A számítástudomány alapjai 2014. I. félév

10. 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 $a \mid b$.

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 $p \mid ab, \quad a, b \in \mathbb{N} \Rightarrow p \mid a$ 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: Tetszőleges n egész (melyre $2 \leq |n|$) a tényezők sorrendjétől és esetleges (-1) tényezőktől eltekintve egyértelműen áll elő felbonthatatlan számok szorzataként.

Köv.: Egy p egész szám pontosan akkor felbonthatatlan, ha 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 $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$.

Def: 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 $(a, b) = 1$, azaz nincs közös prímosztójuk (a kanonikus alakjaikban szereplő prímkek különbözők).

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 $(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}$, $[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)}$, valamint $ab = (a, b) \cdot [a, b]$. (Azaz a lnko-t a és b prímosztóit a kisebb hatványon, a lkkt-t pedig ugyanezen prímosztókat a nagyobb hatványon összeszorozva kapjuk meg.)

Köv.: Ha $d \mid a$ és $d \mid b$ közös osztó, akkor $d \mid (a, b)$.

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

Euklideszi algoritmus Input: $a, b \in \mathbb{Z}$. 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 $(a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \ldots = (a_k, 0) = a_k$ a keresett lnko. **Köv.:** Ha $a, b \in \mathbb{Z}_+$, akkor létezik $k, l \in \mathbb{Z}$, melyre $(a, b) = ka + lb$.

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

Csebisev tétel: Minden $0 < n \in \mathbb{N}$-re létezik p prím, melyre $n \leq p \leq 2n$.

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

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. Ma van Dzsenifer születésnapja. Matekórán a tanítónénije szólt, hogy tavaly ilyenkor az életkora osztója volt az az aktuális évszámnak. Hány éves Dzsenifer?
5. Bizonyítsuk be, hogy bármely öt szomszédos pozítív egész szám között van olyan, amely a másik négyhez relatív prím.
6. Melyik az a legkisebb n pozitív egész szám, amire $3 \nmid n$ és n osztóinak száma $d(n) = 12$?
7. Legyen $k \geq 2$ és jelölje $(a_1, a_2, \ldots, a_k)$ az $a_1, a_2, \ldots, a_k$ számok legnagyobb közös osztóját, $[a_1, a_2, \ldots, a_k]$ pedig az $a_1, a_2, \ldots, a_k$ számok legkisebb közös többszörösét. Mutassuk meg, hogy $(a_1, a_2, \ldots, a_k) \cdot [a_1, a_2, \ldots, a_k] = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ akkor és csak akkor áll fönn minden pozitív egészekbol álló szám k-asra, ha $k = 2$. (ZH '02)
8. Legyen n olyan páratlan egész szám, amelyik egyetlen prím négyzetével sem osztható. Bizonyítsuk be, hogy n pozitív osztóinak átlaga egész. (ZH '03)
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. Legyen az n pozitív egész szám prímtényezős felbontása $n = \Pi_{i=1}^{k} p_i^{\alpha_i}$. Mennyi a $\sum_{d \mid n} \frac{1}{d}$ érték, vagyis hogyan számítható ki az n szám osztói reciprokának az összege? (V '99)
11. Melyik az a legkisebb pozitív egész, aminek pozitív osztói száma 10-zel osztható?
12. Számítsuk ki a $(372, 504)$ ill. $(612, 834)$ legnagyobb közös osztókat.
13. 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.
14. Igazoljuk, hogy az Euklideszi algoritmusban $2a_{i+2} \leq a_i$. Módosítsuk úgy az algoritmust, hogy abban csak az összeadásra és a 2-vel oszásra legyen szükség, maradékos osztásra pedig ne.