Kapitola I

Celá čísla a co s nimi

I.1 Celá čísla – sčítání a odčítání

I.1.1 Nezabývejme se tím, kde se vzalo, ale máme tu celé množství (rozuměj: množinu) $\mathbb{Z}$ celých čísel, $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$. Množina $\mathbb{Z}$ se rozpadne na disjunktní sjednocení tří podmnožin, $\mathbb{Z} = \mathbb{N}^- \cup \{0\} \cup \mathbb{N}^+$, kde $\mathbb{N}^+ = \{1, 2, 3, 4, \dots\}$ jsou čísla kladná (v dalším budeme používat jednodušší zápis $\mathbb{N}^+ = \mathbb{N}$) a $\mathbb{N}^- = \{\dots, -4, -3, -2, -1\}$ jsou pak čísla záporná. Čísla z $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ se nazývají nezáporná a čísla z $\mathbb{N}_0^- = \mathbb{N}^- \cup \{0\}$ slují nekladná.

I.1.2 Sčítání. Na množině $\mathbb{Z}$ máme definovanou operaci sčítání $(a, b) \to a + b$. Tato operace je komutativní, t.j. $a + b = b + a$. Je také asociativní, t.j. $a + (b + c) = (a + b) + c$. Operace sčítání má neutrální prvek (číslo). Je jím číslo 0, neb $a + 0 = a$. Není zde ovšem absorbující prvek. Jinak řečeno, pro každé $a \in \mathbb{Z}$ existuje aspoň jedno $b \in \mathbb{Z}$ tak, že $a + b \neq a$. Pro $a \neq 0$ lze volit $b = a$ a pro $a = 0$ lze volit $b = 1$. Všimněme si, že číslo 0 je jediný aditivně idempotentní prvek. Tedy $0 + 0 = 0$, avšak $a + a \neq a$ pro každé $a \in \mathbb{Z}$, $a \neq 0$.

Množiny $\mathbb{N}, \mathbb{N}_0, \mathbb{N}^-, \mathbb{N}_0^-$ jsou uzavřeny na sčítání. To jest, $a + b \in \mathbb{N}$ pro všechna $a, b \in \mathbb{N}$, atd.

Počítejme! Je $2457 = 169 + 170 + 171 + 172 + 173 + 174 + 175 + 176 + 177 + 178 + 179 + 180 + 181 + 182$ (čtrnáct sčítanců) a také $2457 = 183 + 184 + 185 + 186 + 187 + 188 + 189 + 190 + 191 + 192 + 193 + 194 + 195$ (třináct sčítanců). Podobně je $400 + 401 + \dots + 420 = 8610 = 421 + 422 + \dots + 440$ (dvacetjeden sčítanec a dvacet sčítanců).

A teď: $7941 = 7777 + 9 + 44 + 111$, $7942 = 7777 + 99 + 44 + 22$, $7946 = 7777+99+4+66$, $7496 = 777+44+9+6666$, $7679 = 7+6666+7+999$, $7672 = 777+6666+7+222$, $8486 = 888+44+888+6666$, $8664 = 888+6666+666+444$.

I.1.3 Odčítání. Na množině $\mathbb{Z}$ je také definována operace odčítání $(a, b) \to a - b$. Je $0 - 1 = -1 \neq 1 = 1 - 0$, $3 - (2 - 1) = 3 - 1 = 2 \neq 0 = 1 - 1 = (3 - 2) - 1$. Operace odčítání není ani komutativní, ani asociativní. Nicméně platí následující rovnosti: $a - (b - c) = c - (b - a), (a - b) - c = (a - c) - b, a - (a - b) = b, a - a = b - b (= 0), a - 0 = a, -a = 0 - a, -(-a) = a$. Číslo 0 je pravý neutrální prvek pro odčítání, nikoli však levý neutrální prvek.

Žádná z množin $\mathbb{N}, \mathbb{N}_0, \mathbb{N}^-, \mathbb{N}_0^-$ není uzavřená na operaci odčítání. Restrikce (čili zúžení) odčítání na tyto množiny poskytuje pouze operace částečné (neboli parciální).

I.1.4 Sčítání a odčítání dohromady. Operace sčítání a odčítání spolu souvisí rovností $a + (b - a) = b$. Také máme $a - b = a + (-b) = a + (0 - b)$, $a + b = a - (-b) = a - (0 - b)$.

Množina $\mathbb{Z}$ je komutativní (neboli Abelova) grupa vůči operaci sčítání. Množiny $\mathbb{N}, \mathbb{N}_0, \mathbb{N}^-$ a $\mathbb{N}_0^-$ jsou komutativní pologrupy vůči sčítání.

Pro $a, b \in \mathbb{Z}$ je $a + b = a - b$ právě když $b = 0$. Je $a - b = b - a$ právě když $a = b$. Je $a - (b - c) = (a - b) - c$ právě když $c = 0$.

I.1.5 Malá Sčítalka a Odčítalka.

Nejdříve Malá Sčítalka:

n + m

+	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	2	3	4	5	6	7	8	9	10
2	3	4	5	6	7	8	9	10	11
3	4	5	6	7	8	9	10	11	12
4	5	6	7	8	9	10	11	12	13
5	6	7	8	9	10	11	12	13	14
6	7	8	9	10	11	12	13	14	15
7	8	9	10	11	12	13	14	15	16
8	9	10	11	12	13	14	15	16	17
9	10	11	12	13	14	15	16	17	18

Všimněme si hlavní a vedlejší diagonály!

