Kapitola 5

Teorie čísel

Definice 5.1. Buďte 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)**.** *Buďte $a \in \mathbb{N}$ 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 funkcí* $\varphi\colon \mathbb{N} \to \mathbb{N}$ 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)**.** *Buďte $a, m \in \mathbb{N}$ takové, že $(a,m) = 1$. Pak*

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

kde φ je Eulerova funkce.

Návodný příklad 5.1. Buďte 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. Nechť $a, b \in \mathbb{Z}$. Dokažte, že $\forall n \in \mathbb{N}$ platí $(a-b) \mid (a^n - b^n)$.

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

Návodný příklad 5.4. Pomocí rovnosti Sophie Germainové

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

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. Nechť 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 čísly $\{1, \ldots, p-1\}$ je navíc takové b určeno jednoznačně.

5.1 Příklady

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

Řešení. Předpokládejme sporem, že prvočísel tvaru $4k+3$ existuje jen konečně mnoho. Nechť jsou $p_1 = 3$, $p_2 = 7, \ldots, p_n$ všechna taková prvočísla. Uvažme

$$N = 3 + 4 \cdot \prod_{i=2}^{n} p_n.$$

Nechť $N = q_1^{\alpha_1} \cdot \cdots \cdot q_m^{\alpha_m}$ je rozklad čísla N na prvočísla. Protože $N \equiv 3 \pmod 4$, musí být mezi prvočísly q_i nějaké ve tvaru $4k+3$. Protože ale $p_i \nmid N$ pro žádné $i = 1, 2, \ldots, n$, dostáváme další prvočíslo tvaru $4k+3$, což nám dává požadovaný spor. ■

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

Řešení. Zřejmě $p > q$. Nejprve vyřešme případy, kdy $q \leq 3$. Je-li $q = 2$, máme $p^2 = 9$, tj. $p = 3$. Pro $q = 3$ máme $p^2 = 19$, což nám řešení nedá. Pro $p, q > 3$ platí

$$p, q \equiv \pm 1 \pmod 6.$$

Když se tedy na zadanou rovnost podíváme modulo 6, dostáváme

$$(\pm 1)^2 - 2(\pm 1)^2 \equiv 1 \pmod 6.$$

Jediné řešení je tedy $(p, q) = (3, 2)$. ■

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

Řešení. Zřejmě $p \neq 2$. Pro $p = 3$ máme $p^2 + 2 = 11$ a $p^3 + 2 = 29$. Pro $p > 3$ je číslo $p^2 + 2$ dělitelné třemi, proto pro žádné $p > 3$ není splněn předpoklad implikace a tvrzení platí. ■

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

Řešení. Nechť

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

kde $a_i \in \mathbb{Z}$. Jistě $(c-d) \mid \left(c^i - d^i\right)$ pro každé $i = 0, \ldots, n$. Proto také $(c-d) \mid a_i \left(c^i - d^i\right)$ a součtem přes i dostáváme $(c-d) \mid \sum_{i=0}^{n} (a_i) \left(c^i - d^i\right) = f(c) - f(d)$. Kdyby hledaný polynom existoval, pak by $11 - 7 \mid f(11) - f(7)$, tj. $4 \mid 2$, což neplatí. ■

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

Řešení. Označme x první cifru hledaného čísla a y číslo, které nám vznikne odstraněním této cifry. Pak

$$10^n x + y = 57y,$$

kde n je počet cifer čísla y. Odtud

$$10^n x = 56y.$$

Protože $56 = 2^3 \cdot 7$ a $(7, 10^n) = 1$, platí $7 \mid x$, tj. $x = 7$ ($1 \leq x \leq 9$, vždyť x je cifra). Dostáváme

$$10^n = 8y.$$

Proto $y = 125 \cdot 10^{n-3}$, přitom vidíme, že nutně $n \geq 3$. Původní číslo je tedy tvaru

$$10^n x + y = 7125 \cdot 10^{n-3}.$$

Nejmenší z nich je pro $n = 3$, tj. 7125. ■

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

Řešení. Nejprve upravme

$$12^m + 9^m + 8^m + 6^m = (4^m + 3^m) \cdot (3^m + 2^m).$$

Protože poslední cifra m je 5, můžeme psát $m = 10a + 5 = 5 \cdot (2a + 1)$. Protože $2a + 1$ je liché, dostáváme

$$\left(4^5 + 3^5\right) \mid (4^m + 3^m) \qquad \text{a} \qquad \left(3^5 + 2^5\right) \mid (3^m + 2^m).$$

Odtud

$$\left(4^5 + 3^5\right) \cdot \left(3^5 + 2^5\right) \mid (12^m + 9^m + 8^m + 6^m),$$

přitom $\left(4^5 + 3^5\right) \cdot \left(3^5 + 2^5\right) = 1267 \cdot 275 = 5^2 \cdot 7 \cdot 11 \cdot 181$. Protože $1991 = 11 \cdot 181$, dostáváme výsledek z tranzitivity relace dělitelnosti. ■

Příklad 5.7. Nechť 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.

