

Kapitola 5

Teorie čísel

Definice 5.1. Bud' $a, b, m \in \mathbb{N}$. Řekneme, že číslo a je *kongruentní* s číslem b modulo m , píšeme

$$a \equiv b \pmod{m},$$

jestliže $m \mid a - b$.

Věta 5.2 (Malá Fermatova). Bud' $a \in \mathbb{N}$ a p prvočíslo. Pak platí

$$a^p \equiv a \pmod{p}.$$

Pokud navíc $(a, p) = 1$, tak

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definice 5.3. Eulerovou funkci $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ definujeme předpisem

$$\varphi(n) = |\{k \in \mathbb{N} \mid k \leq n, (k, n) = 1\}|,$$

tj. Eulerova funkce nám udává počet čísel nesoudělných s číslem n , která nepřesáhnou n .

Věta 5.4 (Eulerova). Bud' $a, m \in \mathbb{N}$ takové, že $(a, m) = 1$. Pak

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kde φ je Eulerova funkce.

Návodný příklad 5.1. Bud' $a, b, c \in \mathbb{Z}$ takové, že $a \mid b \cdot c$. Jestliže $(a, b) = 1$, pak $a \mid c$.

Návodný příklad 5.2. Necht' $a, b \in \mathbb{Z}$. Dokažte, že $\forall n \in \mathbb{N}$ platí $(a - b) \mid (a^n - b^n)$.

Návodný příklad 5.3. Necht' $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$ je liché. Dokažte, že $(a + b) \mid (a^n + b^n)$.

Návodný příklad 5.4. Pomocí rovnosti Sophie Germainové

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$$

dokažte, že pro $n \in \mathbb{N}$, $n > 1$ je číslo $n^4 + 4^n$ složené.

Návodný příklad 5.5. Dokažte, že rovnice $15x^2 - 7y^2 = 9$ nemá v oboru celých čísel žádné řešení.

Návodný příklad 5.6. Necht' p je prvočíslo a $a \in \mathbb{N}$ je takové, že $(a, p) = 1$. Pak existuje $b \in \mathbb{N}$ takové, že

$$a \cdot b \equiv 1 \pmod{p}.$$

Mezi čísla $\{1, \dots, p-1\}$ je navíc takové b určeno jednoznačně.

5.1 Příklady

Příklad 5.1. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $4k + 3$.

Příklad 5.2. Nalezněte všechna prvočísla p, q taková, že $p^2 - 2q^2 = 1$.

Příklad 5.3. Bud' $p \in \mathbb{N}$. Jsou-li p a $p^2 + 2$ prvočísla, pak je i $p^3 + 2$ prvočíslo.

Příklad 5.4. Dokažte, že neexistuje polynom $f(x)$ s celočíselnými koeficienty takový, že $f(7) = 11$, $f(11) = 13$.

Příklad 5.5. Nalezněte nejmenší přirozené číslo takové, že odstraněním první cifry se toto číslo zmenší 57krát.

Příklad 5.6. Dokažte, že pokud poslední cifra čísla $m \in \mathbb{N}$ je 5, pak $1991 \mid (12^m + 9^m + 8^m + 6^m)$.

Příklad 5.7. Necht' jsou dána $a, b, c, d \in \mathbb{N}$ taková, že $ab = cd$. Dokažte, že $\forall n \in \mathbb{N}$ je $a^n + b^n + c^n + d^n$ číslo složené.

Příklad 5.8. Dokažte, že $n \in \mathbb{N}$, $n > 1$ je prvočíslo právě tehdy, když $n \mid ((n-1)! + 1)$.

Hint. Využijte návodného příkladu 5.6 a faktu, že pro prvočíslo p má kongruence

$$x^2 \equiv 1 \pmod{p}$$

právě dvě řešení (v případě $p = 2$ dostáváme dvojnásobný kořen). Tento fakt dokazovat nemusíte.

Příklad 5.9. Dokažte, že $2015 \mid \underbrace{55 \dots 5}_{360}$.

Příklad 5.10. Necht' α, β jsou dvě kladná iracionální čísla taková, že $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Uvažme posloupnosti $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty}$ zadané pomocí předpisů $a_n = \lfloor n\alpha \rfloor, b_n = \lfloor n\beta \rfloor$. Dokažte, že:

1. Posloupnosti $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty}$ jsou disjunktní, tj. $\forall m, n \in \mathbb{N}: a_m \neq b_n$.
2. Sjednocením obou posloupností jsou přirozená čísla, tj. $\forall k \in \mathbb{N} \exists n \in \mathbb{N}: k = a_n$ nebo $k = b_n$.

Příklad 5.11. Dokažte, že pro nekonečně mnoho složených čísel n platí $n \mid 3^{n-1} - 2^{n-1}$.

Hint. Hledejte n ve tvaru $n = 3^{2^t} - 2^{2^t}$ pro $t \in \mathbb{N}$.

Hint (Alternativní hint). Využijte návodného příkladu 5.2.

Příklad 5.12. Dokažte, že rovnice $x^2 + y^2 + z^2 = x^3 + y^3 + z^3$ má nekonečně mnoho celočíselných řešení.

Příklad 5.13. Dokažte, že existuje nekonečně mnoho přirozených čísel n takových, že 2^n končí na n .

Hint. Nejmenší n , které tuto podmínku splní je 36: $2^{36} = 68\,719\,476\,736$. Množinu řešení konstruuje induktivně. Ukažte, že pokud je n řešení a $2^n = \dots dn$ pro nějaké číslo $d = g \cdot 10^m$, kde $g \in \{1, \dots, 9\}$ (přitom dn neznamená násobení, ale zřetězení), pak je i dn řešení.

Jinými slovy: další řešení nalezneme tak, že v dekadickém zápise čísla 2^n připojíme k n všechny předcházející cifry až po první nenulovou (včetně). To, že nestačí brát jen další cifru lze odůvodnit tím, že uvedeným postupem bychom dostali $2^{75\,353\,432\,948\,736} = \dots 075\,353\,432\,948\,736$.