

Számelméleti függvények; rend, primitív gyök, négyzetes maradék

1. Igazolja, hogy ha létezik $n > 1$ páratlan tökéletes szám, akkor van olyan $p > 2$ prímszám és olyan $m > 1$ egész szám, amelyre $n = pm^2$.
2. Mutassa meg, hogy bármely n természetes számra érvényesek az alábbi egyenlőségek, és fogalmazza meg a bizonyított állításokat a *konvolúció*, az *összegzési függvény*, illetve a *megfordítási függvény* fogalmak segítségével:
 - (a) $\sum_{d|n} \tau(d) \mu\left(\frac{n}{d}\right) = 1$;
 - (b) $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$;
 - (c) $\sum_{d|n} \mu^2(d) = 2^{\nu(n)}$, ahol $\nu(n)$ az n különböző prímosztóinak számát jelöli;
 - (d) $(\sigma(n))^2 = \sum_{d|n} \frac{n}{d} \sigma(d^2)$;
 - (e) $\sum_{d|n} \sigma(d) \varphi\left(\frac{n}{d}\right) = n\tau(n)$;
3. Van-e olyan a egész szám, amelyre $o_m(a) = 4$, ha
 - (a) $m = 11$,
 - (b) $m = 12$,
 - (c) $m = 17$?
4. A rend fogalmának felhasználásával igazolja, hogy $n \mid \varphi(a^n - 1)$ tetszőleges $a > 1$ és $n > 0$ egészekre.
5. Mutassa meg, hogy
 - (a) a $11^{40} \equiv -1 \pmod{17}$ kongruencia fennállásából következik, hogy 11 primitív gyök modulo 17;
 - (b) ha a^k primitív gyök modulo m , akkor a is az;
 - (c) ha g primitív gyök modulo m , akkor g inverze modulo m szintén primitív gyök modulo m ;
 - (d) ha a p, q páratlan prímekre $p = 2q + 1$, és a olyan egész szám, hogy $a^3 \not\equiv a \pmod{p}$, akkor a vagy $-a$ primitív gyök modulo p ;
 - (e) ha $m > 2$ és g primitív gyök modulo m , akkor g négyzetes nemmaradék modulo m .
6. Bizonyítsa be, hogy ha $p > 3$ prím, akkor a modulo p inkongruens primitív gyökök szorzata 1-gyel kongruens modulo p .