Mat-tanári szak, első évfolyam, második félév

Részletes vizsgatematika

A vizsgára az előadáson készített jegyzet és a gyakorlatokon szereplő feladatsorok segítségével érdemes készülni (ezeket legalább az államvizsgáig őrizzük meg). A tanulás során haladjunk a konkréttól az absztrakt felé. Például az Euler-Fermat tétel klasszikus számelméleti bizonyítását (ami szerepel a jegyzetekben) vessük össze azzal a bizonyítással, amikor a $\mathbb{Z}_n^\times$ csoportban számolunk (ez a két gondolatmenet lényegében ugyanaz). Ha egy absztrakt fogalmat akarunk megérteni, akkor előbb konkrét eseteket vizsgáljunk, például az egység általános fogalmát akkor láthatjuk át, ha felfedezzük magunknak az azonosságokat és a különbségeket az egész számok, a Gauss-egészek és a polinomgyűrűk egységei között.

Az anyagot sokszor át kell venni. Először a legelemibb módon, a legkonkrétabb esetekben értsük meg a fogalmakat, számolásokat. A későbbi ismétlések során egyre magasabbról láthatjuk az állításokat, egyre mélyebb összefüggéseket fedezhetünk fel. Ezt elősegítendő, az alábbi tematikában nagyon sok hivatkozás szerepel különböző forrásokra, ezeket egymással is érdemes összevetni. A kiosztott, körosztási polinomokról szóló jegyzet is többször olvasandó, tartalmaz olyan részeket is, amikhez a szükséges fogalmakat még nem tanultuk, a másodévet záró szigorlatra készülés során azonban már minden részletét meg lehet érteni.

A nehezebb tételeket úgy tanuljuk, hogy próbáljuk meg az állítást magunk bebizonyítani. A rutinlépéseket megtéve valahol elakadunk: ez a megoldás első ötlete. Miután ezt megtaláltuk a jegyzetünkben, folytassuk a próbálkozást. Amikor a bizonyítás végére értünk, előttünk áll az ötletek listája, elég ezeket megtanulni. Pár nap múlva ismét próbáljuk meg felidézni a bizonyítást, ekkor kibuknak azok a részletek, amiket elsőre nem értettünk meg rendesen. Így megtanuljuk azt is, hogy hogyan kell egy matematika könyvet *önállóan* megemészteni. Mivel a kötelező számelméleti tanulmányokat befejeztük, mostantól mindenki magára van utalva abban, hogy könyvek, feladatgyűjtemények, specik segítségével mélyítse és fejlessze tudását. A saját sorsát nehezíti, és nem is lesz jó tanár az, aki ezt egy életen át, puszta érdeklődésből és élvezetből, nem teszi folyamatosan, több területen is.

A tematikában római számmal a gyakorlaton szerepelt feladatsorokra utalunk. A Kn.k a körosztási polinomokról szóló jegyzetben szereplő n.k állításra hivatkozik. Sz = Szalay: *Számelmélet* (középiskolás tagozatos tankönyv); F = Fuchs: *Algebra*; FBII jelentése Fuchs: *Bevezetés az algebrába és a számelméletbe* II. kötet; Gy = Turán-Gyarmati: *Számelmélet*; ezek egyetemi jegyzetek. Az NB jelentése: a bizonyítást nem kell tudni.

Vizsgaidőpontok: május 29. (péntek), és június 18. (csütörtök) 9-től 1-ig a Gólyavárban. *Konzultációk:* május 28. és június 17. (reggel 9), továbbá igény szerint. A harmadik vizsga időpontját az érintettekkel a második vizsga eredményhirdetésekor egyeztetjük.

Korrekciók, kiegészítések: A körosztási polinomról szóló jegyzetben az 1.10 és 1.11 megoldásában a $\cos 22.5^\circ + i\sin 22.5^\circ$ primitív tizenhatodik egységgyök, és ezért mindenhol az x^8+1 polinommal kell számolni x^4+1 helyett. *Waring problémakör:* $g(k)$ a legkisebb szám, hogy minden pozitív egész előáll ennyi darab k-adik hatvány összegeként, és $G(k)$ a legkisebb szám, hogy **véges sok kivétellel** minden pozitív egész előáll ennyi darab k-adik hatvány összegeként. A Hardy-Littlewood sejtés: ha k kettőnél nagyobb kettő-hatvány, akkor $G(k) = 4k$, egyébként $G(k) \le 2k+1$.

Összesen három oldal!

Absztrakt és konkrét struktúrák. Kétváltozós művelet, asszociativitás, kommutativitás (FI/1.§, VI/10), neutrális elem, inverz, ezek egyértelműsége (FI/2.§, VI/3), szorzat inverze (F1.5). Csoport; kommutatív vagy Abel-csoport (FII/1.§). Gyűrű; kommutatív, egységelemes, nullosztómentes gyűrű; test (FIII/1–3.§). Az R gyűrű additív csoportja R^+, az egységelemes R gyűrű multiplikatív csoportja $R^\times$ (az invertálható elemek a szorzásra nézve, VIII/7). Nullosztómentes gyűrűben szabad egyszerűsíteni (vö. F3.2). Minden test nullosztómentes (vö. F3.3). Hatványozás csoportban (FI/3.§), elemrend, két hatvány mikor egyenlő, a hatvány rendjének képlete (vö. FII/5.§, VIII/8,13).