A nyní Malá Odčítalka:

n − m

−	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	0	−1	−2	−3	−4	−5	−6	−7	−8
2	1	0	−1	−2	−3	−4	−5	−6	−7
3	2	1	0	−1	−2	−3	−4	−5	−6
4	3	2	1	0	−1	−2	−3	−4	−5
5	4	3	2	1	0	−1	−2	−3	−4
6	5	4	3	2	1	0	−1	−2	−3
7	6	5	4	3	2	1	0	−1	−2
8	7	6	5	4	3	2	1	0	−1
9	8	7	6	5	4	3	2	1	0

Opět si všimněme obou diagonál.

I.2 Celá čísla – násobení a dělení

I.2.1 Násobení. Na množině $\mathbb{Z}$ celých čísel máme též definovánu operaci násobení $(a, b) \to a \cdot b$ $(= ab = a \times b)$. Opět jde o operaci komutativní a asociativní $(ab = ba,\ a(bc) = (ab)c)$. Tato operace má neutrální prvek, a sice číslo 1. Je $a \cdot 1 = a$. Násobení má také absorbující prvek, a sice číslo 0. Je $a \cdot 0 = 0$. Všimněme si, že číslo 1 a číslo 0 jsou jediné multiplikativně idempotentní prvky.

Množiny $\mathbb{N}$ a $\mathbb{N}_0$ jsou uzavřeny na násobení a množiny $\mathbb{N}^-, \mathbb{N}_0^-$ nikoliv. Nicméně množina $\mathbb{Z} \setminus \{0\} = \mathbb{N} \cup \mathbb{N}^-$ je též uzavřena na násobení. Množiny $\mathbb{Z}, \mathbb{N}, \mathbb{N}_0$ a $\mathbb{N} \cup \mathbb{N}^-$ tvoří komutativní pologrupy vzhledem k násobení.

Buďtež $a, b \in \mathbb{Z}$ taková čísla, že $ab = 1$. Pak buďto $a = 1 = b$, nebo $a = -1 = b$. Čísla $1, -1$ jsou jediná taková, která mají inversní (opačný) prvek vzhledem k násobení. Množina $\{1, -1\}$ je tedy (dvouprvková) grupa vzhledem k násobení.

Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $a + b = ab$. Pak $a(b-1) = b$, $b(a-1) = a$, z čehož snadno plyne, že $ab = ab(a-1)(b-1)$. Je-li $a = 0$ popř. $b = 0$, pak $a = 0 = b$. Je-li však $a \neq 0 \neq b$, pak $(a-1)(b-1) = 1$, čili $a - 1, b - 1 \in \{1, -1\}$ a $a = 2 = b$.

Nalezli jsme, že $a + b = ab$ pouze pro $(a, b) = (0, 0), (2, 2)$.

Obdobně nalezneme, že $a - b = ab$ pouze pro $(a, b) = (0, 0), (-2, 2)$.

Počítejme! Je $3578 \cdot 28 = 100100$ a $3581 \cdot 31 = 111011$. Je $2 \cdot 6819 = 13638$, $2 \cdot 6918 = 13836$. Je $3 \cdot 6819 = 20457$ a $3 \cdot 6918 = 20754$ (zde navíc levé a pravé strany rovnosti nemají společnou číslici). Je $9 \cdot 1089 = 9801$ a $9 \cdot 1090 = 9810$. Je $2 \cdot 6891 = 13782$, $2 \cdot 6981 = 13962$, $96 - 78 = 18$, $2 \cdot 1896 = 3792$, $2 \cdot 1986 = 3972$, $97 - 79 = 18$. Je $1679 = 23 \cdot 73$, kde $23 = 1 + 6 + 7 + 9$. Je $21 \cdot 6 = 126$ a $41 \cdot 35 = 1435$. Je $742 = 3 \cdot 247 + 1$ a $793 = 2 \cdot 397 - 1$.

Číslo 2114 je zajímavé tím, že $2 \cdot 1 \cdot 1 \cdot 4 = 8 = 2 + 1 + 1 + 4$. Je $142857 \cdot 1 = 142857$, $142857 \cdot 2 = 285714$, $142857 \cdot 3 = 428571$, $142857 \cdot 4 = 571428$, $142857 \cdot 5 = 714285$, $142857 \cdot 6 = 857142$, $142857 \cdot 7 = 999999$, $142857 \cdot 8 = 1142856$, $142857 \cdot 9 = 1285713$, $142857 \cdot 10 = 1428570$, $142857 \cdot 11 = 1571427$. Jaké poučení z toho plyne? Je určitě dobře si povšimnout, že $1000000 = 142857 \cdot 7 + 1$.

I.2.2 Dělení. Dělení celých čísel je v oboru celých čísel pouze operace částečná. Je $c = a/b$ $(= \frac{a}{b} = a : b)$, jestliže $b \neq 0$ a $a = cb$. Např. $-2/2 = -1, 6/-3 = -2, 12/3 = 4$, atd. Oproti tomu $1/2$ není definováno v celých číslech, neboť $2a \neq 1$ pro každé celé číslo a. Otázkám dělitelnosti se budeme věnovat velmi velice.

Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $a/b = ab$. Pak $ab^2 = a$ a snadno vidíme, že buďto $a = 0$ a nebo $b = \pm 1$.

Počítejme! Všechna celá čísla, co dělí číslo $125(=5^3)$ jsou $\pm1, \pm5, \pm25, \pm125$. Je $125/\pm1 = \pm125, 125/\pm5 = \pm25, 125/\pm25 = \pm5$ a $125/\pm125 = \pm1$. Je $4988/29 = 172$, kde $29 = 4+9+8+8$. Je $5700/75 = 1140/15 = 228/3 = 76$. Je $6171/17 = 363, 363/3 = 121, 121/11 = 11$. Je $5940/495 = 12$. Je $2^7 \cdot 3^2 \cdot 7 = 8064 = (1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9)/(1+2+3+4+5+6+7+8+9)$. Je $8959/31 = 289, 31 = 8+9+5+9$. Je $1088/17 = 64, 17 = 1+0+8+8$. Je $510/15 = 34, 1+5 = 6, 3+4 = 7, 4 = 5-1$. Je $10000000001/8779 = 11390819, 8+7+7+9 = 31, 1+1+3+9+0+8+1+9 = 32$. Je $2100/12 = 175$.

