

## Teorie čísel – Řešení

Jakub „šněk“ Opršal, 2. března 2009

**Příklad 1.** Dokažte, že přirozené číslo  $p$  je prvočíslo právě když  $p$  dělí  $(p-1)! + 1$ .

*Řešení:* Uvažme polynom  $x^{p-1} - 1$ . Když do něj budeme dosazovat postupně zbytky  $1, 2, \dots, p-1$  dostaneme pokaždé číslo dělitelné  $p$ . Postupně si vyjádříme  $x^{p-1}$  pomocí kořenových činitelů  $x-1, x-2, \dots, x-(p-1)$ . Z dělení polynomů se zbytkem  $x^{p-1} = (x-1)q_1(x) + r_1$ , kde nutně  $p \mid r-1$ . Dále postupujeme indukcí necht  $x^{p-1} = (x-1)(x-2) \cdots (x-k)q_k(x) + r_k(x)$ , kde  $p$  dělí všechny koeficienty polynomu  $r_k(x)$ . Pak  $q_k(x) = (x-k-1)q_{k+1}(x) + s_{k+1}$ , kde opět  $p$  musí dělit  $s_{k+1}$  (aby  $(k+1)^{p-1} \equiv 1 \pmod{p}$ ), za  $r_{k+1}$  položíme  $(x-1)(x-2) \cdots (x-k)s_{k+1} + r_k(x)$  a opět  $p$  dělí všechny koeficienty  $r_{k+1}$ . Nakonec dostaneme  $x^{p-1} = (x-1)(x-2) \cdots (x-p+1) + r_{p-1}(x)$  (rozmysli si, že  $q_{p-1}$  musí nutně opravdu být 1) a porovnáním absolutních členů dostáváme právě  $(-1)^{p+1}(p+1)! \equiv -1 \pmod{p}$ , což pro  $p$  liché dá požadované a pro  $p=2$  také, neboť  $-1 \equiv 1 \pmod{2}$ . Zbývá pačná implikace, pokud  $p=cd$  je složené, že  $c, d > 1$ .  $c \mid (p-1)!$  protože se v něm přímo vyskytuje, tj. nemůže platit  $(p-1)! + 1$  je násobek  $n$ , protože je s  $c$  nesoudělné.

**Příklad 2.** Dokažte, že pro každé  $n \in \mathbb{N}$  lze z číslic 1, 2 sestavit  $n$ -ciferné číslo, které je dělitelné  $2^n$ .

*Řešení:* Budeme postupovat matematickou indukcí. Prvně pro  $n=1$  Určitě  $2 \mid 2$ . Předpokládejme tedy, že pro  $n-1$  existuje  $a_{n-1}$   $n-1$ -ciferné číslo, že  $2^{n-1} \mid a_{n-1}$  složené jen z cifer 1, 2. Nutně musí platit  $a_{n-1} \equiv 0$  nebo  $a_{n-1} \equiv 2^{n-1} \pmod{2^n}$ . Přitom  $10^{n-1} \equiv 2^{n-1} \pmod{2^n}$ . Tedy pokud nastane první možnost, tak k  $a_{n-1}$  přidáme na začátek dvojku, pokud druhá, tak jedničku – tj.  $a_n = 10^{n-1} + a_{n-1} \equiv 2^{n-1} + 2^{n-1} \equiv 0 \pmod{2^n}$ .

Můžete si rozmyslet, že něco podobného bude platit i pro mocniny čísla 5, jen budete potřebovat pět cifer místo dvou (rozmyslete si, které to jsou).

**Příklad 3.** Dokažte, že součin dvou čísel tvaru  $a^2 + ab + b^2$  (pro  $a, b \in \mathbb{Z}$ ) je opět tohoto tvaru.

*Řešení:* Odvodíme identitu platnou v tělese komplexních čísel. Necht  $\omega$  je kořen polynomu  $x^2 + x + 1$ , rozmysli si, že i  $\omega^2$  bude kořen tohoto polynomu. Pak  $(a - \omega b)(a - \omega^2 b) = a^2 + ab + b^2$ . Roznásobíme teď závorky:

$$(a - \omega b)(c - \omega d) = x - \omega y$$

Za  $\omega^2$  můžeme dosadit  $-1 - \omega$ , tedy nám vyjdou nějaká celá čísla  $x$  a  $y$ . Poslední, co si musíme uvědomit je, že pak i

$$(a - \omega^2 b)(c - \omega^2 d) = x - \omega^2 y$$

neboť  $\omega$  i  $\omega^2$  má stejné algebraické vlastnosti, vlastně bychom jen zopakovali přechozí výpočet. Nutně pak vynásobením těchto dvou rovností:

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = (x^2 + xy + y^2)$$

Kdybychom výpočty opravdu provedli (což se nám samozřejmě nebude chtít, když to dělat nemusíme) dostali bychom:

$$\begin{aligned}x &= ac - bd \\ y &= bc + ad + bd\end{aligned}$$

**Příklad 4.** Najděte všechny dvojice přirozených čísel  $x, y$ , pro která platí:

$$x(x+1)(x+2)(x+3) = y^2$$

*Řešení:* Neuvedeno.

