Kapitola 6

Teorie čísel II

6.1 Teorie

Definice 6.1. Buď $n \in \mathbb{N}$. Pro každé prvočíslo p je jednoznačně určený exponent v prvočíselném rozkladu čísla n. Tento exponent budeme označovat $v_p(n)$ a říkat mu p-valuace čísla n. Je-li $(p,n) = 1$, pak $v_p(n) = 0$.

Věta 6.2. *Pro libovolná $a,b \in \mathbb{N}$ a prvočíslo p platí*

(i) $v_p(ab) = v_p(a) + v_p(b)$

(ii) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

(iii) Pokud $v_p(a) \neq v_p(b)$, pak dokonce $v_p(a+b) = \min\{v_p(a), v_p(b)\}$.

(iv) $v_p((a,b)) = \min\{v_p(a), v_p(b)\}$

(v) $v_p([a,b]) = \max\{v_p(a), v_p(b)\}$

Věta 6.3. *Buď p liché prvočíslo. Buďte $a,b \in \mathbb{N}$ nedělitelná p taková, že $p \mid (a-b)$. Pak pro všechna $n \in \mathbb{N}$ platí*

$$v_p(a^n - b^n) = v_p(n) + v_p(a-b).$$

Věta 6.4. *Buď p liché prvočíslo. Buďte $a,b \in \mathbb{N}$ nedělitelná p taková, že $p \mid a+b$. Pak pro všechna $n \in \mathbb{N}$* **lichá** *platí*

$$v_p(a^n + b^n) = v_p(n) + v_p(a+b).$$

Věta 6.5 (Wilsonova)**.** *Přirozené číslo $n \geq 2$ je prvočíslo právě tehdy, když*

$$(n-1)! \equiv -1 \pmod{n}.$$

6.2 Příklady

Příklad 6.1. Nechť pro $a,b,c \in \mathbb{N}$ platí $a \mid b^3$, $b \mid c^3$, $c \mid a^3$. Dokažte, že $abc \mid (a+b+c)^{13}$.

Příklad 6.2. Nechť $a,b,c,d \in \mathbb{N}$ splňují $ab = cd$. Ukažte, že platí

$$(a,c)\cdot(a,d) = a\cdot(a,b,c,d).$$

Příklad 6.3. Buďte $a_1,a_2,\ldots,a_k,b_1,b_2,\ldots,b_k \in \mathbb{N}$ taková, že $(a_i,b_i)=1$ pro každé $i \in \{1,2,\ldots,k\}$. Dále buď $m = [b_1,\ldots,b_k]$. Ukaž, že platí

$$\left(\frac{a_1 m}{b_1}, \frac{a_2 m}{b_2}, \ldots, \frac{a_k m}{b_k}\right) = (a_1,a_2,\ldots,a_k).$$

Příklad 6.4. Najděte všechna přirozená čísla n, pro která existují přirozená x,y a k taková, že $(x,y) = 1, k>1$ a $3^n = x^k + y^k$.

Příklad 6.5. Nechť p je prvočíslo a $m>1$ je přirozené číslo. Ukažte, že pokud pro přirozená $x>1$, $y>1$ platí

$$\frac{x^p+y^p}{2} = \left(\frac{x+y}{2}\right)^m,$$

pak $m=p$.

Příklad 6.6. Najděte všechna přirozená $a,b>1$ splňující $b^a \mid a^b - 1$.

Příklad 6.7. Nechť p je liché prvočíslo. Dokažte

$$p \equiv 1 \pmod 4 \quad \Leftrightarrow \quad \exists m \in \mathbb{N}\colon\ p \mid m^2+1.$$

Příklad 6.8. Žádné prvočíslo nelze zapsat jako součet dvou čtverců více než jedním způsobem.

Příklad 6.9. Nechť p je liché prvočíslo. Dokažte

$$p \equiv 1 \pmod 4 \quad \Leftrightarrow \quad \exists x,y \in \mathbb{N}\colon\ p = x^2+y^2.$$

Příklad 6.10. Nechť $n \in \mathbb{N}_0$ je libovolné. Dokažte, že existují čísla $a,b,c,d \in \mathbb{Z}$ taková, že

$$a^2+b^2+c^2+d^2 = n.$$

Můžete využít Eulerovu identitu o čtyřech čtvercích:

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)\cdot(b_1^2+b_2^2+b_3^2+b_4^2) = {}& (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2+\\ &+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2+\\ &+(a_1b_3-a_2b_4-a_3b_1+a_4b_2)^2+\\ &+(a_1b_4+a_2b_3-a_3b_2-a_4b_1)^2\end{aligned}$$

Příklad 6.11. Dokažte, že neexistuje žádný polynom f s celočíselnými koeficienty takový, že

$$f(23) = 36 \quad \text{a} \quad f(11) = 6.$$