Důkaz. Protože $ab = cd$, vydělením bc dostáváme

$$\frac{a}{c} = \frac{d}{b} = \frac{x}{y}$$

pro nějaká $x, y \in \mathbb{N}$, kde $(x, y) = 1$. Odtud

$$a = ux, \quad c = uy, \quad d = vx, \quad b = vy.$$

pro nějaká $u, v \in \mathbb{N}$. Tedy

$$a^n + b^n + c^n + d^n = u^n x^n + u^n y^n + v^n x^n + v^n y^n = (u^n + v^n)(x^n + y^n).$$

Jistě obě závorky dávají čísla > 1. Proto $a^n + b^n + c^n + d^n$ je 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.

Řešení. V řeči kongruencí tvrzení říká, že $n > 1$ je prvočíslo $\Leftrightarrow (n-1)! \equiv 1 \pmod{n}$.
„$\Rightarrow$“: Buď p prvočíslo. Prvky z množiny $M = \{2, 3, \ldots, p-2\}$ spárujeme tak, že každá dvojice (a, b) splní $a \cdot b \equiv 1 \pmod{p}$. Víme, že ke každému prvku $a \in M$ bude existovat (a to jednoznačně) prvek $b \in M$, neboť $(a, p) = 1$. Kdyby $a = b$, pak $a^2 \equiv 1 \pmod{p}$, ale víme, že jediná řešení kongruence $x^2 \equiv 1 \pmod{2}$ jsou 1 a $p-1$. Díky tomuto párování máme

$$\prod_{a \in M} a \equiv 1 \pmod{p},$$

což nám celkem dává

$$(p-1)! = 1 \cdot (p-1) \cdot \prod_{a \in M} a \equiv p-1 \equiv -1 \pmod{p}.$$

Přitom pro $p = 2, 3$ využíváme konvence, že $\prod_{\emptyset} a = 1$ (případně snadno rozmyslíme, že pro tato prvočísla tvrzení platí).
„$\Leftarrow$“: Pro $n = 4$ máme $(n-1)! \equiv 2 \pmod{4}$ a pro ostatní složená čísla máme $(n-1)! \equiv 0 \pmod{n}$. ■

Příklad 5.9. Dokažte, že $2015 \mid \underbrace{55\ldots5}_{360}$.

Řešení. Vydělením pěti dostáváme

$$403 \mid \underbrace{11\ldots1}_{360},$$

kde

$$\underbrace{11\ldots1}_{360} = \frac{10^{360}-1}{9}.$$

Protože $(403, 9) = 1$, dostáváme ekvivalentní podmínku (kterou chceme dokázat)

$$403 \equiv 10^{360} - 1.$$

Uvažme Eulerovu funkci: $\varphi(403) = \varphi(13) \cdot \varphi(31) = 360$. Protože $(10, 403) = 1$, dostáváme z Eulerovy věty

$$10^{\varphi(403)} = 10^{360} \equiv 1 \pmod{403},$$

tedy

$$403 \mid 10^{360} - 1,$$

což jsme chtěli dokázat. ■

Příklad 5.10. Nechť 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 $k = b_n$.

Řešení. 1. Předpokládejme sporem, že existují $n, m \in \mathbb{N}$ takové, že $a_m = b_n$, tj. $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$. Pak

$$q < \alpha m < q+1, \qquad q < \beta n < q+1,$$

přitom ostré nerovnosti jsou díky iracionalitě α a β. Odtud

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q}, \qquad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}.$$

Sečtením obou řetězců nerovností dostaneme

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q}.$$

To nám dává

$$q < m+n < q+1,$$

což je spor. Nutně jsou tedy obě posloupnosti disjunktní.

