Prvočísla přednáška s čokoládou

Radek Erban

Prvočíslo je takové přirozené číslo, které má právě dva kladné dělitele. Ačkoliv je to pojem značně známý a často studovaný, je až úžasné, že současná matematika neumí odpovědět na některé základní otázky týkající se prvočísel, které byly zformulovány před mnoha a mnoha věky. Začneme však věcmi nejzákladnějšími, aby bylo patrné, k čemu může být odpověď na některé na první pohled umělé akademické problémy dobrá.

Asi nebude pro Tebe příliš těžké dokázat následující poučku, která se často nazývá základní větou aritmetiky :

Věta : *Každé číslo* $a \in \mathbb{N}, a \geq 2$ *se dá vyjádřit ve tvaru* $a = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_n^{q_n}$, *kde* $p_1, \ldots, p_n$ *jsou po dvou různá prvočísla a* $q_1, \ldots, q_n \in \mathbb{N}$. *Toto vyjádření je jednoznačné až na pořadí činitelů.*

Z uvedené věty je vidět, že z prvočísel a násobení můžeme „vybudovat“ všechna přirozená čísla. Tj. prvočíslo je v podstatě základní stavební kámen přirozených čísel vzhledem k násobení (stejně jako jednička vzhledem ke sčítání). Mnohé slavné (Fermatova věta, Waringův problém, ap.) i méně slavné problémy v teorii čísel, které něco tvrdí pro všechna přirozená čísla, proto „stačí“ často řešit jen pro prvočísla, neboť z tohoto pak obecná tvrzení snadno vyplývají.

Rozložení prvočísel v množině přirozených čísel

Již starý Eukleidés ve svých „Základech“ dokazuje tvrzení, že prvočísel je nekonečně mnoho, čili prvočísla tvoří nekonečnou posloupnost čísel. Naskýtá se samozřejmě otázka, jaké má tato posloupnost zákonitosti. Prvních několik set prvočísel je uvedeno v následující tabulce :

2	67	157	257	367	467	599	709	829	967	1087	1217	1327	1483	1607	1741	1879
3	71	163	263	373	479	601	719	839	971	1091	1223	1361	1487	1609	1747	1889
5	73	167	269	379	487	607	727	853	977	1093	1229	1367	1489	1613	1753	1901
7	79	173	271	383	491	613	733	857	983	1097	1231	1373	1493	1619	1759	1907
11	83	179	277	389	499	617	739	859	991	1103	1237	1381	1499	1621	1777	1913
13	89	181	281	397	503	619	743	863	997	1109	1249	1399	1511	1627	1783	1931
17	97	191	283	401	509	631	751	877	1009	1117	1259	1409	1523	1637	1787	1933
19	101	193	293	409	521	641	757	881	1013	1123	1277	1423	1531	1657	1789	1949
23	103	197	307	419	523	643	761	883	1019	1129	1279	1427	1543	1663	1801	1951
29	107	199	311	421	541	647	769	887	1021	1151	1283	1429	1549	1667	1811	1973
31	109	211	313	431	547	653	773	907	1031	1153	1289	1433	1553	1669	1823	1979
37	113	223	317	433	557	659	787	911	1033	1163	1291	1439	1559	1693	1831	1987
41	127	227	331	439	563	661	797	919	1039	1171	1297	1447	1567	1697	1847	1993
43	131	229	337	443	569	673	809	929	1049	1181	1301	1451	1571	1699	1861	1997
47	137	233	347	449	571	677	811	937	1051	1187	1303	1453	1579	1709	1867	1999
53	139	239	349	457	577	683	821	941	1061	1193	1307	1459	1583	1721	1871	2003
59	149	241	353	461	587	691	823	947	1063	1201	1319	1471	1597	1723	1873	2011
61	151	251	359	463	593	701	827	953	1069	1213	1321	1481	1601	1733	1877	2017

