1. Számelméleti függvények

Multiplikatív számelméleti függvény

Definíció (FGy6.1.1, 6.1.2, 6.1.3)
Számelméleti függvény: a pozitív egészeken értelmezett, komplex értékű f függvény. Az f *totálisan multiplikatív*, ha minden a, b-re $f(ab) = f(a)f(b)$.
Multiplikatív, ha ezt csak $(a, b) = 1$ esetén tesszük föl.

Az Euler-függvényről beláttuk, hogy multiplikatív (FGy2.3.1).
Az osztók számát megadó $d(n)$ függvény is multiplikatív.
Valóban, ha $(a, b) = 1$, akkor a kanonikus alakjuk felírható így: $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ és $b = q_1^{\beta_1} \dots q_m^{\beta_m}$, ahol mindegyik p_i különbözik mindegyik q_j-től. Így ab kanonikus alakja $p_1^{\alpha_1} \dots p_n^{\alpha_n} q_1^{\beta_1} \dots q_m^{\beta_m}$.
A $d(n)$ már igazolt képletét használva (FGy1.6.3): $d(a) = (\alpha_1+1) \dots (\alpha_n+1)$ és $d(b) = (\beta_1+1) \dots (\beta_m+1)$, végül $d(ab) = (\alpha_1+1) \dots (\alpha_n+1)(\beta_1+1) \dots (\beta_n+1)$.
Láthatjuk, hogy tényleg $d(ab) = d(a)d(b)$. □

Az osztók összege

Tétel (FGy6.2.2, 6.2.8)
Jelölje $\sigma(n)$ az $n \geq 1$ pozitív osztóinak az összegét. Ha n kanonikus alakja $p_1^{\alpha_1} \dots p_r^{\alpha_r}$, akkor $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$. A $\sigma(n)$ függvény multiplikatív.

Tanultuk, hogy n osztói egyértelműen írhatók $p_1^{\beta_1} \dots p_r^{\beta_r}$ alakba,
ahol $0 \leq \beta_i \leq \alpha_i$ minden $1 \leq i \leq r$ esetén. Ezeknek az összege
$\prod_{i=1}^{r}(1 + p_i + p_i^2 + \dots + p_i^{\alpha_i})$ (ellenőrizzük r = 2-re).
A mértani sor összegképletét alkalmazva beláttuk az állítást.
A multiplikativitás bizonyítása $d(n)$-éhez hasonló. □

HF: Mutassuk meg, hogy ha $(a, b) = 1$, akkor ab minden (pozitív) osztója egyértelműen írható cd alakban, ahol $c \mid a$ és $b \mid d$. Vezessük le ebből is, hogy $d(n)$ és $\sigma(n)$ multiplikatív.

Tökéletes számok

Definíció (FGy6.3.1)
Az $n > 0$ egész *tökéletes szám*, ha n önmagától különböző (azaz valódi) osztóinak összege maga a szám. Képletben: $\sigma(n) = 2n$.

Tétel (FGy6.3.2)
Az n pontosan akkor *páros* tökéletes szám, ha $n = 2^{p-1}(2^p - 1)$ alakban írható, ahol p is, $2^p - 1$ is prím. (Pl. 6, 28, 496, 8128.)

Belátjuk, hogy ha $2^m - 1$ prím, akkor m is az. Valóban, ha $m = ab$, akkor $2^{ab} - 1 = (2^a)^b - 1$ osztható $2^a - 1$-gyel. Ezért vagy $2^a - 1 = 1$, és így $a = 1$, vagy $2^a - 1 = 2^{ab} - 1$ és akkor $b = 1$. □

A $2^p - 1$ alakú prímeket *Mersenne-prímeknek* nevezzük (FGy5.2). Nem ismert, hogy van-e végtelen sok ilyen prím. A legnagyobb *ismert* prímek Mersenne-prímek, mert viszonylag gyors ellenőrizni, hogy $2^p - 1$ prím-e (Lucas-Lehmer teszt, FGy5.2.4).

A tökéletes számokról szóló tétel bizonyítása

HF ellenőrizni, hogy az ilyen alakú számok tényleg tökéletesek.
Megfordítva, legyen $n = 2^k t$ páros tökéletes, ahol t már páratlan.
Mivel n páros, $k > 0$. A σ függvény multiplikatív, és $(2^k, t) = 1$,
ezért $\sigma(n) = \sigma(2^k)\sigma(t) = (2^{k+1} - 1)\sigma(t)$. Másrészt n tökéletes,
így ez $\sigma(n) = 2n = 2^{k+1}t$. Vagyis $2^{k+1}t = (2^{k+1} - 1)\sigma(t)$.
Átrendezve $(2^{k+1} - 1)\big(\sigma(t) - t\big) = t$.

