A számítástudomány alapjai 2021. I. félév

11. gyakorlat. Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

Tudnivalók

Def: Ha $a, b, k \in \mathbb{Z}$ és $b = k \cdot a$, akkor a *osztója* b-nek (b *többszöröse* a-nak), jelölése $a \mid b$. Az a és b számok *legnagyobb közös osztója* az a és b közös osztói közül a legnagyobb: $(a, b) := \max\{d : d \mid a, d \mid b\}$, *legkisebb közös többszörösük* pedig az a és b pozitív közös többszörösei közül a legkisebb: $[a, b] := \min\{0 < d : a \mid d, b \mid d\}$. Az a és b egészek *relatív prímek*, ha $(a, b) = 1$.

Példa: $3 \mid -9$, $-1 \mid 2019$, $13 \mid 0$, $0 \mid 0$, $0 \nmid 42$, $(-100, 24) = 4$, $(42, 0) = 42$, $[-15, -25] = 75$.

Megf $(d \mid a, d \mid b) \iff (d \mid a, d \mid b - a)$ **Köv.:** $\{a$ és b közös osztói$\} = \{a$ és $b - a$ közös osztói$\}$.

Köv.: Ha a, b egészek, akkor $(a, b) = (a - b, b) = (a - kb, b)$ tetszőleges egész k esetén.

Euklideszi algoritmus Input: $a_0 > a_1 \in \mathbb{Z}$. Output: (a_0, a_1). Működés: Legyen $i = 0, 1, \ldots$-re $a_i = h_{i+1}a_{i+1} + a_{i+2}$, ahol $0 \leq a_{i+2} < a_{i+1}$. Ha $a_{k+1} = 0$, akkor $(a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \ldots = (a_k, 0) = a_k$ a keresett lnko. **Köv.:** : Tetsz. $a, b \in \mathbb{Z}$ esetén $\{a$ és b közös osztói$\} = \{(a, b)$ osztói$\}$.

Def: A $p \in \mathbb{Z}$, $|p| > 1$ szám *felbonthatatlan*, ha csak $1 \cdot p, p \cdot 1, (-1) \cdot (-p)$ és $(-p) \cdot (-1)$ alakban áll elő egészek szorzataként. (Azaz, ha $a \mid p$ és $1 < |a|$, akkor $|a| = |p|$.) A $z \in \mathbb{Z}$ *összetett*, ha $|z| > 1$ és z nem felbonthatatlan. A $p \in \mathbb{Z}$, $|p| > 1$ szám *prím*, ha $p \mid ab$, $a, b \in \mathbb{Z} \Rightarrow p \mid a$ vagy $p \mid b$. (Egészek szorzatát csak úgy oszthatja, ha valamelyik tényezőt osztja.)

Állítás: Tetszőleges 1-nél nagyobb egész szám előáll felbonthatatlan számok szorzataként.

A számelmélet alaptétele: Ha n egész szám és $|n| > 1$, akkor n a tényezők sorrendjétől és előjelétől eltekintve egyért. áll elő felbonthatatlan számok szorzataként.

Köv.: A p szám pontosan akkor felbonthatatlan ha p prím.

Def: Az n *kanonikus alakja* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, ahol a p_i-k prímek, és $1 \leq \alpha_i \in \mathbb{N}$ $\forall i$.

Állítás: Egy $d > 0$ egész pontosan akkor osztója n-nek, ha d kan. alakjában csak n prímosztói szerepelnek, legf az n kan. alakjában szereplő kitevőn. ($n = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow d = \prod_{i=1}^{k} p_i^{\beta_i}$, $0 \leq \beta_i \leq \alpha_i$.)

Köv.: Ha $1 < n$ kan. alakja $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor n poz. osztóinak száma $d(n) = \prod_{i=1}^{k}(\alpha_i + 1)$.

Állítás: Ha $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ és $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ ($\alpha_i = 0$ és $\beta_i = 0$ is lehet), akkor $(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}$, ill. $[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)}$.

Tétel: Végtelen sok prímszám van. Bármely $n \in \mathbb{N}$-re létezik n egymást követő összetett szám.

Nagy prímszámtétel: $\pi(x) \sim \frac{x}{ln(x)}$, azaz $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{ln(x)}} = 1$, ahol $\pi(x)$ az 1 és x közti prímek száma.

Def: $a, b, m \in \mathbb{Z}$ esetén $a \equiv b (\mathrm{mod}\ m)$ (a *kongruens* b *modulo* m, röviden $a \equiv b(m)$), ha $m \mid a - b$.

Megfigyelés: A $\mathbb{Z}$ halmaz előáll m db diszjunkt halmaz uniójaként azzal a tulajdonsággal, hogy két egész pontosan akkor kongruens modulo m, ha ugyanabba a részhalmazba esnek. (Az i-dik ilyen részhalmazba a $\{i + km : k \in \mathbb{Z}\}$ számok tartoznak.) E részhalmazok az m *szerinti maradékosztályok*.

