Rozhledy matematicko-fyzikální

Lukáš Moudrý

Pokrývací systémy a soustava rovnic

Rozhledy matematicko-fyzikální, Vol. 99 (2024), No. 2, 27–32

Persistent URL: http://dml.cz/dmlcz/152487

Pokrývací systémy a soustava rovnic

Lukáš Moudrý, Plzeň

Abstrakt. V 19. století vyslovil Alphonse de Polignac následující domněnku: Pro libovolné liché číslo k existuje takové přirozené číslo n, že $2^n + k$ je prvočíslo. V minulém století ji však vyvrátil Paul Erdős, a to za použití tzv. pokrývacích systémů. Jak tyto systémy fungují a jak pomocí nich tuto domněnku vyvrátit, si vysvětlíme v tomto článku.

Pokrývací systémy

Nezáporná celá čísla můžeme rozdělit na dvě skupiny, lichá a sudá čísla. V řeči kongruencí [1] je číslo n sudé, právě když splňuje

$$n \equiv 0 \mod 2,$$

a liché, právě když platí

$$n \equiv 1 \mod 2.$$

Např. číslo tři je liché, protože platí $3 \equiv 1 \bmod 2$, a číslo čtyři sudé, protože $4 \equiv 0 \bmod 2$. Tyto dvě kongruence tvoří pokrývací systém, neboť všechna přirozená čísla splňují jednu z těchto kongruencí.

Pojďme zavést pojem pokrývací systém formálně matematicky.

Definice 1. Mějme d přirozených čísel $m_1, m_2, \ldots, m_d$ a celá nezáporná čísla $r_1, r_2, \ldots, r_d$ taková, že $r_1 < m_1$, $r_2 < m_2$, $\ldots, r_d < m_d$. Řekneme, že páry (m_1, r_1), (m_2, r_2), $\ldots$, (m_d, r_d) tvoří *pokrývací systém*, pokud ke každému přirozenému číslu n lze nalézt pár (m_i, r_i) takový, že n má zbytek r_i po dělení m_i, tj. $n \equiv r_i \bmod m_i$.

Příklad 1. Je zřejmé, že páry $(2, 0)$ a $(2, 1)$ tvoří pokrývací systém. Stejně tak pro libovolné $m \in \mathbb{N}$, páry $(m, 0)$, $(m, 1)$, $\ldots$, $(m, m-1)$ tvoří pokrývací systém.

[1] Nechť $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$. Řekneme, že a je kongruentní b modulo m, pokud m dělí beze zbytku rozdíl $a - b$. Píšeme $a \equiv b \bmod m$. Pro více informací o kongruencích a práci s nimi doporučujeme [1, 2].

Příklad 2. Existují i pokrývací systémy, kde některým přirozeným číslům odpovídá více párů. Například pro pokrývací systém $(2,0)$, $(2,1)$, $(4,1)$ platí, že číslu 5 přísluší páry $(2,1)$ i $(4,1)$, protože $5 \equiv 1 \bmod 2$ a také $5 \equiv 1 \bmod 4$.

Pro prezentaci Erdősova důkazu bude třeba pracovat s pokrývacím systémem, kde jsou všechna modula vzájemně různá. Zkusme si pro ilustraci jeden takový odvodit. Zafixujeme si kongruenci $n \equiv 0 \bmod 2$ a budeme postupně upravovat $n \equiv 1 \bmod 2$ tak, aby modulo bylo u každé kongruence jiné. Všechna lichá čísla splňují jednu z následujících dvou kongruencí:

$$\begin{aligned} n &\equiv 1 \mod 4, \\ n &\equiv 3 \mod 4. \end{aligned}$$

Nyní si upravíme kongruenci $n \equiv 3 \bmod 4$. Aby bylo jasnější, co se děje, napišme si několik prvních přirozených čísel splňujících tuto kongruenci

$$3,\ \underline{7},\ \underline{\underline{11}},\ 15,\ \underline{19},\ \underline{\underline{23}},\ 27,\ \underline{31},\ \underline{\underline{35}},\ 39,\ \underline{43},\ \underline{\underline{47}},\ 51,\ \underline{55},\ \underline{\underline{59}},\ 63,\ \ldots$$

Všimněme si, že počínaje trojkou je každé třetí číslo dělitelné třemi (viz nepodtržená čísla). Tato čísla tedy pokryjeme kongruencí

$$n \equiv 0 \mod 3.$$

Dále si všimněme, že počínaje sedmičkou je každé třetí číslo o jedna více než nějaký násobek šestky (viz podtržená čísla). Tato čísla pokryjeme kongruencí

$$n \equiv 1 \mod 6.$$

A nakonec si všimněme, že od jedenáctky dál je každé třetí číslo o jedenáct víc než nějaký násobek dvanáctky (viz dvakrát podtržená čísla). Tato čísla pokryjeme kongruencí

$$n \equiv 11 \mod 12.$$

Získali jsme tedy pokrývací systém, kde jsou všechna modula různá:

$$(2,0),\ (4,1),\ (3,0),\ (6,1),\ (12,11).$$

Co kdyby nám někdo naopak ukázal tyto páry a chtěl by po nás ověřit, jestli jde opravdu o pokrývací systém? Pro jaká všechna čísla musíme ověřit, že splňují alespoň jednu z daných kongruencí?

