Bsc Algebra és számelmélet gyakorlat

A 13. előadás-diához tartozó feladatsor feladatainak megoldásai

1. Legyen $\Lambda(n) = \log(p)$ ha $n > 1$ egy p prím hatványa, 0 egyébként; $f(n) = 1$ ha $n = 1$ és 0 egyébként; $g(n) = -3\log(n)$; $h(n) = (-1)^{n+1}$. Melyek multiplikatívak/additívak? □

Az f nem additív, mert $2 = f(1) + f(1) \neq f(1+1) = 0$, de totálisan multiplikatív, azaz $f(ab) = f(a)f(b)$ minden $a, b \geq 1$ esetén, hiszen mindkét oldalon 0 áll, kivéve ha $a = b = 1$. A g totálisan additív, de nem multiplikatív, h multiplikatív, de nem totálisan multiplikatív és nem is additív, végül Λ se nem additív, se nem multiplikatív (von Mangoldt-függvény).

2. Van-e olyan f multiplikatív függvény, amely az $f(1) = 1$-et kivéve mindenhol negatív? □

Nincs, ha $f(2)$ és $f(3)$ negatív, akkor $f(6) > 0$.

3. Legyenek $f(n)$ és $g(n)$ nem azonosan nulla multiplikatív függvények. Bizonyítsuk be, hogy $h(n) = f(n) + g(n)$ nem multiplikatív! □

Az 1-nél $f(n) + g(n)$ értéke 2, és 1 vagy 0 kellene, hogy legyen.

4. A török szultán börtönében száz cella van, mindben egy-egy rab senyved. A szultán úgy dönt, hogy néhány rabot szabadon bocsát. Alaphelyzetben minden cella zárva van, a kulcsot csak egyetlen irányba lehet forgatni (egy fordítás kinyit, két fordítás újra bezár). A szultán elküld egy őrt, hogy fordítson egyet minden záron. Aztán elküld egy másikat, hogy fordítson minden másodikon. És így tovább, a századik őr csak a századik ajtó zárján fordít (a rabok nem szöknek meg közben). A századik őr akciója után amelyik cella ajtaja nyitva van, onnan a rab távozhat. Hány rab fog szabadulni, és honnan? □

Az m-edik cella rabja akkor szabadul, ha m osztóinak száma páratlan. Ezek pontosan a négyzetszámok. Ez látszik $d(n)$ képletéből, hiszen $(\alpha_1 + 1)\dots(\alpha_k + 1)$ akkor páratlan, ha mindegyik α_i páros. (*Másik meggondolás:* párosítsuk $d \mid m$-et m/d-vel. Mindenki a párjától különböző, kivéve, ha $d = m/d$, azaz $m = d^2$.) Tehát 10 rab szabadul ki.

5. A 100-nál kisebb számok közül melyiknek van a legtöbb osztója? □

A feladatot „irányított próbálgatással" oldjuk meg. Ha a $\prod p_i^{\alpha_i}$ számban valamelyik p_i-t csökkentjük úgy, hogy a prímek továbbra is különbözők maradjanak, akkor a szám csökken, de az osztók száma nem változik. Ugyanez történik akkor is, ha két prímet megcserélünk úgy, hogy a kisebbik prímhez tartozzon a nagyobb kitevő. Tehát csak azokat a számokat kell megnézni, ahol a prímek sorban $2, 3, 5, \dots$, a kitevők pedig csökkennek. A legnagyobb ilyen 100-nál kisebb számok a következők: $d(2^6) = 7$, $d(2^5 \cdot 3) = 12$, $d(2^3 \cdot 3^2) = 12$, $d(2^2 \cdot 3 \cdot 5) = 12$. Könnyű végiggondolni, hogy csak a felsorolt 100-nál kisebb számoknak van 12 osztója.

6. Igazoljuk, hogy ha p és $2^p - 1$ egyszerre prímszám, akkor $2^{p-1}(2^p - 1)$ tökéletes szám. □

$\sigma\big(2^{p-1}(2^p - 1)\big) = (2^p - 1)(1 + 2^p - 1) = 2 \cdot 2^{p-1}(2^p - 1)$.