**Příklad 5.** Rozhodněte, zda existují taková přirozená čísla  $x, y$ , že čísla  $x+y, 2x+y$  a  $x+2y$  jsou všechna druhé mocniny přirozených čísel.

*Řešení:* Nejdříve označme čtverce v pořadí, jak jsou v zadání  $a^2, b^2$  a  $c^2$ . Podívejme se na číslo  $3(x+y)$ :

$$3a^2 = 3(x+y) = (2x+y) + (x+2y) = b^2 + c^2$$

Podívejme se teď na rovnici  $3a^2 = b^2 + c^2$  a dokažme, že nemá žádné řešení  $a, b, c$ .

Rozdělme si případ na  $a$  je sudé a  $a$  je liché. Prvně  $a$  je sudé a nechť  $a = 2^m r$ , kde  $r$  je liché (takový rozklad existuje z jednoznačného rozkladu na prvočísla). Pak  $4^m \mid 3a^2$ , tj.  $4 \mid b^2 + c^2$  a z kvadratických zbytků modulo 4 dostaneme  $b = 2b'$  a  $c = 2c'$  pro nějaké  $b', c' \in \mathbb{N}$  a můžeme celou rovnici pokrátit čtyřmi, tj. položíme ještě  $a' = 2^{m-1}r$  a dostaneme opět  $3a'^2 = b'^2 + c'^2$ . Indukcí dolů dojdeme až k  $m = 0$  a  $a$  je liché.

Je-li  $a$  liché, tak  $3a^2 \equiv 3 \pmod{4}$  a dostáváme rovnou  $b^2 + c^2 \equiv 3 \pmod{4}$  což je rovnou spor s kvadratickými zbytky modulo 4. Úloha tedy nemá žádné řešení.

**Příklad 6.** Nechť  $a, b, c$  a  $d$  jsou přirozená čísla a platí  $ab = cd$ . Dokažte, že pro každé  $n \in \mathbb{N}$  je číslo  $a^n + b^n + c^n + d^n$  složené.

*Řešení:* Z rovnosti  $ab = cd$  nahlédněme, že

$$(a^n + b^n + c^n + d^n)a^n = (a^n + c^n)(a^n + d^n)$$

Tuto rovnost podělme  $a^n$ , dostaneme na obou stranách celá čísla. Nechť rovnou  $s, r \in \mathbb{N}$  taková, že  $s \mid a^n + c^n$ ,  $r \mid a^n + d^n$  a  $a^n = rs$  (rozmyslete si, proč musí existovat).

$$\begin{aligned} (a^n + b^n + c^n + d^n) &= \frac{(a^n + c^n)(a^n + d^n)}{a^n} \\ (a^n + b^n + c^n + d^n) &= \frac{a^n + c^n}{s} \cdot \frac{a^n + d^n}{r} \end{aligned}$$

Tedy máme rozklad čísla  $a^n + b^n + c^n + d^n$ . Tento rozklad je netriviální, protože  $s, r \leq a^n$ , tedy:

$$\frac{a^n + c^n}{s} \geq \frac{a^n + c^n}{a^n} > 1$$

a obdobně pro druhý zlomek.

**Příklad 7.** Nechť  $a, b, c, d, e$  jsou přirozená čísla taková, že  $25 \mid a^5 + b^5 + c^5 + d^5 + e^5$ . Dokažte, že pak  $5 \mid abcde$ .

*Řešení:* Prvně nahlédněme, že  $x^5$  může nabývat jen pěti zbytků modulo 25 a to 1, 7, -7, -1 a 0. Dokažeme, že je-li  $a \equiv b \pmod{5}$  pak  $a^5 \equiv b^5 \pmod{25}$ . Rozložme:

$$a^5 - b^5 = (a - b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4)$$

Nutně  $5 \mid a - b$ , protože  $a \equiv b \pmod{5}$ . Použijme tento argument ještě jednou a spočtěme hodnotu druhé závorky modulo 5. Můžeme za  $b$  dosadit  $a$ , protože dávají stejný zbytek a kongruenci to tedy nezmění:

$$a^4 + a^3b + a^2b^2 + ab^3 + b^4 \equiv 5a^4 \equiv 0 \pmod{5}$$

Tedy 5 dělí obě závorky a tedy 25 dělí jejich součin. Zbývá nám tedy určit pět hodnot, to uděláme umocněním čísel 0, 1, 2, -2 a -1 na pátou.

