Václav Veselý

Něco o prvočíslech

Časopis pro pěstování matematiky a fysiky, Vol. 63 (1934), No. 1, R1--R4

Persistent URL: http://dml.cz/dmlcz/122522

ROZHLEDY
MATEMATICKO-PŘÍRODOVĚDECKÉ.

ROČNÍK 13 (1933/34). ČÍSLO 1.

Něco o prvočíslech.

Napsal *Václav Veselý*.

I. Je vám jistě známo, že celá kladná čísla lze rozděliti podle počtu celistvých kladných dělitelů na: *a*) čísla s jediným takovým dělitelem: 1; *b*) čísla se dvěma děliteli — prvočísla; *c*) čísla s více než dvěma děliteli — čísla složená.

V dalším si všimneme blíže prvočísel. Dovedete jistě rozhodnouti, zda celé kladné číslo a je prvočíslem či ne podle toho, zda je či není dělitelné některým prvočíslem $< \sqrt{a}$. Dovedete také *Eratosthenovým* sítem vybrat ze všech celých čísel $< A$ všechna prvočísla. Ale dobře víte, že pro velká čísla nelze těchto metod prakticky použít. Je vám proto asi nepochopitelné, jak se podařilo na př. Leonhardu Eulerovi (1707-1783) ukázat, že číslo $2^{2^5} + 1 = 4\,294\,967\,297$ není prvočíslem a vyvrátit tak tvrzení, které bez důkazu vyslovil Pierre de Fermat (1601—1665), že totiž číslo $2^{2^n} + 1$ je prvočíslem pro každé celé kladné n.

Je právě úkolem těchto řádků ukázat vám na tomto příkladě myšlenkový postup, kterého lze užít i při jiných velkých číslech.

II. Nejprve si dokážeme dvě věty. Věta 1. (t. zv. *Fermatova věta*): *Buď p prvočíslo a b číslo nedělitelné p, pak $b^{p-1} - 1$ je dělitelné p.*

Důkaz[1]): 1. Především je zřejmo, že binomický koeficient $\binom{p}{k} = \frac{p!}{k! \,.\, (p-k)!}$ pro $1 \leqq k \leqq p-1$ je dělitelný prvočíslem p, protože čitatel je, ale jmenovatel není dělitelný p. Pak ale také číslo

$$B = (c+1)^p - c^p - 1 = \binom{p}{1} c^{p-1} + \binom{p}{2} c^{p-2} + \ldots + \binom{p}{1} c$$

je dělitelno p, ať je c jakékoli celé číslo.

[1]) Weber-Wellstein: Encyklopädie der Elementar-Mathematik, I, str. 193—4.

2. Provedeme nyní úplnou indukcí důkaz, že číslo $C = b^p - b$ je vždy dělitelno prvočíslem p.

a) Platí-li toto tvrzení pro $b = c$, pak vzhledem k tomu, že

$$B = (c+1)^p - c^p - 1 = [(c+1)^p - (c+1)] - (c^p - c)$$

je dělitelno p, platí i pro $b = c + 1$.

b) Pro $b = 2$ tvrzení platí, neboť podle binomické poučky

$$2^p - 2 = (1+1)^p - 2 = \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{1}.$$

Je tedy číslo C dělitelno p pro každé celé kladné b.

3. Předpokládáme-li ale, že b je nedělitelné p, pak v součinu $b^p - b = b\,(b^{p-1} - 1)$ musí být dělitelný p druhý činitel, c. b. d.

Dále si dokážeme větu 2.: *Je-li r nejmenší celé kladné číslo takové, že $d^r - 1$ je dělitelno prvočíslem p a je-li $d^m - 1$ dělitelno p, kdež d je celé kladné číslo nesoudělné s p, pak m je dělitelno r.*

Poznámka: Že takové r vůbec existuje, plyne z Fermatovy věty, neboť podle ní nejméně pro jednu hodnotu i, a to $i = p - 1$ je $d^i - 1$ dělitelno p.

