Úloha č.1

Dělitelnost
aneb "Modulární aritmetika"

Mirko Rokyta, KMA MFF UK Praha
Janov, 15.10.2011

1 Trochu o kritériích dělitelnosti

Dobře známá jsou kritéria, určující, kdy je nějaké přirozené číslo a dělitelné následujícími čísly:

2	poslední cifra a je sudá (tj. dělitelná dvěma)
3	ciferný součet a je dělitelný 3
4	poslední dvojčíslí a je dělitelné 4
5	poslední cifra a je 0 nebo 5 (tj. dělitelná pěti)
(6	a je dělitelné 2 a 3)
8	poslední trojčíslí a je dělitelné 8
9	ciferný součet a je dělitelný 9
10	poslední cifra zkoumaného čísla je 0

7? 11? ...

Obecnější než zkoumat dělitelnost je zkoumat zbytek při dělení.

Definice. Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n.

Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$11 \bmod 2 = 1$, $53 \bmod 7 = 4$,
$11 \equiv 1 \pmod 2$, $53 \equiv 4 \pmod 7$,
$22 \equiv 71 \pmod 7$, $10 \equiv -1 \pmod{11}$.

Platí:

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad n \text{ dělí } (a-b).$$

2 Modulární aritmetika

... aneb počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:
  hodiny, týdny, roky ... $14 \equiv 2 \pmod{12}$, $730 \equiv 0 \pmod{365}$,...

[scale=0.4]hodiny.eps

- Dobrá zpráva č.2: sčítání, odečítání, násobení i umocnění kongruencí je snadné:

Tvrzení 2.1.

$$\begin{aligned} a_1 &\equiv b_1 \pmod n \\ a_2 &\equiv b_2 \pmod n \end{aligned}$$

$$\Downarrow$$

$$\begin{aligned} (a_1 + a_2) &\equiv (b_1 + b_2) \pmod n \\ (a_1 - a_2) &\equiv (b_1 - b_2) \pmod n \\ (a_1 \cdot a_2) &\equiv (b_1 \cdot b_2) \pmod n \\ a_1^k &\equiv b_1^k \pmod n \qquad \text{pro } k \in \mathbb{N}. \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12},\ 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12},\ 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 2 \cdot 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 = 322 \equiv 1 \pmod{12}$
- $10 \equiv -1 \pmod{11}$
  $\Rightarrow \quad 10^k \equiv (-1)^k \pmod{11}, \qquad k \in \mathbb{N},$
  $\Rightarrow \quad a_k 10^k \equiv a_k (-1)^k \pmod{11}, \quad a_k \in \{0, \ldots, 9\},$
  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k (-1)^k \pmod{11}.}$

3 Zpátky k dělitelnosti

...
$\Rightarrow \quad \sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k (-1)^k \pmod{11}$
$\Rightarrow$

Tvrzení 3.1. *Číslo* $a \in \mathbb{N}$*, jehož dekadický zápis je*

$$a = \overline{a_n a_{n-1} \cdots a_1 a_0}$$

je dělitelné 11 *právě tehdy, když je dělitelné* 11 *číslo*

$$a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \,.$$

(Dokonce platí: obě čísla dávají při dělení 11 stejné zbytky).

Příklady:

- Je číslo $9\,888\,888\,888$ dělitelné číslem 11?

  Odpověď:

  $$9\,888\,888\,888 \equiv 8 - 8 + \cdots + 8 - 9 = -1 \equiv 10 \pmod{11}\,.$$

  Číslo $9\,888\,888\,888$ není dělitelné číslem 11, dokonce víme, že při dělení dostaneme zbytek 10.

- Rodná čísla jsou dělitelná 11. (Opatření proti zfalšování rodného čísla... které všichni znají).

  $$930106/1213 \;\Rightarrow\; 9301061213 \;\Rightarrow\; 11 - 15 = -4$$

  ... falešné rodné číslo.

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3\,, \qquad k \in \mathbb{N}\,,$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3\,, \quad a_k \in \{0, \ldots, 9\}\,,$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Tím je ukázáno, že přirozené číslo dává při dělení třemi stejný zbytek jako jeho ciferný součet.

Dělitelnost sedmi:

- $10 \equiv 3 \pmod 7$

  $\Rightarrow \quad 10^k \equiv 3^k \pmod 7\,, \qquad k \in \mathbb{N}\,,$

  $\Rightarrow \quad a_k 10^k \equiv a_k 3^k \pmod 7\,, \quad a_k \in \{0, \ldots, 9\}\,,$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k 3^k \pmod 7.}$

Příklad:
Určete zbytek při dělení sedmi čísla 1 111 111.
Řešení:
$1\,111\,111 \equiv 1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 = \frac{3^7 - 1}{3 - 1} = 1093 \pmod 7$
$1093 \equiv 3 + 9 \cdot 3 + 1 \cdot 3^3 = 57 \equiv 1 \pmod 7$.