Nakonec nahlédněme, že jedno z čísel musí být 0, tj. BÚNO  $a^5 \equiv 0 \pmod{25}$  ale pak nutně  $5 \mid a$  a tedy i  $5 \mid abcde$ . Kdyby byla všechna čísla nenulová, tak jejich součtem nemůžeme dostat žádné číslo dělitelné 25. Jediná čísla, která přicházejí v úvahu jsou 0, 25 a -25, neboť nejméně můžeme dostat  $-7 \cdot 5 = 35$  a nejvíce  $7 \cdot 5 = 25$ .

Součet 0 není možný, protože sčítáme pět lichých čísel. Součet 25 bychom mohli dostat jako  $x \cdot 7 + y$ , kde  $x$  je počet 7 minus počet -7, obdobně  $y$  je počet 1 minus počet -1.  $25 = 3 \cdot 7 + 4$  Tedy musím použít alespoň 4 jedničky a tři 7, což není možné. Pro -25 zopakujeme tu samou úvahu jen s opačným znaménkem.

**Příklad 8.** Nechť  $m, n$  jsou přirozená čísla taková, že rovnice

$$(x + n)(x + m) = x + m + n$$

Má alespoň jedno celočíselné řešení. Dokažte, že platí

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

*Řešení:* Tento příklad se vyskytl na CK v Litoměřicích 2006. Řešení tedy najdete na stránkách matematické olympiády.

**Příklad 9.** Uvažme posloupnost  $a_n$  danou vztahem:

$$a_n = 2^n + 3^n + 6^n - 1$$

Dokažte, že pro každé prvočíslo  $p$  existuje  $n$ , že  $p \mid a_n$ .

*Řešení:* (IMO 2006, México) Nejdříve pro  $p = 2, 3$  najdeme přímo člen, které bude dělitelný šesti:

$$a_2 = 4 + 9 + 36 - 1 = 48$$

Dále necht  $p > 3$  prvočíslo. Pak  $p$  je nesoudělné s 6, tj. vynásobením  $a_n$  šesti nezmění dělitelnost  $p$ , za  $n$  rovnou dosadíme  $p - 2$  a z malé Fermatovy věty dostaneme:

$$6a_{p-2} = 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 \equiv 0 \pmod{p}$$

Tedy  $p \mid a_{p-2}$ .

**Příklad 10.** Dokažte, že pro každé přirozené  $n > 1$  je číslo  $n^4 + 4^n$  složené.

*Řešení:* Pro  $n$  sudé je číslo  $n^4 + 4^n$  dělitelné dvěma. Necht tedy  $n = 2k + 1$  pro nějaké  $k > 1$ . Pak:

$$x^4 + 4^{2k+1} = x^4 + 4 \cdot (2^k)^4$$

Ale číslo  $a^4 + 4b^4$  je pro  $a > 1$  složené, neboť:

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

Přičemž obě závorky jsou ostře větší než 1 (rozmyslete si, neměl by to být takový problém, kdyžtak se maximálně použije jednoduchá AG nerovnost).

**Příklad 11.** Necht  $n \in \mathbb{N}$ . Dokažte, že číslo  $2^{2^n} + 2^{2^{n-1}} + 1$  má alespoň  $n$  různých prvočíselných dělitelů.

*Řešení:* Budeme postupovat indukcí. Označme si pro jednoduchost  $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ . Číslo  $a_1 = 2^2 + 2 + 1 = 7$  má prvočíselného dělitele. Dále předpokládejme, že tvrzení platí pro  $n - 1$ . Nahlédněme rovnost:

$$a_n = (2^{2^n} + 2^{2^{n-1}} + 1) = (2^{2^{n-1}} - 2^{2^{n-2}} + 1)(2^{2^{n-1}} + 2^{2^{n-2}} + 1) = (2^{2^{n-1}} - 2^{2^{n-2}} + 1)a_{n-1}$$

Dokonce platí obecně  $a^4 + a^2 + 1 = (a^2 + a + 1)(a^2 - a + 1)$ .

Víme už, že  $a_{n-1}$  má  $n - 1$  různých prvočíselných dělitelů. Zbývá jen nahlédnout, že druhá závorka je ostře větší než 1, což je zřejmé, a nesoudělná s  $a_{n-1}$ .

Nesoudělnost ověříme „Euklidovým algoritmem“:

$$2^{2^{n-1}} + 2^{2^{n-2}} + 1 = (2^{2^{n-1}} - 2^{2^{n-2}} + 1) + 2 \cdot 2^{2^{n-2}}$$

Tedy společný dělitel musí dělit  $2^{2^{n-2}+1}$ , ale žádné takové  $d$  krom  $d = 1$  nedělí  $a_n$ , neboť to je liché a  $d$  je sudé.

**Příklad 12.** Necht  $k > 1$  je přirozené číslo. Ukažte, že  $2^{2^n} + k$  je složené pro nekonečně mnoho přirozených čísel  $n$ .

*Řešení:* Neuvedeno.