Kongruenciák tulajdonságai: $\forall a, b, c, d, m \in \mathbb{Z}$-re (1) $a \equiv a(m)$, (2) $a \equiv b(m) \Rightarrow b \equiv a(m)$
(3) $a \equiv b(m), b \equiv c(m) \Rightarrow a \equiv c(m)$ (4) $a \equiv b(m)$, $c \equiv d(m) \Rightarrow a + c \equiv b + d(m)$, $ac \equiv bd(m)$
(5) $a \equiv b(m) \iff ac \equiv bc(mc)$ (6) $ad \equiv bd(m) \iff a \equiv b\left(\frac{m}{(m,d)}\right)$

Állítás: Ha $a \equiv b(m)$ (a és b ugyanabból a mod m maradékosztályból valók) akkor $(a, m) = (b, m)$.

Köv.: Ha $(a, m) = 1$, akkor az a maradékosztályának bármely eleme relatív prím a modulushoz.

Def: $\varphi(m)$ az m-hez relatív prím modulo m maradékosztályok száma.

Megfigyelés: Mivel az $1, 2, \ldots, m$ számok különböző modulo m maradékosztályba esnek, ezért $\varphi(m)$ megegyezk az m-hez relatív prím, 1 és m közé eső számok számával.

Tétel: Ha p prím, akkor (1) $\varphi(p) = p - 1$, (2) $\varphi(n) = (p - 1)p^{\alpha - 1}$.
(3) $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$. (4) Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

Euler-Fermat tétel: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1(m)$. **Kis Fermat tétel:** p prím, $a \in \mathbb{Z} \Rightarrow a^p \equiv a(p)$.

Def: *Lineáris kongruencia*: $ax \equiv b(m)$, ahol $a, b \in \mathbb{Z}$ és $m > 1$ egész. A lineáris kongruencia *megoldása* alatt mindazon $x \in \mathbb{Z}$ számok meghatározását értjük, amelyekre a kongruencia teljesül.

Tétel (lineáris kongruenciák megoldása): Az $ax \equiv b(m)$ kongruencia megoldható $\iff$ $(a, m) \mid b$. Ekkor (a, m) db modulo m maradékosztály a megoldás.

Lin. kongruencia gyakorlati megoldása I. módszer: Ügyeskedés. Az $ax \equiv b(m)$ lin kongruenciában az $|a|$-t csökkentjük 1-ig az alábbi ekvivalens az átalakítások segítségével.

(1) a-t vagy a b-t vele m-mel kongruens, alkalmas másik számmal helyettesítjük,
(2) ha $d = (a, b) > 1$, akkor d-vel osztunk (az m modulust pedig (m, d)-vel osztjuk ekkor),
(3) az m **modulushoz relatív prímmel** szorzunk (és a modulust nem bántjuk).
Az átalakítások során a cél az x ismeretlen a együtthatója abszolút értékének csökkentése 1-ig.

II. módszer: az Euklideszi algoritmus mintájára. Az $ax \equiv b(m)$ kongruenciát a triviális $mx \equiv 0(m)$ kongruenciával egy kongruenciarendszerré egészítjük ki. Egy lépésben abból a kongruenciából, ahol nagyobb az x együtthatója kivonjuk a másikat és e különbségre cseréljük a nagyobb együtthatós kongruenciát. Ezt a lépést addig végezzük, amig valamelyik kongruenciában x együtthatója 0 nem lesz. Ha itt a jobb oldalon nem 0 áll, akkor nincs megoldás, különben a másik kongruenciát kell leosztani x együtthatójával.