7. Igazoljuk, hogy $a, b \geq 1$ esetén $d(ab) \leq d(a)d(b)$, és egyenlőség akkor áll, ha $(a, b) = 1$. □

Írjuk föl közös kanonikus alakban a számokat, ekkor az $(\alpha_i + 1)(\beta_i + 1) \geq (\alpha_i + \beta_i + 1)$ egyenlőtlenséget kell vizsgálni. Ez azzal ekvivalens, hogy $\alpha_i\beta_i \geq 0$. Ez persze mindig igaz, és egyenlőség csak akkor van, ha α_i és β_i valamelyike nulla mindegyik i-re, azaz számok relatív prímek. *Második megoldás, ötlet:* ab minden osztója felírható mn alakban, ahol $m \mid a$ és $n \mid b$. Ez a felírás akkor egyértelmű, ha $(a, b) = 1$. Ilyen (m, n) párból $d(a)d(b)$ van.

8. Igazoljuk, hogy $d(n) \le n/2+1$, továbbá $d(n) \le n/3+2$, stb. Hol végződik a sorozat? □

Az n egyetlen $n/2$-nél nagyobb osztója maga n. Általában, ha $n = md$ és $d > n/k$, akkor $m < k$. Ha k egész, akkor m csak $1, 2, \dots, k-1$ lehet, ezért $d(n) \le n/k + k - 1$. Ezek a kifejezések csökkennek addig, amíg $n > k(k+1)$, utána nőni kezdenek. Az $n/x + x - 1$ függvény minimuma $x = \sqrt{n}$-nél van. De ha k nem egész, akkor m felvehet k-féle értéket is. Ezért ilyenkor csak $d(n) \le n/k + k$ teljesül biztosan. Speciálisan ha $k = \sqrt{n}$, akkor $d(n) \le 2\sqrt{n}$. Pl. ha $n = 6$, akkor $n/2 + 2 - 1 = n/3 + 3 - 1 = 4 = d(6)$ és $2\sqrt{6} \approx 4.9$.

9. Oldjuk meg a $\sigma(x) = x + 3$ egyenletet. □

A feltétel szerint 3-mal egyenlő x valódi osztóinak összege (tehát azoké, amelyek x-től különböznek). Ez csak $1 + 2$ lehet, vagyis $x = 4$ (különben $x/2 > 2$ is valódi osztó lenne).

10. Bizonyítsuk be, hogy ha $n > 2$ egész szám, akkor $\sigma(n) < 2n \log n$. □

Az n osztói n/d alakúak, ahol $1 \le d \le n$. Ezért $\sigma(n) \le n \sum_{d=1}^{n} (1/d) \le n(1 + \log n)$ (ami analízisből ismeretes). Ez nagyon durva becslés, lásd FGy-könyv, 6.4.6-os feladat.

11. Igazoljuk, hogy $d(n) + \varphi(n) \le n + 1$. Mikor van egyenlőség? □

Ha $1 < d \le n$, akkor $d \mid n$ és $(d, n) = 1$ egyszerre nem teljesülhet, ezért igaz az egyenlőtlenség. Ha egyenlőség van, akkor minden d, ami nem relatív prím n-hez, osztója n-nek. Ez igaz, ha $n = 1, 4$, vagy ha n prím. Máskor nem, mert ha p az n legkisebb prímosztója, akkor $n-p$ nem relatív prím n-hez, így $n - p \mid n$. Tehát $n - p \le n/2$, azaz $p \ge n/2$. Ezért $n = 2p$ és $p = 2$.

12. Mely egész számokra teljesül, hogy $\varphi(n^2) = \varphi(n) + 10$? □

Az Euler-függvény képlete miatt $\varphi(n^2) = n\varphi(n)$. Ezért $10 = \varphi(n)(n-1)$. Tehát $n - 1 \mid 10$, azaz $n = 2, 3, 6, 11$. Ezek közül a 6 és 11 megfelelő.