Pokud si uvedenou tabulku pozorně prohlédneme, zjistíme, že „hustota“ prvočísel postupně klesá. Je samozřejmě otázkou, jak rychle. Není příliš obtížné ukázat, že existuje libovolně dlouhý úsek přirozených čísel bez prvočísel. Pro přirozené číslo n totiž stačí vzít n-tici $(n+1)!+2$, $(n+1)!+3$, $(n+1)!+4$, $\ldots$, $(n+1)!+n+1$, ve které není zřejmě ani jedno

prvočíslo. (Sám si rozmysli proč.) Takže vidíme, že posloupnost všech prvočísel je „libovolně děravá“. Uvedené díry však nemohou být „libovolně brzo“, neboť dle Bertrandova postulátu (**Věta 2**) existuje vždy mezi n a $2n$ nějaké prvočíslo (samozřejmě pro $n \geq 2$).

Úplně perfektní by samozřejmě bylo, kdyby se nám podařilo nalézt nějakou formulku, do které bychom dosadili n a vypadlo by nám n-té prvočíslo. Bohužel takový vzoreček nemáme. Matematici se však snažili i o tvrzení trochu slabší, a to nalézt takový vzoreček, který by dával pro všechna přirozená čísla prvočíselný výsledek. Z historie nejznámější jsou asi tzv. Fermatova a Mersennova prvočísla[†] . Zastavme se u prvních z nich.

Asi tak kolem roku 1640 vyslovil slavný Pierre Fermat domněnku, že pro každé $n \in \mathbb{N}_0$ je $F_n = 2^{2^n} + 1$ prvočíslo. Skutečně, pro čísla $n = 0, 1, 2, 3, 4$ je tato hypotéza pravdivá. Bohužel však posloupnost F_n se zvětšujícím se n velice rychle roste, což prověřování této hypotézy přímým výpočtem značně znesnadňuje. Proto až téměř o sto let později Leonhard Euler ukázal, že se Fermat spletl (!) a že již číslo F_5 je číslo složené[‡], konkrétně, že $641|F_5$.

Pokud trošičku slevíme z našich požadavků a budeme hledat vzoreček, který často dává prvočíslo, stojí za zmínku například polynomy $x^2 + x + 17$, resp. $x^2 + x + 41$, které po řadě nabývají prvočíselných hodnot pro $x = 0, 1, \ldots, 15$, resp. $x = 0, 1, \ldots, 39$.

Abychom nějak přesněji vystihli rozložení prvočísel, definujeme funkci π. Pro přirozené číslo n její hodnota $\pi(n)$ označuje počet všech prvočísel menších nebo rovno n. Funkce π je zřejmě neomezená a neklesající, zajímavou otázkou však je, jak rychle tato funkce vlastně roste. Na konci minulého století (1896) dokázali francouzští matematikové Jacques Hadamard a Charles Jean de la Vallée-Poussin vztah :

$$\lim_{n\to\infty} \frac{\pi(n) \cdot \ln n}{n} = 1. \qquad (PNT)$$

Tento vztah nám v postatě říká, že funkce π roste „přibližně“ stejně rychle jako funkce $\frac{n}{\ln n}$. Jak je to splněno pro malá n uvádí následující tabulka :

n	$\pi(n)$	$\frac{n}{\ln n}$	$\frac{n}{\pi(n)}$
10	4	4	2.5
10^2	25	22	4.0
10^3	168	145	6.0
10^4	1229	1086	8.1
10^5	9592	8686	10.4
10^6	78498	72382	12.7
10^7	664579	620421	15.0
10^8	5761455	5428681	17.4
10^9	50847534	48254942	19.7
10^{10}	455052512	434294482	22.0

[†]Mersennova prvočísla jsou prvočísla tvaru $2^n - 1$. Snad poslední objevené prvočíslo tohoto typu je $2^{2976221} - 1$, které má 895932 číslic. (Gordon-Space, 24.8.1997)

[‡]Pro zajímavost ukážeme jeden značně trikový postup, jak se dá nahlédnout, že $641|\mathrm{F}_5$. Zřejmě $641 = 2^4 + 5^4 = 5.2^7 + 1$, proto $2^4 = 641 - 5^4$ a $2^{32} = 2^4 \cdot 2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 = 641.2^{28} - (641 - 1)^4 = 641 \cdot \mathrm{k} - 1$, což dává náš výsledek.

