Chapter I

Dělitelnost

I.1 Relace dělitelnost

I.1.1 Pro celá čísla n, m píšeme $n \mid m$ právě tehdy když n dělí m, neboli m je násobkem čísla m, $m = k \cdot n$ pro nějaké $k \in \mathbb{Z}$. Tímto způsobem získáváme binární relaci dělitelnosti na množině celých čísel. Jakožto bunární relace je to vlastně množina příslušných dvojic celých čísel. Tato relace má řadu vlastností.

Pro zábavu a poučení se přesvědčíme o tom, že $29 \mid 4988$, $29 = 4+9+8+8$, $75 \mid 5700$, $17 \mid 6171$, $495 \mid 5940$, $25 \mid 125$, $5/25$, $5 \mid 5$, $33 \mid 99$, $99 \mid 693$, $99 \mid 9009$, $11 \mid 1001$, $22 \mid 2002$, $33 \mid 3003$, ..., $88 \mid 8008$ (viz též V.6.2 XXX).

Na druhé straně $11 \nmid 1010$ (to jest, nedělí) a $75 \nmid 570$. Ovšem $11 \mid 1100$ a $125 \mid 1125$ ($1125/125 = 9$).

I.1.2 Věta. Relace dělitelnosti $\mid$ je reflexivní a tranzitivní (tedy je to kvaziuspořádání).

Důkaz. Pro každé $n \in \mathbb{Z}$ je $n = 1n$, čili $n \mid n$. Dále, je-li $n \mid m$ a $m \mid k$, pak $m = ln$, $k = tm$, a tak $k = (tl)n$ a $n \mid k$. Tím jsme dokázali požadované vlastnosti reflexivity a tranzitivity. □

I.1.3 Věta. (i) $n \mid 0$ pro každé $n \in \mathbb{Z}$
(ii) $1 \mid n$ a $-1 \mid n$ pro každé $n \in \mathbb{Z}$

Důkaz. (i) $0 = n \cdot 0$.
(ii) $n = 1 \cdot n = (-1) \cdot (-n)$. □

I.1.4 Věta. (i) Je-li $n \in \mathbb{Z}$ takové, že $0 \mid n$, pak $n = 0$.
(ii) Je-li $n \in \mathbb{Z}$ takové, že $1 \mid n$ a nebo $-1 \mid n$ pak $n = \pm 1$.

Důkaz. (i) $n = k \cdot 0 = 0$.
(ii) Je $nk = \pm 1$. □

I.1.5 Věta. Nechť $n, m \in \mathbb{Z}$. Potom $n \mid\mid m$ (t.j. $n \mid m$ a $m \mid n$) právě tehdy když $n = m$ a nebo $n = -m$ (t.j. $n = \pm m$).

Důkaz. Nejdříve, je-li $m = kn$ a $n = lm$, pak $m = kln$, $(1 - kl)m = 0$ a, podobně, $(1 - kl)n = 0$. Pro $m = 0$ dostáváme $n = lm = l \cdot 0 = 0 = m$. Buď tedy $m \neq 0$. Pak rovnost $(1 - kl)m = 0$ implikuje rovnost $1 = kl$, a tak buď $k = 1$ a $m = n$, a nebo $k = -1$ a $m = -n$.

Nyní naopak. Je-li $m = n$, pak zjevně $n \mid\mid m$. Je-li $n = -m$, pak $n = (-1)m$ a $m = (-1)n$ a opět $n \mid\mid m$. □

I.1.6 Relace dělitelnost $\mid$ na množině $\mathbb{Z}$ není antisymetrická. Je to kvaziuspořádání, jehož jedinou ekvivalencí je relace $\mid\mid$. Z předchozí věty vidíme, že tato ekvivalence není "velká". Bloky ekvivalence jsou množiny $\{0\}$ a $\{n, -n\}$, $n \in \mathbb{N}$.

I.1.7 Věta. Nechť $m, n, k, l \in \mathbb{Z}$.

(i) Jestliže $n \mid m$, pak $kn \mid km$.

(ii) Jestliže $n \mid m$ a $k \mid l$, pak $nk \mid ml$.

(iii) Jestliže $nk \mid mk$ a $k \neq 0$, pak $n \mid m$.

Důkaz. (i) Je $m = tn$, a tedy $km = ktn$.

(ii) $m = tn$, $l = uk$ a tedy $nktu = ml$.

(iii) Je $mk = nkl$ pro nějaké $l \in \mathbb{Z}$. Je-li $m = 0$, pak $n \mid m$. Je-li $m \neq 0$, pak $mk \neq 0$ a tedy $n \neq 0 \neq l$. Ovšem $k(m - nl) = 0$, $k \neq 0$, takže $m = nl$ a $n \mid m$. □

I.1.8 Jak vidíme, relace dělitelnosti $\mid$ je stabilní (čili stálá) vůči operaci násobení. Ekvivalence $\mid\mid$ je tedy kongruencí multiplikativní pologrupy oboru $\mathbb{Z}$. Ovšem, tyto relace nejsou stabilní vůči sčítání. Např. $1 \mid 2$ a $1 + 1 = 2 \nmid 3 = 1 + 2$. Nicméně jestliže $n \mid m_1, \ldots, n \mid m_k$, $k \geq 1$, pak $n \mid m_1 + \cdots + m_k$.

Nechť $n \mid m$ a $k \mid l$, $n, m \in \mathbb{Z}$, $k, l \in \mathbb{N}_0$. Je $m = nu$ a $l = kv$, $u \in \mathbb{Z}$, $v \in \mathbb{N}_0$. Nyní $m^k = n^k u^k$ a $m^l = m^{kv} = (n^l u^k)^v = n^{kv} \cdot u^{kv}$. Tedy $n^k \mid m^l$ v tomto případě. Je-li však $v = 0$, pak $l = 0$ a $m^l = m^0 = 1$. V tomto případě $n^k \mid m^l = 1$ právě když buďto $k = 0$ nebo $n = 1$ a nebo $n = -1$.

I.1.9 Věta. Nechť $n_1, n_2, n_3, \ldots$ je nekonečná posloupnost celých čísel taková, že $n_{i+1} \mid n_i$ pro každé $i \geq 1$. Potom existuje $k \geq 1$ tak, že $n_{k+j} = \pm n_k$ pro všechna $j \geq 0$. Tedy $|n_k| = |n_{k+1}| = |n_{k+2}| = \ldots$.

Důkaz. Je $n_i = n_{i+1} t_i$ pro vhodné číslo $t_i \in \mathbb{Z}$. Pak ovšem $|n_i| = |n_{i+1}||t_i|$, čili $|n_{i+1}| \mid |n_i|$. Tedy buď to $n_i = 0$, a nebo $|n_{i+1}| \leq |n_i|$. Je-li $n_k = 0$ pro nějaké $k \geq 2$, pak $0 \mid n_{k-1}$, a tak $n_{k-1} = 0$. Indukcí tak dostaneme $n_k = n_{k-1} = n_{k-2} = \ldots = n_1 = 0$. Můžeme tedy předpokládat, že $r \geq 1$

jsou všechna čísla $n_r, n_{r+1}, n_{r+2}, \dots$ nenulová. Jak jsme si všimli, potom je $|n_r| \geq |n_{r+1}| \geq |n_{r+1}| \geq \dots 1$. Množina kladných čísel $|n_{r+l}|$, $l \geq 0$, má nejmenší člen, a sice číslo n_j. Pak ale $n_j = |n_{j+l}|$, $l \geq 0$. □

I.1.10 Poznámka. Relace dělitelnosti $|$ jsouc vztažena na množinu $\mathbb{N}_0$ nezáporných celých čísel je již uspořádáním této množiny. Zbývající vlastnost antisymetrie již plyne z I.1.5.

Číslo 0 je největším prvkem a číslo 1 je nejmenším prvkem v tomto uspořádání. Navíc, jestliže $n \mid m$, kde $n, m \in \mathbb{N}$, pak $n \leq m$. Ovšem, $k \mid 0$ a $0 \leq k$ pro všechna $k \in \mathbb{N}_0$.

Uspořádání $|$ není lineární. Např. $2 \nmid 3$ a $3 \nmid 2$. Tedy čísla 2 a 3 jsou nesrovnatelná v uspořádání dělitelnosti.

