Rozhledy matematicko-fyzikální

Mikuláš Kučera
Devítková vlastnost prvočísel

Rozhledy matematicko-fyzikální, Vol. 99 (2024), No. 2, 1–5

Persistent URL: http://dml.cz/dmlcz/152482

Terms of use:

© Jednota českých matematiků a fyziků, 2024

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

„Devítková" vlastnost prvočísel

Mikuláš Kučera, FJFI ČVUT, Praha

Ukážeme si jednu z mnoha zajímavých vlastností prvočísel – konkrétně vlastnost period jejich převrácených hodnot, kterou poprvé dokázal roku 1836 francouzský matematik Etienne Midy (1775–1846) [1].

Začněme s číslem 1/7. Klasickým algoritmem dělení zjistíme:

$$\frac{1}{7} = 0{,}\overline{142857}. \tag{1}$$

Tedy získáme periodu 142857. Rozdělme ji v polovině na čísla 142 a 857 a ta sečtěme:

$$142 + 857 = 999.$$

Získali jsme číslo ze samých devítek. Totéž si můžete zkusit například s číslem 1/13:

$$\frac{1}{13} = 0{,}\overline{076923}, \qquad 076 + 923 = 999.$$

Zdá se, že obdobný postup bude fungovat s libovolným prvočíslem $p \geq 7$, jehož perioda je sudé délky. Označme $\mathbb{P}$ množinu všech prvočísel. Pro potřeby formulace problému vyslovme nejprve definici. Není-li řečeno jinak, budeme v celém článku ztotožňovat čísla a jejich reprezentace v desítkové soustavě.

Reálné číslo $a \in (0,1)$ nazveme *periodickým*, pokud je jeho rozvoj za desetinnou čárku zakončen *periodou*, tj. pravidelně se opakující nenulovou n-ticí číslic. Periodu značíme pruhem, tj.

$$a = 0, b_1 b_2 \dots b_m \overline{a_1 a_2 \dots a_n}.$$

n-tici $a_1 a_2 \dots a_n$ nazýváme *perioda délky n*, m-tici $b_1 b_2 \dots b_m$ nazýváme *předperioda délky m*. Má-li číslo prázdnou předperiodu ($m = 0$), nazýváme je *ryze periodické* (angl. *purely periodic*), v opačném případě ($m \neq 0$) jde o číslo *posléze periodické* (angl. *eventually periodic*).

Poznámka. Za periodická nepovažujeme čísla s periodou 9, neboť např. $1 = 0{,}\overline{9}$. Dále je zřejmé, že periodu (i předperiodu) vždy musíme uvažovat nejkratší možnou pro jednoznačnost definice.

Příklad. Číslo $1/3 = 0,\overline{3}$ je ryze periodické s periodou 3 délky 1. Číslo $1/6 = 0,1\overline{6}$ je posléze periodické s předperiodou 1 délky 1 a periodou 6 délky 1.

Úkol 1. Ukažte, že každé periodické číslo je racionální, tj. pokud a je periodické, pak $a = r/q$, kde r a q jsou celá čísla.

Midyho věta

Tvrzení, že pozorování z úvodu skutečně platí pro všechna prvočísla $p \geq 7$, je obsahem tzv. Midyho věty. Nejprve ukážeme, že převrácené hodnoty těchto prvočísel jsou ryze periodické.

Tvrzení 1. *Nechť $p \in \mathbb{P} \setminus \{2, 5\}$. Potom $1/p$ je v desítkové soustavě ryze periodické.*

K důkazu využijeme následující slavnou větu.