Itt $2^{k+1} - 1 > 1$, hiszen $k > 0$. Ezért $d = \big(\sigma(t) - t\big) < t$ valódi osztója t-nek. De $d + t = \sigma(t)$, így t-nek nincs több osztója. Ez csak úgy lehet, hogy t prím és $d = 1$, vagyis $2^{k+1} - 1 = t$. Láttuk, hogy ekkor $p = k + 1$ is prím. Így végül $n = 2^k(2^{k+1} - 1)$. Ezért a tételben megadott előállítást kapjuk. □

Megoldatlan probléma, hogy van-e páratlan tökéletes szám. Ha van, akkor nagyobb, mint 10^{1500}, és legalább 100 prím szorzata.

Fermat-prímek

Fermat-prímnek nevezzük a $2^m + 1$ alakú prímeket (FGy5.2).

Itt m szükségképpen 2-hatvány.
Valóban, ha nem így lenne, akkor m-nek volna egy páratlan p prímosztója. Ha $m = pd$, akkor az $a+b \mid a^{2k+1}+b^{2k+1}$ oszthatóság miatt $2^d+1 \mid 2^m+1$ állna. □
A $2^{2^k} + 1$ szám prím, ha $0 \le k \le 4$, de $641 \mid 2^{32} + 1$ nem az. Nem tudjuk, van-e több Fermat-prím. Ha van, az legalább $2^{2^{33}} + 1$.
$F_n = 2^{2^n} + 1$ pontosan akkor prím, ha $3^{(F_n-1)/2} \equiv -1$ (F_n) (Pepin-teszt, FGy5.2.2). Pl. $3^{2^3} \equiv 81^2 \equiv (-4)^2 \equiv -1$ (17).

Gauss tétele (K6.8.11)
Szabályos n-szög akkor és csak akkor szerkeszthető körzővel és vonalzóval, ha $\varphi(n)$ 2-hatvány, azaz ha n előáll egy 2-hatvány, és páronként különböző Fermat-prímek szorzataként.

HF: Lássuk be, hogy ha $\varphi(n)$ 2-hatvány, akkor n ilyen alakú.

2. Prímtesztek

Álprímek
Számok szorzatra bontására nem tudunk gyors algoritmust. Hogyan dönthető el mégis, hogy egy szám prímszám-e?
A kis-Fermat-tételből adódik az alábbi teszt.

Ha $n > 2$ és $2^{n-1} \not\equiv 1$ (n), akkor n összetett.

Definíció (FGy5.7)
Az n szám *álprím* (vagy *pszeudoprím*), ha $2^{n-1} \equiv 1\ (n)$, de n mégis összetett.

A 2000-nél kisebbek: $341, 561, 645, 1105, 1387, 1729, 1905$. Az álprímek száma elhanyagolható a prímek számához képest. Pl. 10^{10}-ig csak 14887 álprím van, míg prímszámból több, mint 455 millió. Ezért ha $2^{n-1} \equiv 1\ (n)$, akkor n *nagy valószínűséggel* összetett (nem determinisztikus teszt).

Ismételt négyzetre emelés
Hogyan tudjuk 2^{n-1} maradékát kiszámítani mod n? Mindig szorzunk 2-vel, és redukálunk mod n. Ha a kitevő 2^k, akkor gyorsabb k-szor négyzetre emelni. Ötlet: írjuk fel a kitevőt 2-es számrendszerben.

Példa
Legyen $n = 341$, a 340 a kettes számrendszerben 101010100.
Azaz $340 = 2^2 + 2^4 + 2^6 + 2^8$. Ezért $2^{340} = 2^{2^2} \cdot 2^{2^4} \cdot 2^{2^6} \cdot 2^{2^8}$.

Ismételt négyzetre emeléssel $2^{2^2} = 16$, $2^{2^3} = 16^2 = 256$,
$2^{2^4} = 256^2 \equiv 64\ (341)$, $2^{2^5} \equiv 64^2 \equiv 4\ (341)$,
$2^{2^6} \equiv 4^2 = 16\ (341)$, $2^{2^7} \equiv 16^2 = 256\ (341)$,
$2^{2^8} \equiv 256^2 \equiv 64\ (341)$.
Összeszorozva $2^{340} \equiv 16 \cdot 64 \cdot 16 \cdot 64 \equiv 1\ (341)$.
Mivel $341 = 11 \cdot 31$, ezért 341 tényleg álprím.
Megjegyezzük, hogy 2 hatványai 10-esével periodikusak mod 341.

Determinisztikus prímteszt

Miller-Lenstra-Rabin teszt (FGy5.7.5)
Legyen $n > 1$ páratlan, és $n - 1 = 2^k r$, ahol r páratlan.
Az a^r, a^{2r}, a^{4r}, $\ldots$, $a^{2^{k-1}r} = a^{(n-1)/2}$ *jó sorozat*,
ha $a^r \equiv 1\ (n)$, vagy ha valamelyik tag -1-gyel kongruens mod n.
Ha n prím, akkor $n \nmid a$ esetén jó sorozatot kapunk. Ha n összetett, akkor a sorozatoknak legfeljebb a fele lesz jó, midőn a egy teljes maradékrendszert fut be mod n.

