

11. előadás, fogalmak, definíciók, állítások

A nyolcadik előadáson dolgozatot írtunk

Számelmélet (tanár, 4. félév)

2024 tavasz

- Néhány alaptulajdonságot összegyűjtöttünk:
 - rend osztja a jó kitevőket.
 - Rend osztja $\varphi(m)$ -et.
 - $a^u \equiv a^v \pmod{m}$ pontosan akkor, ha $u \equiv v \pmod{o_m(a)}$.
 - $o_m(a)$ különböző maradékokat adó hatványok van a -nak.
- Primitív gyök fogalma.
- Példák.
- Tétel: $\mathbb{Z}/p\mathbb{Z}$ van primitív gyök, ha p prim.
- Tétel: $\sum_{d|p-1} \varphi(d) = p - 1$.
- Tétel: Pontosán milyen m -ekre van $\mathbb{Z}/m\mathbb{Z}$ primitív gyök.