I.2.3 Sčítání a násobení dohromady. Máme $a(b+c) = ab+ac$ pro všechna celá čísla a, b, c. Násobení je tedy distributivní (neboli rozdělovací) vůči sčítání. Je však také $a(b-c) = ab-ac, a(-b) = (-a)b = -ab, (-a)(-b) = ab, a^2 = (-a)^2$. Dále, $(a+b)/c = a/c + b/c$ za předpokladu, že oba podíly $a/c, b/c$ jsou definovány.

Počítejme! Je $2926 = 19\cdot154 = (2+9+2+6)\cdot2\cdot7\cdot11, 2919 = 21\cdot139 = (2+9+1+9)(29+91+19)$. Je $3\cdot9+1 = 28, 28/2 = 14, 14/2 = 7, 3\cdot7+1 = 22, 22/2 = 11, 3\cdot11+1 = 34, 34/2 = 17, 3\cdot17+1 = 52, 52/2 = 26, 26/2 = 13, 3\cdot13+1 = 40, 40/2 = 2, 20/2 = 10, 10/2 = 5, 3\cdot5+1 = 16, 16/2 = 8, 8/2 = 4, 4/2 = 2$ a konečně $2/2 = 1$ $(3\cdot1+1 = 4, 4/2 = 2, 2/2 = 1)$. Je $3\cdot15+1 = 46, 46/2 = 23, 3\cdot23+1 = 70, 70/2 = 35, 3\cdot35+1 = 106, 106/2 = 53, 3\cdot53+1 = 160, 160/32 = 5, 3\cdot19+1 = 58, 58/2 = 29, 3\cdot29+1 = 88, 88/8 = 11$. Je $18 = 2\cdot9 = 2(1+8), 81 = 9\cdot9 = (8+1)(8+1)$.

Je $10\cdot11\cdot12\cdot13\cdot14 = 16\cdot3\cdot5\cdot7\cdot11\cdot13, 10+11+12+13+14 = 60 = 4\cdot3\cdot5$. $10\cdot1\cdot12\cdot13\cdot14/(10+11+12+13+14) = 4\cdot7\cdot11\cdot13 = 4004$. Je $1\cdot2\cdot3\cdot4\cdot5 = 120$, $1+2+3+4+5 = 15$, $120/15 = 8$. Je $1\cdot2\cdot3 = 6 = 1+2+3$. Je $2100/12 = 175 = 7\cdot25 = 5\cdot35$, $1+7+5 = 13 = 5+3+5$, $7+2+5 = 14$, $1+4 = 5$.

I.2.4 Malá Násobilka (čili Množilka aneb Stoleček Pythagorův).

n · m

·	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	21	24	27
4	4	8	12	16	20	24	28	32	36
5	5	10	15	20	25	30	35	40	45
6	6	12	18	24	30	36	42	48	54
7	7	14	21	28	35	42	49	56	63
8	8	16	24	32	40	48	56	64	72
9	9	18	27	36	45	54	63	72	81

Všimněme si obou diagonál.

I.2.5 Faktoriál. Faktoriál $n!$ nezáporného čísla n definujeme takto:

$0! = 1 = 1!$ a $n! = 1 \cdot 2 \cdots n$ pro $n \geq 2$. Je tedy $(n+1)! = n! \cdot (n+1)$ pro každé $n \geq 0$. Máme $2! = 2, 3! = 6, 4! = 24, 5! = 120, 6! = 720, 7! = 5040, 8! = 40320, 9! = 362880$ a $10! = 3628800$. O faktoriálech si toho budeme hodně povídat později.

Je $2204 = 4 \cdot 19 \cdot 29$, kde $4 = 2^2$ a $19, 29$ jsou prvočísla. A teď $2! + 2! + 0! + 4! = 2 + 2 + 1 + 24 = 29$, přičemž 29 je největší prvočíslo, co dělí 2204. Navíc, $2^2 + 2^2 + 0^2 + 4^2 = 4 + 4 + 0 + 16 = 24 = 4!, 2^3 + 2^3 + 0^3 + 4^3 = 8 + 8 + 0 + 64 = 80 = 10(2 + 2 + 0 + 4)$.

Je zábavné, že $(6!-6)+(5!-5)+(7!-7)+(6!-6) = 714+115+5033+714 = 6576$.

I.2.6 Poznámka. Je $1 + 2 + \cdots + n = n(n+1)/2 = (n+1)!/(n-1)! \cdot 2$ pro všechna $n \geq 1$.

I.2.7 Příklad. Je $(1-1)!+1 = 2, (2-1)!+1 = 2, (3-1)!+1 = 3, (4-1)!+1 = 7, (5-1)! + 1 = 25 = 5^2, (6-1)! + 1 = 126 = 2 \cdot 9 \cdot 7$.

Je-li $n \geq 6$, pak $n^2 - 6n = n(n-6) \geq 0, n^2 - 6n + 4 \geq 4, (n-1)! + 1 > (n-1)! > 2(n-1)(n-2) = 2(n^2-3n+2) = 2n^2-6n+4 \geq n^2+4$. Skutečně, $(n-1)! + 1 \neq n^2$.

Zjistili jsme, že $n = 5$ je jediné kladné číslo n takové, že $(n-1)!+1 = n^2$.

Je známo, že 13^2 dělí číslo $(13-1)! + 1$ a 563^2 dělí číslo $(563-1)! + 1$. S malými obtížemi spočteme $(13-1)! + 1 = 12! + 1 = 479001600 + 1 = 479001601, 13^2 = 169$ a $479001601/169 = 36846277/13 = 2834329$ (což už je prvočíslo). Tedy $(13-1)! + 1 = 13^2 \cdot 2834329$ (prvočíselný rozklad).