Gyakorlatok

1. Melyek p prímre lesz (a) $p+10$ és $p+14$ prím? (b) p^2+2 prím? (c) p^2+4 és p^2+6 prím?
2. Igazoljuk, hogy bármely hat egymást követő egész szám szorzata osztható 720-szal.
3. Bizonyítsuk be, hogy minden n pozitív egész egyértelműen írható $n = k^2 \cdot l$ alakban, ahol k és l pozitív egészek, továbbá l egyetlen négyzetszám osztója az 1.(✓)
4. Számítsuk ki a $(372, 504)$ ill. $(612, 834)$ legnagyobb közös osztókat.(✓)
5. Legyen $F_0 = 0, F_1 = 1$, és $n \geq 2$ esetén az n-dik Fibonacci szám $F_n = F_{n-1} + F_{n-2}$. Igazoljuk, hogy F_n és F_{n+1} relatív prímek.
6. Öröm és boldogság: ma van Dzsenifer születésnapja. Ezért matek és földrajz helyett Britnivel, a barátnőjével plázába mentek okostelefont nézni. Kipróbálták a legújabb, facebookon agyonhájpolt, minden eddiginél okosabb születésnapi appot és megállapították, hogy Dzsenifernek feltétlenül vennie kell egy rózsaszín szelfibotot a jóképű eladótól, ugyanis ma (2015-ben) az életkora osztója az aktuális évszámnak. Márpedig az app szerint ilyenkor különösen sok szerencse éri a horoszkópiában kellőképpen jártas beavatottakat. Meg tudjuk-e mondani a fizetős appra történő regisztráció nélkül, hogy legutóbb mikor történt ez meg és hogy legközelebb mikor fog ismét bekövetkezni Dzsenifer életében ez a csodálatos, születésnapi konstelláció?
7. Bizonyítsuk be, hogy bármely öt szomszédos pozítív egész szám között van olyan, amely a másik négyhez relatív prím.
8. Melyik az a legkisebb n pozitív egész szám, amire $3 \nmid n$ és n osztóinak száma $d(n) = 12$?
9. Hány olyan pozitív egész szám van, ami az $n = 2^3 \cdot 7^5 \cdot 11^2$ és $m = 2^5 \cdot 5^3 \cdot 7 \cdot 13$ számok közül legalább egynek osztója?
10. Melyik az a legkisebb pozitív egész, aminek pozitív osztói száma 10-zel osztható?(✓)
11. Hány pozitív osztója van 10!-nak? És $n = \binom{12}{6}$-nak?(✓) (pZH '15)
12. Igazoljuk, hogy tetszőleges n szám 9-es osztási maradéka megegyezik a 10-es számrendszerben felírt alakjában szereplő számjegyei összegének 9-es maradékával.
13. Mi a 8-as oszthatósági szabály 9-es számrendszerben?
14. Igazoljuk, hogy tetszőleges 10-es számrendszerben felírt $a_n a_{n-1} \dots a_1 a_0$ szám 11-es osztási maradéka megegyezik az $a_1 - a_2 + a_3 \dots \pm a_n$ szám 11-es maradékával.
15. Igazoljuk a 7-tel való oszthatóság ellenőrzésére szolgáló alábbi módszer helyességét. Az n szám pontosan akkor osztható 7-tel, ha 7-tel osztható az a szám, amit n tízes számrendszerbeli alakjából úgy kapunk, hogy az utolsó számjegy levágásaval kapott számból levonjuk az utolsó számjegy kétszeresét. Pl. 2002 pontosan akkor osztható 7-tel, ha $200 - 2 \cdot 2 = 196$ osztható 7-tel. Ez pedig igaz, hisz $7 \mid 19 - 2 \cdot 6 = 7$, tehát $7 \mid 2002$.
16. Oldogassunk lineáris kongruenciákat. Pl: (a) $202x \equiv 157(203)$, (b) $309x \equiv 451(617)$
(c)$5x \equiv 13(137)$, (d) $113x \equiv 77(120)$, (e) $11x \equiv 12(18)$,
(f) $14x - 4 \equiv 80(21)$ (g) $49^{49}x \equiv 3(15)$ (h) $3^{80}x \equiv 23(80)$
17. Dzsúlió már régóta gyűjt nagy álmára, hogy volt barátnője, Vanessza mobiltelefonon őrzött arcképét a bicepszére tetováltassa. Legjobb barátja, Rodzser tanácsára, míg össze nem jön az ehhez szükséges 35000 forint, átváltja az ezer forintosokban tartott megtakarítását az egyébként ritkaságszámba menő, Piréziában kiadott euróra, amit a Rodzser által ajánlott Rikárdótól (az ismeretségre tekintettel) szuperkedvezményes 330 Ft-os árfolyamon vesz meg. Miután Rikárdó centekkel nem foglalkozik, Dzsúliónak éppen 140 Ft marad a megtakarításából, amiből Rodzserrel közösen lottószelvényt vesznek azzal, hogy a nyereményt majd felezik. Hány piréz euró boldog birtokosának mondhatja magát Dzsúlió a sikeres tranzakció után?

18. Ura születésnapjára Tűzvirág egy 77 gyönggyel díszített, mangalicabőr tokot varrt Vérbulcsú ivótülkéhez. Annyira elégedett volt az eredménnyel, hogy Vérbulcsú hagyományőrző dorombegyüttesének minden tagját is ugyanilyen tokkal lepte meg, hogy jól mutasson a csapat a tarsolylemezek mellett csüngő tülkökkel amikor fellépnek Dobogókőn a táltosünnep 50 személyes központi jurtájában. Mivel a kínai boltban százasával árulják a gyöngyöket, 7 gyöngy kimaradt. Ezekkel Tűzvirág a hétköznapi pártáját ékesítette. Hányan dorombolnak Vérbulcsú zenekarában? (ZH '15)
19. Melyik az a legnagyobb m modulus, amelyre a $42x \equiv 2015(m)$ lineáris kongruenciának megoldása az $x = 3$? (pZH '15)
20. Hány olyan $m > 1$ egész szám létezik, amelyre a $7x \equiv 7(m)$ kongruenciának megoldása az $x = 7$? (pZH '18)
21. Milyen maradékot ad 59^{99} 101-gyel osztva? (ZH '03)
22. Bb: ha $p > 5$ prím, akkor az $1, 11, 111, \ldots$ számok között végtelen sok többszöröse van! (ZH '01)
23. Bb: $17 | 2002^{2002} + 1$ (ZH '02)
24. Mely n természetes számokra igaz, hogy $\varphi(5n) + \varphi(3n) = 7\varphi(n)$? (ZH '03)