Összeadás és szorzás mod m; a $\mathbb{Z}_m$ gyűrű akkor és csak akkor nullosztómentes ha test, akkor és csak akkor, ha m prím (VI/7); $\mathbb{Z}_m$ invertálható elemei éppen az m-hez relatív prím elemek; a $\mathbb{Z}_m^\times$ csoport. A mod m maradékképzés művelettartó $\mathbb{Z}$-ből $\mathbb{Z}_m$-be (VI/8, K3.1), és az együtthatókra végezve $\mathbb{Z}[x]$-ből $\mathbb{Z}_m[x]$-be is (K3.2). Ha p prím, akkor $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (K3.3). Következmény: a kis-Fermat tétel (K3.5).

Számelméleti fogalmak egységelemes, kommutatív, nullosztómentes gyűrűben: oszthatóság, egység (VI/2,4), asszociált, felbonthatatlan, prímelem, kitüntetett közös osztó és többszörös, ezek egyértelműsége (FIII/10.§, III/Főfeladat, III/13, VI/6). Euklideszi (X/9,10) és alaptételes gyűrű (X/15,16,18,19). Minden euklideszi gyűrű alaptételes (vö. F3.19, FIII/11.§, III/15, a bizonyítás általában csak jövőre lesz, de test feletti polinomgyűrűben kell tudni). Példa nem alaptételes gyűrűre (Gy450–451, M10.10, FIII/10.§, X/7,8).

A Gauss-egészek gyűrűje (Gy253–257), a norma fogalma és tulajdonságai (IX/3a,b), erre nézve eukideszi gyűrűt kaptunk (Gy261–265, vö. IX/9). Az egységek és asszociáltak jellemzése a norma segítségével (IX/3c). Prím normájú Gauss-egész mindig Gauss-prím. A Gauss-prímek leírása (Gy267–270, IX/8). A kvaterniók fogalma, műveletek, ezekre egységelemes, de nemkommutatív gyűrűt kaptunk (NB). Kvaternió konjugáltja és normája (X/12), elemi tulajdonságok, kvaternió inverzének képlete, a kvaterniók ferdetestet alkotnak (F87-88). Az x^2+1 polinom gyökei a kvaterniók között (X/13), ennek jelentősége.

Polinomok. Kommutatív, egységelemes gyűrű feletti polinomgyűrű (FBII51–54, I/6); ez is kommutatív, egységelemes gyűrű. Polinomok egyenlősége, a polinom egyértelműen meghatározza az együtthatóit, nullapolinom. Nem nulla polinom foka, főegyüttható, normált polinom (I/5,7). Ha R nullosztómentes, kommutatív, egységelemes gyűrű, akkor $R[x]$ is az, sőt $R[x]$-ben szorzat foka a fokok összege. A polinomgyűrű invertálható elemei (egységei).

A polinomfüggvény fogalma (FBII58–61, I/8), polinom gyöke. A gyöktényező kiemelhetősége (a kommutativitás kell!). Nullosztómentes gyűrű fölött a gyöktényezős alak egyértelműsége, a gyökök és együtthatók összefüggése (FBII76–78, I, V/11=K2.11), gyök multiplicitása (I/9), a gyökök maximális száma (VI/5, X/13), a polinomok azonossági tétele (II/11). Végtelen gyűrű fölött a polinomfüggvények és a polinomok kapcsolata kölcsönösen egyértelmű, de általában nem. Példa kommutatív, nem nullosztómentes, illetve nemkommutatív, nullosztómentes gyűrű feletti polinomra, melynek több gyöke van, mint a foka.

Egységelemes, kommutatív, nullosztómentes gyűrű felett minden olyan polinommal lehet maradékosan osztani, amelynek a főegyütthatója invertálható (FBII54–56). A maradékos osztás egyértelmű. Test feletti polinomgyűrű euklideszi, euklideszi algoritmus, a lineáris diofantikus egyenlet megoldhatósága, a kitüntetett közös osztó kiemelési tulajdonsága, a felbonthatatlan (=irreducibilis) és a prímtulajdonságú elemek viszonya, az alaptétel bizonyítása (az egészekéhez hasonló módon: azonosságok és különbségek).

