$a^p \equiv a \bmod p$

Generalisering av Euler

$\gcd(a,n)=1,\ n>1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$

Setning 71

$n>1$ i $\mathbb{Z}$, $n = p_1 p_2 \cdots p_t$, der $p_i \neq p_j$ for $i \neq j$, primtall (n kvadratfritt). For $a \in \mathbb{Z}$, så har vi

$$a^{\varphi(n)+1} \equiv a \bmod n$$

Bevis: $a=0$: Resultatet holder.

$a \neq 0$: La $d = \gcd(a,n)$. Da er $a = a'd$ og $n = n'd$.

Har $\gcd(d, \frac{n}{d}) = 1$, siden n er kvadratfritt

Alltid: $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$

Til sammen gir dette $\gcd(a, \frac{n}{d}) = 1$

Da gir Euler

$$a^{\varphi(\frac{n}{d})} \equiv 1 \bmod \frac{n}{d}$$

$\gcd(d, \frac{n}{d}) = 1 \Rightarrow \varphi(n) = \varphi(d \cdot \frac{n}{d}) = \varphi(d)\varphi(\frac{n}{d})$

$$\Rightarrow a^{\varphi(n)} = \left(a^{\varphi(\frac{n}{d})}\right)^{\varphi(d)}$$

$$\equiv 1^{\varphi(d)} \bmod \frac{n}{d}$$

$$\equiv 1 \bmod \frac{n}{d}$$

$\Rightarrow \frac{n}{d} \mid a^{\varphi(n)} - 1$ $\quad a'\cdot -$

$d\cdot -$

$\Rightarrow n = d\frac{n}{d} \mid d(a^{\varphi(n)}-1) \mid \underbrace{a'd}_{a}(a^{\varphi(n)}-1)$ $\quad 1 \mid$

$a(a^{\varphi(n)}-1) = a^{\varphi(n)+1} - a$

$\Rightarrow a^{\varphi(n)+1} \equiv a \bmod n.$ $\square$