

Számelmélet 2004/2005

Bónusz házi feladatok (csak javításra)

1. Tegyük fel, hogy $\varphi(m) = 2^n$ valamely n pozitív egészre és az alábbi feltételek közül legalább az egyik teljesül m -re:

- (i) $8 \mid m$;
- (ii) van két különböző páratlan prím m osztói között;
- (iii) $4 \mid m$ és van m -nek páratlan prímosztója.

Bizonyítsuk be, hogy ekkor az

$$x^{2^n-1} - 1$$

polinomnak 2^n gyöke van modulo m .

2. Bizonyítsuk be, hogy ha $p, q \geq 3$ különböző prímek, $\{a_1, a_2, \dots, a_{\varphi(pq)}\}$ redukált maradékrendszer modulo pq , akkor

$$\prod_{i=1}^{\varphi(pq)} a_i \equiv 1 \pmod{pq}.$$

(Erre két lényegesen különböző megoldást is tudok, aki mindkettőt beadja dupla pontot kap.)

3. Legyen $p \geq 3$ prím, a, b, c egész számok, $(a, p) = 1$. Adjunk szükséges és elégséges feltételt az

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

másodfokú kongruencia megoldhatóságára.

4. Határozzuk meg (a paraméter függvényében), hogy modulo m hány megoldása van az $x^2 \equiv a \pmod{m}$ kongruenciának, ha $(a, m) = 1$.

Minden feladat helyes megoldása 2 pontot ér.