Dělitelnost (např.) 77:

- $n = 35 \cdot 987654321$ není dělitelné 77 (Proč?)
- Jaký je zbytek při dělení $n = 35 \cdot 987654321$ číslem 77?
  - $77 = 7 \cdot 11$ (a čísla 7, 11 nemají společné dělitele).
  - n je dělitelné 7 (je násobkem sedmi). (Proč?)
  - Protože $77 = 7 \cdot 11$, musí být násobkem sedmi i zbytek čísla n při dělení 77. (Proč?)
  - Zbytek čísla n při dělení 11 je $1 - 2 + 3 - 4 + 5 - 6 + 7 - 8 + 9 = 5$
  - Tedy $35 \cdot 987654321 \equiv 2 \cdot 5 = 10 \mod 11$.
  - Zbytek čísla n při dělení 77 je tedy z množiny $\{10, 21, 32, 43, 54, 65, 76\}$. Z nich jedině číslo 21 je dělitelné 7.
- Tedy $35 \cdot 987654321 \equiv 21 \pmod{77}$.

Úloha.
Učitel si myslí číslo, které končí číslicí 6 a které dává při dělení 13 zbytek 9. Jaký zbytek dává toto číslo při dělení 65?

$65 = 5 \cdot 13$ (a čísla 5, 13 nemají společné dělitele).
$n \equiv 9 \pmod{13}$ $\quad$ $n \equiv 1 \pmod{5}$
Hledaný zbytek je z množiny $\{9, 22, 35, 48, 61\}$.
(Nebo z množiny $\{1, 6, 11, \ldots, 56, 61\}$.)

4 Malá Fermatova věta

Věta 4.1 (Fermat)**.** *Buď'te p prvočíslo, $a \in \mathbb{N}$, takové, že p nedělí a. Potom*

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

Jinak řečeno: $a^p \equiv a \pmod{p}$.
Důkaz.
Indukcí podle a:

- $a = 1$: $1^p \equiv 1 \pmod{p}$
- $(a+1)^p = a^p + pa^{p-1} + \cdots + p + 1 \equiv a^p + 1 \equiv a + 1 \mod p$

Příklad.
Zbytek přidělení 2^{2011} různými čísly.
$2^{2011} \mod 3$? $\quad$ $2^{2011} \mod 13$?

- Malá Fermatova věta: $2^2 \equiv 1 \pmod{3}$

  Umocnění v modulární aritmetice:

  $(2^2)^{1005} \equiv 1 \pmod{3}$

  $2^{2010} \equiv 1 \pmod{3}$

  $2^{2011} \equiv 2 \pmod{3}$

- Malá Fermatova věta: $2^{12} \equiv 1 \pmod{13}$

  Umocnění v modulární aritmetice:

  $(2^{12})^{17} \cdot 2^7 \equiv 2^7 \pmod{13}$, protože $2011 = 12 \cdot 17 + 7$, nebo jinak: $2011 \equiv 7 \pmod{12}$

  $2^{2011} \equiv 2^7 = 128 \pmod{13}$

  $2^{2011} \equiv 11 \pmod{13}$

5 Dokonalá čísla

Definice (Nicomachos, 100 n.l. (!))**.** Číslo $n \in \mathbb{N}$ se nazývá **dokonalé**, pokud je součtem všech svých dělitelů (kromě sebe sama).

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \\ 496 &= 1+2+4+8+16+31+61+124+248 \\ 8128 &= \dots \end{aligned}$$

Eukleides:

- Všechna výše uvedená čísla jsou tvaru $2^{n-1}(2^n - 1)$.
- Pokud je p prvočíslo a $(2^p - 1)$ je také prvočíslo, tak číslo $2^{p-1}(2^p - 1)$ je dokonalé.

Eukleides:

- Není jasné, jestli jsou ještě jiná dokonalá čísla než čísla tvaru $2^{p-1}(2^p - 1)$.

Co víme dnes:

- Není jasné, jestli jsou ještě jiná dokonalá čísla než čísla tvaru $2^{p-1}(2^p - 1)$.
- Všechna dosud známá dokonalá čísla jsou tedy sudá.
- Otevřený problém: jsou nějaká lichá dokonalá čísla? Počítače: pokud ano, tak musí být větší než 10^{300}.