



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OPVK – CZ.1.07/2.3.00/09.0017

**MATES – Podpora systematické práce se žáky SŠ v oblasti rozvoje matematiky**

## Výjezdní seminář Karlov pod Pradědem, 5.–8. května 2012

### Základní poznatky

Celé číslo  $a$  dělí celé číslo  $b$ , vlastnosti dělení, dělení se zbytkem, největší společný dělitel a Eukleidův algoritmus. Součin největšího společného dělitele a nejmenšího společného násobku dvou celých čísel. Prvočíslo, základní věta aritmetiky (věta o jednoznačném rozkladu na součin prvočísel), nekonečnost množiny prvočísel. Vzorec pro pythagorejské trojice čísel, kongruence, Čínská zbytková věta, celá část, vlastnosti celé části. Polynomy s celými koeficienty, vlastnosti.

### Malá Fermatova věta.

Nechť  $a$  je (kladné) celé číslo a  $p$  prvočíslo. Potom

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

resp. pro (kladná) celá čísla  $a$  nesoudělná s prvočíslem  $p$  platí

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

Opačná implikace neplatí! Fermatův prvočíselný test (podobně také testy Solovay–Strassen, Miller–Rabin). Například  $341 \mid 2^{341} - 2$ . Dále viz Carmichaleova čísla.

Počet všech čísel z množiny  $\{1, 2, \dots, m\}$  nesoudělných s číslem  $m$  značíme  $\phi(m)$ . Funkce  $\phi$  se obvykle nazývá *Eulerova funkce*  $\phi$ . Dá se ukázat, že jestliže  $m = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$  je rozklad čísla  $m$  na součin prvočísel, potom

$$\begin{aligned} \phi(m) &= (p_1^{k_1} - p_1^{k_1-1}) (p_2^{k_2} - p_2^{k_2-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) = \\ &= m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right). \end{aligned}$$

Například pro prvočíslo  $p$  platí  $\phi(p) = p - 1$ .

### Eulerova věta.

Nechť  $m$  je přirozené číslo a  $a$  je (kladné) celé číslo nesoudělné s  $m$  ( $D(a, m) = 1$ ). Potom

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky

RSA šifrovací algoritmus, Diffie-Hellmanův protokol.

Přirozené číslo  $a$  se nazývá primitivním kořenem modulo  $m$ , právě když nejmenší přirozená mocnina  $s$  čísla  $a$ , pro kterou platí

$$a^s \equiv 1 \pmod{m},$$

je  $s = \phi(m)$ .

**Gauss.**

Pro přirozené číslo  $n$  existuje primitivní kořen modulo  $n$ , právě když  $n$  je jednoho z tvarů  $1, 2, 4, p^k, 2p^k$ , kde  $p$  je liché prvočíslo a  $k$  přirozené číslo.

**Wilsonova věta.**

Přirozené číslo  $p > 1$  je prvočíslo, právě když

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

**Identita Sofie Germainové.**

Nechť  $a, b$  jsou celá čísla, potom  $a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$ .

### Příklady

1. Pro přirozené číslo  $n > 1$  je číslo  $n^4 + 4^n$  vždy složené. Dokažte.
2. Je  $4^{545} + 545^4$  prvočíslo?
3. Nechť  $n$  je celé nezáporné číslo. Potom číslo  $2^{2^n} + 2^{2^{n-1}} + 1$  je dělitelné alespoň  $n$  navzájem různými prvočísly. Dokažte.
4. Najděte všechna prvočísla tvaru  $n^n + 1$  menší než  $10^{19}$ , kde  $n$  je přirozené číslo.
5. Může být číslo  $A$ , jehož desítkový zápis obsahuje 600 číslic 6 a několik číslic 0 druhou mocninou přirozeného čísla?
6. Rovnice  $15x^2 - 7y^2 = 9$  nemá řešení v oboru přirozených čísel. Dokažte.
7. Devítimístné číslo, jehož desítkový zápis obsahuje všechny číslice s výjimkou nuly a které končí číslicí 5, není druhou mocninou celého čísla. Dokažte.
8. Neexistuje polynom  $f(x)$  s celými koeficienty takový, že  $f(7) = 11$ ,  $f(11) = 13$ . Dokažte.
9. Nechť  $p$  je prvočíslo. Najděte všechna řešení rovnice  $\frac{1}{x} + \frac{1}{y} = \frac{1}{p}$  v oboru přirozených čísel.
10. Začnu nějakým víceciferným číslem  $a_1$ , potom vytvářím posloupnost čísel  $a_1, a_2, a_3, \dots$ . Číslo  $a_{n+1}$  vznikne z čísla  $a_n$  připsáním číslice různé od devítky. Ukažte, že takto nemohu vytvořit posloupnost, která by obsahovala jen konečný počet složených čísel.
11. V posloupnosti  $1, 9, 7, 7, 4, 7, 5, 3, 9, 4, 1, \dots$  je každá číslice od páté rovna součtu předcházejících čtyř číslic modulo 10. Rozhodněte, zda se někde dále za sebou objeví číslice: a) 1234, b) 3269, c) 1977, d) 0197.
12. Ukažte, že rovnice  $x^2 + y^2 + z^2 = 2xyz$  nemá v oboru celých čísel jiné řešení než  $x = u = z = 0$ .
13. Dokažte, že  $f(n) = n^5 + n^4 + 1$  je pro  $n > 1$  číslo složené.
14. (\*) Jestliže  $n \geq 3$  je přirozené číslo, potom  $2^n$  můžeme vyjádřit ve tvaru  $2^n = 7x^2 + y^2$ , kde  $x$  a  $y$  jsou lichá čísla.
15. (\*) Jestliže  $a, b$  a  $q = (a^2 + b^2)/(ab + 1)$  jsou přirozená čísla, potom  $q$  je druhou mocninou celého čísla. Dokažte.
16. (\* Pellova rovnice) Nechť  $d$  je přirozené číslo, najděte všechna řešení rovnice  $x^2 - dy^2 = 1$  v oboru přirozených čísel.