Důkaz: Buď $m = qr + s$, kdež q je celé kladné číslo a $0 \leqq s < r$. A dále

$$d^m - 1 = d^{qr+s} - d^{qr} + d^{qr} - 1 = d^{qr}(d^s - 1) + (d^r)^q - 1 = \\ = d^{qr}(d^s - 1) + (d^r - 1)[(d^r)^{q-1} + \ldots + 1].$$

Avšak podle předpokladu je $(d^r - 1)[(d^r)^{q-1} + \ldots + 1]$ dělitelno p, stejně i $d^{sn} - 1$. Musí tedy být i $d^{qr}(d^s - 1)$ dělitelno p, což vzhledem k předpokladu o d znamená, že $d^s - 1$ je dělitelné p. Avšak $s < r$ a r je nejmenší celé kladné číslo takové, že $d^r - 1$ je dělitelné p, tudíž $s = 0$ a $m = qr$, c. b. d.

III. Obraťme se nyní k vlastní věci. Myšlenka celého postupu je v této větě 3.: *Každé prvočíslo, které je dělitelem čísla $K_n = 2^{2^n} + 1$ je tvaru $2^{n+1} \cdot x + 1$.*

Poznámka: Jestliže tedy máme rozhodnouti, zda číslo $2^{2^n} + 1$ je či není prvočíslo, není třeba probírat dělitelnost K_n všemi prvočísly $< 2^{2^{n-1}}$, nýbrž jen těmi z nich, která jsou tvaru $2^{n+1} \cdot x + 1$.

Důkaz[2]): 1. Nechť $2^{2^n} + 1$ je dělitelno prvočíslem p. Zřejmě je p číslo liché. Hledejme nyní nejmenší číslo celé, kladné r, pro které $2^r - 1$ je dělitelno p. Že takové číslo existuje, víme z poznámky u věty 2., která se na tento případ vztahuje, protože 2 není jistě dělitelno p.

[2]) Weber-Wellstein: Encyklopädie, I, str. 286—7.

2. Vzhledem k tomu, že $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$ je dělitelno p, je

$$r \leqq 2^{n+1}.$$

Jestliže by nebylo $r = 2^{n+1}$, pak podle věty 2. by musilo býti r dělitelem čísla 2^{n+1}, t. j. r samo by bylo tvaru $r = 2^l$, kdež $l < n + 1$. Avšak musilo by býti $l < n$, protože číslo $2^{2^n} - 1$ není jistě dělitelné p, neboť $2^{2^n} - 1 = 2^{2^n} + 1 - 2$ a 2 není dělitelno p. Ale $l < n$ je nemožné, neboť pak by bylo $2^n = 2^l \cdot 2^{n-l}$ a tedy

$$2^{2^n} - 1 = (2^{2^l} - 1)[(2^{2^l})^{2^{n-l}-1} + (2^{2^l})^{2^{n-l}-2} + \ldots + 1]$$

musilo by býti dělitelno p. Je tedy $r = 2^{n+1}$ nejmenším číslem takovým, že $2^r - 1$ je dělitelno p.

3. Konečně podle věty Fermatovy je $2^{p-1} - 1$ dělitelno p, tudíž podle věty 2. musí býti $p - 1$ dělitelno číslem $r = 2^{n+1}$. Tedy $p = 2^{n+1} \cdot x + 1$, kdež x je nějaké celé kladné číslo, c. b. d.

IV. Užijme nyní tohoto výsledku ke zkoumání správnosti Fermatova tvrzení, že číslo $K_n = 2^{2^n} + 1$ je pro každé n prvočíslem. Je tu pro

$n =$	0,	1,	2,	3,
$K_n =$	3,	5,	17,	257.

V těchto případech dovedete si sami lehko určiti, že K_n je prvočíslo. Pro $n = 4$ je ale $K_4 = 65\,537$. Zde by to již byla pro vás větší práce. Avšak podle věty 3. stačí zkoumati, zda 65 537 je dělitelno jen těmi prvočísly < 256, která jsou tvaru $32 \cdot x + 1$. To jsou ale jen dvě: 97 a 193 a 65 637, jak se přesvědčíte, není ani jedním z nich dělitelno. Tedy i pro $n = 4$ je K_n prvočíslo.