13. Számítsuk ki $k(n) = \sum_{d \mid n} \mu(d) \frac{\sigma(d)}{\varphi(d)}$ értékét expliciten (Möbius-megfordítás, 29. dia). □

Legyen f multiplikatív és $g(n) = \sum_{d \mid n} \mu(d) f(d)$. Ha d nem négyzetmentes, akkor $\mu(d) = 0$. Így $g(n) = g(m)$, ahol m az n „négyzetmentes része", vagyis n prímosztóinak szorzata. Ha viszont d négyzetmentes, akkor $d \mid m$ és $(d, m/d) = 1$, tehát a Möbius-függvény multiplikativitása miatt $\mu(d)\mu(m/d) = \mu(m)$. Mivel $\mu(m/d) = \pm 1$, és így reciproka önmaga, azt kapjuk, hogy $\mu(d) = \mu(m)\mu(m/d)$. Legyen $h(n) = \sum_{d \mid n} \mu(n/d) f(d)$ az f Möbius-megfordítási függvénye, erről tudjuk, hogy multiplikatív. Ekkor tehát $g(n) = g(m) = \mu(m)h(m)$. Ezért g szintén multiplikatív, mert ha $(a, b) = 1$, és a négyzetmentes részük u, illetve v, akkor ab négyzetmentes része uv, és így $g(ab) = g(uv) = \mu(uv)h(uv) = \mu(u)h(u)\mu(v)h(v) = g(u)g(v) = g(a)g(b)$.

Mindezek alapján a feladatbeli $k(n)$ függvény értékét elég prímszámokra kiszámolni, hiszen $k(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = k(p_1) \dots k(p_k)$ (feltéve, hogy mindegyik $\alpha_i \ge 1$). Az eredmény $\prod 2/(1 - p_i)$.

14. Mikor lesz $\sigma(p^4)$ négyzetszám? (A p prím.) □

Tudjuk, hogy $\sigma(p^4) = 1 + p + p^2 + p^3 + p^4$. Ha $p = 2$, akkor ez 31, ami nem négyzetszám. Ha p páratlan, akkor $\left(p^2 + (p \pm 1)/2\right)^2 = p^4 + p^3 \pm p^2 + p^2/4 \pm p/2 + 1/4$. Amikor mínusz van a képletben, akkor ez kisebb, mint $\sigma(p^4)$, mert $(-3/4)p^2 - p/2 + 1/4 < p^2 + p + 1$. Amikor plusz van, akkor nagyobb vagy egyenlő, mert $(5/4)p^2 + p/2 + 1/4 \ge p^2 + p + 1$, átrendezve és 4-gyel szorozva $p(p-2) \ge 3$, ami igaz, mert $p \ge 3$. Egyenlőség csak $p = 3$ esetén lehetséges. Így $\sigma(p^4)$-t két szomszédos négyzetszám közé zártuk, tehát csak $p = 3$-ra lesz négyzetszám.

15. Oldjuk meg a $3x^2+5x-2\equiv 0$ (12) és az $x^3+x+3\equiv 0$ (125) kongruenciákat. □

Az első esetben mod 3 és mod 4 kell vizsgálódni, ezek kis modulusok, a próbálgatás a legcélravezetőbb. A $3x^2+5x-2\equiv 0$ (3) kongruencia valójában elsőfokú, egyetlen gyöke $x\equiv 1$ (3), azaz $x\equiv 1,4,7,10$ (12). Mod 4 az $x\equiv 2,3$ felel meg, és így $x\equiv 7,10$ (12) a megoldás.

A második esetben a Hensel-lemmát alkalmazzuk kétszer. Próbálgatással kapjuk, hogy $x\equiv 1$ az egyetlen megoldás mod 5. Mivel x^3+x+1 deriváltja $3x^2+1$, ami az 1 helyen 5-tel nem osztható, a lemma alkalmazható. Első körben a $-(1+1+3)/5\equiv t(3+1)$ (5) kongruenciát kell t-re megoldani, az eredmény $t\equiv 1$ (5). Ezért $1+1\cdot 5=6$ lesz a megoldás mod 25. Második körben a $-(6^3+6+3)/25\equiv t(3\cdot 6+1)$ (5) kongruenciát kell megoldani. Az eredmény $t\equiv 4$ (5), és ezért a feladat megoldása $6+4\cdot 25=106$ mod 125.

---

16. Tegyük fel, hogy p páratlan prím és $p\nmid a$. Igazoljuk, hogy az $x^2\equiv a$ (p) kongruencia pontosan akkor oldható meg, ha az $x^2\equiv a$ (p^n) kongruencia minden $n\geq 1$-re megoldható. □

Tegyük fel, hogy $x^2\equiv a$ (p) megoldása $\pm b$. A feladat feltevése szerint $p\nmid a$, ezért $b\not\equiv 0$ (p). Mivel p páratlan, az x^2-a deriváltja, azaz $2x$ nem vesz fel nullát a b helyen mod p. Ezért a Hensel-lemma szerint van megoldás modulo p^n is, minden n-re.

