1. Oszthatóság, legnagyobb közös osztó, maradékos osztás, euklideszi algoritmus, az euklideszi algoritmus gyorsasága.
2. Prímszám és felbonthatatlan szám, a számelmélet alaptétele, Legendre-formula (azaz, az $n!$ kanonikus alakja).
3. Prímszámok: végtelen sok prím van, a prímek közötti hézagok, Dirichlet-tétel ($4k \pm 1$ eset bizonyítása), prímek reciprokösszege.
4. Csebisev-tétel bizonyítása
5. Fermat- és Mersenne-számok, tökéletes számok, szabályos n-szög szerkeszthetősége (nem biz.).
6. Kongruenciák tulajdonságai, maradékosztály, teljes és redukált maradékrendszer.
7. Az Euler-féle φ függvény, φ multiplikativitása és kanonikus alakja, Euler–Fermat-tétel, kis Fermat-tétel.
8. Lineáris kongruenciák megoldásszáma és megoldása, kibővített euklideszi algoritmus, inverz modulo m, a $\mathbb{Z}_m$ gyűrű, Wilson-tétel.
9. Szimultán kongruenciarendszerek, kínai maradéktétel, összetett modulusú kongruenciák visszavezetése prímhatvány modulusúakra, prímhatvány modulusú polinom kongruenciák.
10. Egész szám rendje modulo m, primitív gyök (mod p primitív gyök létezése), index.
11. Prím modulusú binom kongruenciák megoldhatósága és megoldásszáma, kvadratikus maradék, kvadratikus kongruenciák megoldása.
12. Legendre-szimbólum, kvadratikus reciprocitási tétel, Jacobi-szimbólum.
13. Számelméleti függvények: $d(n)$, $\sigma(n)$, $\varphi(n)$; multiplikativitás, konvolúció, összegzési függvény, Möbius-függvény, megfordítási tétel, összegzési és megfordítási függvény multiplikativitása.
14. Számelméleti függvények aszimptotikus viselkedése: $\lim_{n\to\infty} \varphi(n)$, Hegytétel, Völgytétel Prímszámtétel (nem biz.), n-edik prím nagyságrendje.
15. Prímtesztek, álprímek, Solovay–Strassen-prímteszt, Miller–Lenstra–Rabin prímteszt, nyilvános kulcsú titkosírás, RSA-séma.
16. Diofantoszi egyenletek: lineáris diofantoszi egyenletek megoldása, pitagoraszi számhármasok, $x^2 + y^2 = n$ alakú kongruenciák megoldhatósága, Gauss-egészek.