Wilson tétel

Tétel*(Wilson)* Legyen p prím. Ekkor

$$(p-1)! \equiv -1 \mod p \tag{1}$$

1. Bizonyítás A baloldalon $(p-1)$ darab — a $p=2$ triviális esettõl eltekintve, páros számú — tényezõ szorzata áll. Párosítsuk össze a tényezõket, úgy, hogy a párok szorzata 1 legyen. Mivel egy $ax \equiv 1 \mod p$ kongruencia megoldható és pontosan egy megoldása lesz, mivel $(a,p)=1|1$, ezért minden elemnek lesz párja és az egyértelmũ lesz. Azt is meg kell vizsgálni, hogy mely elemeknek lesz saját maga a párja: $aa = a^2 \equiv 1 \mod p$, azaz $p|a^2-1$, és tudjuk, hogy p prím, ezért $p|(a-1)$ vagy $p|(a+1)$. Tehát az $a \equiv 1$ ill. $a \equiv -1$ esetekben. Ebbõl következik, hogy a szorzat -1-gyel kongruens, hiszen a párok szorzata 1, ezt még 1-gyel ill. -1-gyel meg kell szorozni.

2. Bizonyítás Az Euler-Fermat tételt felhasználva: $x^{p-1} \equiv 1 \mod p$, ha p prím és $(x,p)=1$. Tekintsünk két polinomot: legyen $f(x) = x^{p-1}-1 \mod p$ és $g(x) = (x-1)(x-2)\dots(x-p+1) \mod p$. Világos, hogy $f(i) = g(i) = 0, \forall i \in \{1,2\dots(p-1)\}$. Mivel f és g $(p-1)$-edfokú polinomok és $(p-1)$ helyen megegyeznek, ezért a két polinom azonos. Ebbõl viszont következik, hogy a nullában felvett értékük is megegyezik, azaz $f(0) = g(0)$, tehát $-1 \equiv (-1)(-2)\dots(-p+1) \mod p$.