17. Igazoljuk, hogy ha $a\equiv 1$ (8), akkor $x^2\equiv a$ (2^n) minden $n\geq 1$-re megoldható. □

Most a Hensel-lemma nem alkalmazható, mert x^2-a deriváltja azonosan nulla mod 2. Nyilván $c_2=c_3=1$ megoldás mod 4 és mod 8. A 27. diasorozat 13-as diáján látható bizonyításhoz hasonlóan „két kitevőnyit" lépünk fölfelé. Illusztráló példa: $a=17$. Ennek megoldása $x\equiv 1$ (16), de mod 32 már nem. Viszont $1+8=9$ megoldás lesz mod 32, mert $9^2\equiv 17$ (32). Általában, ha $c_k^2\equiv a$ (2^k), ahol $k\geq 3$, akkor keressük c_{k+1}-et c_k+t2^{k-1} alakban (a Hensel-lemma bizonyításában c_k+tp^k szerepelt). Ekkor $(c_k+t2^{k-1})^2=c_k^2+c_kt2^k+t^22^{2k-2}$. Mivel $k\geq 3$, ezért $2^{k+1}\mid 2^{2k-2}$. Átrendezve és 2^k-nal osztva $-(c_k^2-a)/2^k\equiv c_kt$ (2). Itt $c_k\equiv 1$ (2) (hiszen $c_k^2\equiv a\equiv 1$ (8).) Ezért van megoldás t-re. Összefoglalva: ha $c_k^2\equiv a$ (2^k) és $k\geq 3$, akkor c_k^2 vagy $(c_k+2^{k-1})^2$ kongruens lesz a-val mod 2^{k+1}.

18. Igazoljuk, hogy ha $n>1$, akkor $\sigma(n)\varphi(n)\leq n^2-1$ és $\sigma(n)+\varphi(n)\geq 2n$. Mikor áll egyenlőség? □

Tegyük fel, hogy $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, ahol mindegyik $\alpha_i\geq 1$. Ekkor σ és φ képlete alapján $\sigma(n)\phi(n)=\prod(p_i^{\alpha_i+1}-1)p_i^{\alpha_i-1}\leq\prod(p_i^{2\alpha_i}-1)$, és itt egyenlőség csak akkor lehet, ha mindegyik $\alpha_i=1$. De $(a-1)(b-1)\leq ab-1$, ha $a,b\geq 1$, és egyenlőség csak $a=b=1$ esetén áll. Így k szerinti indukcióval $\prod(p_i^{2\alpha_i}-1)\leq\prod p_i^{2\alpha_i}-1=n^2-1$, és egyenlőség csak akkor lehetséges, ha egy tényező van. Ezért $\sigma(n)\varphi(n)=n^2-1$ pontosan akkor, ha n prímszám.

A $\sigma(p^\alpha)+\varphi(p^\alpha)=(p^{\alpha+1}-1)/(p-1)+p^{\alpha-1}(p-1)\geq 2p^\alpha$ egyenlőtlenség igaz, mert $p-1$-gyel szorozva és átrendezve ekvivalens azzal, hogy $p^{\alpha-1}\geq 1$. Egyenlőség akkor áll, ha $\alpha=1$. Ha több prímtényezőre akarunk áttérni, akkor meg kell gondolni, hogy ha $(m,\ell)=1$, akkor $\sigma(m)+\varphi(m)\geq 2m$-ből és $\sigma(\ell)+\varphi(\ell)\geq 2\ell$-ből következik-e, hogy $\sigma(m\ell)+\varphi(m\ell)>2m\ell$. Ha $m>1$, akkor $\sigma(m)>m>\varphi(m)$ és hasonlóan, ha $\ell>1$, akkor $\sigma(\ell)>\varphi(\ell)$. Vagyis elég belátni, hogy ha $a>b$ és $c>d$, akkor $ac+bd>(a+b)(c+d)/2$. Ez tényleg teljesül, mert átrendezve $(a-b)(c-d)>0$ adódik. Ha egyenlőség van, azaz ha $\sigma(n)+\varphi(n)=2n$, akkor csak egy prímhatvány-tényező lehet, és ebben is 1 a kitevő, tehát n prímszám.