Pro každé $n \geq 2$ a $i \geq 0$ je $n^i \mid n^{i+1}$ a $n^i < n^{i+1}$. Tedy nekonečná posloupnost $(1 =)n^0, (n =)n^1, n^2, n^3, \dots$ je ostře rostoucí v obou uspořádáních $|$ a $\leq$. Z toho vidíme, že v množině $\mathbb{N}_0$ neexistují žádné duální atomy. To jest, čísla maximální v $\mathbb{N} = \mathbb{N}_0 \setminus 0$. Na druhé straně, atomů (t.j., čísel minimálních vzhledem k dělitelnosti v množině $\{0, 2, 3, \dots\} = \mathbb{N}_0 \setminus 1$ existuje mnoho. Říkáme jim prvočísla.

I.1.11 Věta. Následující podmínky jsou ekvivalentní pro celé číslo q:

(i) Čísla ± 1 a $\pm q$ jsou jediní (celočíselní) dělitelé čísla q.

(ii) Číslo q má nejvýše čtyři celočíselné dělitele.

(iii) Buďto $q = \pm 1$, a nebo absolutní hodnota $|q|$ je atomem v množině $\mathbb{N}_0$ uspořádané relací dělitelnost (viz I.1.10).

(iv) $q \neq 0$ a jestliže $n, m \in \mathbb{Z}$, jsou taková čísla, že $q \mid nm$, pak buďto $q \mid n$ či $q \mid m$.

Důkaz. (i) implikuje (ii).Tato implikace je triviální.

(ii) implikuje (iii). Buď $n \in \mathbb{N}_0$ takové, že $n \mid q$. Z (ii) plyne, že buďto $n = 1$ nebo $n = |q|$. To ale znamená, že buďto $|q| = 1$, a nebo $|q|$ je zmíněný atom.

(iii) implikuje (iv). Zřejmě $q \neq 0$. Uvažme nyní množinu A všech kladných celých čísel tvaru $aq + bn$, $a, b \in \mathbb{Z}$. Zřejmě $q \in A$, a tak množina A je neprázdná. Buď $r = a_1 q + b_1 n$ nejmenší číslo z množiny A. Podle **??** je $q = cr + d$, kde $c, d \in Z$ a $0 \leq d < r$. Potom $d = q - cr = q - ca_1 q - cb_1 b = (1 - ca_1)q + (-cb_1)n$. Ovšem $d \notin A$, a tedy nutně $d = 0$. Tím jsme dokázali, že $r \mid q$. Zcela obdobně zjistíme, že $r \mid n$. Odkud $1 \leq r \leq |q|$, a tak $q \mid n$ v případě, že $r = |q|$. Je-li $r < |q|$, pak $r = 1$ plyne z (iii) a můžeme psát $m = 1m = rm = (a_1 q + b_1 n)m = a_1 mq + b_1 nm$. Jelikož $q \mid nm$, tak $q \mid m$.

(iv) implikuje (i). Nechť $t \in \mathbb{Z}$, $t \mid q$. Potom $q = tk$ pro vhodné $k \in \mathbb{Z}$ a, ovšem, $q \mid tk$. Jestliže $q \mid t$, $t = aq$, pak $q = qak$, $q(1 - ak) = 0$, $ak = 1$ (neboť $q \neq 0$), $k = pm1$ a $t = \pm q$. Jestliže $q \nmid t$, tak $q \mid k$, $k = bq$, $q = qbt$, $1 = bt$ a $t = \pm 1$. □

I.1.12 Poznámka. Jestliže $0 \mid nm$,kde $n, m \in \mathbb{Z}$, pak $nm = 0$, a tedy buďto $n = 0$ a $0 \mid n$, či $m = 0$ a $0 \mid m$. Z tohoto důvodu musíme v podmínce **??**(iv) předpokládat, že $\neq 0$.

I.1.13 Definice. Celé číslo q nazveme (multiplikativně) nerozložitelné, neboli ireducibilní, jestliže $q \neq \pm 1$ a q splňuje ekvivalentní podmínky I.1.11.

Zřejmě číslo q je nerozložitelné právě když $-q$ je takové. Kladná nerozložitelná čísla se nazývají prvočísla.

Multiplikativně neutrální číslo 1 a invertibilní číslo -1 nejsou dle naší definice nerozložitelná čísla. Ve skutečnosti ale stejně nejdou rozložit a mají vlastnosti obdobné.

Číslo $2 = 1 + 1$ je zřejmě nejmenší prvočíslo. Je-li totiž $1 \leq n$ takové, číslo, že $n \mid 2$, pak $n \leq 2$, a tedy buďto $n = 1$, či $n = 2$. Z tabulky malé násobilky (viz I.2.4) snadno nahlédneme, že čísla 3,5 a 7 jsou postupně další prvočísla. Čísla $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$ a $9 = 3 \cdot 3$ prvočísla nejsou.

Množinu všech prvočísel označíme symbolem $\mathbb{P}$. Tedy $2, 3, 4, 7 \in \mathbb{Z}$ a $0, 1 \notin \mathbb{P}$.

Aditivně neutrální číslo je číslo 0. Všechna celá čísla jsou aditivně invertibilní a žádné není aditivně nerozložitelné (aditivně ireducibilní). Pokud se omezíme na čísla nezáporná (popřípadě kladná), pak jediným aditivně nerozložitelným číslem bude číslo 1.

I.1.14 Cvičení. Je snadným cvičením ověřit, že čísla $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101$ jsou právě všechna prvočísla menší (či rovna) čísla(u) 102. Je jich právě $26 (= 3^3 - 1)$ a jejich postupné rozdíly jsou čísla $1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 5, 6, 8, 4$.

Uvedená prvočísla je dobré znát nazpaměť, a to i pozpátku. Další prvočísla jsou $103, 107, 109, 113, 127, \ldots$. Prvočísel menších číslu (či rovných) čísla(u) $128 = 2^7$ je tedy $31 = 2^5 - 1$.

I.1.15 Příklad. Čísla $13, 31, 17, 71, 37, 73, 79, 97, 107, 701, 109, 907, 113, 311$ jsou prvočísla. Stejně tak čísla $3, 31, 331, 3331, 33331, 333331, 3333331, 3333331$ jsou prvočísla, ale číslo $33333331 = 17 \cdot 19607843$ prvočíslo není.

Číslo 2221 je prvočíslo, přičemž čísla $21, 221$ a 22221 prvočísla nejsou.

Čísla $991, 99991$ a 9999991 jsou prvočísla.

Čísla $2, 3, 5, 7$ jsou prvočísla a taková jsou i čísla 2357 a 3257. Čísla $31621, 16213, 162133, 1621333, 16213333$ jsou prvočísla.

Obdobně 229 je prvočíslo a $1151 = 229 + 922$ je opět prvočíslo.

I.1.16 Věta. Nechť p je prvočíslo a nechť $n_1, \ldots, n_k$, $k \geq 1$ jsou taková celá čísla, že $p \mid n_1 \cdots n_k$. Potom $p \mid n_i$ pro alespoň jedno i, $1 \leq i \leq k$.

Důkaz. Tvrzení plyne snadnou indukcí z I.1.11(iv). □

I.1.17 Příklad. Nechť $k \in \mathbb{Z}$, $a = 33k + 14$ a $b = (12k + 5)(18k + 7) = 216k^2 + 174k + 35$. Číslo a je sudé a číslo b je liché. Tedy $a \nmid b$. Dále, $a + 1 = 36k + 15 = 3(12k + 5)$, $3 \mid a + 1$ a $b = 3(72k^2 + 58k + 11) + 2$. Tedy $3 \nmid b$ a $a + 1 \nmid b$. Dále, $a = 2(18k + 7)$, $18k + 7 \mid a$, $18k + 7 \mid b$ a nutně $18k + 7 \nmid b + 1$. Tedy $a \nmid b + 1$. Podobně $a + 1 = 3(12k + 5)$, $12k + 5 \mid a + 1$, $12k + 5 \mid b$ a nutně $12k + 1 \nmid b + 1$. Tedy $a + 1 \nmid b + 1$.

Ověřili jsem, že žádné z čísel $a, a+1$ nedělí žádné z čísel $b, b+1$. Nicméně $a(a+1) = (36k+14)(36k+15) = 6(12k+5)(18k+7) = 6b$, $b+1 = 6(65k+1)$ a tedy $a(a + 1)(65k + 1) = 6b(65k + 1) = b(b + 1)$. Takže $a(a + 1) \mid b(b + 1)$.

