MB141 – 10. cvičení
Dělitelnost

Martin Čadek

Jarní semestr 2020

Příklad 1. Dokažte, že pro libovolná celá čísla a platí:

A

1. a^2 má po dělení 4 zbytek 0 nebo 1.
2. a^2 má po dělení 8 zbytek 0, 1 nebo 4.
3. a^4 má po dělení 16 zbytek 0 nebo 1.

Před tím, než budeme úlohu řešit, připomeneme si binomickou větu: Pro reálná čísla x a y ze střední školy známe, že

$$(x+y)^2 = x^2 + 2xy + y^2$$

Možná i také, že

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Pro libovolné přirozené n platí

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \dots + \binom{n}{n-2} x^2 y^{n-2} + \binom{n}{n-1} x y^{n-1} + y^{n-1}.$$

Zde $\binom{n}{k}$ jsou binomické koeficienty: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

kde $j! = j(j-1)(j-2)\cdots 1$

Příklad 1. Dokažte, že pro libovolná celá čísla a platí: (B)

1. a^2 má po dělení 4 zbytek 0 nebo 1.
2. a^2 má po dělení 8 zbytek 0, 1 nebo 4.
3. a^4 má po dělení 16 zbytek 0 nebo 1.

Napišme si číslo a ve tvaru $a = 2b + r$, kde r je zbytek po dělení dvěma, tedy $r = 0$ nebo 1.

Spočítáme a^2:

$$a^2 = (2b+r)^2 = (2b)^2 + 2(2b)\cdot r + r^2 = 4b^2 + 4br + r^2.$$

Tedy po dělení 4 dává a^2 zbytek $r^2 = 0^2 = 0$ nebo $1^2 = 1$.

Nyní pišme $a = 4c + z$, kde $z = 0, 1, 2, 3$ je zbytek po dělení 4. Platí

$$a^2 = (4c+z)^2 = (4c)^2 + 2(4c)z + z^2 = 16c^2 + 8cz + z^2.$$

Tedy a^2 má po dělení 4 zbytek jako z^2, tj: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$. Zbytek po dělení 4 čísla 9 je 1.

Příklad 1. Dokažte, že pro libovolná celá čísla a platí:

C

1. a^2 má po dělení 4 zbytek 0 nebo 1.
2. a^2 má po dělení 8 zbytek 0, 1 nebo 4.
3. a^4 má po dělení 16 zbytek 0 nebo 1.

Pro $a = 4c + z$, kde $z = 0, 1, 2, 3$, spočítáme

$$a^4 = (4c+z)^4 = (4c)^4 + \binom{4}{1}(4c)^3 z + \binom{4}{2}(4c)^2 \cdot z^2 + \binom{4}{3}(4c) z^3 + z^4$$

$$= 16^2 c^4 + 4 \cdot 4^3 c^3 z + 6 \cdot 4^2 c^2 z^2 + 4 \cdot 4 c z^3 + z^4 = 16m + z^4$$

Zbytek a^4 po dělení 16 je stejný jako zbytek čísel $0^4, 1^4, 2^4, 3^4$ po dělení 16, tj. 0, 1, 0, 1.

A

Příklad 2. Jaké jsou poslední dvě cifry čísel: 4^{81}, 7^{14}, 3^{59}?

Poslední cifra nějakého čísla je dána zbytkem po dělení číslem 10. Poslední dvě cifry jsou dány zbytkem po dělení číslem $100 = 4 \cdot 25$.

Číslo 4^{81} je dělitelné číslem 4. Zjistíme, jaký zbytek dává po dělení číslem $25 = 5^2$.

Použijeme, že pro mocniny platí $x^{a+b} = x^a \cdot x^b$, a binomickou větu:

$$4^{81} = 4^{80} \cdot 4 = (5-1)^{80} \cdot 4 = \Big(5^{80} + 80 \cdot 5^{79}(-1) + \dots + \binom{80}{78} 5^2 (-1)^{78}$$
$$+ 80 \cdot 5(-1) + (-1)^{80}\Big) \cdot 4 = (25m+1) \cdot 4 = 100m + 4$$

Tedy 4^{81} dává po dělení 100 zbytek 4, poslední dvě cifry jsou 04.