Ha $n = 341$, akkor $340 = 2^2 \cdot 85$, tehát ha $b = a^{85}$, akkor a b és b^2 számokat kell vizsgálni mod 341. A 341-et már $a = 2$ „lebuktatja” (azaz mutatja, hogy nem prím): ismételt négyzetre emeléssel $b = 2^{85} \equiv 32\ (341)$, azaz nem 1, viszont $b^2 \equiv 1\ (341)$, tehát a sorozatban a -1 nem szerepel.
Magyarázat: $b^2 \equiv 1\ (341)$ miatt $341 \mid b^2 - 1 = (b+1)(b-1)$, azaz $341 \mid 33 \cdot 31$, valójában $341 = 11 \cdot 31$.

3. Az RSA titkosírás

Nyilvános kulcsú titkosírás
Titkosírás: Egy u üzenet helyett a kódolt változatát, $c(u)$-t küldjük.
Dekódolás: Egy d függvény, amelyre $d\big(c(u)\big) = u$.
A c függvény nyilvános, de d kiszámítására nincs gyors algoritmus.
Rivest–Shamir–Adleman: Használjuk ki, hogy számok prímtényezőkre bontására nem ismerünk gyors algoritmust.
Az üzenet a 0, 1, …, $N-1$ számok egyike, N nyilvános.

Kódolás (RSA séma)
$c(u) = u^t$ maradéka N-nel osztva. A t kitevő nyilvános.

Dekódolás
$d(v) = v^s$ maradéka N-nel osztva. Az s kitevő titkos.

Azt szeretnénk, hogy $u^{ts} \equiv u\ (N)$ teljesüljön minden u-ra, de s-et nehéz legyen kiszámítani N-ből és t-ből.

A kulcsok konstrukciója

A kis Fermat-tétel általánosítása
Tegyük fel, hogy N minden prímosztója különböző (azaz N *négyzetmentes*, nincs 1-nél nagyobb négyzetszám osztója). Ekkor $u^{k\varphi(N)+1} \equiv u\ (N)$ teljesül minden k egészre.

Elég belátni, hogy ha p prímosztója N-nek, akkor a kongruencia fennáll mod p (mert ezek páronként relatív prímek, és szorzatuk N).
Ha $N = pM$, akkor $\varphi(N) = \varphi(p)\varphi(M) = (p-1)\varphi(M)$. Ezért ha $p \nmid u$, akkor $u^{\varphi(N)} = (u^{\varphi(p)})^{\varphi(M)} \equiv 1^{\varphi(M)} = 1\ (p)$.
Ha $p \mid u$, akkor $u^{k\varphi(N)+1} \equiv u\ (p)$ mindkét oldala 0 mod p. □

FGy5.8.1: Legyen $N = pq$, ahol p és q különböző prímek.
$u^{ts} \equiv u\ (N)$ teljesül, ha $ts = 1 + k\varphi(N)$ (k egész).

Vagyis a kulcs feltöréséhez a $ts - k\varphi(N) = 1$ diofantikus egyenletet kellene megoldani. Ehhez ki kell tudni számítani $\varphi(N)$-et.

Praktikus szempontok
$\varphi(pq) = (p-1)(q-1) = pq - p - q + 1$. Ezért N és $\varphi(N)$ ismeretében p és q is kiszámítható, és így N faktorizálható lenne.

N és t kiválasztása
Nagy prímszámokat lehet találni a prímtesztek segítségével. Ügyelni kell, hogy p és q ne legyen túl közel egymáshoz. $(t, \varphi(N)) = 1$ szükséges s létezéséhez.
Titkos: p, q, $\varphi(N)$ és s.

Ha A és B akar titkosan kommunikálni, akkor mindkettőjüknek van egy nyilvános és egy titkos kulcsa: t_A, s_A, t_B, s_B. Ha A üzen B-nek, akkor a t_B kulccsal kódol, B dekódolja s_B-vel.
Digitális aláírás: A az u üzenetből nyilvános algoritmussal készít egy (viszonylag rövid) $h(u)$ kódot, ezt kódolja s_A-val és elküldi. B ezt A nyilvános t_A kulcsával tudja dekódolni. Mivel u-t már megkapta, tudja ellenőrizni, hogy $h(u)$ az-e, amit kapott. Ha igen, tényleg A a küldő, mert ismernie kellett s_A-t.

4. Összefoglaló

A 13. előadáshoz tartozó vizsgaanyag

Fogalmak
(Totálisan) multiplikatív számelméleti függvény (FGy6.1–3).
Tökéletes szám (FGy6.3.1).
Mersenne- és Fermat-prím (FGy5.2). Álprím (FGy5.7).

Tételek
Az osztók összegének képlete, ez multiplikatív (FGy6.2.2, 6.2.8).
A páros tökéletes számok jellemzése (FGy6.3.2).
$2^{32}+1$ összetett. Pepin-teszt (FGy5.2.2).
Szabályos sokszögek szerkeszthetősége (K6.8.11, NB).
Miller-Lenstra-Rabin teszt (FGy5.7.5, NB).
Az RSA-módszer (FGy5.8.1).