Pro $n = 5$ je $K_5 = 4\,294\,967\,297$ a nutno zkoumati dělitelnost všemi prvočísly $< 65\,536$ tvaru $64 \cdot x + 1$. To jsou

193, 257, 449, 577, 641, 769, 1153, ...

A zde shledáte, že $4\,294\,967\,297 = 641 \cdot 6\,700\,417$. Abychom rozhodli, zda číslo 6 700 417 je prvočíslem, stačí zkoumati, zda je dělitelné některým prvočíslem < 2588 tvaru $64 \cdot x + 1$. Stačí ale začíti prvočíslem 641. Další jsou 769, 1153, 1217, 1409, 1601, 2113. Shledáte, že číslo 6 700 417 opravdu je prvočíslem.

Vidíte tedy, že Fermatovo tvrzení pro $n = 5$ není správné. Stejně číslo K_n pro $n = 6$ má dělitele 274 177, pro $n = 12$ má dělitele 114 689, pro $n = 23$ dělitele 167 772 161, pro $n = 36$ dělitele 2 748 779 069 441.

V. V předchozím jste se seznámili s jedním případem, ve kterém lze dospěti k rozhodnutí, zda a je prvočíslo či ne, způsobem jednodušším než vám známým. Jsou ale i jiné případy, ve kterých lze na podkladě jiných poznatků dospěti k větě obdobné větě 3.,

jejíž pomocí lze pak v takovém případě rozhodnouti, zda se jedná o prvočíslo či ne. (Některé takové případy najdete v knize K. Rychlík: Úvod do elementární teorie číselné, Praha 1931, kde také najdete i jinak provedený důkaz zobecněné věty 1. a věty 2.) A jsou také i jiné postupy, než jaký představuje věta 3.

Konečně uvedu vám alespoň jedny tabulky této věci se týkající, velmi obsáhlé. Jsou to: Lehmer: Factor table for the first ten millions, Washington, 1909. V nich je ke každému číslu nedělitelnému 2, 3, 5, 7 od 0 do 10 017 000 uveden nejmenší kladný celý dělitel.

Důkaz velké Fermatovy poučky pro exponent 4.

Dr. *Jos. Matoušek*, Jindř. Hradec.

Věta Fermatova pro exponent 4 praví:

Číselná rovnice

$$X^4 + Y^4 = Z^4 \text{ při } X, Y, Z > 0^1)$$

jest nemožnou.

Elementární naukou o číslech provedli důkaz o tom již Euler a Dr. Edmund Landau. Oba tito vědci předpokládají při svých důkazech znalost řešení rovnice $X_1^2 + Y_1^2 = Z_1^2$ celými čísly, na němž své další vývody zakládají. Hodlám zde ukázati, že důkaz dá se provésti přímým způsobem, t. j. bez znalosti řešení rovnice $X_1^2 + Y_1^2 = Z_1^2$.

Zkrátíme-li číselnou rovnici $X^4 + Y^4 = Z^4$ největším společným dělitelem, obdržíme novou $x^4 + y^4 = z^4$, v níž veličiny x, y a z jsou mezi sebou relativně nesoudělné. Dvě z nich musí tedy býti lichými a třetí jest sudou, poněvadž ani součet ani rozdíl dvou lichých čísel nemůže býti lichým. Jedna z veličin x a y jest tudíž určitě lichou. Budiž x liché; pak se snadno přesvědčíme, že y musí býti sudé [součet dvou lichých bikvadrátů — číselně $8h + 1 + 8k + 1 = 2(4l + 1)$ — nemůže býti bikvadrátem.[2])]

Seznali jsme tedy, že v naší rovnici $x^4 + y^4 = z^4$ veličiny x, y a z jsou mezi sebou relativně nesoudělné, y jest číslo sudé, x a z čísla lichá.

Rovnici tuto ve tvaru $z^4 - y^4 = x^4$ rozložíme ve faktory

$$(z^2 + y^2)(z^2 - y^2) = x^4.$$

---

[1]) V celém článku značí nám latinská písmena — velká či malá, s indexem či bez něho — vždy jen čísla celistvá, positivní a konečná.

[2]) Že lichý bikvadrát lze psáti ve tvaru $8h + 1$, je patrno z rovnice

$$(2k + 1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 = 8h + 1.$$