Číslo 7^{14}: Použijeme, že $x^{a \cdot b} = (x^a)^b$ a binomickou větu.

(B)

Příklad 2. Jaké jsou poslední dvě cifry čísel: 4^{81}, 7^{14}, 3^{59}?

$$7^{14} = 7^{2\cdot 7} = (7^2)^7 = 49^7 = (50-1)^7 = 50^7 - 7\cdot 50^6\cdot 1 +$$

$$\binom{7}{2} 50^5\cdot 1^2 - \binom{7}{3} 50^4\cdot 1^3 + \binom{7}{4} 50^3\cdot 1^4 - \binom{7}{5} 50^2\cdot 1^5$$

$$+ 7\cdot 50\cdot 1^6 - 1^7 = 100m + 350 - 1 = 100m + 349 =$$

$$= 100(m+3) + 49$$

Tedy 7^{14} dává po dělení 100 zbytek 49. Poslední dvě cifry jsou 49.

Číslo 3^{59}: Počítáme: $3^{59} = 3^{58}\cdot 3 = (3^2)^{29}\cdot 3 = (10-1)^{29}\cdot 3 =$

$$= \left(10^{29} - 29\cdot 10^{28} + \ldots - \binom{29}{27} 10^2\cdot 1^{27} + 29\cdot 10\cdot 1^{28} - 1^{29}\right)\cdot 3 =$$

$$= (100m + 290 - 1)\cdot 3 = (100(m+2) + 89)\,3 = 100(3m+6) + 267$$

Poslední dvě cifry jsou 67.

Příklad 3. Najděte největšího společného dělitele čísel

(a) 227, 133,

(b) 3441, 2665.

A

Použijeme Eukleidův algoritmus. Podle něj největší společný dělitel čísel $a_1 \geq a_2 \geq 1$ dostaneme postupným dělením se zbytkem

$$a_1 = a_2 \cdot q_2 + a_3 \qquad 0 \leq a_3 < a_2$$

$$a_2 = a_3 \cdot q_3 + a_4 \qquad 0 \leq a_4 < a_3$$

$$- - - - - - - - - -$$

$$a_{k-1} = a_k q_k + a_{k+1} \qquad 0 < a_{k+1} < a_k$$

$$a_k = a_{k+1} q_{k+1} + 0$$

Největší společný dělitel čísel a_1, a_2 je pak a_{k+1}

$$(a_1, a_2) = a_{k+1}.$$

Přitom platí $(a_1, a_2) = (a_2, a_3) = \dots = (a_k, a_{k+1}) = a_{k+1}$.

Příklad 3. Najděte největšího společného dělitele čísel

B

(a) 227, 133,

(b) 3441, 2665.

Podle předchozího počítáme

$$(227, 133) = (133, 94) = (94, 39) = (39, 16) = (16, 7)$$
$$= (7, 2) = 1$$

$$(3441, 2665) = (2665, 776) = \cancel{(776, 437) = (437, 339)}$$
$$\cancel{= (339, 98) = (98, 43) = (43, 12) = (12, 7) = 1.}$$
$$= (776, 337) = (337, 102) = (102, 31) =$$
$$= (31, 9) = (9, 4) = (4, 1) = 1$$

Příklad 4. Nalezněte celá čísla x a y tak, aby $883x + 487y = d$ byl největší společný dělitel čísel 883 a 487. Spočtěte x a y i pro dvojice čísel z předchozíhom příkladu.

A

Využijeme skutečnosti, že největší společný dělitel $d = (a, b)$ dělí všechna čísla tvaru $ax + by$. Dále kombinací $ax + by = d$ dostaneme z kombinací

$$a \cdot 1 + b \cdot 0 = a,$$

$$a \cdot 0 + b \cdot 1 = b.$$

Odtud plyne náš algoritmický výpočet. Píšeme tabulku

x	y	$ax+by$
1	0	a
0	1	b

a doplňujeme ji o řádky, které vzniknou kombinací dvou předchozích tak, aby vpravo bylo číslo menší než v předchozím řádku.