Pro $k = 0$ dostaneme $a = 14, b = 35, a + 1 = 15, b + 1 = 36$. $a(a + 1) = 210, b(b + 1) = 1260 = 6 \cdot 210$. Pro $k = 1$ dostaneme $a = 50, b = 425$. Pro $k = -1$ dostaneme $a = -22, b = 77$.

I.1.18 Příklad. (i) Je $n^2-1 = (n-1)(n+1)$ a tak $n-1 \mid n^2-1, n+1 \mid n^2-1$ pro všechna $n \in \mathbb{Z}$.

(ii) Je $n^2+1 = n(n-1)+(n+1) = n(n+1)-(n-1)$. Jestliže $n-1 \mid n^2+1$, pak $n-1 \mid n+1, n-1 \mid 2 = (n+1)-(n-1), n-1 = \pm 1, \pm 2 a n \in \{-1, 0, 2, 3\}$ (a naopak).

Samozřejmě, druhý výsledek plyne z prvního, neboť $n + 1 = -(-n - 1)$ a $n^2 + 1 = (-n)^2 + 1$.

(iii) Je $n^3 - 1 = (n - 1)(n^2 + n + 1)$ a $n - 1 \mid n^3 - 1$ pro každé $n \in \mathbb{Z}$.

Je $n^3 + 1 = (n + 1)(n^2 - n + 1)$ a $n + 1 \mid n^3 + 1$ pro každé $n \in \mathbb{Z}$.

(iv) Je $n^3 - 1 = (n^3 + 1) - 2$. Takže $n + 1 \mid n^3 - 1$ právě když $n + 1 \mid -2$. Tedy $n \in \{-3, -2, 0, 1\}$.

(v) Je $n^3 + 1 = (n^3 - 1) + 2$. Takže $n - 1 \mid n^3 + 1$ právě když $n - 1 \mid 2$. Tedy $n \in \{-1, 0, 2, 3\}$.

I.2 Tabulka malých prvočísel

I.2.1 Tabulka. A zde uvidíme tabulku malých prvočísel. Prvních 1236 prvočísel v pořadí, jak jdou za sebou.

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439
1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783
1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069
2081	2083	2087	2089	2099	2111	2113	2129	2131	2137	2141	2143
2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267
2269	2273	2281	2287	2293	2297	2309	2311	2333	2339	2341	2347
2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543
2549	2551	2557	2579	2591	2593	2609	2617	2621	2633	2647	2657
2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713
2719	2729	2731	2741	2749	2753	2767	2777	2789	2791	2797	2801
2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903

2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011
3019	3023	3037	3041	3049	3061	3067	3079	3083	3089	3109	3119
3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221
3229	3251	3253	3257	3259	3271	3299	3301	3307	3313	3319	3323
3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527
3529	3533	3539	3541	3547	3557	3559	3571	3581	3583	3593	3607
3613	3617	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697
3701	3709	3719	3727	3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989	4001	4003
4007	4013	4019	4021	4027	4049	4051	4057	4073	4079	4091	4093
4099	4111	4127	4129	4133	4139	4153	4157	4159	4177	4201	4211
4217	4219	4229	4231	4241	4243	4253	4259	4261	4271	4273	4283
4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493	4507	4513
4517	4519	4523	4547	4549	4561	4567	4583	4591	4597	4603	4621
4637	4639	4643	4649	4651	4657	4663	4673	4679	4691	4703	4721
4723	4729	4733	4751	4759	4783	4787	4789	4793	4799	4801	4813
4817	4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003	5009	5011
5021	5023	5039	5051	5059	5077	5081	5087	5099	5101	5107	5113
5119	5147	5153	5167	5171	5179	5189	5197	5209	5227	5231	5233
5237	5261	5273	5279	5281	5297	5303	5309	5323	5333	5347	5351
5381	5387	5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521	5527	5531
5557	5563	5569	5573	5581	5591	5623	5639	5641	5647	5651	5653
5657	5659	5669	5683	5689	5693	5701	5711	5717	5737	5741	5743
5749	5779	5783	5791	5801	5807	5813	5821	5827	5839	5843	5849
5851	5857	5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053	6067	6073
6079	6089	6091	6101	6113	6121	6131	6133	6143	6151	6163	6173
6197	6199	6203	6211	6217	6221	6229	6247	6257	6263	6269	6271
6277	6287	6299	6301	6311	6317	6323	6329	6337	6343	6353	6359
6361	6367	6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571	6577	6581
6599	6607	6619	6637	6653	6659	6661	6673	6679	6689	6691	6701
6703	6709	6719	6733	6737	6761	6763	6779	6781	6791	6793	6803
6823	6827	6829	6833	6841	6857	6863	6869	6871	6883	6899	6907
6911	6917	6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103	7109	7121
7127	7129	7151	7159	7177	7187	7193	7207	7211	7213	7219	7229
7237	7243	7247	7253	7283	7297	7307	7309	7321	7331	7333	7349
7351	7369	7393	7411	7417	7433	7451	7457	7459	7477	7481	7487

7489	7499	7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643	7649	7669
7673	7681	7687	7691	7699	7703	7717	7723	7727	7741	7753	7757
7759	7789	7793	7817	7823	7829	7841	7853	7867	7873	7877	7879
7883	7901	7907	7919	7927	7933	7937	7949	7951	7963	7993	8009
8011	8017	8039	8053	8059	8069	8081	8087	8089	8093	8101	8111
8117	8123	8147	8161	8167	8171	8179	8191	8209	8219	8221	8231
8233	8237	8243	8263	8269	8273	8287	8291	8293	8297	8311	8317
8329	8353	8363	8369	8377	8387	8389	8419	8423	8429	8431	8443
8447	8461	8467	8501	8513	8521	8527	8537	8539	8543	8563	8573
8581	8597	8599	8609	8623	8627	8629	8641	8647	8663	8669	8677
8681	8689	8693	8699	8707	8713	8719	8731	8737	8741	8747	8753
8761	8779	8783	8803	8807	8819	8821	8831	8837	8839	8849	8861
8863	8867	8887	8893	8923	8929	8933	8941	8951	8963	8969	8971
8999	9001	9007	9011	9013	9029	9041	9043	9049	9059	9067	9091
9103	9109	9127	9133	9137	9151	9157	9161	9173	9181	9187	9199
9203	9209	9221	9227	9239	9241	9257	9277	9281	9283	9293	9311
9319	9323	9337	9341	9343	9349	9371	9377	9391	9397	9403	9413
9419	9421	9431	9433	9437	9439	9461	9463	9467	9473	9479	9491
9497	9511	9521	9533	9539	9547	9551	9587	9601	9613	9619	9623
9629	9631	9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
9739	9743	9749	9767	9769	9781	9787	9791	9803	9811	9817	9829
9833	9839	9851	9857	9859	9871	9883	9887	9901	9907	9923	9929
9931	9941	9949	9967	9973	10007	10009	10037	10039	10061	10067	10069

Všimněme si, že $p(1) = 2, p(10) = 29, p(100) = 541, p(1000) = 7919$ a dále $p(10000) = 104729, p(100000) = 1299709$ a $p(1000000) = 15485863$.

Je tedy $14p(1) < p(10) < 15p(1)$, $18p(10) < p(100) < 19p(10)$, $14p(100) < p(1000) < 15p(100)$.

Posloupnost $p(i) - i$, kde $i \geq 1$, je ostře rostoucí a prvních pár členů jsou čísla $1, 2, 3, 6, 7, 10, 11, 14, 19, 20, 25, 28, \ldots$. První chybějící čísla jsou $4, 5, 8, 9, 12, 13, 15, 16, \ldots$.

I.2.2 Eratosthenovo síto Čísla 2,3,5,7,11 prvních pět prvočísel. Chceme-li najít další prvočísla, máme jednu prastarou metodu (která není příliš rychlá). Tuto metodu si osvětlíme na jednoduchém příkladě:

Chceme nalézt všechna prvočísla menší než číslo 150. Čísla do 150 včetně si napišme do tabulky a podtrhávejme vlastní násobky prvočísel 2,3,5,7,11

(postupně). Dostáváme:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Nejprve jsme podtržením označili násobky 2 (čili sudá čísla). Mohli jsme tedy rovnou vynechat každé druhé číslo. Potom vlastní násobky 3, čili jsme mohli vynechat každé třetí číslo. Dále násobky prvočísel $5, 7, 11$. Zbyla nám čísla 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

je $12^2 = 144 < 150 < 169 = 13^2$. Je-li nyní číslo n takové, že $2 \leq n \leq 150$, pak existuje alespoň jedno prvočíslo p tak, že $p \mid n$. Jestliže n není prvočíslo, pak $p < n$, $n_1 = n : p \geq 2$ a opět existuje prvočíslo q tak, že $q \mid n_1$. Tedy $pq \min n$. Je-li $t = \min(p, q)$, pak $t^2 \leq n$. Takže $t \leq 12$ a p nebo q leží v množině $\{2, 3, 5, 7, 11\}$. Číslo n bylo tedy vskutku z tabulky vyškrnuto.