I.2.8 Počítání. Nechť $m \geq 2$ a $a_1, \ldots, a_m$ jsou po dvou různá kladná celá čísla. Můžeme je seřadit podle velikosti, a tak existuje permutace σ intervalu $\{1, \ldots, m\}$ taková, že $1 \leq a_{\sigma(1)} \leq \cdots \leq a_{\sigma(m)}$. Snadnou indukcí nalezneme $a_{\sigma(i)} \geq i + 1$ pro každé $i = 1, \ldots, m$. Tedy $a = a_1 \cdots a_m \geq m!$. Je $a = m!$ právě když $\{a_1, \ldots, a_m\} = \{1, \ldots, m\}$.

I.2.9 Krácení. Součin nenulových celých čísel je opět nenulové celé číslo. Jinak řečeno, je-li $ab = 0$ pro $a, b \in \mathbb{Z}$, pak $0 \in \{a, b\}$. Jsou-li nyní $a, b, c \in \mathbb{Z}$ taková čísla, že $ab = ac$, pak $a(b-c) = ab - ac = 0$. Tedy buďto $a = 0$ a nebo $b = c$. To je vlastnost krácení nenulovým číslem.

Množina $\mathbb{Z}$ tvoří okruh vzhledem k operacím sčítání a násobení. Je to komutativní okruh s jednotkovým prvkem. Vzhledem ke krácení jde o obor integrity (kratčeji obor). Množiny $\mathbb{N}$ a $\mathbb{N}_0$ jsou polookruhy (poloobory).

I.3 Uspořádání celých čísel

I.3.1 Na množině $\mathbb{Z}$ máme definováno uspořádání $\leq$ dané předpisem $a \leq b$ právě když $b-a \in \mathbb{N}_0$ (nebo $a-b \in \mathbb{N}_0^-$). To jest, $b = a+c$ pro nějaké $c \in \mathbb{N}_0$. Je to relace reflexivní, tranzitivní a antisymetrická. Navíc platí následující implikace a ekvivalence:

(1) $a \leq b \Rightarrow a + c \leq b + c$;
(2) $a \leq 0 \Leftrightarrow a \in \mathbb{N}_0^-$;
(3) $0 \leq a \Leftrightarrow a \in \mathbb{N}_0$;
(4) $a \leq b \Leftrightarrow -b \leq -a$;
(5) $a \leq b$, $0 \leq c \Rightarrow ac \leq bc$;
(6) $a \leq b$, $c \leq 0 \Rightarrow bc \leq ac$;
(7) $ac \leq bc$, $0 \leq c \Rightarrow a \leq b$.

Uspořádaná množina $(\mathbb{Z}, \leq)$ nemá ani největší ani nejmenší prvek (číslo). Nicméně platí následující velmi důležitá vlastnost: Každá zdola (popř., shora) omezená neprázdná množina celých čísel má nejmenší (popř. největší) prvek. Tedy, je-li $Z \subseteq \mathbb{Z}, Z \neq \emptyset$ a existuje-li $a \in \mathbb{Z}$ takové číslo, že $a \leq b$ (popř., $b \leq a$) pro všechna $b \in Z$, pak existuje $a_0 \in Z$ takové číslo, že $a_0 \leq b$ ($b \leq a_0$).

Ostré uspořádání příslušné k uspořádání $\leq$ označíme symbolem $<$. Tedy $a < b$ právě když $a \leq b$ a $a \neq b$ (neboli $b-a \in \mathbb{N}$). Relace $<$ je antireflexivní, antisymetrická a tranzitivní.

Uspořádání $\leq$ je úplné (či lineární). To jest, pro všechna $a, b \in \mathbb{Z}$ platí právě jedna z následujících tří možností: $a < b$, $a = b$, $b < a$.

Je-li $a \in \mathbb{Z}$, pak $a < a + 1$ a pro všechna $b \in \mathbb{Z}$, $b \neq a, a + 1$, je buďto $b < a$ či $a + 1 < b$. Číslo $a + 1$ je bezprostřední následník čísla a. Podobně, číslo $a - 1$ je bezprostřední předchůdce čísla a.

Čísla z $\mathbb{N}$ se nazývají kladná. Nejmenší kladné číslo je 1. Čísla z $\mathbb{N}_0$ jsou nezáporná a nejmenší takové číslo je 0. Čísla z $\mathbb{N}^-$ jsou záporná a největší z nich je -1. Čísla z $\mathbb{N}_0^-$ jsou nekladná a největší z nich je opět číslo 0.

Nechť $a \geq 3$, $b \geq 2$, $a \geq b$. Je-li $b = 2$, pak $ab = 2a > a + 2 = a + b$. Je-li $b \geq 3$, pak $ab = 2a + (b-2)a \geq 2a + a = 3a > a + a \geq a + b$. Takže $ab > a + b$. Z učiněné úvahy plyne, že $ab > a + b$, kdykoliv $a, b \in \mathbb{N}$, $a \geq 2$, $b \geq 2$, $a + b \geq 5$. Samozřejmě, $2 \cdot 2 = 4 = 2 + 2$ a $a \cdot 1 = a < a + 1$.

Platí implikace:

(8) $a < b \Rightarrow a + c < b + c$;
(9) $a < b$, $0 < c \Rightarrow ac < bc$;
(10) $a < b$, $c < 0 \Rightarrow bc < ac$;
(11) $a \neq 0 \Rightarrow 0 < a^2$;
(12) $1 < a \Rightarrow a < a^2$.
(13) $a \neq 0, \pm 1 \Rightarrow a < a^2$.

