Alk. mat. I. évf. **Vizsgatételek** *2000. december*

1. Oszthatóság, legnagyobb közös osztó, maradékos osztás, euklideszi algoritmus.
2. Prímszám és felbonthatatlan szám, a számelmélet alaptétele, Legendre-formula (azaz, az $n!$ kanonikus alakja).
3. Prímszámok: végtelen sok prím van, Dirichlet-tétel (csak a $4k \pm 1$ speciális esetek bizonyításával), a prímek közötti hézagok, Csebisev-tétel az n és $2n$ közötti prímszám létezéséről (nem biz.).
4. Fermat- és Mersenne-számok, tökéletes számok, szabályos n-szög szerkeszthetősége (nem biz.).
5. Kongruenciák tulajdonságai, maradékosztály, teljes és redukált maradékrendszer.
6. Az Euler-féle φ függvény, φ multiplikativitása és kanonikus alakja, Euler–Fermat-tétel, kis Fermat-tétel.
7. Lineáris kongruenciák megoldhatósága és megoldása, kibővített euklideszi algoritmus, inverz modulo m, a $\mathbb{Z}_m$ gyűrű, Wilson-tétel.
8. Szimultán kongruenciarendszerek, kínai maradéktétel, összetett modulusú kongruenciák visszavezetése prímhatvány modulusúakra, prímhatvány modulusú polinom kongruenciák.
9. Egész szám rendje modulo m, primitív gyök, index.
10. Prím modulusú binom kongruenciák megoldhatósága, kvadratikus maradék, prím modulusú polinom kongruenciák fokának redukálása.
11. Legendre-szimbólum, kvadratikus reciprocitási tétel, Jacobi-szimbólum.
12. Számelméleti függvények: $d(n)$, $\sigma(n)$, $\varphi(n)$; multiplikativitás, összegzési függvény multiplikativitása, Möbius-függvény, megfordítási tétel.
13. Számelméleti függvények aszimptotikus viselkedése: $\lim\limits_{n\to\infty} \varphi(n)$, Völgytétel, Hegytétel (nem biz.), Prímszámtétel (nem biz.), prímek reciprokösszege (nem biz.).
14. Alsó becslés $\pi(x)$-re, nyilvános kulcsú titkosírás, RSA-séma.
15. Prímtesztek, álprímek, Solovay–Strassen-prímteszt.
16. Lineáris diofantikus egyenletek, pitagoraszi számhármasok, Fermat-sejtés.