Zbylá čísla jsou vskutku prvočísla a to všechna menší než 150.

Popsanou metodu objevil řecký matematik Erastothenes ($\pm$ 274 – 149 AC), který byl hlavním knihovníkem v Alexandrijské knihovně.

I.3 Základní věta aritmetiky

I.3.1 Věta. Nechť $n \geq 2$. Potom $n \in \{m, 2 \leq m, m \mid n\}$ a, je-li p nejmenší číslo v této množině čísel, potom p je prvočíslo.

Důkaz. Je $p \geq 2$. Jestli6e $q \geq 1$ je takové číslo, že $q \mid p$, pak $q \leq p$ a $q \mid n$. Tedy buďto $q = 1$, a nebo $q = p$. To znamená, že $p \in \mathbb{P}$. □

I.3.2 Věta. Pro každé $n \in \mathbb{Z}$, $n \neq \pm 1$, existuje alespoň jedno prvočíslo $p \in \mathbb{P}$ takové, že $p \mid n$.

Důkaz. Je-li $n = 0$, tak $2 \mid 0$. Je-li $n \neq 0$, tak $|n| \geq 2$ a podle I.3.1 existuje $p \in \mathbb{P}$ tak, že $p \mid |n|$. Samozřejmě $p \mid n$. □

I.3.3 Věta. Množina $\mathbb{P}$ všech prvočísel je nekonečná.

Důkaz. Je nutné a postačující dokázat, že ke každému prvočíslu p existuje větší prvočíslo. Máme $2 < 3 < 5 < 7 < 11$, čili tvrzení platí pro první čtyři prvočísla a my můžeme předpokládat, že $p > 7$. Nechť $(2 =)p(1) < (3 =)p(2) < (5 =)p(3) < \cdots < p(n) = p$, $n \geq 5$, je posloupnost všech prvočísel menších či rovných našemu prvočíslu p. Položme $m = (p(1)p(2)\dots p(n)) + 1$. Jistě je $m \geq 2$ (ve skutečnosti je $m > 1609$) a podle I.3.2 existuje prvočíslo q takové, že $q \mid m$. Ovšem, $q \nmid 1$, čili $q \nmid m - p(1)p(2)\dots p(n)$, pročež $q \neq p(i)$, pro všechna $i = 1, 2, \dots, n$. Pak ale $q > 2$. □

I.3.4 Věta. (Základní věta aritmetiky) Nechť n je celé číslo, $n \neq 0, \pm 1$. Potom existují jednoznačně určené číslo $s \geq 1$, jednoznačně určená množina $\{p_1, p_2, \dots, p_s\}$ obsahující s vesměs různých prvočísel a jednoznačně určené exponenty $r_1, r_2, \dots r_s \geq 1$ takové, že $n = \pm p_1^{r_1} \dots p_s^{r_s}$.

Důkaz. Nejdříve dokážeme existenci prvočíselného rozkladu čísla n.

Zřejmě můžeme předpokládat, že $n \geq 2$. Příklad, kdy n je samo prvočíslo je zřejmý. Nicméně, podle I.3.2 existuje prvočíslo p a číslo $m \geq 1$ tak, že $n = pm$. Je-li $m = 1$, je $n = p$ a jsme hotovi. Je-li $m \neq 1$, pak $2 \leq m < n$ a podle indukčního předpokladu má číslo m prvočíselný rozklad. Pak ale totéž platí i pro $n = pm$.

Nyní dokážeme jednoznačnost prvočíselného rozkladu čísla n. Opět budeme předpokládat $n \geq 2$.

Předpokládejme, že $p_1^{r_1} \dots p_s^{r_s} = n = g_1^{u_1} \dots q_v^{u_v}$ jsou dva různé prvočíselné rozklady čísla n. Můžeme rovněž předpokládat, že $p_1 < p_2 < \cdots < p_s$ a $q_1 < q_2 < \cdots < q_v$. Z I.1.16 plyne, že pro každé $i, 1 \leq i \leq s$, existuje $f(i)$ tak, že $1 \leq f(i) \leq v$ a $p_i \mid q_{f(i)}$. Je $p_i \geq 2$ a $q_{f(i)}$ je prvočíslo, takže máme rovnost $p_i = q_{f(i)}$. Jelikož $p_i < p_j$ pro $i < j$, tak $q_{f(i)} < q_{f(j)}$ a $f(i) < f(j)$.

Obdobně, pro každé $i, 1 \leq i \leq v$, existuje $g(i)$ tak, že $1 \leq g(i) \leq s$ a $q_i = p_{g(i)}$. Nyní je jasné, že $s = v$ a $f(i) = i$ pro každé i.

Máme $p_1^{r_1} \dots p_s^{r_s} = n = p_1^{u_1} \dots p_s^{u_s}$. Je-li $r_1 > u_1$, pak $p_1 \mid p_2^{u_2} \dots p_s^{u_s}$, spor s I.1.16. Tedy $r_1 \leq u_1$, zcela obdobně $u_1 \leq r_1, r_1 = u_1$ a $p_2^{r_2} \dots p_s^{r_s} = n = p_2^{u_2} \dots p_s^{u_s}$ (pro $s \geq 2$). Nyní lze postupovat indukcí. □

I.3.5 Důležitá definice Nechť $p \in \mathbb{P}$. Pro každé $n \in \mathbb{Z}$, $n \neq 0$, existuje jednoznačně určené nezáporné celé číslo r takové, že $p^r \mid n$ a $p^{r+1} \nmid n$. Budeme psát $r = cont_p(n)$ a budeme toto číslo nazývat p-obsah čísla n. Máme $n = p^r n_1, n_1 \in \mathbb{Z}, p \nmid n_1$.

Pro úplnost můžeme položit $cont_p(0) = +\infty$.

I.3.6 Věta. $cont_p(nm) = cont_p(n) + cont_p(nm)$ pro všechna $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$.

Důkaz. Můžeme předpokládat $n \neq 0 \neq m$. Máme $n = p^a \cdot n_1$, $m = p^b m_1$, $nm = p^c \cdot k$, kde $a = cont_p(n)$, $b = cont_p(m)$, $c = cont_p(nm)$, $p \nmid n_1, m_1, k$. Odtud $p^c \cdot k = nm = p^{a+b} n_1 m_1$. Z I.1.16(iv) plyne, že $p \nmid n_1 m_1$ a tedy $a + b = c$. □

I.3.7 Proposice. Nechť $p \in \mathbb{P}$. Potom:
(i) $cont_p(1) = 0 = cont_p(-1)$.
(ii) $cont_p(p^k) = k = cont_p(-p^k)$ pro každé $k \geq 0$.
(iii) $cont_p(n) = cont_p(-n)$ pro každé $n \in \mathbb{Z}$

Důkaz. Vše plyne přímo z definice I.3.5. □

I.3.8 Proposice. Nechť $s, r_1, \dots, r_s$ jsou kladná celá čísla a $p_1, \dots, p_s$ jsou po dvou různá prvočísla. Buď $n = \pm p_1^{r_1} \dots p_s^{r_s}$. Potom:
(i) $cont_{p_i}(n) = r_i$ pro každé $1 \leq i \leq s$.
(ii) $cont_p(n) = 0$ pro každé $p \in \mathbb{P}$, $p \notin \{p_1, \dots, p_s\}$

Důkaz. (i) Jelikož $p_i^{r_i} \mid n$, tak $r \leq cont_{p_i}(n)$. Z I.1.16 plyne, že $p_i \nmid n/p_i^{r_i} = m_i$ a tedy $cont_{p_i}(m_i) = 0$. Podle I.3.6 je $cont_{p_i}(n) = cont_{p_i}(p_i^{r_i}) + cont_{p_i}(m_i) = r_i + 0 = r_i$ (použije se I.3.7(ii)).

(ii) Z I.1.16 plyne, že $p \nmid n$. □

I.3.9 Věta. Pro každé $n \in \mathbb{Z}$, $n \neq 0$, platí rovnost $n = \pm \prod_{p \in \mathbb{P}} p^{cont_p(n)}$ ($cont_p(n) \neq 0$ jen pro konečně mnoho prvočísel p).

