

A számítástudomány alapjai 2015. I. félév

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

Tudnivalók

Tétel: Végtelen sok prímszám van. Avagy: bármely $n \in \mathbb{N}$ -re létezik n -nél nagyobb prím.

Állítás: Minden n -re van legalább n méretű hézag szomszédos prímek között, azaz létezik n egymást követő összetett szám.

Def: Az 1 és x közé eső prímek számát $\pi(x)$ jelöli.

Nagy prímszám tétel: $\lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$, azaz $\pi(x) \sim \frac{x}{\ln x}$.

Csebisev tétel: Minden $1 \leq n$ -re létezik p prím, melyre $n \leq p \leq 2n$. ($\pi(2x) > \pi(x)$ ha $x \geq 1$.)

Dirichlet tétel: Ha $(a, d) = 1$, akkor az $a, a + d, a + 2d, \dots$ számtani sorban ∞ sok prím van.

Állítás: Ha $d \mid a$ akkor $(d \mid b \iff d \mid b - a)$.

Köv.: a és b közös osztói azonosak a és $b - a$ közös osztóival.

Köv.: Ha a, b egészek, akkor $(a, b) = (a, b - a)$. Sőt: tetszőleges k egészre $(a, b) = (a, b - ka)$.

Def: $a = q \cdot b + r$ maradékos osztás, ha $q \in \mathbb{Z}$ a hányados és $0 \leq r < b$ a maradék.

Pl a -17 szám 5 -ös osztási maradéka pl. 3 , de ugyanennyi a -4 -es osztási maradéka is.

Euklideszi algoritmus Input: $a, b \in \mathbb{N}$. Output: (a, b) .

Tfh $a \geq b$. Legyen $a_0 := a, a_1 := b$ és $a_0 = a_1 h_1 + a_2$, ahol $0 \leq a_2 < a_1$ (maradékos osztás). Általában $a_{i-1} = a_i h_i + a_{i+1}$, ahol $0 \leq a_{i+1} < a_i$. Ha $a_{k+1} = 0$, akkor $(a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \dots = (a_k, 0) = a_k$ a keresett ltko.

Köv.: Ha $a, b \in \mathbb{Z}_+$, akkor létezik $k, l \in \mathbb{Z}$, melyre $(a, b) = ka + lb$.

Def: Tetszőleges rögzített $m > 1$ esetén a \mathbb{Z} halmaz előáll m db halmaz diszjunkt uniójaként, az egyes halmazokban azok a számok vannak, amelyek m -mel osztva ugyanannyi maradékot adnak. (Konkrétan az i -dik ilyen részhalmazba a $\{i + km : k \in \mathbb{Z}\}$ számok tartoznak.) E részhalmazok az m szerinti maradékosztályok.

Megfigyelés: a és b ugyanabba az m szerinti maradékosztályba tartoznak $\iff m \mid a - b$.

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

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

Def: $a, b, m \in \mathbb{Z}$ esetén $a \equiv b \pmod{m}$ (a kongruens b modulo m , röviden $a \equiv b(m)$), ha $m \mid a - b$. Két szám tehát pontosan akkor kongruens egymással modulo m , ha ugyanabba az m szerinti maradékosztályba tartoznak, azaz, ha m -mel osztva ugyanannyi maradékot adnak.

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) $ad \equiv bd(m) \Rightarrow a \equiv b \left(\frac{m}{(m,d)} \right)$

Def: Az $\{a_1, a_2, \dots, a_m\} \subset \mathbb{Z}$ halmaz teljes maradékrendszer modulo m (röviden $tmr \pmod{m}$), ha minden \pmod{m} maradékosztályból pontosan egy elemet tartalmaz, azaz $a_i \equiv a_j(m) \Rightarrow i = j$. (Pl. $\{2015, -444, 42, 13, 999\} \pmod{5}$, vagy $\{1, 2, \dots, m\} \pmod{m}$.)

Def: Az $ax \equiv b(m)$ neve *lineáris kongruencia*, ha a, b, m adottak ($m \geq 2$) és x pedig ismeretlen. A lineáris kongruencia megoldásai mindazon egész számok, melyeket x helyébe helyettesítve a kongruenciát igazgá teszik.

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.

Konkrét lineáris kongruenciák gyakorlati megoldása Ha van megoldás, akkor először leosztunk az (a, m) ltko-val, így feltehető, hogy $(a, m) = 1$.

I. módszer: ügyeskedés ekvivalens az átalakítások segítségével. Az $ax \equiv b(m)$ lin kongruenciában

- (1) a -t vagy a b -t vele kongruens, alkalmas másik számmal helyettesítjük,
- (2) ha $d = (a, b) > 1$, akkor osztunk (az m modulust is (m, d) -vel),
- (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 kiegészítjük az $mx \equiv 0(m)$ kongruenciával egy kongruenciarendszerré, és ezt oldjuk meg. 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, amíg valamelyik kongruenciában x együtthatója 1 nem lesz. Az így kapott kongruencia adja a megoldást.

Gyakorlatok

1. Igazoljuk, hogy tetszőleges a, b egészekre $(a, b) = (a, b - a)$ teljesül.
2. Számítsuk ki a $(372, 504)$ ill. $(612, 834)$ legnagyobb közös osztókat.
3. 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.
4. Igazoljuk, hogy az Euklideszi algoritmusban $2a_{i+2} \leq a_i$. Módosítsuk úgy az algoritmust, hogy abban csak az összeadásra és a 2-vel osztásra legyen szükség, maradékos osztásra pedig ne.
5. Igazoljuk, hogy tetszőleges n szám 9-es osztási maradéka megegyezik a 10-es számrendszerben felírt alakjában szereplő számjegyei összegének 9-es maradékával.
6. Mi a 8-as oszthatósági szabály 9-es számrendszerben?
7. 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.
8. 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 levágásával 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 $7 \mid 2002$.
9. Igazoljuk a 23-mal való oszthatóság ellenőrzésére szolgáló alábbi módszer helyességét. Az n szám pontosan akkor osztható 23-mal, ha 23-mal osztható az a szám, amit n tízes számrendszerbeli alakjából úgy kapunk, hogy az utolsó két számjegy levágásával kapott számhoz hozzáadjuk az utolsó két számjegy alkotta szám háromszorosát. Pl. 2024 pontosan akkor osztható 23-mal, ha $20 + 3 \cdot 24 = 92$ osztható 23-mal. Ez igaz, tehát $23 \mid 2024$.
10. Alkossunk gyors módszert az előző feladatok mintájára, amellyel egy szám 17-es oszthatóságát tudjuk eldönteni.
11. 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) $3^{80}x \equiv 23(100)$
12. 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 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 euró boldog birtokosának mondhatja magát Dzsúlió a sikeres tranzakció után?