Věta (Malá Fermatova). [1] *Nechť $p \in \mathbb{P}$, $a \in \mathbb{N}$, $a \perp p$ (a je nesoudělné s p). Potom*

$$a^{p-1} \equiv 1 \bmod p. \tag{2}$$

Při dělení $1/p$ napočítáme prvních n číslic za desetinnou čárkou jako $\lfloor 10^n/p \rfloor$ s n-tým zbytkem $r_n = 10^n \bmod p$. K výpočtu další číslice dělíme $10r_n/p$ atd. Stačí tedy, aby v některém kroku dělení vyšel zbytek 1. A zde využijeme právě malou Fermatovu větu (2). Stačí volit $n \coloneqq p - 1$ a $a \coloneqq 10$ a zjistíme, že po $p - 1$ vypočítaných číslicích se desetinný rozvoj začne opakovat. Skutečně, jelikož $10^{p-1} \equiv 1 \bmod p$, je $r_{p-1} = 1$. p-tou číslici za desetinnou čárkou tedy, stejně jako tu první, vypočteme coby $\lfloor 10/p \rfloor$ s p-tým zbytkem $r_p = r_1 = 10 \bmod p$ a obdobně pro číslice následující.

Úkol 2. Ukázali jsme, že $1/p$ je ryze periodické. Sami si rozmyslete, že navíc platí, že délka jeho periody musí dělit $p - 1$. Ověřte na příkladech pro $p = 7$ a $p = 13$.

Věta 2 (Midy). *Nechť $p \in \mathbb{P}$, $p \geq 7$. Pokud periodu čísla $1/p$ lze rozdělit na dva bloky stejné délky, pak jejich součet je tvořen pouze číslicemi 9.*

---

[1] Pro důkazy a další zajímavosti týkající se malé Fermatovy věty čtenáře odkazujeme na literaturu [2].

Poznámka. Uvědomme si, že zde povolujeme čísla, jejichž zápis začíná číslicí 0, jak jsme viděli například pro číslo 1/13.

Nechť tedy

$$\frac{1}{p} = 0{,}\overline{xy}, \tag{3}$$

kde x a y jsou n-tice číslic (to tedy znamená, že $2n$ je nejmenší přirozené číslo takové, že $10^{2n} \equiv 1 \bmod p$). Chceme ukázat, že $x+y$ je číslo tvořené pouze číslicemi 9. Jistě platí následující odhady:

$$0 \leq x \leq 10^n - 1, \qquad 0 \leq y \leq 10^n - 1.$$

Protože však x a y nemohou být současně tvořeny pouze nulami (pak by platilo $1/p = 0$) ani pouze devítkami (jinak $1/p = 1$), získáváme odhad

$$0 < x + y < 2(10^n - 1). \tag{4}$$

Vynásobením rovnice (3) číslem 10^{2n} dostaneme

$$\frac{10^{2n}}{p} = 10^n x + y + 0{,}\overline{xy} = 10^n x + y + \frac{1}{p}.$$

Odtud jednoduchou úpravou

$$\frac{(10^n - 1)(10^n + 1)}{p} = \frac{10^{2n} - 1}{p} = 10^n x + y.$$

Jelikož p je prvočíslo a nedělí $10^n - 1$ (v opačném případě $10^n \equiv 1 \bmod p$, což je spor s předpokladem, že $1/p$ má periodu délky $2n$), musí dělit $10^n + 1$. To znamená, že

$$\frac{10^n x + y}{10^n - 1} \in \mathbb{N}.$$

Snadno vidíme, že platí

$$x + y = 10^n x - (10^n - 1)x + y \equiv 10^n x + y \equiv 0 \bmod (10^n - 1).$$

Číslo $x+y$ je dělitelné $10^n - 1$ a ve spojení s odhadem (4) máme kýženou rovnost $x + y = 10^n - 1$, což je číslo ze samých devítek.

O krok dál – Ginsbergova věta

Když jsme úspěšně vyřešili úvodní problém, můžeme se ještě jednou vrátit k číslu $1/7 = 0,\overline{142857}$ (1). Zkusme periodu tentokrát rozdělit na tři bloky délky 2 a ty sečíst:

$$14 + 28 + 57 = 99.$$

Opět dostáváme číslo ze samých devítek! Snadno ověříme tentýž výsledek pro $1/13$:

$$07 + 69 + 23 = 99.$$

Zdá se, že devítková vlastnost platí i při dělení period na třetiny. Že je tomu skutečně tak, dokázal Ginsberg (2004) [1]. Jak uvidíme, důkaz je už o něco složitější.