Důkaz. Tvrzení plyne snadnou kombinací z I.3.4 a I.3.8 (viz též I.3.7). □

I.3.10 Věta. Nechť $n, m \in \mathbb{Z}$. Potom $n \mid m$ právě když $cont_p(n) \leq cont_p(m)$ pro každé $p \in \mathbb{P}$.

Důkaz. Jestliže $n \mid m$, pak nerovnost $cont_p(n) \leq cont_p(m)$ plyne ihned z **??**. Jestliže $r = cont_p(n) \leq cont_p(m) = s \leq +\infty$, pak $p^r \mid p^s \mid m$. Je-li $s = +\infty$, pak $m = 0$ a $n \mid m$ triviálně. Zbytek důkazu je jasný z I.3.9 □

I.3.11 Věta. Nechť $n, m \in \mathbb{Z}$. Potom $|n| = |m|$ právě když $cont_p(n) = cont_p(m)$ pro každé $p \in \mathbb{P}$.

Důkaz. Tvrzení plyne snadno z I.3.10. □

I.3.12 Proposice. Nechť $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$, $n \neq 0 \neq m$, $n \neq -m$. Potom:
(i) $cont_p(n + m) \geq \min(cont_p(n), cont_p(m))$.
(ii) Je-li $cont_p(n) \neq cont_p(m)$, pak $cont_p(n+m) = \min(cont_p(n), cont_p(m))$.
(iii) Je-li $cont_2(n) = cont_2(m)$, pak $cont_2(n + m) > cont_2(n)$.

Důkaz. Je $n = p^r \cdot n_1$, $m = p^s \cdot m_1$, kde $r, s \in \mathbb{N}_0$, $p \nmid n_1$, $p \nmid m_1$. Můžeme předpokládat, že $r \geq s$. Potom $n + m = p^s \cdot k$, $k = p^{r-s} n_1 + m_1$. Je-li $r > s$, pak $p \nmid k$. Je-li $r = s$ a $p = 2$, pak $p = 2 \mid k$. □

I.3.13 Proposice. Nechť $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$, $n \neq 1 \neq m$. Potom $cont_p(nm - 1) \geq cont_p(n - 1), cont_p(m - 1))$.

Důkaz. Buď $m-1 = p^a u$, $m-1 = p^k v$, kde $a, b \in \mathbb{N}_0$, $a \geq b$, $u, v \in \mathbb{Z}$, $p \nmid u$, $p \nmid v$. Máme $nm-1 = (n-1)m+(m-1) = p^a um+p^b v = p^b(p^{a-1} \cdot um+v)$. □

I.3.14 Proposice. Nechť $k \geq 1$, $n_1, \ldots, n_k \in \mathbb{Z}$, $n_i \neq \pm 1$. Potom pro každé $p \in \mathbb{P}$ platí $cont_p(n_1 \ldots n_k - 1) \geq \min(cont_p(n_i - 1), 1 \leq i \leq k)$.

Důkaz. Tvrzení platí triviálně pro $k = 1$ a pro $k = 2$ je dokázáno v I.3.13. Dále postupujeme snadno indukcí dle $k \geq 2$. □

I.3.15 Proposice. Nechť $n \in \mathbb{Z}$, $n \neq 0, 1, -1$. Potom $cont_p(n - 1) \geq \min(cont_p(q - 1), q \in \mathbb{P}, q \mid n)$.

Důkaz. Podle I.3.4 je $n = \pm p_1^{r_1} \ldots p_s^{r_s}$, kde $s, r_i \geq 1$, $p_i \in \mathbb{P}$, p_i vesměs různá. Samozřejmě $p_i \neq \pm 1$ a podle I.3.14 máme $cont_p(n - 1) \geq \min(cont_p(p_i - 1))$. □

I.3.16 Poznámka. (i) Základní věta aritmetiky nás poučuje o tom, že multiplikativní pologrupa $\mathbb{N}'(\cdot)$, kde $\mathbb{N}' = \{n, n \geq 2\}$je volná komutativní pologrupa nekonečné spočetné hodnosti a množina $\mathbb{P}$ všech prvočísel je (jediná) množina volných generátorů této pologrupy. Multiplikativní pologrupa $\mathbb{N}(\cdot)$ je pak volný monoid.

(ii) Seřaďme všechna prvočísla do posloupnosti tak, jak jsou za sebou: $(2 =)p_{(1)} < (3 =)p_{(2)} < \ldots$. Pro každé $n \in \mathbb{Z}$ sestrojíme nekonečnou posloupnost $\alpha(n) = (cont_{p_{(1)}}(n), cont_{p_{(2)}}(n), cont_{p_{(1)}}(n), \ldots$. Je-li $n \neq 0$,

pak $\alpha(n)$ je nekonečná posloupnost nezáporných celých čísel, kde ovšem jen konečně mnoho čísel je nenulových. Např. $\alpha(1) = \alpha(-1) = (0, 0, 0, \dots)$, $\alpha(p_i) = (0, 0, \dots, 0, 1, 0 \dots$, kde 1 se nachází na i-tém místě, $\alpha(105) = (0, 1, 1, 1, 0, 0, \dots$, atd. Je $\alpha(0) = (+\infty, +\infty, +\infty, \dots)$.

Na množině nekonečných posloupností nezáporných celých čísel a symbolu $+\infty$ definujme uspořádání předpisem $(a_1, a_2, a_3, \dots) \leq (b_1, b_2, b_3, \dots$ právě když $a_i \leq b_i$ pro všechna $i = 1, 2, \dots$. Z I.3.10 nyní plyne, že pro $n, m \in \mathbb{Z}$ platí $n \mid m$ právě tehdy když $\alpha(n) \leq \alpha(m)$ ve smyslu právě definovaného uspořádání.

I.3.17 Příklad. Čísla $599, 601$ a 607 jsou prvočísla. $600 = 2^3 \cdot 3 \cdot 5^2$. Ovšem, $602 = 2 \cdot 7 \cdot 43$, $603 = 3^2 \cdot 67$, $604 = 2^2 \cdot 151$, $605 = 5 \cdot 11^2$ a $606 = 2 \cdot 3 \cdot 101$. Zde $2, 3, 5, 7, 11, 43, 67, 101$ a 151 jsou prvočísla.

I.3.18 Příklad. Hříčka Je $9196 = 2^2 \cdot 11^2 \cdot 19$. Je $9331 = 7 \cdot 31 \cdot 43$, $9 \cdot 3 \cdot 3 \cdot 1 = 81 = 7 + 31 + 43$, $31 \cdot 43 = 1333$, $93 = 3 \cdot 31$, $9331 = 31 \cdot 301$. Je $432 = 2^4 \cdot 3^3 = 4 \cdot 3^3 \cdot 2^2$

I.3.19 Definice. Pro každé $n \in \mathbb{Z}$ buď $\underline{P}(n) = \{p \in \mathbb{P}, p \mid n\}$.

Zřejmě $\underline{P}(n) = \underline{P}(-n)$, $\underline{P}(0) = \mathbb{P}$, $\underline{P}(1) = \emptyset$. Je-li $|n| \geq 2$, pak $\underline{P}(n) = \{p \in \mathbb{P}, cont_p(n) \geq 1$ je neprázdná konečná množina prvočísel.

Zřejmě je $\underline{P}(nm) = \underline{P}(n) \cup \underline{P}(m)$ pro všechna $n, m \in \mathbb{Z}$.

I.3.20 Příklad. Je $14 = 2 \cdot 7$ a $224 = 2^5 \cdot 7$. Tedy $\underline{P}(14) = \underline{P}(224)$. Dále, $15 = 14+1$, $225 = 224+1$, $15 = 3 \cdot 5$, $225 = 3^2 \cdot 5^2$ a $\underline{P}(15) = \{3.5\} = \underline{P}(225)$.

Je $418 = 2 \cdot 11 \cdot 19$, $\underline{P}(418) = \{2, 11, 19\}$ a $2 + 11 + 19 = 32 = 4 \cdot 1 \cdot 8$.

I.3.21 Proposice. Nechť $n, m \in \mathbb{Z}$. Následující dvě podmínky jsou ekvivalentní:

(i) $\underline{P}(n) = \underline{P}(m)$.

(ii) Existují $k, l \in \mathbb{N}$ tak, že $n \mid m^k$ a $m \mid n^l$.

