

Primitív gyök, index, gyökkvonás mod p

101. a) Készítsünk indextáblázatot mod 17.
b) Vonjunk 20-ik gyököt a 13-ból mod 17.
102. Fogalmazzuk meg és bizonyítsuk be az indexre a logaritmusazonosságok megfelelőit.
103. Mutassuk meg, hogy ha p prím, akkor egy szám mod p rendjének és (valamely primitív gyök szerint vett) indexének a szorzata mindig osztható $p - 1$ -gyel.
104. Mely p prímek esetén adnak ki minden lehetséges p -vel való osztási maradékot (a) a négyzetszámok; (b) a köbszámok?
105. Legyen $p > 2$ prím.
a) Bizonyítsuk be, hogy két primitív gyök szorzata sohasem lehet primitív gyök.
*b) Mely p -kre lesz bármely három primitív gyök szorzata is primitív gyök?
106. Milyen maradékot ad 101-gyel osztva $1^k + 2^k + \dots + 100^k$, ha (a) $k = 567$; (b) $k = 1000$; (c) $k = 2222$?
107. Legyen p és q az ebben a pillanatban ismert két legnagyobb prímszám és $m = pq$. Milyen maradékot ad m -mel osztva $2010^{\varphi(m)/2}$?