V posledním sloupečku naší tabulky je uveden podíl $\frac{n}{\pi(n)}$. Když si zkusíš spočítat rozdíl dvou po sobě jdoucích členů v tomto sloupci, vyjde Ti přibližně číslo 2,3. Pokud si nyní uvědomíš, že $\ln 10$ je roven přibližně tomuto číslu, snadno nahlédneš, jak můžeme dospět ke znění tvrzení (PNT). (Uvedenou poučku jako hypotézu zformuloval už francouzský matematik Adrian-Marie Legendre na počátku minulého století.)

S prvočísly souvisí samozřejmě mnoho dalších hypotéz[†], o kterých se zde z nedostatku přiděleného prostoru nemůžeme zmínit, ale uveďme zde ještě jedno zajímavé, ale těžké **Tvrzení**, které dokázal německý matematik Peter Gustav Lejeune Dirichlet :

Tvrzení : *Jsou-li a, b nesoudělná přirozená čísla, pak posloupnost $a + n \cdot b$, kde n probíhá všechna přirozená čísla, obsahuje nekonečně mnoho prvočísel.*

Zkuste si sami za cvičení dokázat toto **Tvrzení** pro čísla tvaru $4n + 3$ a $6n + 5$. To není tak těžké, stačí mírně modifikovat původní Eukleidův důkaz nekonečnosti počtu prvočísel.

Dokázat některé hypotézy okolo prvočísel se dodnes nepodařilo, u jiných jsou důkazy značně obtížné, každopádně elementárními prostředky lze dokázat na základě **Lemmatu** níže uvedené dvě věty, které nám o rozložení prvočísel dávají také jistou informaci.

Lemma : *Nechť $n \geq 1$. Pak*

(i) $2^n \leq \binom{2n}{n} < 2^{2n}$

(ii) $\prod_{n<p\leq 2n} p | \binom{2n}{n}$

(iii) *Nechť $r(p)$ splňuje $p^{r(p)} \leq 2n < p^{r(p)+1}$, pak $\binom{2n}{n} | \prod_{p\leq 2n} p^{r(p)}$*

(iv) *Pokud $n > 2$ a $2n/3 < p \leq n$, pak $p \nmid \binom{2n}{n}$*

(v) $\prod_{p\leq n} p < 4^n$

Toto **Lemma** bude nám nástrojem k důkazu dalších vět. Povšimněme si samotného bodu (v). Ten má také pro nás jistou hodnotu. Říká nám, že mezery mezi prvočísly nemohou být příliš malé. Snadno z bodu (v) by se Ti mohlo podařit dokázat, že v přirozených číslech existuje libovolně dlouhý úsek bez prvočísel, což bylo již výše ukázáno trikem z faktoriály.

Věta 1 : *Pokud $n > 1$, pak $\frac{n}{8 \ln n} < \pi(n) < \frac{6n}{\ln n}$.*

Tato věta nám tvrdí, že existují takové konstatny a, b, že platí $a \cdot \frac{n}{\ln n} < \pi(n) < b \cdot \frac{n}{\ln n}$ a že je lze volit jako $a = \frac{1}{8}$, $b = 6$. To jsou konstanty trochu nadsazené a dají se dále zlepšovat. Výsledek tohoto typu (s lepšími konstantami) dokázal v polovině minulého století ruský matematik Pafnutij Lvovič Čebyšev.

Věta 2 (Bertrandův postulát) : *Pokud $n \in \mathbb{N}$, pak existuje prvočíslo p splňující $n < p \leq 2n$.*

Ze svých výsledků týkajících se odhadů funkce $\pi(n)$ ho odvodil Čebyšev. Důkaz pomocí výše uvedeného lemmatu je od Erdöse.

[†]Goldbachova hypotéza, Riemannova hypotéza, problém prvočíselných dvojčat, výskyt prvočísel v intervalech, ...