Důkaz. Snadno nahlédneme, že se lze omezit na $n \geq 2$ a $m \geq 2$. Pak $n = p_1^{r_1} \dots p_s^{r_s}$ a $m = q_1^{u_1} \dots q_v^{u_v}$, kde $s, v, r_i, u_j \in \mathbb{N}$, $p_i, q_i \in \mathbb{P}$. $p_1 < \dots < p_s$ a $q_1 < \dots < q_v$.

Je-li $\underline{P}(n) = \underline{P}(m)$, pak $s = v$, $p_i = q_i$, $n \mid m^k$ pro $k \geq \max(r_i)$ a $m \mid n^l$ pro $l \geq \max(u_i)$.

Naopak, jestliže $n \mid m^k = q_1^{ku_1} \dots q_v^{ku_v}$, pak $\underline{P}(n) \subseteq \underline{P}(m)$. A naopak, pokud $m \mid n^l$, $\underline{P}(m) \subseteq \underline{P}(n)$. □

I.3.22 Příklad. (i) Je $1919 = 19 \cdot 101$, $1920 = 2^7 \cdot 3 \cdot 5$, $1921 = 17 \cdot 113$ (prvočíselné rozklady).

(ii) $1933 \mid 11 \dots 1$ (21x).

(iii) Je $3833 = 17 \cdot 199$ (prvočíselný rozklad). Je také $3 \cdot 3 \cdot 8 \cdot 3 = 216 = 17 + 199$.

I.3.23 Proposice. Nechť $n \in \mathbb{Z}$, $n \neq \pm 1$. Buď q nejmenší číslo takové, že $q \geq 2$ a $q \mid n$. Potom q je prvočíslo.

Navíc, je-li $q \neq |n|$, pak $q^2 \leq n$.

Důkaz. Podle I.3.2 existuje prvočíslo p tak, že $p \mid q$. Pak $p \mid n$ a z minimality čísla q plyne rovnost $p = q$. Tedy q je prvočíslo.

Je-li $q \neq< |n|$, pak $q \leq |n/q|$ a $q^2 \leq |n| \cdot |n/q| = |n|$. □

I.3.24 Lemma. Nechť $n, m \in \mathbb{Z}$ a $k \in \mathbb{N}$ jsou taková čísla, že $n^{k|m^k}$. Potom $n \mid m$.

Důkaz. Tvrzení je zřejmé pro $m = 0$ a také pro $n = 0, \pm 1$. Nechť tedy $m \neq 0$ a $|n| \geq 2$. Pro každé $p \in \mathbb{P}$ je $kcont_p(n) = cont_p(n^k) \leq cont_p(m^k) = kcont_p(m)$ a tedy $cont_p(n) \leq cont_p(m)$. Podle I.3.10 máme $n \mid m$. □

I.3.25 Lemma. Nechť $n, m \in \mathbb{Z}$ a $k, l \in \mathbb{N}$ jsou taková čísla, že $l \leq k$ a $n^k \mid m^l$. Buď t největší číslo takové, že $tl \leq k$. Je $t \geq 1$ a $n^t \mid m$. Navíc, je-li $m = n^t u$, pak $n^{k-tl} \mid u^l$, $0 \leq k - tl < l$.

Důkaz. Je $0 \leq k - tl < l$, což plyne z maximality čísla t. Dále, $(n^t)^l = n^{tl} \mid n^k \mid m^l$ a $n^t \mid m$ dle I.3.24. Nakonec, $n^k \mid m^l = n^{tl} \cdot u^l$ a $n^{k-tl} \mid u^l$. □

I.3.26 Lemma. Nechť $n \geq 1$ a $m \in \mathbb{Z}$ jsou taková čísla, že $m \mid p - 1$ pro každé $p \in \underline{P}(n)$. Potom $m \mid n - 1$.

Důkaz. Tvrzení je zřejmé pro $n = 1$. Je-li $n \geq 2$, pak $n = p_1 \dots p_s$, kde $s \geq 1$ a $p_i \in \mathbb{P}$ (prvočísla p_i nemusí být různá). Nyní, $m \mid p_1 - 1$, $m \mid p_1 p_2 - p_2$, $m \mid p_2 - 1$, $m \mid (p_1 p_2 - p_2) + (p_2) - 1 = p_1 p_2 - 1$, $m \mid p_1 p_2 p_3 - p_3$, $m \mid p_3 - 1$, $m \mid p_1 p_2 p_3 - 1, \dots$, $m \mid p_1 p_2 \dots p_s - 1$. □

I.3.27 Lemma. Nechť $n \geq 2$ a $q \in \mathbb{P}$. Potom $cont_q(n-1) \geq \min(cont_q(p - 1), p \in \underline{P}(n)$.

Důkaz. Pro každé $p \in \underline{P}(n)$ je $cont_q(p - 1) = r(p)$ a $q^{r(p)} \mid p - 1$. Je-li $r = \min(r(p), p \in \underline{P}(n))$, pak $q^r \mid n - 1$ podle I.3.26. □

I.3.28 Poznámka. Nechť $n \geq 2$, $n = p_1^{r_1} \dots p_s^{r_s}$, $s, r_i \geq 1$, p_i po dvou různá prvočísla. Buď $q \in \mathbb{P}$ a $s_i = cont_q(p_i + 1)$. Položme $r = r_1 + \dots + r_s$. Je-li $z = \min(s_i . 1 \leq i \leq s)$, potom $q^z \mid n - (-1)^r$. Je-li r sudé, tak $q^z \mid n - 1$ a $cont_q(n - 1) \geq z$. Je-li r liché, tak $q^z \mid n + 1$ a $cont_q(n + 1) \geq z$.

I.4 Složená čísla

I.4.1 Definice. Celé číslo, které není nerozložitelné ve smyslu I.1.13 se nazývá (multiplikativně) rozložitelné. Nenulové rozložitelné číslo se nazývá složené.

I.4.2 Věta. Následující podmínky jsou ekvivalentní pro $n \in \mathbb{Z}$:

(i) Číslo n je složené.

(ii) Existují prvočísla p_1, p_2, p_3 (ne nutně různá) taková, že $p_1p_2 \mid n$, avšak $p_3 \nmid n$.

(iii) $n \neq 0$ a existují prvočísla p_1, p_2 (ne nutně různá) taková, že $p_1p_2 \mid n$.

(iv) $n \neq 0$, $n \neq \pm 1$, $n \neq \pm p$, $p \in \mathbb{P}$.

(v) Existuje $m \in \mathbb{Z}$ tak, že $2 \leq m < |n|$ a $m \mid n$.

(vi) Počet dělitelů čísla n je konečný a větší než 4.

(vii) Počet dělitelů čísla n je konečný a a je alespoň 6.

(viii) $n = \pm p_1^{r_1} \dots p_s^{r_s}$, $s, r_i \in \mathbb{N}$, $p_i \in \mathbb{P}$ (p_i vesměs různá a $\sum r_i > 1$.

(ix) $n = n_1 n_2$, kde $2 \leq |n_1|$ a $2 \leq |n_2|$.

(x) $|n| \geq 2$ a $|n| \notin \mathbb{P}$.

Důkaz. Stačí uvážit I.1.13, I.3.4 a I.4.1. □

I.4.3 Příklad. (i) Nechť $n \geq 2$. Uvažme n po sobě jdoucích čísel $(n+1)!+2$, $(n+1)!+3, \dots, (n+1)!+(n+1)$. Je-li $2 \leq m \leq n+1$, pak $m \mid (n+1)!$, $m \mid m$ a tak $m \mid (n+1)!+m$. Ovšem, $(n+1)!+m < 0 \geq 2$. Takže číslo $(n+1)!+m$ je složené (viz I.4.2. Tedy n po sobě jdoucích čísel $(n+1)!+2$, $(n+1)!+3, \dots, (n+1)!+(n+1)$ jsou vesměs čísla složená a žádné z nich není prvočíslo.

Pro $n = 2$ dostáváme čísla 8, 9 (10 je také složené). Pro $n = 3$ čísla 26, 27, 28 (ovšem i čísla 24 a 25 jsou složená). Pro $n = 4$ čísla 122,123,124,125 (ovšem složená jsou i čísla 114, ... 126 - tedy 13 po sobě jdoucích složených čísel).

Pro $n = 5$ čísla 722, 723, 724m 725m 726 (720 a 721 jsou složená a 719 a 727 jsou prvočísla).

(ii) Každé z 33 po sobě jdoucích čísel 1328,..., 1360 je složené (viz I.2.1).

