**Mat-tanári szak, első évfolyam, második félév**
*Vizsgadolgozat — 1998. június 18.*

Minden kérdéscsoportot **külön lapra** írjunk, és minden lapon legyen rajta a szerző és a gyakorlatvezető neve. Aki felírja az *email címét* is, annak a javító igyekszik mihamarabb az eredményét emailben elküldeni. *Eredményhirdetés:* június 23 (kedd), délelőtt 11, az Algebra Tanszék környékén.

Valamennyi megoldásban **indoklás** (azaz bizonyítás vagy ellenpélda) **szükséges**, a puszta eredményért nem jár pont. A kétpontos kérdésekre a válasz általában mindössze egy-két sor, ami sokszor csak egy hivatkozás egy tételre (ez lehet olyan is, amit az előadáson nem bizonyítottunk) vagy egy definícióra. Ne keressünk hosszú, vagy trükkös megoldásokat. A két pont a teljesen helyes és precíz válaszért jár. Aki hibázik, de a lényeget látja, az egy pontot kap, ha a lényeg hiányzik, nulla pontot.

**A vizsgán az átmenés szükséges és elégséges feltétele:** Lényegében helyesen (azaz apróbb hibáktól eltekintve) le kell írni az első feladatban a bizonyítást, **ÉS** meg kell szerezni a dolgozat összpontszámának felét. Jeles az összpontszám 80 százalékáért jár (ha megvan a bizonyítás is).

**1.** *(10 pont)*
*Mutassuk meg, hogy minden $n > 0$ egészre végtelen sok prímszám van az $nk+1$ sorozatban ($k = 1, 2, \dots$). Bizonyítás nélkül használhatók az elemrendnek, a polinomok deriválásának, valamint a körosztási polinomoknak az alapvető tulajdonságai, az összes többi segédállítást bizonyítani kell.*

**2.** *(2+2+2+2=8 pont)*

a) *Határozzuk meg az $i + j - k$ kvaternió inverzét.*

b) *Adjunk példát olyan konkrét maradékos osztásra, ami $\mathbb{Z}[x]$-ben nem végezhető el (és bizonyítsuk is be, hogy ez nem végezhető el).*

c) *Adjunk példát egy egységelemes, kommutatív gyűrű fölötti olyan harmadfokú polinomra, melynek legalább négy gyöke van.*

d) *Magyarázzuk el, mi az oka annak, hogy a polinomok gyökeinek multiplicitását, és deriváltjuk gyökeinek multiplicitását összekapcsoló, $\mathbb{C}$ fölött bizonyított tétel nem igaz tetszőleges test fölött.*

**3.** *(2+2+2+2=8 pont)*

a) *Adjuk meg az összes olyan tizedfokú, racionális együtthatós polinomot, melynek $i + 1$ kétszeres, $i - 1$ pedig háromszoros gyöke.*

b) *Adjunk meg egy harmadfokú irreducibilis polinomot $\mathbb{Z}_5$ fölött.*

c) *Legyen $f$ egész együtthatós primitív polinom. Igaz-e, hogy tetszőleges $g \in \mathbb{Z}[x]$ esetén, ha $f \mid g$ a $\mathbb{Q}$ fölött, akkor az oszthatóság igaz $\mathbb{Z}$ fölött is?*

d) *Hány különböző polinomfüggvény van $\mathbb{Z}_2$ fölött?*

**4.** *(2+2+2+2=8 pont)*

a) *Hogyan lehet* **gyorsan** *kiszámítani, hogy $o_{71}(2)$ osztója-e 35-nek?*

b) *Adjunk meg olyan $m$ és $n$ egészeket, hogy tetszőleges $g$ egészre, ha $g^n$ és $g^m$ mod 97 értékét ismerjük, akkor ebből már további számolás nélkül el tudjuk dönteni, hogy $g$ primitív gyök-e mod 97.*

c) *Melyek azok a páratlan $p$ prímek, melyekre a $-1$-ből vonható negyedik gyök $\mathbb{Z}_p$-ben?*

d) *Melyik az a legkisebb $k$ nemnegatív egész szám, melyre minden $a \in \mathbb{Z}$ esetén teljesül, hogy $a^{\varphi(46)+k} \equiv a^k \ (46)$?*

**5.** *(2+2+2=6 pont)*

a) *Hányféleképpen írható fel a 90000 két* **pozitív** *egész szám négyzetének összegeként, ha a sorrendet nem vesszük tekintetbe?*

b) *Teljes 6-odik hatvány-e a Gauss-egészek között a 8?*

c) *Prímtulajdonságú-e a 3 az $\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ gyűrűben?*