3. $a \neq 0$, p – просте

Дов: $\exists x \in \mathbb{Z}: x^n \equiv a \pmod p \iff a^{\frac{p-1}{(p-1,n)}} \equiv 1 \pmod p$

Нехай $a \in$ лишкам n-го степеня.

Скільки розв'язків у $\mathbb{Z}/p\mathbb{Z}$ має конгруенція $x^n \equiv a \pmod p$

$(\Rightarrow)$ Знаємо, що $\exists x \in \mathbb{Z}: x^n \equiv a \pmod p$

Тоді

$$a^{\frac{p-1}{(p-1,n)}} \equiv (a^n)^{\frac{p-1}{(p-1,n)}} = a^{\frac{n(p-1)}{(p-1,n)}} =$$

$$= (a^{\frac{n}{(p-1,n)}})^{p-1} \equiv 1 \pmod p$$

$\leftarrow$ мала теорема Ферма

$(\Leftarrow)$ Знаємо, що $a^{\frac{p-1}{(p-1,n)}} \equiv 1 \pmod p$

p – просте, тому $(\mathbb{Z}/p\mathbb{Z})^\times$ – циклічна.

Тому $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$

і $\exists k \in \{0, \dots, p-2\}: a = g^k$

Нехай $\exists x \in \mathbb{Z}: x^n \equiv a \pmod p \Leftrightarrow$

$\Leftrightarrow \exists m \in \mathbb{Z}: (g^m)^n \equiv g^k \pmod p \Leftrightarrow$

$\Leftrightarrow \exists m \in \mathbb{Z}: mn \equiv k \pmod{(p-1)}$

Так як $a^{\frac{p-1}{(p-1,n)}} \equiv 1 \pmod p$, то

$g^{\frac{k(p-1)}{(p-1,n)}} \equiv 1 \pmod p \Rightarrow (p-1) \mid \frac{k(p-1)}{(p-1,n)} \Rightarrow$

$\Rightarrow \exists z \in \mathbb{Z}: \frac{k(p-1)}{(p-1,n)} = (p-1)z \Rightarrow$

$\Rightarrow \exists z \in \mathbb{Z}: k = z(p-1,n) \Rightarrow (p-1,n) \mid k$

Нехай:

$\exists m \in \mathbb{Z}: mn \equiv k \pmod{(p-1)} \Leftrightarrow$

$\Leftrightarrow (p-1) \mid (mn-k) \Leftrightarrow$

$\Leftrightarrow \frac{(p-1)}{(p-1,n)} \mid \left(m\frac{n}{(p-1,n)} - \frac{k}{(p-1,n)}\right) \Leftrightarrow$

$\Leftrightarrow m\frac{n}{(p-1,n)} \equiv \frac{k}{(p-1,n)} \pmod{\left(\frac{p-1}{(p-1,n)}\right)}$

але $\gcd\left(\frac{n}{(p-1,n)}, \frac{p-1}{(p-1,n)}\right) = 1$, тому

$\frac{n}{(p-1,n)}$ має обернене по модулю $\frac{p-1}{(p-1,n)}$

і маємо

$\Leftrightarrow m \equiv \frac{k}{(p-1,n)} \left(\frac{n}{(p-1,n)}\right)^{-1} (\mathrm{mod}\ \frac{p-1}{(p-1,n)})$

але такі m існують.

~~Вираз справа~~

Серед всіх елементів $(\mathbb{Z}/p\mathbb{Z})^\times$ рівно (бо очевидно не перетинаються) рівно $(p-1,n)$ мають такі значення по модулю $\frac{p-1}{(p-1,n)}$ тобто якщо $a \in$ множині n-го степеня, то серед $\mathbb{Z}/p\mathbb{Z}$ це рівняння має $(p-1,n)$ розв'язків.