I.4.4 Poznámka. Uvažujme nenulová čísla n taková, že $p^2 \mid n$ kdykoliv $p \in \mathbb{P}$, $p \mid n$ (t.j. $cont_p(n) \geq 2$, kdykoliv $cont_p(n) \neq 0$. Těmto číslům se někdy říká mocná. Nám se více zamlouvá jim říkat vydatná.

Samozřejmě, pro každé $n \neq 0$ a každé $k \geq 2$ je mocnina n^k vydatné číslo. Číslo $-n^k$ je také vydatné.

Čtrnáct čísel 1,4,8,9,16,25,27,32,36,49,64,72,81,100 jsou právě všechna vydatná čísla mezi 1 až 100. Mezi těmito čísly pouze 72 není druhou či vyšší mocninou.

$8 = 2^3$ a $9 = 3^2$ je dvojice po sobě jsoucích vydatných čísel. $12167 = 23^3$ $12168 = 2^{3\cdot 3^2 \cdot 13^2}$ je také dvojice vydatných čísel.

Není známo, zda existují tři po sobě jdoucí vydatná čísla. Nicméně, je-li n sudé číslo, tak $4 \mid n$, $n+2$ je také sudé číslo a $4 \nmid n+2$. Tedy $n+2$ není vydatné. Zjistili jsme tedy, že nemohou existovat čtyři po sobě jdoucí vydatná čísla.

Vydatná čísla jsou uzavřená na součiny.

I.4.5 Proposice. Kladné celé číslo n je vydatné, právě tehdy když $n = a^2b^3$ pro nějaká $a, b \in \mathbb{N}$.

Důkaz. Nejdříve, nechť n je vydatné číslo. Lze předpokládat $n \geq 4$. Je $n = p_1^{r_1} \dots p_s^{r_s}$, kde $s, r_i \geq 1$ a $p_1, \dots, p_s$ jsou různá prvočísla. Jelikož n je vydatné, tak $r_i \geq 2$ pro každé i. Jsou-li všechna čísla r_i sudé, pak $n = a^2 \cdot 1^3$, kde $a = p_1^{r_1/2} \dots p_s^{r_s/2}$. Jsou-li všechna čísla r_i lichá, pak $n = a^2 \cdot b^3$, kde $a = p_1^{(r_1-3)/2} \dots p_s^{(r_s-3)/2}$, $b = p_1 \dots p_s$. Nenastává-li ani jeden z těchto dvou případů, pak $s \geq 2$ a existuje $1 \leq t < s$ tak, že po vhodném přečíslování prvočísel $p_1, \dots, p_s$ jsou čísla $r_1, \dots, r_t$ sudá a čísla $r_{t+1}, \dots, r_s$ lichá. Nyní $n = a^2b^3$, kde $a = p_1^{r_1/2} \dots p_t^{r_t/2} p_{t+1}^{(r_{t+1}-3)/2} \dots p_s^{(r_s-3)/2}$ a $b = p_{t+1} \dots p_s$.

Naopak, nechť $n = a^2b^3$, $a, b \in \mathbb{N}$. Čísla a^2, b^3 jsou vydatná a takový je i jejich součin. □

I.4.6 Poznámka. Kladné vydatné číslo (viz I.4.4, které není druhou, či vyšší mocninou, je známo jako Achiltovo číslo.

Čísla $72 = 2^3 \cdot 3^2$, $108 = 2^2 \cdot 3^3$ a $200 = 2^3 \cdot 3^2$ jsou nejmenší tři Achiltova čísla. Číslo $5000 = 2^3 5^4$ je také Achiltovo. Říká se, že $5425069447 = 7^3 41^2 97^2$ a $5425069448 = 2^3 \cdot 26041^2$ je nejmenší dvojice po sobě jdoucích Achiltových čísel.

Nejmenší liché Achiltovo číslo je $675 = 3^3 5^2$. Pro každé $p \in \mathbb{P}$, $p \geq 5$ a každí $k \geq 3$, k liché, jsou čísla $2^k \cdot p^2$ a $3^k p^2$ Achiltova. To je nekonečně mnoho různých čísel sudých i lichých.

I.4.7 Proposice. Nechť n je složené číslo. Potom existuje alespoň jedno prvočíslo p takové, že $p \mid n$, přičemž $p^2 < |n|$.

Důkaz. Viz I.3.23. □

I.5 Bezčtvercová čísla

I.5.1 Číslo n nazveme bezčtvercové, jestliže $p^2 \nmid n$ pro každé $p \in \mathbb{P}$.

Zřejmě 0 není bezčtvercové číslo a n je bezčtvercové právě když $-n$ je takové. Každé prvočíslo je bezčtvercové.

Čísla 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 37, 38, 39, 41, 42, 43, 46, 47, 51, 53, 55, 57, 58, 59, 61, 62, 65, 66, 67, 69, 70, 71, 73, 74, 77, 78, 79, 82, 83, 85, 86, 87, 89, 91, 93, 94, 96, 97 je všech 62 bezčtvercových přirozených čísel menších než 100. Zbývá 37 čísel, která nejsou bezčtvercová a sice 4, 8, 9, 12, 16, 20, 24, 25, 27, 28, 32, 36, 40, 44, 45, 48, 49, 50, 52, 54, 56, 60, 63, 64, 68, 72, 75, 76, 80, 81, 84, 88, 90, 92, 95, 98 a 99. Číslo 100 také není bezčtvercové.

Je-li $n \in \mathbb{Z}$, pak aspoň jedno z čísel n, $n+1$, $n+2$ a $n+3$ je dělitelné číslem 4 a tak není bezčtvercové.

Čísla 1, 2, 3 jsou bezčtvercová. Podobně 5, 6, 7 a 13, 14, 15. Čísla 8, 9 nejsou bezčtvercová a 48, 49, 50 je první trojice po sobě jdoucích kladných čísel, která nejsou bezčtvercová.

Později (IV.4.6) si dokážeme, že pro každé $n \geq 2$ existuje n po sobě jdoucích čísel takových, že žádné z nich není bezčtvercové (srovnej s I.4.3.

Čísla n^3-3 jsou vesměs bezčtvercová pro $-26 \leq 2 \leq 26$ ($27-3 = 2{\cdot}3{\cdot}11^2$).

I.5.2 Věta. Celé číslo n je bezčtvercové, právě když buďto $n = \pm 1$ a nebo $n = \pm p_1 \dots p_s$, kde $s \geq 1$ a $p_1, dots, p_s$ jsou po dvou různá prvočísla.

Důkaz. Čísla ± 1 jsou zřejmě bezčtvercová. Je-li $n \geq 2$ bezčtvercové, pak prvočíselný rozklad $n = \pm p_1 \dots p_s$ je důsledkem I.3.4,

Naopak, je-li $n = \pm p_1 \dots p_s$, pak číslo n je zjevně bezčtvercové dle definice. □

I.5.3 Věta. Nechť $n \in \mathbb{Z}$, $n \neq 0$. Potom existují jednoznačně určená čísla $m \in \mathbb{Z}$ a $k \in \mathbb{N}$ taková, že $n = mk^2$, přičemž číslo m je bezčtvercové.

Důkaz. Je-li $n = \pm 1$, pak volíme $m = n$ a $k = 1$. Buď $n \geq 2$. Podle I.3.4 je $n =^{r_1} \dots p_s^{r_s}$, kde $s, r_i \geq 1$ a $p_1, \dots p_s$ jsou po dvou různá prvočísla.

Jsou-li všechna čísla r_i sudé, pak $m = 1$, kde $n = p_1^{r_1} \dots p_s^{r_s}$. Jsou-li všechna čísla r_i lichá, pak $m = 1$, kde $a = p_1^{r_1)/2} \dots p_s^{r_s/2}$, $b = p_1 \dots p_s$. Nenastává-li ani jeden z těchto dvou případů, pak $s \geq 2$ a existuje $1 \leq t < s$ tak, že po vhodném přečíslování prvočísel $p_1, \dots, p_s$ jsou čísla $r_1, \dots, r_t$ sudá a čísla $r_{t+1}, \dots, r_s$ lichá. Nyní $k = p_1^{r_1/2} \dots p_t^{r_t/2} p_{t+1}^{(r_{t+1}-1)/2} \dots p_s^{(r_s-1)/2}$ a $m = p_{t+1} \dots p_s$. Tím je dokázána existence čísel m a k.