Nechť $p \in \mathbb{P}$, $p \geq 7$ a

$$\frac{1}{p} = 0,\overline{xyz} = 0,\overline{x_1 \dots x_n y_1 \dots y_n z_1 \dots z_n} \tag{5}$$

je číslo s periodou délky $3n$. Jednoduchým odhadem analogickým důkazu Midyho věty získáme

$$0 < x + y + z < 3(10^n - 1). \tag{6}$$

Stejně tak vynásobením (5) číslem 10^{3n} odvodíme

$$\frac{(10^n - 1)(10^{2n} + 10^n + 1)}{p} = \frac{10^{3n} - 1}{p} = 10^{2n}x + 10^n y + z. \tag{7}$$

A stejnou argumentací jako dříve (p je prvočíslo a nedělí $10^n - 1$) obdržíme dělitelnost $x + y + z$ číslem $10^n - 1$:

$$\begin{aligned} x + y + z &= 10^{2n}x + 10^n y + z - (10^n - 1)(10^n + 1)x - (10^n - 1)y \equiv \\ &\equiv 10^{2n}x + 10^n y + z \equiv 0 \bmod (10^n - 1). \end{aligned} \tag{8}$$

Díky (6) a (8) je součet $x+y+z$ roven buď $10^n - 1$, nebo $2(10^n - 1)$. Pro důkaz Ginsbergovy věty tedy stačí ukázat $x + y + z \equiv -1 \equiv 9 \bmod 10$.

Označme r_x, r_y, r_z postupně zbytky při výpočtu prvních n, $2n$, $3n$ cifer čísla $1/p$, tedy zbytky při dělení $10^n/p$, $10^{2n}/p$, $10^{3n}/p$. Potom

$$\frac{10^n - r_x}{p} = x, \quad \frac{10^{2n} - r_y}{p} = 10^n x + y, \quad \frac{10^{3n} - r_z}{p} = 10^{2n}x + 10^n y + z. \tag{9}$$

Z (9) odvodíme následující dvě pozorování:

1. Vynásobením rovnic číslem p a kongruencí mod 10 máme

   $$px \equiv -r_x \bmod 10, \qquad py \equiv -r_y \bmod 10, \qquad pz \equiv -r_z \bmod 10.$$

   Sečtením těchto kongruencí získáme výsledek

   $$p(x+y+z) \equiv -(r_x + r_y + r_z) \bmod 10. \tag{10}$$

2. Přímo z (9) plyne

   $$r_x \equiv 10^n \bmod p, \qquad r_y \equiv 10^{2n} \bmod p, \qquad r_z \equiv 10^{3n} \bmod p.$$

   Dle (7) p dělí číslo $10^{2n}+10^n+1$, proto musí dělit i $10^{3n}+10^{2n}+10^n$. Sečtením předchozích kongruencí proto dostaneme

   $$r_x + r_y + r_z \equiv 10^n + 10^{2n} + 10^{3n} \equiv 0 \bmod p.$$

   Současně víme, že r_z je posledním zbytkem při dělení před zopakováním periody, tedy $r_z = 1$ (viz (7) a (9)). Protože $r_x \leq p-1$ a $r_y \leq p-1$, máme $0 < r_x + r_y + r_z < 2p$ a díky kongruenci výše pak

   $$r_x + r_y + r_z = p. \tag{11}$$

Zbytek důkazu je jednoduchý – stačí dosadit rovnost (11) do kongruence (10), a jelikož p je nesoudělné s 10, můžeme jím obě strany vydělit. Získali jsme kýžený výsledek

$$x + y + z \equiv -1 \equiv 9 \bmod 10.$$

Skutečně tedy $x + y + z = 10^n - 1$, což je opět číslo tvořené samými devítkami.

Literatura

[1] Martin, H. W.: Generalizations of Midy's theorem on repeating decimals. *Electronic Journal of Combinatorial Number Theory*, roč. 7 (2007), č. 1, s. 1–7, `https://eudml.org/doc/127779`.

[2] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel: Od velkých objevů k aplikacím.* Academia, Praha, 2009.