2. Jistě $\alpha, \beta > 1$. Navíc právě jedno z nich musí být < 2 (jinak by součet převrácených hodnot byl < 1). Jistě tedy a_1 nebo $b_1 = 1$. Sporem předpokládejme, že v intervalu $(q, q+1)$ pro $q \geq 2$ neleží žádný člen zadaných posloupností, tedy

$$\alpha m < q < q+1 < \alpha(m+1), \qquad \beta n < q < q+1 < \beta(n+1),$$
$$\frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1}, \qquad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}.$$

Sečtením obou řetězců nerovností dostáváme

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1}.$$

Odtud

$$m+n < q < q+1 < m+n+2,$$

což je spor.

■

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.

Řešení. Pro volbu $n = 3^{2^t} - 2^{2^t}$ dostáváme, že chceme ukázat

$$3^{2^t} - 2^{2^t} \mid 3^{3^{2^t} - 2^{2^t} - 1} - 2^{3^{2^t} - 2^{2^t} - 1}.$$

Protože $x - y \mid x^k - y^k$ pro každé $k \in \mathbb{N}$, stačí ukázat, že

$$2^t \mid 3^{2^t} - 2^{2^t} - 1.$$

Zejména tedy chceme ukázat, že

$$3^{2^t} \equiv 1 \pmod{2^t}.$$

Protože $(2,3) = 1$ a $\varphi(2^t) = 2^{t-1}$, máme z Eulerovy věty

$$3^{2^t} = \left(3^{2^{t-1}}\right)^2 \equiv 1^2 = 1 \pmod{2^t},$$

což jsme chtěli dokázat. ■

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

Řešení. Hledejme řešení, pro která $y=-z$, pak dostáváme

$$x^2+2y^2=x^3.$$

Separací proměnných dostáváme

$$x^2\frac{x-1}{2}=y^2.$$

Odtud plyne, že $\frac{x-1}{2}$ je čtverec, tj. $\frac{x-1}{2}=t^2$. Tedy

$$x=2t^2+1, \qquad y=2t^3+t.$$

Pro každé $t\in\mathbb{N}$ dostáváme řešení $\left(2t^2+1,2t^3+t,-2t^3-t\right)$. ■

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 konstruujte induktivně. Ukažte, že pokud je n řešení a $2^n=\ldots dn$ pro nějaké číslo $d=g\cdot 10^m$, kde $g\in\{1,\ldots,9\}$ (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 $2^{75\,353\,432\,948\,736}=\ldots 075\,353\,432\,948\,736$.

Řešení. Nechť n je nějaké řešení. Označme g první nenulovou cifru čísla 2^n, která předchází n. Buď dále k počet cifer čísla n, l počet nul mezi g a n. Konečně označme $d=g\cdot 10^l$. Tedy

$$2^n=\ldots dn, \qquad \text{kde} \qquad d=g\underbrace{0\ldots 0}_{l\times}$$

Pak $dn=n+g\cdot 10^{k+l}$. Chceme ukázat implikaci

$$2^n\equiv n+g\cdot 10^{k+l} \pmod{10^{k+l+1}} \quad\Rightarrow\quad 2^{n+g\cdot 10^{k+l}}\equiv n+g\cdot 10^{k+l} \pmod{10^{k+l+1}}.$$

Díky Čínské zbytkové větě nám stačí ukázat, že

$$2^n\equiv 2^{n+g\cdot 10^{k+l}} \pmod{2^{k+l+1}} \qquad \text{a} \qquad 2^n\equiv 2^{n+g\cdot 10^{k+l}} \pmod{5^{k+l+1}}.$$

Protože k je počet cifer čísla n a $n\geq 36$, je $k<<n$. Je-li l dostatečně malé (nejvýše exponenciální vůči n), pak též $k+l<n$. Odtud

$$2^n\equiv 0\equiv 2^{n+g\cdot 10^{k+l}} \pmod{2^{k+l+1}}.$$

Protože $\varphi\left(5^{k+l+1}\right)=4\cdot 5^{k+l}$, dostáváme z Eulerovy věty

$$2^{d\cdot 10^{k+l}}=\left(2^{d\cdot 2^{k+l-2}}\right)^{\varphi\left(5^{k+l+1}\right)}\equiv 1 \pmod{5^{k+l+1}}.$$

Tím dostáváme

$$2^{n+g\cdot 10^{k+l}}=2^n\cdot 2^{g\cdot 10^{k+l}}\equiv 2^n \pmod{5^{k+l+1}}.$$

Ukázali jsme tedy, že je-li n řešení, pak je řešení i $dn=n+g\cdot 10^{k+l}$. ■