így az indexe értelmezett.
2. Vegyük észre, hogy az index nem más, mint a logaritmus mod m analogonja (ezért szokás „diszkrét logaritmusnak" is nevezni). Nem meglepő tehát, hogy hasonló tulajdonságokkal rendelkezik.

Index.

Tétel.

Legyen g primitív gyök modulo m,
$a, b \in \mathbb{N}$, $\ln.\,k.\,o.(a, m) = \ln.\,k.\,o.(b, m) = 1$, továbbá k tetszőleges egész szám. Ekkor érvényesek a következő azonosságok.

1. $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$,
2. $\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$,
3. $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$,
4. $\operatorname{ind}_g (ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.