KOMPUTER ALGEBRA

Számelméleti alapok

Definíció. Azt mondjuk, hogy a b szám *osztható* a nemnulla a számmal, ha van olyan x szám, melyre $b = ax$.

Jelölések: $a|b$, $a \nmid b$

Tétel.

1. $a|b$-ből következik $a|bc$ minden egész c esetén;

2. $a|b$ és $b|c$-ből következik $a|c$;

3. $a|b$ és $a|c$-ből következik, hogy

   $$a|(bx + cy)$$

   minden egész x, y esetén

4. ha $m \neq 0$, akkor $a|b$ és $ma|mb$ ekvivalensek

Tétel. (A maradékos osztás tétele)

Teszőleges $a > 0$ és b egész számokhoz létezik olyan, egyértelműen meghatározott q és r egész szám, amelyekre

$$b = aq + r, \quad 0 \leq r < a.$$

Bizonyítás. Tekintsük a

$$\ldots, (b-2a), (b-a), b, (b+a), (b+2a), \ldots$$

sorozatot. A legkisebb nem negatív tagot jelöljük r-el, így $r = b - qa$. Egyértelműség bizonyítása indirekt úton.

Definíció. Ha b és c közül legalább az egyik nem 0, akkor közös osztóik legnagyobbikát b és c *legnagyobb közös osztójának* nevezzük és (b, c)-vel jelöljük.

Tétel. Ha g a b és c számok legnagyobb közös osztója, akkor létezik olyan x_0 és y_0 egész úgy, hogy

$$g = (b, c) = bx_0 + cy_0.$$

Tétel. A b és c számok g legnagyobb közös osztója jellemezhető a következő két módon:

1. a $bx + cy$ alak legkisebb pozitív értéke, ahol x és y végigfut az egész számokon;

2. b és c közös osztója, amely b és c minden közös osztójával osztható.

Tétel. Minden pozitív m számra

$$(ma, mb) = m(a, b).$$

Tétel. Ha $d|a$ és $d|b$ és $d > 0$, akkor

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

Ha $(a, b) = g$, akkor

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

Definíció. Azt mondjuk, hogy a és b *relatív prímek*, ha $(a, b) = 1$.

Tétel. Minden x esetén

$$(a, b) = (a, b + ax).$$

Tétel.(Euklideszi algoritmus)

Adott b és $c > 0$ egészekre ismételten alkalmazzuk a maradékos osztás tételét, s ezzel az egyenletek következő sorozatát kapjuk:

$$b = cq_1 + r_1, \quad 0 < r_1 < c,$$

$$c = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{j-2} = r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1},$$

$$r_{j-1} = r_jq_{j+1}.$$

A b és c számok (b, c) legnagyobb közös osztója r_j, az osztási eljárás utolsó nemnulla maradéka.

Definíció. A $p > 1$ egész számot *prímszámnak* nevezzük, ha p-nek nincs olyan d osztója, melyre $1 < d < p$. Ha az a egész nem prím, akkor *összetett számnak nevezzük*

Tétel. (A számelmélet alaptétele) Bármely $n > 1$ egész szám felbontása prímek szorzatára egyértelmű, eltekintve az egységfaktortól és a prímek sorrendjétől. (Gauss 1801.)

Megjegyzések a faktorizációról

$$n = fa, \qquad f \leq a$$

$$a = \frac{n}{f} \Rightarrow f \leq \frac{n}{f} \Rightarrow f^2 < n$$

$$f < \sqrt{n}$$

100 jegyű szám esetén

$$n > 10^{100} \Rightarrow \sqrt{n} > 10^{50}$$

Ha 10^{10} lépés végez a számítógép másodpercenként, akkor 10^{40} másodperc, kb. 10^{31} év szükséges. Az univerzum életkora kb. $2 \cdot 10^{11}$ év.

Tétel. (Euklidész) A prímszámok száma végtelen.

Tétel. A prímek sorozatában tetszőleges nagy hézag van, másszóval tetszőleges k egész számhoz létezik k egymásutáni összetett szám.

Definíció. Jelölje $\pi(x)$ minden valós x-re az x-nél nem nagyobb prímszámok számát.

(Riemann 1859.)

Tétel. (Csebisev) Létezik olyan a és b pozitív állandó, hogy

$$a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}.$$

Megjegyzés.

$$\frac{\sqrt{x}}{\pi(x)} < \frac{\log x}{a\sqrt{x}}$$

$$\frac{\pi(x)}{x} < \frac{b}{\log x}$$

Tétel.(Prímszámtétel 1896.)

$$\lim_{n\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

Megjegyzés. Hadamard, de la Vallée-Poussin

Tétel. Minden p prímszám előállítható négy négyzetszám összegeként.

Tétel. Adott egy $f(x)$ egész együtthatós polinom, végtelen sok pozitív m létezik, amelyre $f(m)$ összetett.

Definíció. Az $M(n) = 2^n - 1$ alakú számokat, ahol n nem negatív egész *Mersenne számoknak* nevezzük.

(M. Mersenne (1588–1648)

Megjegyzés.

(a) Tökéletes számok ($2 \cdot 6 = 1 + 2 + 3 + 6$)

Euklidesz, $2^{n-1}(2^n - 1)$ tökéletes szám, ha $2^n - 1$ prím.

(b) $M(n)$ prím, ha $n = 2, 3, 5, 7, 13, 17, 19, \ldots$, de $M(11) = 2047 = 23 \cdot 89$

(c) Ha r osztja n-et, akkor $M(r)$ osztja $M(n)$-t.

(d) $M(3\,021\,377)$ prím, 1 819 050 jegyű (1998)

Definíció. Az $F(n) = 2^{2^n} + 1$ alakú számokat, ahol n nem negatív egész *Fermat számoknak* nevezzük.

(P. Fermat 1601–1665)

Megjegyzés.

(a) $F(5)$ összetett szám.

(b) Létezik-e végtelen sok Mersenne prím, Fermat prím, páratlan tökéletes szám?

(c) Legyen $f(x) = x^2 + 1$ határozzuk meg, hogy mely x-ek esetén állít elő prímeket.