I.3.2 Příklad. (i) Je $n + 1 < 2(n + 1)$ pro každé $n \geq 0$. Pro $n = -1$ je $n + 1 = 0 = 2 \cdot 0 = 2(n + 1)$. Pro $n \leq -2$ je $2(n + 1) < n + 1$.

(ii) Je $2n + 1 < 2(n + 1)$ pro každé $n \in \mathbb{Z}$.

(iii) Je $2(n + 3) < 3n + 1$ pro všechna $n \geq 6$. Pro $n = 5$ je $2(n + 3) = 16 = 3n + 1$. Pro $n \leq 4$ je $3n + 1 < 2(n + 3)$.

(iv) Je $2 \cdot 1052 = 2104 < 2105$.

I.3.3 Příklad. Je $2(n + m) < nm + 1$ pro všechna $n \geq 4$, $m \geq 4$.

Vskutku. Předpokládejme $m \leq n$ a postupujme indukcí podle m. Je-li $m = 4$, pak $2(n + m) = 2n + 8 < 2n + 9 \leq 2n + 2n + 1 = 4n + 1 = nm + 1$. Je-li $m \geq 4$, pak $2(n+m+1) = 2(n+m)+2 < 2(n+m)+4 < nm+1+n = n(m + 1) + 1$ (využit indukční předpoklad).

Je $2(n + 3) < 3n + 1$ právě když $n \geq 6$. Je $2(n + 2) > 2n + 1$ pro každé $n \in \mathbb{Z}$. Je $2(n+1) < n+1$ právě když $n \leq -2$. Je $2n < 1$ právě když $n \leq 0$.

I.3.4 Příklad. (i) Nechť $0 \leq m \leq n$. Potom $2(n + m) < nm$ právě když buďto $3 \leq m$, $7 \leq n$ anebo $4 \leq m$, $5 \leq n$.

Vskutku. Je-li $5 \leq m$, pak $2(n+m) = 2(n+(m-1))+2 < n(m-1)+3 = nm+3-n \leq nm-2 < nm$ dle I.3.3. Je-li $m = 4$, pak $2(n+m) = 2n+8 < 4n$ právě když $5 \leq n$. Je-li $m = 3$, pak $2(n + m) = 2n + 6 < 3n$ právě když $7 \leq n$. Je-li $m = 2$, pak $2(n + m) = 2n + 4 > 2n$. Je-li $m = 1$, pak $2(n + m) = 2n + 2 \geq n$. Je-li $m = 0$, pak $2(n + m) = 2n \geq n$ ($> n$ pro $n \geq 1$).

(ii) Nechť $0 \leq m \leq n$. Potom $2(n+m) = nm$ právě když buďto $n = 0 = m$ nebo $n = 4 = m$ anebo $n = 6$, $m = 3$.

Vskutku. Je-li $n = m$, pak $2(n + m) = 4n$, $nm = n^2$ a $4n = n^2$ právě pro $n = 0, 4$. Nechť tedy $n > m$ a $2(n + m) = nm$. Z (i) plyne, že $m \leq 3$. Je-li $m = 3$, pak $2(n + m) = 2n + 6$, $nm = 3n$, a tak $n = 6$. Je-li $m = 2$, pak $2(n+m) = 2n+4$, $nm = 2n$ a to nejde. Je-li $m = 1$, pak $2(n+m) = 2m+2$, $nm = n$, nelze. Nakonec, je-li $m = 0$, pak $2(n + m) = 2n$, $nm = 0$, opět nelze.

(iii) Nechť $0 \leq m \leq n$. Potom $2(n + m) \leq nm$ právě když buďto $n = 0 = m$ nebo $m \geq 4$ anebo $n \geq 6$, $m \geq 3$.

Toto tvrzení plyne snadnou kombinací (i) a (ii).

(iv) Je $2(n+3) > 3n$ pro $n \leq 5$. Je $2(n+2) > 2n$ pro všechna n. Je $2(n+1) > 2n$ pro všechna n. Je $2(n+0) > 0 (= 0 \cdot n)$ pro všechna $n \geq 1$.

I.3.5 Absolutní hodnota. Pro $a \in \mathbb{N}_0$ buď $|a| = a$. Pro $a \in \mathbb{N}^-$ buď $|a| = -a$. Tedy $|a| \in \mathbb{N}_0$ a toto číslo se nazývá absolutní hodnota čísla a. Platí rovnost $|ab| = |a| \cdot |b|$ pro všechna $a, b \in \mathbb{Z}$. Dále, $|a| = |-a|$.

I.3.6 Věta. (Trojúhelníková nerovnost) Je $|a+b| \leq |a|+|b|$ pro všechna $a, b \in \mathbb{Z}$.

Důkaz. Předpokládejme, že $a \leq b$. Je-li $0 \leq a$, pak $0 \leq b$, $0 \leq a+b$, $|a+b| = a+b = |a|+|b|$. Je-li $b \leq 0$, pak $a \leq 0, a+b \leq 0$, $|a+b| = -(a+b) = (-a)+(-b) = |a|+|b|$. Buď tedy $a < 0 < b$. Pak $|a|+|b| = b-a$. Dále, $a < -a, b+a < b-a$. Je-li tedy $a+b \geq 0$, pak $|a+b| = a+b < -a+b = |a|+|b|$. Je-li však $a+b < 0$, pak $|a+b| = -(a+b) = -a-b$. Ovšem, $-b < b, -a-b < -a+b$. Tudíž $|a+b| = -a-b < -a+b = |a|+|b|$ i v tomto případě. □

I.3.7 Poznámka. V důkazu předchozí věty jsme zjistili, že $|a+b| = |a|+|b|$ právě když obě čísla a, b jsou buďto současně nezáporná anebo současně nekladná. Tedy pro $a < 0 < b$ je $|a+b| < |a|+|b|$.

