

## 1 Prvočísla tvaru $x^2 + y^2$

**Věta 1.1.** *Nechť  $p$  je liché prvočíslo splňující  $p \equiv 1 \pmod{4}$ . Pak forma  $f(x, y) = x^2 + y^2$  vyjadřuje  $p$ .*

*Důkaz.* Protože  $p \equiv 1 \pmod{4}$ , tak existuje číslo  $n \in \mathbb{N}$  takové, že  $p = 4n + 1$ . Označme  $m = (2n)!$ , pak  $m^2 \equiv -1 \pmod{p}$ , neboť

$$-1 \equiv (p-1)! = [1 \cdot 2 \cdots 2n] \cdot [(p-1)(p-2) \cdots (p-2n)] \equiv [(2n)!][(-1)^{2n}(2n)!] = m^2 \pmod{p}$$

Díky tomu máme

$$x^2 + y^2 \equiv (x + my)(x - my) \pmod{p} \quad (1.1)$$

Označme  $l(x, y) = x + my$ . Dále budeme uvažovat dvojice  $(x, y)$  celých čísel, které splňují

$$0 \leq x < \sqrt{p}, \quad 0 \leq y < \sqrt{p}. \quad (1.2)$$

Počet dvojic  $(x, y)$  celých čísel splňujících (1.2) je

$$\left\lceil \sqrt{p} \right\rceil \cdot \left\lceil \sqrt{p} \right\rceil \geq \sqrt{p} \cdot \sqrt{p} = p,$$

kde  $\lceil x \rceil$  značí horní celou část reálného čísla. Rovnost by zde nastala pouze v případě, že  $\sqrt{p}$  by bylo celé, což není. To znamená, že počet dvojic splňujících (1.2) je větší než  $p$ . Proto existují dvě různé dvojice  $(x_1, y_1)$  a  $(x_2, y_2)$  celých čísel splňujících 1.2 takové, že

$$l(x_1, y_1) \equiv l(x_2, y_2) \pmod{p}.$$

Položme  $x_0 = x_2 - x_1$ ,  $y_0 = y_2 - y_1$ . Protože  $l(x, y)$  je lineární, tak platí

$$l(x_0, y_0) = l(x_2 - x_1, y_2 - y_1) = l(x_2, y_2) - l(x_1, y_1) \equiv 0 \pmod{p}$$

a podle (1.1) máme

$$x_0^2 + y_0^2 \equiv 0 \pmod{p}. \quad (1.3)$$

Protože dvojice  $(x_1, y_1)$  a  $(x_2, y_2)$  jsou různé a splňují (1.2), tak  $(x_0, y_0) \neq (0, 0)$  a platí

$$|x_0| < \sqrt{p}, \quad |y_0| < \sqrt{p}.$$

Díky tomu snadno odvodíme

$$0 < x_0^2 + y_0^2 < 2p,$$

a proto s ohledem na (1.3) dostáváme, že

$$x_0^2 + y_0^2 = p,$$

což jsme chtěli dokázat. □