Test felett az irreducibilis polinomok azok a nem konstans polinomok, amelyek nem bonthatók alacsonyabb fokúak szorzatára, itt minden elsőfokú polinom irreducibilis (III/11, VI/4), a másod- és harmadfokúak pedig pontosan akkor irreducibilisek, ha nincs az alaptestben gyökük. Ha egy legalább másodfokú polinomnak van az alaptestben gyöke, akkor nem irreducibilis (de ha nincs gyöke, attól még lehet reducibilis, V/1, K5.3). Az algebra alaptétele (FBII70–73, NB): $\mathbb{C}$ felett minden nem konstans polinomnak van gyöke. Az irreducibilis polinomok $\mathbb{C}$ felett az elsőfokúak. Egy $\mathbb{R}$ feletti polinomnak minden komplex szám ugyanannyiszoros gyöke, mint a konjugáltja (FBII74-76, II/6). Az $\mathbb{R}$ feletti irreducibilis polinomok az elsőfokúak, és azok a másodfokúak, melyeknek diszkriminánsa negatív.

$\mathbb{Z}[x]$ számelmélete (lásd FBII123–129 is, III/10, 11). Gauss Lemma I: ha p prímszám, akkor $\mathbb{Z}[x]$-ben, mint konstans polinom, prímtulajdonságú. Bizonyítás: $\mathbb{Z}_p[x]$ nullosztómentes. A primitív polinom fogalma. Gauss Lemma II: primitív polinomok szorzata is primitív. Gauss Lemma III: egész együtthatós polinom $\mathbb{Q}$ feletti felbontása $\mathbb{Z}$ feletti felbontássá módosítható. $\mathbb{Z}[x]$-ben az irreducibilis polinomok éppen a konstans felbonthatatlan számok, valamint a $\mathbb{Q}$ felett irreducibilis primitív polinomok (IV/7,8,9,10). A számelmélet alaptétele $\mathbb{Z}[x]$-ben. A Schönemann-Eisenstein kritérium (bizonyítása $\mathbb{Z}_p[x]$-beli számolással, IV/6, VI/9, IV/3=K3.11, K3.12). A racionális gyökteszt (FBII68–70), módszerek az irreducibilitás eldöntésére (IV eleje, IV/10, V/3).

Polinom formális deriváltja, összeg, szorzat deriváltja, láncszabály (FBII104–117). Ha az f polinomnak egy b alaptestbeli elem k-szoros gyöke (ahol $k \geq 1$), akkor a deriváltjának b legalább $k-1$-szeres gyöke, és $\mathbb{C}$ felett pontosan $k-1$-szeres gyöke. Ezért f többszörös gyökei éppen (f, f') gyökei. Egy polinomnak pontosan akkor nincs többszörös gyöke $\mathbb{C}$-ben, ha relatív prím a deriváltjához. Többszörös tényezők (V/5,6,7, K3.7).

A körosztási polinom definíciója (K2.2) és rekurzív képlete (K2.5 és előbb). A körosztási polinom egész együtthatós (K2.7). A körosztási polinom kiszámítása (K2.8, K2.9, K2.10, V/13=K2.13, K2.14, IV/4=K2.16) és irreducibilitása $\mathbb{Z}$ és $\mathbb{Q}$ felett (K5.1).

Számelméleti alkalmazások. Az Euler-függvény fogalma, multiplikativitása és képlete (Sz2.32, Sz2.38, VII/8,9,11, VII/10=K2.18, K2.19). Az Euler-Fermat tétel (GyT2.16, Sz2.35), bizonyítása a $\mathbb{Z}_m^\times$ csoport segítségével, következménye a kis-Fermat tétel. A számelméleti elemrend fogalma és elemi tulajdonságai (GyD3.1, GyT3.7, Sz2.44, Sz2.54), ha $(a, n) = 1$, akkor $o_n(a) \mid \varphi(n)$ (Sz2.46). Gyors hatványozás, prímtesztek, álprímek (VII/7). Az RSA nyilvános jelkulcsú titkosírás alapjai (Sz135–139, VII/5,6,14).

Legyen p prím. Az $x^2 \equiv -1$ (p) megoldhatóságának szükséges feltétele levezethető a kis Fermat-tételből (vö. VIII/9). Az $x^p - x$ gyöktényezős alakja $\mathbb{Z}_p$ felett. Következmények: a Wilson-tétel új bizonyítása (GyT3.3, Sz2.25, és egy harmadik bizonyítás: VIII/11), primitív gyök létezése mod p (K4.1, Sz2.47). Szám indexe egy primitív gyök alapra nézve (GyD3.3). A binom kongruencia megoldhatóságának két szükséges és elégséges feltétele prím modulusra, a megoldások száma (GyT3.14, VIII/10). Kvadratikus maradékok és nemmaradékok, számuk, az Euler-lemma (GyT4.2, GyT4.3, Sz2.16, Sz2.21, VIII/4,5,24).

A Dirichlet-tétel $nk+1$ esetének bizonyítása (K4.4, VIII/6=K4.3 és előbb, K4.7). A két négyzetszám összegeként előállítható számok leírása és az előállítások száma a Gauss-egészek felhasználásával (GyT7.24). A lényegesen különböző felbontások száma (X/1,2). A négy négyzetszám tétel (Lagrange) bizonyítása kvaterniókkal (vö. GyT7.27). A három négyzetszám tétel (GyT7.26, NB). A Waring problémakör (Gy288, Gy292–293, X/4,5).