Teorie čísel

Radek Erban

Témata přednášek budou zvolena podle zájmu posluchačů. V následujícím textu jsem se proto rozhodl uvést přehled několika vět z elementární teorie čísel. V samotných přednáškách se můžeme buď zaměřit na nějaký slavný problém v teorii čísel (dokonalá čísla, Velká Fermatova věta, Waringův problém, ...), nebo můžeme dokázat nějaká zajímavá složitější tvrzení (o součtech čtverců, rozložení prvočísel, diofantických rovnicích, ...), nebo se můžeme bavit o něčem úplně jiném — jak budete chtít.

V tomto textu používám následující značení: Množinu přirozených čísel budeme označovat písmenem $\mathbb{N}$ (tj. $\mathbb{N} = \{1,\ 2,\ 3,\ 4, \dots\}$), množinu celých čísel písmenem $\mathbb{Z}$, reálných $\mathbb{R}$, množina celých nezáporných čísel bude pojmenována $\mathbb{N}_0$. Pro $\alpha \in \mathbb{R}$ budeme symbolem $\lfloor \alpha \rfloor$ značit celou část čísla α, tj. $\lfloor \alpha \rfloor$ je největší celé číslo menší nebo rovno α.

Dělitelnost

Nechť a, b jsou dvě celá čísla. Říkáme, že a *dělí* b (resp. b *je násobkem* a) a zapisujeme to $a|b$, pokud existuje celé číslo c takové, že $b = a \cdot c$.

Věta. (Základní vlastnosti dělitelnosti) *Nechť* $a,\ b,\ c,\ x,\ y \in \mathbb{Z}$. *Pak platí*

(i) Pokud platí $a|b$ *a* $b|c$, *pak také* $a|c$.

(ii) Pokud platí $a|b$, *pak* $ac|bc$.

(iii) Pokud platí $a|b$ *a* $a|c$, *pak také* $a|bx + cy$.

(iv) $1|a,\ a|-a,\ a|0,\ a|a$.

Věta. (O dělení se zbytkem) *Pro každé* $a \in \mathbb{Z}$, $b \in \mathbb{N}$ *existují* $q,\ r \in \mathbb{Z}$ *takové, že* $a = b \cdot q + r$ *a* $0 \leq r < b$.

Čísla q, r z této věty nazýváme *celočíselným podílem a zbytkem při celočíselném dělení* čísla a číslem b. Společným dělitelem čísel a, b nazýváme každé číslo d takové, že $d|a$, $d|b$. *Největší společný dělitel* čísel a, b nazýváme každý jejich společný dělitel, který je násobkem všech jejich společných dělitelů. Největší společné dělitele čísel a, b se mohou lišit jen znaménkem. Nezáporný největší společný dělitel čísel a, b budeme označovat (a, b). *Nejmenší společný násobek* čísel a, b nazveme takové číslo n, které je jejich společným násobkem (tj. $a|n$, $b|n$) a je dělitelem všech jejich společných násobků. Nezáporný nejmenší společný násobek čísel a, b budeme označovat $\mathrm{nsn}(a, b)$. Čísla a, b nazýváme *nesoudělná*, pokud $(a, b) = 1$. Pokládáme $(0, 0) = 0$, $\mathrm{nsn}(0, 0) = 0$.

Věta. *Pro každé $a, b, c \in \mathbb{Z}$ platí*
(i) $(a, 0) = |a|,\ (b, a) = (a, b) = (a - b \cdot c, b),\ (c \cdot a, c \cdot b) = |c| \cdot (a, b)$.
(ii) $\operatorname{nsn}(a, b) \cdot (a, b) = |a| \cdot |b|$.

Prvočísla a rozklad na prvočinitele

Prvočíslo je takové přirozené číslo, které má právě dva kladné dělitele. Existuje nekonečně mnoho prvočísel. Prvních 300 prvočísel udává tabulka na konci tohoto textu.

Věta. *Celé číslo $x > 1$ je prvočíslo právě tehdy, když neexistuje žádný jeho dělitel d, $1 < d \leq \sqrt{x}$.*

Věta. (rozklad na prvočinitele) *Každé číslo $a \in \mathbb{N},\ a \geq 2$ se dá vyjádřit ve tvaru $a = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdots p_n^{q_n}$, 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.*

Věta. *Nechť $a,\ b \in \mathbb{N}$, $p_1, \ldots, p_n$ jsou po dvou různá prvočísla a nechť platí*

$$a = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdots p_n^{q_n},\quad b = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdots p_n^{r_n},$$

přičemž $q_1, \ldots, q_n,\ r_1, \ldots, r_n \in \mathbb{N}_0$. Pak
(i) $a|b$ právě tehdy, když $q_i \leq r_i$ pro všechna $i = 1,\ 2, \ldots, n$.
(ii) a je k-tou mocninou přirozeného čísla právě tehdy, když $k|q_i$ pro všechna $i = 1,\ 2, \ldots, n$.
(iii) $(a, b) = p_1^{\min(q_1, r_1)} \cdot p_2^{\min(q_2, r_2)} \cdot p_3^{\min(q_3, r_3)} \cdots p_n^{\min(q_n, r_n)}$.
(iv) $\operatorname{nsn}(a, b) = p_1^{\max(q_1, r_1)} \cdot p_2^{\max(q_2, r_2)} \cdot p_3^{\max(q_3, r_3)} \cdots p_n^{\max(q_n, r_n)}$.