I.3.8 Příklad. Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $a/b = a+b$ (I.2.2). Je tedy $a = cb$, $b \neq 0$, $c = a/b = a+b = cb+b = b(c+1)$. Rozebereme si následující případy:

(a) Je-li $a = 0$, pak $0 = c = a+b = b$, spor.

(b) Je-li $b = 1$, pak $a = c = a+b = a+1$, $0 = 1$, opět spor.

(c) Je-li $c = -1$, pak $-1 = c = b(c+1) = 0$, spor.

(d) Z (a), (b) a (c) plyne $a \neq 0$, $b \neq 1$, $c \neq -1$.

(e) Nechť $a > 0$, $b > 0$. Pak je $0 < c < c+1 \leq b(c+1)$, spor.

(f) Nechť $a < 0$, $b < 0$. Pak je $b(c+1) < 0 < c < c+1$, spor.

(g) Nechť $a < 0 < b$. Je $2 < b$, $c < 0$, $c = b(c+1) \leq 2(c+1) = 2c+2$, $0 < -c \leq 2$, $c = -1, -2$. Je-li $c = -1$, pak $-1 = b \cdot 0 = 0$, spor. Je-li $c = -2$, pak $-2 = c = b(c+1) = -b$, $b = 2$, $a = -4$.

(h) Nechť $b < 0 < a$. Je $0 < c < c+1 < 0$ (neb $c \leq -2$), $0 < b(c+1) = c$, spor.

Zjistili jsme, že rovnosti $a/b = a+b$ vyhovují pouze čísla $a = -4$, $b = 2$.

I.4 Mocniny celých čísel

I.4.1 Definice. Nezáporné mocniny celých čísel definujeme takto: $n^0 = 1$ a $n^{k+1} = n^k \cdot n$ pro všechna $n \in \mathbb{Z}$ a $k \geq 0$. Je tedy $n^1 = n, n^2 = n \cdot n, n^3 = n \cdot n \cdot n, \ldots$.

I.4.2 Lemma. Lemma $n^k \cdot n^l = n^{k+l}$ pro všechna $n \in \mathbb{Z}$ a $k, l \in \mathbb{N}_0$.

Důkaz. Postupuje se indukcí podle k. Je-li $k = 0$, tak $n^k \cdot n^l = 1 \cdot n^l = n^{0+l} = n^{k+l}$. Je-li $k \geq 1$, tak $n^k \cdot n^l = n \cdot n^{k-1} \cdot n^l = n \cdot n^{k+l-1} = n^{k+l}$ podle indukčního předpokladu a definice mocniny. □

I.4.3 Lemma. $n^k \cdot m^k = (nm)^k$ pro všechna $n, m \in \mathbb{Z}$ a $k \in \mathbb{N}_0$.

Důkaz. Opět postupujeme indukcí podle k. Tvrzení je zřejmé pro $k = 0$. Je-li $k \geq 1$, tak $n^k \cdot m^k = n^{k-1}m^{k-1} \cdot nm = (nm)^{k-1} \cdot nm = (nm)^k$. □

I.4.4 Lemma. $(n^k)^l = n^{kl}$ pro všechna $n \in \mathbb{Z}$ a $k, l \in \mathbb{N}_0$.

Důkaz. Indukcí podle l. Zřejmé pro $l = 0$. Je-li $l \geq 1$, tak $(n^k)^l = (n^k)^{l-1} \cdot n^k = n^{k(l-1)} \cdot n^k = n^{k(l-1)+k} = n^{kl}$ (použije se I.4.2). □

I.4.5 Lemma. Nechť $n \geq 2$, pak $n^0(= 1) < n^1(= n) < n^2 < n^3 < n^4 < \ldots$.

Důkaz. Plyne snadno z I.3.1(9). □

I.4.6 Lemma. Nechť $n \leq -2$, pak $\cdots < n^5 < n^3 < n^1(= n) < n^0(= 1) < n^2 < n^4 < n^6 < \ldots$.

Důkaz. Plyne snadno z I.3.1(9) a (10). □

I.4.7 Poznámka. Je $0^0 = 1$, $0^k = 0$ pro všechna $k \geq 1$. Je $1^l = 1$ pro všechna $l \geq 0$. Je $(-1)^u = 1$ a $(-1)^v = -1$ pro každé sudé $u \geq 0$ a každé liché $v \geq 1$.

I.4.8 Lemma. Nechť $0 \leq n < m$. Potom $n^k < m^k$ pro všechna $k \geq 1$.

Důkaz. Indukcí podle k. Je-li $k = 1$, pak $n^k < m^k$ triviálně. Je-li $k \geq 2$, tak $n^{k-1} < m^{k-1}$ podle indukčního předpokladu. Tedy $n^k = n \cdot n^{k-1} < n \cdot m^{k-1} < m \cdot m^{k-1} = m^k$ podle I.3.1(9). □

I.4.9 Poznámka. Je $(n^k)^l = (n^l)^k$ pro všechna $n \in \mathbb{Z}$ a $k, l \in \mathbb{N}_0$. Podobně $(n^k)^l = (-n^l)^k$, jestliže alespoň jedno z čísel k, l je sudé. Obecně, jsou-li $k, l, b, c \in \mathbb{N}_0$ taková čísla, že $kl = bc$, pak $(n^k)^l = (n^b)^c$. Navíc, je-li alespoň jedno z čísel k, l, b, c sudé, pak $(n^k)^l = (-n^b)^c$.

Samozřejmě $0^k = 0^l$ pro všechna $k, l \in \mathbb{N}$. Dále, $n^0 = 1^k = (-1)^l$ pro všechna $n \in \mathbb{Z}$, $k, l \in \mathbb{N}_0$, l sudé. Podobně $(-1)^l = (-1)^k$ pro všechna lichá $k, l \in \mathbb{N}$.

