N=bizonyítás nélkül, SZ=Freud Róbert – Gyarmati Edit: Számelmélet;
ALG=Kiss Emil: Bevezetés az algebrába; LA=Freud Róbert: Lineáris algebra

Primitív gyök, index. (SZ: 3.3–3.5.)

Primitív gyök létezése páratlan prímre. Index, binom kongruencia (konkrét példán).

Gauss-egészek. (SZ: 7.4, 7.5.1 tétel, 7.2, 7.5.10 feladat.)

Norma, egységek, maradékos osztás, legnagyobb közös osztó, felbonthatatlan, prím, a számelmélet alaptétele. A Gauss-prímek leírása, kanonikus alak. Két négyzetszám tétel. Pitagoraszi számhármasok. Az $x^2 + 4 = y^3$ diofantikus egyenlet.

Ideál, faktorgyűrű, gyűrűhomomorfitmus. (ALG: 5.1, 5.2, 6.4.2–3 tételek, SZ: 11.1, LA: A.6, A.7.18 feladat.)

Ideál, generált ideál, véges sok elem által generált ideál, főideál. Faktorgyűrű, gyűrűhomomorfizmus, homomorfizmustétel(N). A komplex számok mint faktorgyűrű. Testbővítések konstrukciója faktorgyűrű segítségével.

Gyűrűk számelmélete. (SZ: 11.2, 11.3, 10.3.5 tétel, ALG: 5.5.)

Ideálok kapcsolata oszthatósággal és a legnagyobb közös osztóval. A számelmélet alaptételének szükséges(N) és elégséges feltétele, főideálgyűrű, euklideszi gyűrű. A számelmélet alaptételének kérdése az $a + b\sqrt{2}$, illetve $a + b\sqrt{-5}$ alakú számok gyűrűjében ($a, b \in \mathbf{Z}$).

Véges testek. (ALG: 5.8, 6.6, LA: A.8.)

Karakterisztika, prímtest. Véges test elemszáma, additív és multiplikatív szerkezete, leírása az $x^{p^k} - x$ polinom gyökeiként, testbővítésként és faktorgyűrűként.

Prímszámok. (SZ: 5.4, 5.5.1 tétel, 5.5.3 tétel, 5.7, 5.8, 9.5.1 tétel.)

Prímszámtétel(N), alsó és felső becslés $\pi(n)$-re, Csebisev-tétel. Prímteszt és prímfaktorizáció, eltérő időigényük. Nyilvános jelkulcsú titkosírás, RSA-séma. Az e szám irracionális.

Megjegyzés: A vizsgák az előadás anyagát kérik számon (a tételekre más bizonyítás is adható), a tematikában jelzett irodalom általában ennél valamivel bővebb.