Pro každé přirozené číslo a označíme symbolem $\varphi(a)$ počet všech čísel z množiny $\{0,\ 1,\ 2, \ldots, (a-1)\}$ nesoudělných s číslem a, symbolem $\tau(a)$ *počet kladných dělitelů čísla a* a symbolem $S(a)$ *součet všech kladných dělitelů čísla a*. Funkce φ, která každému a přiřazuje $\varphi(a)$, se nazývá *Eulerova funkce*.

Věta. *Nechť přirozené číslo $a \geq 2$ má prvočíselný rozklad $a = p_1^{q_1} \cdot p_2^{q_2} \cdots p_n^{q_n}$, kde $p_1, \ldots, p_n$ jsou po dvou různá prvočísla a $q_1, \ldots, q_n \in \mathbb{N}$. Pak platí*

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right),$$

$$\tau(a) = (q_1 + 1) \cdot (q_2 + 1) \cdots (q_n + 1),$$

$$S(a) = \frac{p_1^{q_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{q_2+1} - 1}{p_2 - 1} \cdots \frac{p_n^{q_n+1} - 1}{p_n - 1}.$$

Věta. *Pro každá dvě nesoudělná čísla* $a,\ b \in \mathbb{N}$ *platí* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),\ \tau(a \cdot b) = \tau(a) \cdot \tau(b),\ S(a \cdot b) = S(a) \cdot S(b)$.

Kongruence

Nechť $a,\ b \in \mathbb{Z},\ m \in \mathbb{N}$. Řekneme, že a je *kongruentní* s b *podle modulu* m, a píšeme $a \equiv b \pmod{m}$, pokud $m|(b-a)$. V tomto případě se m nazývá modul a číslo b zbytek od a při modulu m. Zápis $a \equiv b \pmod{m}$ nazýváme *kongruencí*, pro úsporu místa budeme místo tohoto zápisu někdy používat též $a \equiv b(m)$.

Uvědomme si, že $a \equiv b \pmod{m}$ neznamená nic jiného než, že existuje $q \in \mathbb{Z}$ takové, že $a = b + q \cdot m$. Na základě tohoto pozorování již snadno nahlédneme, že kongruence splňuje vlastnosti uvedené v následující větě:

Věta.
(i) Pokud $a \equiv b(m)$ *a* $c \equiv d(m)$, *pak* $a + c \equiv b + d(m)$ *a* $ac \equiv bd(m)$.
(ii) Pokud $a \equiv b(m)$ *a* $d|m$, *pak* $a \equiv b(d)$.
(iii) Pokud $a \equiv b(m)$, $a = a_0 d$, $b = b_0 d$ *a* $(d, m) = 1$, *pak* $a_0 \equiv b_0(m)$.

Dle této věty tedy vidíme, že kongruence lze mezi sebou sčítat, násobit a za jistých předpokladů dělit číslem. Nechť je nyní $m \in \mathbb{N}$, uvažujme systém m čísel $0,\ 1,\ 2, \ldots, (m-1)$. Je-li nyní $a \in \mathbb{Z}$, je a kongruentní právě s jedním z čísel $0,\ 1,\ 2, \ldots, (m-1)$, všechna celá čísla můžeme tedy rozdělit do m disjunktních skupin podle toho, s kterým z čísel $0,\ 1,\ 2, \ldots, (m-1)$ jsou sledovaná čísla kongruentní.[1] Vybereme-li nyní z každé skupiny po jednom číslu dostáváme systém m čísel, který nazýváme *úplný systém zbytků při modulu* m. Vybereme-li z úplného systému zbytků při modulu m, pouze ta čísla, která jsou nesoudělná s m dostáváme systém $\varphi(m)$ čísel[2], který nazýváme *redukovaný systém zbytků při modulu* m.

Věta. (Eulerova) *Pokud* $(a, m)=1$, *pak* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Věta. (Malá Fermatova) *Je-li* p *prvočíslo, pak* $a^p \equiv a \pmod{p}$.

Věta. (Lagrangeova věta) *Nechť* f *je polynom stupně* n *proměnné* x, p *prvočíslo, pak kongruence* $f(x) \equiv 0 \pmod{p}$ *má maximálně* n *řešení*[3], *nebo jsou všechny koeficienty polynomu* f *kongruentní s nulou podle modulu* p.

[1] Do první skupiny dáme čísla dávající při dělení m zbytek 0, do druhé ta, které dávají zbytek 1, do třetí ta se zbytkem 2, ..., do m-té čísla, která při dělení m dají zbytek $(m-1)$.

[2] $\varphi(m)$ je Eulerova funkce od m zavedená dříve

[3] To znamená, že když vezmeme libovolný úplný systém zbytků při modulu p, nejvýše n čísel z tohoto systému splňuje po dosazení za x uvedenou kongruenci.

Pro $n \in \mathbb{N}_0$ definujme *faktoriál* rekurentně takto $0! = 1,\ (n+1)! = n! \cdot (n+1)$. Dále pro $m, n \in \mathbb{N}_0, n \leq m$ definujme *kombinační číslo* vzorcem $\binom{m}{n} = \frac{m!}{n! \cdot (m-n)!}$.

Věta. (Wilsonova věta) *Pokud p je prvočíslo, pak $(p-1)! \equiv -1 \pmod{p}$.*

Věta. *Pro každé $n \in \mathbb{N}$ je číslo $\binom{2n}{n}$ dělitelné všemi prvočísly p, $n < p \leq 2n$.*

Věta. (Rozklad faktoriálu na prvočinitele) *Pro každé $n \in \mathbb{N},\ n \geq 2$ platí*

$$n! = \prod_{p \leq n} p^{q_p}, \text{ kde } q_p = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

kde p v prvním součinu probíhá všechna prvočísla nepřesahující n.

Tabulka prvních tří set prvočísel

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