Výpočet "odmocnin" modulo prvočíslo p splňující $p \equiv 3 \pmod 4$ (Jaroslav Šeděnka)

Zadání. *Nechť p je prvočíslo splňující $p \equiv 3 \pmod 4$. Buď $m \in \mathbb{Z}_p$ pevně dané. Najděte $k \in \mathbb{Z}_p$ splňující $k^2 \equiv m \pmod p$.*

Řešení: Využijeme vlastnosti, kterou mají všechny druhé mocniny (mod p), a tou je kongruence

$$m^{(p-1)/2} \equiv 1 \pmod p$$

Tuto kongruenci dokážeme posléze jako Lemma 1. Hned vidíme

$$m^{(p+1)/2} \equiv m^{(p-1)/2} m \equiv m \pmod p$$

(Všimněte si, že p je z předpokladů liché, takže $(p-1)/2$ a $(p+1)/2$ jsou celá čísla; v opačném případě bychom na ně vůbec nemohli umocňovat!)

Ovšem dokonce i $(p+1)/4$ je celé číslo, proto můžeme spočíst $k' \equiv m^{(p+1)/4} \pmod p$ a takové číslo bude splňovat $(k')^2 = (m^{(p+1)/4})^2 \equiv m^{((p+1)/4).2} \equiv m^{(p+1)/2} \equiv m \pmod p$. Našli jsme tedy hledanou druhou odmocninu.

Lemma 1. *Nechť $p \equiv 3 \pmod 4$ je prvočíslo, $m \in \mathbb{Z}_p$ je libovolné. Pak platí*

$$m^{(p-1)/2} = \begin{cases} 1 & \text{pokud existuje } k \in \mathbb{Z}_p \text{ splňující } k^2 \equiv m \pmod p \\ -1 & \text{jinak} \end{cases}$$

Důkaz. Buď ζ libovolný primitivní kořen (mod p), pak ζ splňuje rovnici

$$(\zeta^{(p-1)/2} + 1)(\zeta^{(p-1)/2} - 1) = \zeta^{p-1} - 1 \equiv 0 \pmod p$$

(Zejména $\zeta^{p-1} \equiv 1 \pmod p$, protože $\varphi(p) = p - 1$.)
Přitom ζ generuje celé $Z_p \backslash \{0\}$, takže $\zeta^{(p-1)/2} \not\equiv 1 \pmod p$, musí být $\zeta^{(p-1)/2} \equiv -1 \pmod p$.

Když si napíšeme $m = \zeta^a$, máme

$$m^{(p-1)/2} \equiv (s^a)^{(p-1)/2} = (s^{(p-1)/2})^a \equiv (-1)^a \pmod p$$

Pro a sudé je $\zeta^{a/2}$ odmocninou z $m = \zeta^a$, pro a liché taková odmocnina neexistuje:.

□