B

Příklad 4. Nalezněte celá čísla x a y tak, aby $883x + 487y = d$ byl největší společný dělitel čísel 883 a 487. Spočtěte x a y i pro dvojice čísel z předchozíhom příkladu.

x	y	$883x + 487y$	
1	0	883	Od 1. řádku odečteme 2.
0	1	487	Od 2. řádku odečteme 3.
1	-1	396	Od 3. řádku odečteme 4× 4. řádek
-1	2	91	− 4. řádek + 3× 5. řádek
5	-9	32	Od 5. řádku odečteme 6× 6. řádek
16	-29	5	Od 6. řádku odečteme 2× 7. řádek
-91	165	2	
198	-359	✓ 1 = (883, 487)	
-487	883	0	

Tedy $x = 198$, $y = -359$

$883 \cdot 198 - 487 \cdot 359 = 1$

Příklad 4. Nalezněte celá čísla x a y tak, aby $883x + 487y = d$ byl největší společný dělitel čísel 883 a 487. Spočtěte x a y i pro dvojice čísel z předchozíhom příkladu.

C

x	y	$3441x + 2665y$
1	0	3441
0	1	2665
1	-1	776
-3	4	337
7	-9	102
-24	31	31
79	-102	9
-261	337	4
601	-776	1

$x = 601$

$y = -776$

Příklad 5. Najděte všechna přirozená n taková, že $n-1 \mid n^3+1$.

A

Platí vztahy

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

Obecně pro každé k přirozené $k \geq 2$

$$a^k - b^k = (a-b)(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\dots+ab^{k-2}+b^{k-1})$$

Pro součet platí analogie pouze pro liché mocniny:

$$a^3+b^3 = (a+b)(a^2-ab+b^2)$$
$$a^{2k+1}+b^{2k+1} = (a+b)(a^{2k}-a^{2k-1}b+\dots-ab^{2k-1}+b^{2k})$$

Třetí mocniny využijeme pro řešení naší úlohy:
Čísla n^3-1 je blízké číslu n^3+1. Navíc platí
$n^3-1 = n^3-1^3 = (n-1)(n^2+n+1)$. Tedy $n-1 \mid n^3-1$.
Jestliže $n-1 \mid n^3+1$, pak $n-1 \mid (n^3+1)-(n^3-1)=2$. Tedy $n-1$ dělí 2

(B)

Příklad 5. Najděte všechna přirozená n taková, že
$n - 1 \mid n^3 + 1$.

a proto jsou pouze bylo možnosti $n-1=2$, $n-1=1$. Tedy $n=3$, $n=2$.

$n = 3$ $\quad n-1 = 2 \mid n^3+1 = 28$,

$n = 2$ $\quad n-1 = 1 \mid n^3+1 = 9$.

A

Příklad 6. Dokažte, že pro přirozená čísla a, k a n platí: jestliže $k \mid n$, pak $a^k - 1 \mid a^n - 1$. Pomocí toho dokažte: Je-li $2^n - 1$ prvočíslo, pak n musí být také prvočíslo.

Nechť k dělí n. Pak $n = k \cdot q$. Dále

$$a^n - 1 = a^n - 1^n = (a^k)^q - (1^k)^q =$$

$$= \left((a^k) - (1^k)\right)\left((a^k)^{q-1} + (a^k)^{q-2} + \dots + 1\right)$$

$$= (a^k - 1)\, m$$

Tedy $a^k - 1$ dělí $a^n - 1$.

Je-li n složené, tj. $n = c \cdot d$ pro $c \geq 2, d \geq 2$, pak $2^c - 1$ dělí $2^n - 1$

$2^c - 1 \geq 3$, tedy $2^n - 1$ nemůže být prvočíslo.

Proto se velká prvočísla hledají ve tvaru $2^p - 1$, kde p je prvočíslo.

A

Příklad 7. Dokažte, že $25 \mid 4^{2n+1} - 10n - 4$.

S využitím vlastností mocnin a pomocí binomické věty dokážeme

$$4^{2n+1} - 10n - 4 = (5-1)^{2n+1} - 10n - 4 =$$

$$= \underbrace{5^{2n+1} - 5 \cdot 5^{2n} \cdot 1 + \cdots - \binom{2n+1}{2n-1} 5^2 \cdot 1^{2n-1}}_{} + (2n+1) 5 \cdot 1 - 1$$

$$- 10n - 4 = 25m + 10n + 5 - 1 - 10n - 4 = 25m.$$