Rovnost $n^k = m^l$ si podrobně rozebereme později.

I.4.10 Na množině (polookruhu) $\mathbb{N}$ můžeme definovat binární operaci $*$ předpisem $a * b = a^b$ (označení $*$ se zavádí z technických důvodů a pouze pro účely tohoto odstavce). Všimněme si následujících rovností:

$a * 0 = 1$, $a * 1 = a$, $1 * b = 1$, $(a * b) * c = a * (bc) = (a * c) * b$ (tato rovnost říká, že $*$ je zprava permutabilní), $(a * b)(a * c) = a * (b + c)$, $(a * c)(b * c) = (ab) * c$. Navíc $0 * b = 0$ pro $b \geq 1$.

Je $2 * (1 * 2) = 2 < 4 = (2 * 1) * 2$ a $2 * 1 = 2 > 1 = 1 * 2$. Operace $*$ není ani asociativní, ani komutativní.

Případné inversní operace k operaci $*$ budou jen částečné a zde se jimi nebudeme zabývat (jde o odmocniny).

Na celé množině (okruhu) $\mathbb{Z}$ je už operace $*$ částečná a inversní operace jsou částečné a někdy i dvojznačné. Opět se touto problematikou nebudeme zabývat.

Pro $a, b \in \mathbb{N}_0$ je $a * b = b * a$ právě když buďto $a = b$ nebo $(a, b) = (2, 4), (4, 2)$.

I.4.11 Pozorování. Nechť $a \geq 2$, $b \geq 2$, $a + b \geq 5$. Indukcí podle b zjistíme, že $a^b > ab$.

Vskutku. Je-li $b = 2$, pak $a \geq 3$, $a^b = a^2 \geq 3a > 2a = ab$. Dále pro $a \geq 2$, $b \geq 2$ máme $ab \geq 2b > b + 1$, $a^2 b > a(b + 1)$. Je-li nyní $a^b > ab$, pak $a^{b+1} > a^2 b > a(b + 1)$, čímž je dokončen indukční krok.

Samozřejmě $2^2 = 4 = 2 \cdot 2$, $a^1 = a = a \cdot 1$, $a^0 = 1 > 0 = a \cdot 0$. Takže $a^b \geq ab$ pro všechna $a \geq 2$, $b \geq 0$, přičemž rovnost nastává pouze pro $a = 2 = b$ a nebo $a \geq 2$, $b = 1$.

Je-li $a = 1$, $b \geq 2$, pak $a^b = 1^b = 1$, $ab = 1 \cdot b = b$. Tedy v tomto případě je $a^b > ab$ pro $b = 0$ a $a^b \geq ab$ pouze pro $b = 0, 1$.

Je-li $a = 0$, pak $a^b = 0 = ab$ pro $b \geq 1$. Nakonec, $0^0 = 1 \geq 0 \cdot 0$.

Zjistili jsme, že $a^b > ab$ (popřípadě $a^b \geq ab$) pro všechna $a, b \in \mathbb{N}_0$ s výjimkou dvojic $(2, 2)$, $(a, 1)$, $a \geq 2$, $(1, b)$, $b \geq 1$ (popř., $(1, b), b \geq 2$). Speciálně, $a^b = ab$ pro $a, b \in \mathbb{N}_0$ právě když $a = 2 = b$ nebo $b = 1$ a nebo $a = 0$, $b \geq 1$.

I.4.12 Pozorování. Předchozí pozorování a I.3.1 nás poučují o tom, že $a^b > a+b$ pro všechna $a \geq 2$, $b \geq 2$, $a+b \geq 5$. Samozřejmě, $2^2 = 4 = 2+2$ $(= 2 \cdot 2)$, $1^0 = 1 = 1+0$ a $1^b = 1 < 1+b$ pro $b \geq 1$. Dále, $a^1 = a < a+1$ pro $a \geq 0$, $0^0 = 1 > 0+0$, $1^0 = 1 = 1+0$, $a^0 = 1 < a+0$ pro $a \geq 2$.

Zjistili jsme, že $a^b > a+b$ (popř., $a^b \geq a+b$) pro všechna $a, b \in \mathbb{N}_0$ s výjimkou dvojic $(a,b) = (2,2), (2,1), (2,0), (1,0), (1,b), (0,b)$, $b \geq 1$ (popř., $(a,b) = (2,1), (2,0), (1,b), (0,b)$, $b \geq 1$). Specielně, $a^b = a+b$ pro $a, b \in \mathbb{N}_0$ právě tehdy když buďto $a = 2 = b$ a nebo $a = 1$, $b = 0$.

Celkově, $a^b = ab = a+b$ pouze pro $a = 2 = b$.

I.4.13 Malá Mocnilka.

$\mathbf{n^m}$

n \ m	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	1	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	16	32	64	128	256	512
3	1	3	9	27	81	243	729	2187	6561	19683
4	1	4	16	64	256	1024	4096	16384	65536	262144
5	1	5	25	125	625	3125	15625	78125	390625	1953125
6	1	6	36	216	1296	7776	46656	279936	1679616	10077696
7	1	7	49	343	2401	16807	117649	823543	5764801	40353607
8	1	8	64	512	4096	32768	262144	2097152	16777216	134217728
9	1	9	81	729	6561	59049	531441	4782969	43046721	387420489

Malá Mocnilka nemá žádný důležitý význam a není nezbytné ji umět nazpaměť. Nicméně si všimněme, že $9 = 4 \cdot 2 + 1$ a $9^9 = 4 \cdot 96854947 + 1 = 4^9 \cdot 1478 + 60957 = 4^9 \cdot 1478 + 9 \cdot 6773 = 4^9 \cdot 2 \cdot 739 + 9 \cdot 13 \cdot 521$.

