Teorema lui Wilson

Lemă. Dacă p este un număr prim, atunci $x^2 \equiv 1 \pmod{p}$ dacă și numai dacă $x \equiv \pm 1 \pmod{p}$.

Demonstrație. Fie p un număr prim. Dacă $x^2 \equiv 1 \pmod{p}$, adică $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$, atunci, având în vedere că p este prim, fie $p \mid x-1$, fie $p \mid x+1$. Așadar, $x \equiv \pm 1 \pmod{p}$. □

Corolar. Dacă p este un număr prim, atunci, pentru orice număr natural a din intervalul $[2, p-2]$, inversul său multiplicativ modulo p este cuprins tot între 2 și $p-2$, și este diferit de x.

Teorema lui Wilson. Un număr natural $p > 1$ este prim dacă și numai dacă $(p-1)! \equiv -1 \pmod{p}$.

Demonstrație. Fie $p > 1$ un număr natural.

Dacă p este compus, atunci p sigur se poate scrie drept produsul a două numere a și b, unde $2 \leq a \leq \sqrt{p} \leq b \leq p-2$. Distingem două cazuri.

Dacă $a \neq b$, atunci atât a cât și b apar în lista $2, 3, \ldots, p-2$, de unde $a \cdot b \mid (p-1)!$, adică $(p-1)! \equiv 0 \not\equiv -1 \pmod{p}$. În schimb, dacă $a = b$ $(= \sqrt{p})$, atunci avem alte două cazuri.

Dacă $p = 4$, obținem $(p-1)! = 6 \not\equiv -1 \pmod{p}$. Dacă $p > 4$, atunci $a > 2$, așa că $2a < a^2 = p$. Prin urmare, atât a cât și $2a$ se regăsesc în lista $2, 3, \ldots, p-1$. Deci, $a^2 \mid (p-1)!$, adică $(p-1)! \equiv 0 \not\equiv -1 \pmod{p}$.

Dacă p este prim, avem două cazuri. Dacă $p = 2$, atunci $(p-1)! = 1 \equiv -1 \pmod{p}$. Altfel, numărul de elemente din lista $2, 3, \ldots, p-2$ este par. Deci, conform corolarului de mai sus, putem grupa aceste elemente în $(p-1)/2$ perechi de numere (a, b), cu proprietatea că $a \cdot b \equiv 1 \pmod{p}$. Prin urmare, $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$.

Așadar, $(p-1)! \equiv -1 \pmod{p}$ dacă și numai dacă p este prim. □