Mat-tanári szak, első évfolyam, második félév

Második zárthelyi — megoldási útmutató

1. Az euklideszi algoritmussal számolva

$$\begin{aligned} 10 &= (6+3i)(1-i)+(1+3i) \\ 6+3i &= (1+3i)(1-i)+(2+i) \\ 1+3i &= (2+i)\ (1+i)+\ 0 \qquad (3 \text{ pont}). \end{aligned}$$

Ezért a kitüntetett közös osztók a $2+i$ asszociáltjai, vagyis $2+i$, $-1+2i$, $-2-i$ és $1-2i$ (1 pont), végül visszahelyettesítéssel $2+i=(1-2i)(6+3i)+(-1+i)10$.

2. Az indextáblázat készítésekor kiderül, hogy a 2 első 12 hatványa különböző maradékot ad mod 13 (1 pont). A kapott lineáris kongruencia a $100y \equiv 4\ (12)$ (1 pont), ennek megoldásai $1,4,7,10$ mod (12) (3 pont), és így az eredeti kongruencia megoldásai $2,3,10,11$ mod (13) (1 pont). Nem kaphat pontot az, aki az eredeti kongruenciát próbálgatással oldotta meg.

3. A $0,1,\ldots,2x-1$ számok fele, a párosak, nem relatív prímek a $2x$-hez, és így $\varphi(2x)=x-1$ miatt az $1,3,\ldots,2x-1$ számok egy p szám kivételével $2x$-hez relatív prímek. Mivel a páratlan $2x-p$ sem relatív prím $2x$-hez, ezért $2x-p=p$, vagyis $x=p$. Így a p szám (páratlan) prím, hiszen p valódi osztói sem relatív prímek $2x$-hez (5 pont). Megfordítva, ha p páratlan prím, akkor $\varphi(2p)=p-1$ az Euler-függvény képlete miatt (1 pont). **Második megoldás:** Tudjuk, hogy $\varphi(n)$ értéke páros, kivéve ha $n=1,2$ (amik nem adnak megoldást). Ezért $x-1$ páros, vagyis x páratlan. A multiplikativitás miatt $\varphi(2x)=\varphi(2)\varphi(x)=\varphi(x)=x-1$, és ezért x (páratlan) prím (5 pont).

4. Minden b egészre. Mivel $363=3\cdot 11^2$, ezért elég mod 3 és mod 11^2 vizsgálódni. Ha $3 \mid b$, akkor nyilván $3 \mid b^{112}-b^2$. Ha nem, akkor b^2 maradéka 1 hárommal osztva, és ezért b^{112} maradéka is 1 (2 pont). Ha $(b,11^2)=1$, akkor az Euler-Fermat tétel miatt $b^{\varphi(121)}=b^{110}\equiv 1\ (121)$, ezért $b^{112}\equiv b^2\ (121)$ (2 pont). Végül ha $(b,11^2)\neq 1$, akkor $11 \mid b$, és ezért $11^2 \mid b^2 \mid b^{112}-b^2$ (2 pont).

5. A rend definíciója miatt $a^{o_m(a)}\equiv 1\ (m)$. Mivel $n \mid m$, ezért innen $a^{o_m(a)}\equiv 1\ (n)$. De $o_n(a)$ oszt minden kitevőt, amire a-t emelve 1-et kapunk mod n, tehát $o_m(a)$-t is (2 pont). Most legyen a és n rögzített (persze relatív prím), és tegyük fel, hogy $o_n(a)=o_k(a)$ minden olyan $k>0$ egészre, melyre $n \mid k$ és $(a,k)=1$ teljesül. Ekkor a rend definíciója miatt $k \mid a^{o_k(a)}-1=a^{o_n(a)}-1$. De k választható tetszőlegesen nagynak (például $k=n^\ell$ relatív prím az a-hoz). Ez csak úgy lehet, ha $a^{o_n(a)}-1=0$ (2 pont). Ekkor $a=1$, vagy -1. Az $a=1$ minden n-re jó, hiszen az 1 rendje mindig 1 (1 pont). Az $a=-1$ esetben minden $m>2$-re $o_m(-1)=2$, de $o_2(-1)=1$, és így ilyenkor az $n>2$ értékek a jók (1 pont).

6. Igen. Ha $p=5$, akkor $25=16+9$ (1 pont). Tegyük fel, hogy $p\neq 5$. A két négyzetszám tétel miatt $5p=x^2+y^2$ alakban írható, hiszen $5p$-t nem osztja $4k+3$ alakú prím (2 pont). Itt $(x,y)=1$, mert ha lenne közös q prímosztójuk, akkor $q^2 \mid 5p$ teljesülne (3 pont).

Az *általánosítás* a következő: egy pozitív egész szám akkor és csak akkor írható fel két relatív prím négyzetszám összegeként, ha sem néggyel, sem $4k+3$ alakú (pozitív) prímmel nem osztható. Mod 4 vizsgálódva azonnal látható, hogy ha x^2+y^2 osztható néggyel, akkor mindkét tényező páros, és több bizonyítást láttunk arra is, hogy ha egy $4k+3$ alakú p prím osztja x^2+y^2-et, akkor $p \mid x$ és $p \mid y$. Megfordítva, tegyük fel, hogy $n=2^a p_1^{b_1}\ldots p_k^{b_k}$, ahol $p_j\equiv 1\ (4)$ és $a=0$ vagy 1. Legyen $p_j=\pi_j\overline{\pi_j}$, ahol a tényezők Gauss-prímek, és $\alpha=(1+i)^a\pi_1^{b_1}\ldots\pi_k^{b_k}=u+vi$. Ekkor persze $u^2+v^2=\alpha\overline{\alpha}=n$, belátjuk, hogy $(u,v)=1$. Tegyük fel, hogy egy q prím közös osztó. Ekkor $q^2 \mid u^2+v^2=n$, ezért $q\neq 2$, vagyis $q=p_j$ alkalmas j-re. De akkor $\overline{\pi_j} \mid q \mid u+vi=\alpha$, ami ellentmond α választásának, hiszen $\overline{\pi_j}$ Gauss-prím (+12 pont).