Ukážeme si, že se stačí podívat na všechna čísla od 0 až do nejmenšího společného násobku všech modul zmenšeného o jedna, což je v našem případě 11.

$$\begin{aligned}
0 &\equiv 0 \mod 2,\\
1 &\equiv 1 \mod 4,\\
2 &\equiv 0 \mod 2,\\
3 &\equiv 0 \mod 3,\\
4 &\equiv 0 \mod 2,\\
5 &\equiv 1 \mod 4,\\
6 &\equiv 0 \mod 2,\\
7 &\equiv 1 \mod 6,\\
8 &\equiv 0 \mod 2,\\
9 &\equiv 0 \mod 3,\\
10 &\equiv 0 \mod 2,\\
11 &\equiv 11 \mod 12.
\end{aligned}$$

Co když si teď vezmeme libovolné číslo $n \geq 12$? Pro takové n existuje přirozené číslo l, že $n = 12l + j$, kde j je zbytek po dělení 12, tedy $0 \leq j < 12$. Pak ale stačí v pokrývacím systému najít pár (r, m) takový, že $j \equiv r \bmod m$. Takový pár jistě existuje, protože $j < 12$. Jelikož m dělí 12, platí

$$n = 12l + j \equiv j \mod m.$$

Odtud dostáváme $n \equiv r \bmod m$.

Např. pro $n = 257$ lze psát $n = 21 \cdot 12 + 5$. A jelikož $5 \equiv 1 \bmod 4$, platí také $257 \equiv 1 \bmod 4$.

Úkol 1. Ověřte sami, že $(2, 1)$, $(3, 1)$, $(4, 2)$, $(8, 4)$, $(12, 8)$, $(24, 0)$ tvoří pokrývací systém.

Vyvrácení domněnky

Nyní již můžeme popsat, jakým elegantním způsobem Paul Erdős vyvrátil Polignacovu domněnku.

Domněnka 1. Pro libovolné liché přirozené číslo k existuje takové přirozené číslo n, že $2^n + k$ je prvočíslo.

Erdősova strategie byla následující. Uvažoval pokrývací systém z úkolu 1

$$(2,1),\ (3,1),\ (4,2),\ (8,4),\ (12,8),\ (24,0). \tag{1}$$

K číslům $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $m_4 = 8$, $m_5 = 12$ a $m_6 = 24$ našel různá prvočísla p_1, p_2, p_3, p_4, p_5 a p_6 taková, že p_i dělí $2^{m_i} - 1$ pro každé $i \in \{1, 2, 3, 4, 5, 6\}$, tj.

$$2^{m_i} \equiv 1 \mod p_i. \tag{2}$$

Napišme si rozklady $2^{m_i} - 1$ na prvočísla.

$$\begin{aligned}
2^{m_1} - 1 &= 2^2 - 1 = 3,\\
2^{m_2} - 1 &= 2^3 - 1 = 7,\\
2^{m_3} - 1 &= 2^4 - 1 = 15 = 3 \cdot 5,\\
2^{m_4} - 1 &= 2^8 - 1 = 255 = 3 \cdot 5 \cdot 17,\\
2^{m_5} - 1 &= 2^{12} - 1 = (2^6 - 1)(2^6 + 1) = (2^3 + 1)(2^3 - 1)\,65 =\\
&= 3^2 \cdot 7 \cdot 5 \cdot 13,\\
2^{m_6} - 1 &= 2^{24} - 1 = (2^{12} - 1)(2^{12} + 1) =\\
&= 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot (2^4 + 1)(2^8 - 2^4 + 1) = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.
\end{aligned}$$

Lze zvolit $p_1 = 3$, $p_2 = 7$, $p_3 = 5$, $p_4 = 17$, $p_5 = 13$ a $p_6 = 241$. Aby vyvrátil Polignacovu domněnku, zkonstruoval Erdős liché číslo k takové, že pro každé z nalezených prvočísel p_i platí

$$2^{r_i} + k \equiv 0 \mod p_i,$$

přičemž r_i jsou zbytky v pokrývacím systému (1), tj. $r_1 = r_2 = 1$, $r_3 = 2$, $r_4 = 4$, $r_5 = 8$, $r_6 = 0$.

