Mat-tanári szak, első évfolyam, második félév

Válaszok a vizsgakérdésekre (1998. június 18.)

2. a) $(-i-j+k)/3$ a tanult képlet szerint.

b) Például x nem osztható el maradékosan (a nulladfokú) 2-vel, mert ekkor a maradék csak 0 lehetne, de $x = 2q(x)$ nem teljesül semmilyen $q \in \mathbb{Z}[x]$-re.

c) A $\mathbb{Z}_8$ fölötti $x(x^2-1)$ polinomnak gyöke a 0, 1, 3, 5, 7.

d) Az, hogy tetszőleges T testben abból, hogy $nt = 0$ (ahol $t \in T$ és $0 < n \in \mathbb{Z}$) nem következik, hogy $t = 0$. Itt nem a nullosztómentességről van szó, hiszen nt jelentése: adjuk össze t-t n példányban (lásd a körosztási jegyzetben a 3.8-as kérdést).

3. a) $c(x^2-2x+2)^2(x^2+2x+2)^3$, ahol $0 \neq c \in \mathbb{Q}$.

b) Például x^3+x+1, hiszen ennek nincs gyöke $\mathbb{Z}_5$-ben, és mivel harmadfokú, irreducibilis.

c) Igaz. Ha $fq = g$, ahol $q \in \mathbb{Q}[x]$, akkor a Gauss-Lemma III miatt van olyan $c \in \mathbb{Q}$, hogy cf és q/c is egész együtthatós. Mivel f primitív, c egész szám, és így $q \in \mathbb{Z}[x]$.

d) Négy van. Egy (polinom)függvény a 0 és az 1 helyen is kétféle értéket vehet fel, ez összesen négy lehetőség, és ezeket a 0, 1, x, $x+1$ polinomok megvalósítják.

4. a) Azt kell megnézni, hogy $2^{35} \equiv 1$ (71) igaz-e. A kitevőt kettes számrendszerben felírva $35 = 2^5 + 2 + 1$, tehát ötször kell négyzetre emelni mod 71, majd kétszer szorozni.

b) $n = 32$ és $m = 48$ (vagy fordítva). Ezek ugyanis $\varphi(97) = 96$ maximális osztói, és így g akkor és csak akkor primitív gyök mod 97, ha rendje egyiknek sem osztója, vagyis ha g^{32} és g^{48} nem kongruens 1-gyel (sem nullával) mod 97.

c) Az $x^4 \equiv -1$ (p) kongruencia megoldhatóságát kell vizsgálni. Ez binom kongruencia, tehát a tanult tétel szerint akkor és csak akkor oldható meg, ha $(-1)^{(p-1)/(4,p-1)} \equiv 1$ (p), azaz ha $(p-1)/(4,p-1)$ páros szám, vagyis ha a p prím $8k+1$ alakú.

d) A $k = 1$. Ez jó a titkosírásban használt lemma miatt, hiszen a 46 két prím szorzata, a $k = 0$ pedig nem jó például $a = 2$ esetén.

5. a) Kétféleképpen. Mivel $90000 = 2^4 \cdot 3^2 \cdot 5^4$, ezért a felírás létezik (hiszen a 3 kitevője páros), és a tanult képletből $4 \cdot (4+1) = 20$ jön ki. Maga a 90000 négyzetszám, ezért a 20 lehetőségből 4 esetben a két négyzetszám egyike nulla. A fennmaradó 16 esetben az előjelektől és a sorrendtől kell eltekinteni, azaz 8-cal osztani.

b) Nem, mert a 8 kanonikus alakja $i(1+i)^6$, és az egységtényezőből már négyzetgyök sem vonható.

c) Nem; láttuk, hogy $2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$, de 3 nem osztója $1 \pm i\sqrt{5}$-nek, hiszen az $1/3 \pm i/3\sqrt{5}$ nincs benne a gyűrűben.