Teď je potřeba dokázat jednoznačnost čísel m a k. Budeme postupovat indukcí podle n. Případe $n = 2$ je jasný. Nechť nyní $n \geq 3$ a $n = m_1 k_1^2 =$

$m_2k_2^2$, kde $m, 1, m_2, k_1, k_2 \in \mathbb{N}$, m_1, m_2 bezčtvercová čísla. Je-li $m_1 = 1 = m_2$, pak $k_1^2 = k_2^2$ a $k_1 = k_2$. Nechť $m_1 \geq 2$. Pak existuje aspoň jedno prvočíslo p tak, že $p \mid m_1$. Jestliže $p_m id m_2$, máme $m_3k_1^3 = m_4k_2^3$, kde $m_3 = m_1/p$ a $m_4 = m_2/p$. Čísla m_3, m_4 jsou zřejmě bezčtvercová a použijeme indukční předpoklad. Dostaneme $m_3 = m_4$ a $.k_1 = k_2$. Tedy $m_1 = pm_3 = pm_4 = m_2$. Nakonec, nechť $p \nmid m_2$. Pak $p \mid k_2$. Nyní $1 + 2cont_p(k_1) = cont_p(n) = 2cont_p(k_2)$, což nelze.

Pro $n \leq -2$ postupujeme obdobně. □

I.5.4 Lemma. Nechť $n, m, t \in \mathbb{Z}$ a $k \in \mathbb{N}$ jsou taková čísla, že $k \geq 2$, t je bezčtvercové a $n^k = tm^k$. Potom $n \mid m$.

Důkaz. Lze předpokládat, že $m \neq 0$ a $|n| \geq 2$. Je $rn^k = tm^k$ pro $r \in \mathbb{Z}$, $r \neq 0$. Je-li $p \in \mathbb{P}$, pak $cont_p(r) + kcont_p(n) = cont_p(t) + kcont_p(m) \leq 1 + kcont_p(m)$ a $k(cont_p(n) - cont_p(m)) = cont_p(t) - cont_p(r) \leq 1$. Odtud, $cont_p(n) - cont_p(m) \leq 0$ a $cont_p(n) \leq cont_p(m)$. Podle I.3.10 je $n \mid m$. □

I.6 Fermatův rozklad

Rozložit dané (kladné) celé číslo na součin prvočísel je úloha velmi nelehká, ano, často nad míru obtížná a časově náročná. V některých případech však situace není zoufalá. Např., je-li $n = a^2 - b^2$, pak $n = (a-b)(a+b)$ a z tohoto "přerozkladu" lze někdy vyjít.

I.6.1 Úvaha Nechť $n \geq 1$ je liché číslo. $n = ab$, kde $a \geq 1$, $b \geq 1$, $a \geq b$, obě čísla a, b jsou lichá a tak $a + b = 2c$, $a - b = 2d$, $c \geq d \geq 0$. Navíc $4c^2 - 4d^2 = (a+b)^2 - (a-b)^2 = a^2 + 2ab + b^2 - a^2 + 2ab - b^1 = 4ab = 4n$, $n = ab = c^2 - d^2 = (c-d)(c+d)$, $c^2 = n + d^2$ a $d^2 = c^2 - n$. Samozřejmě, $c^2 \geq n$.

Je-li $b \geq 5$, tak $n + 1 > 4c$ podle **??**. Je-li $a \geq 7$, $b \geq 3$, tak $n + 1 > 4c$ podle **??**. Je-li $a = 5$, $b = 3$, tak $n = 5$, $c = 4$, $n + 1 = 16 = 4c$. Je-le $a = 3 = b$, tak $n = 9$, $c = 3$, $n + 1 = 10 > 9 = 3c$. Je-li $b = 1$, tak $n + 1 = a + 1 = 2c$. Vidíme, že $n + 1 \geq 2c$ v každém případě (pro $n > 10$ je $n + 1 \geq 4c$).

Předchozí zjištění lze tu a tam použít pro rozložení lichého čísla n na součin. Předně nechť $m \in \mathbb{N}$ je nejmenší číslo takové, že $m^2 \geq 2$. Je-li $m^2 = n$, jsme hotovi. Je-li $m^2 > n$, pak pátráme, zda $m^2 - n = k_0^2$ pro nějaké $k_0 \geq 1$. Není-li tomu tak, pak nás bude zajímat rovnice $(m+1)^2 - n = k_1^2$, $k_1 \geq 1$. Obecně pak rovnice $(m+l)^2 - n = k_l^2$, $k_l \geq 1$. Tento postup končí! Pro $n > 10$ se stačí zajímat pouze o taková čísla l, že $0 \leq l$, $4l \leq n - 4m + 1$ (viz úvaha výše).

I.6.2 Příklad. Buď $n = 21$. Potom $m = 5$, $5^2 = 25$, $25 - n = 4 = 2^2$, $n = 5^2 - 2^2 = (5-2)(5+2) = 3 \cdot 7$.

I.6.3 Příklad. Buď $n = 2263$. Potom $m = 48$ a dále:
$49^2 - n = 138$
$50^2 - n = 237$
$51^2 - n = 338$
$52^2 - n = 441 = 21^2$.
Takže $n = 52^2 - 21^2 = (52-21)(52+21) = 31 \cdot 73$.

I.6.4 Příklad. Buď $n = 6077$. Potom $m = 78$, $78^2 = 6084$, $6084 - n = 7$, $79^2 = 6241$, $6241 - n = 164$, $80^2 = 6400$, $6400 - n = 323$, $81^2 = 6561$, $6561 - m = 484 = 22^2$.

Tedy $6077 = 81^2 - 22^2 = (81-22)(81+22) = 59 \cdot 103$.

I.6.5 Příklad. Buď $n = 2027651281$. Je $m = 45030$, $m^2 = 2027700900$ a $2m = 90060$. A nyní píšeme

$m^2 - n = 2027700900 - 2027651281 = 49619$

$2m+1 = 90061$
$(m+1)^2 - n = m^2 - n + 2m + 1 = 139680$
$2m+3 = 90063$
$(m+2)^2 - n = (m+1)^2 - n + 2m + 3 = 229743$
$2m+5 = 90065$
$(m+3)^2 - n = (m+2)^2 - n + 2m + 5 = 319808$
$2m+7 = 90067$
$(m+4)^2 - n = (m+3)^2 - n + 2m + 7 = 40872$
$2m+9 = 90069$
$(m+5)^2 - n = (m+4)^2 - n + 2m + 9 = 499944$
$2m+11 = 90071$
$(m+6)^2 - n = (m+5)^2 - n + 2m + 11 = 590015$
$2m+13 = 90073$
$(m+7)^2 - n = (m+6)^2 - n + 2m + 13 = 680088$
$2m+15 = 90075$
$(m+8)^2 - n = (m+7)^2 - n + 2m + 15 = 770163$
$2m+17 = 90077$
$(m+9)^2 - n = (m+8)^2 - n + 2m + 17 = 860240$
$2m+19 = 90079$
$(m+10)^2 - n = (m+9)^2 - n + 2m + 19 = 950319$
$2m+21 = 90081$
$(m+11)^2 - n = (m+10)^2 - n + 2m + 21 = 1040400 = 1020^2$

Takže $n = 45041^2 - 1020^2 = (45041-1020)(45041+1020) = 44021 \cdot 46061$ (prvočíselný rozklad).

Tento příklad je poučný. Předně jsme použili vztah $(m+i+1)^2 - n = (m+i)^2 - n + 2m + 2i + 1$ pro $i = 0, 1, 2, \ldots$. Takže přičítáme pouze čísla $2m+2i+1$ k předchozímu rozdílu $(m+i)^2 - n$. dále je vhodné si uvědomit, že druhé mocniny mohou mít v dekadickém zápise na konci pouze dvojčíslí 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.

Z toho plyne, že v našem příkladě zjišťujeme pouze, zda čísla 499944 a 1040400 jsou druhými mocninami. Ovšem, $499944 = 8 \cdot 62493$. Je tedy $cont_2(499944) = 3$ a 499944 není druhou mocninou. Oproti tomu, $1040400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 17^2 = (2^2 \cdot 3 \cdot 5 \cdot 17)^2 = 1020^2$.

I.6.6 Poznámka. Příklad sestavil samotný Fermat. Pierre de Fermat (1601-1665) byl francouzský matematik a právník působící v Toulouse. Ukazuje se, že Fermatův rozklad funguje nejlépe pro čísla, která jsou součinem dvou přibližně stejně velkých čísel.