Takové číslo k již vyvrací domněnku, protože díky tomu, že (1) je pokrývací systém, lze pro každé přirozené n najít pár (m_i, r_i) takový, že $n \equiv r_i \mod m_i$, tj. $n = r_i + l m_i$ pro nějaké l nezáporné celé číslo. Pak ale s využitím faktu, že $2^{m_i} \equiv 1 \mod p_i$, máme

$$2^n + k = 2^{r_i + l m_i} + k = 2^{r_i} \cdot (2^{m_i})^l + k \equiv 2^{r_i} + k \equiv 0 \mod p_i.$$

To znamená, že prvočíslo p_i dělí $2^n + k$, a tudíž $2^n + k$ je číslo složené.

Zbývá ukázat, že lze nalézt liché číslo k splňující $2^{r_i} + k \equiv 0 \mod p_i$. Dosazením konkrétních hodnot máme pro k systém kongruencí

$$\begin{aligned} 2^1 + k &\equiv 0 \mod 3, \\ 2^1 + k &\equiv 0 \mod 7, \\ 2^2 + k &\equiv 0 \mod 5, \\ 2^4 + k &\equiv 0 \mod 17, \\ 2^8 + k &\equiv 0 \mod 13, \\ 2^0 + k &\equiv 0 \mod 241. \end{aligned} \tag{3}$$

Takový systém kongruencí lze řešit využitím čínské zbytkové věty [3].

Věta 3 (čínská věta o zbytcích)**.** *Nechť $p_1, p_2, \ldots, p_j$ jsou po dvou nesoudělná přirozená čísla a nechť $a_1, a_2, \ldots, a_j$ jsou libovolná celá čísla. Pak systém kongruencí*

$$\begin{aligned} x &\equiv a_1 \mod p_1, \\ x &\equiv a_2 \mod p_2, \\ &\vdots \\ x &\equiv a_j \mod p_j \end{aligned}$$

má celočíselné řešení. Navíc každé řešení $x \in \mathbb{Z}$ splňuje

$$x \equiv c_1 \frac{p}{p_1} + c_2 \frac{p}{p_2} + \cdots + c_j \frac{p}{p_j} \mod p,$$

kde $p = p_1 p_2 \cdots p_j$ a c_i splňují pro každé $i \in \{1, 2, \ldots, j\}$

$$c_i \frac{p}{p_i} \equiv a_i \mod p_i.$$

Přepišme systém kongruencí (3) ekvivalentním způsobem do stejného tvaru, jako je v čínské zbytkové větě.

$$\begin{aligned} k &\equiv 1 \mod 3, \\ k &\equiv 5 \mod 7, \\ k &\equiv 1 \mod 5, \\ k &\equiv 9 \mod 17, \\ k &\equiv 4 \mod 13, \\ k &\equiv -1 \mod 241. \end{aligned} \tag{4}$$

Úkol 2. Pro čtenáře, který hrozně rád počítá, necháme jako domácí cvičení nalézt pomocí čínské zbytkové věty číslo k, které řeší systém kongruencí (4).

Úkol 3. Pro čtenáře, který rád počítá, necháme jako domácí cvičení ověřit, že $k = 1\,518\,781$ řeší systém kongruencí (4).

Závěr tedy zní: *Polignacova domněnka neplatí např. pro* $k = 1\,518\,781$.

Příklad 3. Ukažme pro nějaké „náhodně vybrané“ n, že $2^n + k$ skutečně není prvočíslo. Uvažujme $n = 12$. Toto číslo splňuje $n \equiv 4 \bmod 8$, konkrétně $n = 1 \cdot 8 + 4$. Jelikož $2^8 \equiv 1 \bmod 17$, dostáváme

$$2^n = 2^4 \cdot 2^8 \equiv 2^4 \mod 17.$$

Tudíž

$$2^n + k \equiv 2^4 + k \equiv 0 \mod 17, \qquad \text{viz (3)}.$$

Suma sumárum, 17 dělí číslo $2^n + k = 4\ 096 + 1\,518\,781 = 1\,522\,877$. (Nevěřící Tomášové mohou zkontrolovat na kalkulačce, že $1\,522\,877 = 17 \cdot 89\,581$.)

Pro více informací jsou k dispozici videa [1] na toto téma připravená autorem článku.

Poděkování

Děkuji recenzentovi a také vedoucí redaktorce Ľubomíře Dvořákové za vhodné úpravy, které vedly k vylepšení článku.

Literatura

[1] `https : / / www.youtube.com / watch?v = coplC14mj08&list = PLFbx - hq3ir1mXupqlAfgoW8Ek1eTF3f6k`

[2] `https://prase.cz/library/KongruenceKK/KongruenceKK.pdf`

[3] Pěchoučková, Š.: Armáda v Kocourkově a čínská věta. *Učitel matematiky*, roč. 24 (2016), č. 3, s. 174–181.