Malou Odmocnilku sestavovat nebudeme.

I.4.14 Cvičení. (i) Nechť $n, m \in \mathbb{Z}$, $k, l \in \mathbb{N}$, n dělí m a k dělí l. Ověříme, že n^k dělí m^l.

Vskutku. Je $m = na$, $l = kb$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Nyní, $m^l = (na)^l = n^l \cdot a^l = n^{kb} \cdot a^l = n^k \cdot (n^{k(b-1)}a^l$.

(ii) Je $10^{10} = 2^{10} \cdot 5^{10}$ a $4^4 = 2^8$. Takže 4^4 dělí 10^{10}, přičemž 4 nedělí 10. Dále, 4^4 dělí 10^8, 4 dělí 8, 2^2 dělí 4^3, 2 nedělí 3. Je $21^{21} = 3^{21} \cdot 7^{21}$, $9^9 = 3^{18}$, 9^9 dělí 21^{21}, 9 nedělí 21.

I.4.15 Příklad. (i) Je $169 = 13^2$, $961 = 31^2$, $169 \cdot 961 = 403^2 = 162409$.

(ii) Je $1089 = 33^2$, $9801 = 99^2$, $9081 = 9 \cdot 1089$, $1089 \cdot 9801 = 3267^2 = 10673289$.

(iii) Je $2^5 \cdot 9^2 = 2592 = 50^2 + 10^2 - 2^3 = 51^2 - 3^2$.

(iv) Je $7^3 - 6^3 - 5^3 = 343 - 216 - 125 = 343 - 341 = 2$.

(v) Je $6^3 - 5^3 - 4^3 = 27 = 3^3$, $5^3 - 4^3 - 3^3 = 34$, $4^3 - 3^3 - 2^3 = 29$, $3^3 - 2^3 - 1^3 = 18$, $2^3 - 1^3 - 0^3 = 7$, $1^3 - 0^3 - (-1)^3 = 2$, $0^3 - (-1)^3 - (-2)^3 = 9 = 3^2$, $(-1)^3 - (-2)^3 - (-3)^3 = 34$.

(vi) Je $3 \cdot 5 + 1 = 2^4$, $1 \cdot 5 + 3 = 2^3 = 1 \cdot 3 + 5$, $2 \cdot 4 + 1 = 3^2$.

(vii) Je $1^n + 2^3 = 3^2$ pro každé $n \geq 0$. Je $2^5 + 7^2 = 3^4$. Je $2^2 + 11^2 = 5^3$. Je $2 \cdot 11^2 + 1 = 3^5$.

I.4.16 Co se týká záporných mocnin, pak v oboru celých čísel si můžeme dopřát pouze následující: Pro každé $n \geq 1$ je $1^{-n} = 1$, dále $(-1)^{-n} = 1$ pro n sudé a $(-1)^{-n} = -1$ pro n liché. To je vše.

I.4.17 Cvičení. Pro účely tohoto cvičení položme $t(a, b) = 2a + (a + b)(a + b + 1)$ pro všechna $a, b \in \mathbb{Z}$.

(i) Je $t(a, b) = a^2 + b^2 + 2ab + 3a + b = (a + b)^2 + 3a + b \geq 3a + b$, přičemž číslo $t(a, b)$ je vždy sudé.

(ii) Je $t(a, 0) = a^2 + 3a$, $t(0, b) = b^2 + b$.

(iii) Předpokládejme, že $t(a, b) = t(c, d)$, přičemž $c + d \geq a + b$. Je také $l = (c + d) - (a + b) \geq 0$. Dále, $(a + b)^2 + 3a + b = t(a, b) = t(c, d) = (c+d)^2+3c+d = (a+b)^2+2(a+b)l+l^2+3c+d$, čili $3a+b = 2(a+b)l+l^2+3c+d$. Odtud $(2l - 3)a + (2l - 1)b + l^2 + 3c + d = 0$. Jelikož $c + d = l + a + b$, tak $2(l - 1)a + 2lb + 2c + l^2 + l = 0$.

Je $l \geq 0$ a my tak dostáváme nerovnost $0 \geq (l - 1)a + lb + c$, přičemž rovnost platí pouze pro $l = 0$.

Je-li $l = 0$, pak $a = c$, $b = d$.

Je-li $l = 1$, pak $0 > b + c$ a aspoň jedno z čísel b, c je záporné.

Je-li $l \geq 2$, pak aspoň jedno z čísel a, b, c je záporné.

(iv) Nechť $t(a, b) = t(c, d)$. Pak buďto $a = c$, $b = d$ anebo aspoň jedno z čísel a, b, c, d je záporné. Toto plyne z (iii) a symetrického případu $a + b \geq c + d$.

(v) Je $t(1, 1) = 8 = t(1, -4)$. Je $t(1, 1) = 8 = t(-6, 1)$. Je $t(-3, 0) = 0 = t(0, 0) = t(0, -1)$.

I.4.18 Poučení. V předchozím cvičení jsme zjistili, že zobrazení $t : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ definované předpisem $t(a, b) = 2a + (a + b)(a + b + 1)$ je prosté (čili injektivní). Stejnou vlastnost má i zobrazení s, kde $s(a, b) = t(a, b)/2$.

(i)Je $s(0, 0) = 0, s(0, 1) = 1, s(0, 2) = 3, s(0, 3) = 6, s(0, 4) = 10, s(0, 5) = 15, s(0, 6) = 21, s(0, 7) = 28, s(0, 8) = 36, s(0, 9) = 45, s(0, 10) = 55$.

Je $s(1, 0) = 2, s(2, 0) = 5, s(3, 0) = 9, s(4, 0) = 14, s(5, 0) = 20, s(6, 0) = 27, s(7, 0) = 35, s(8, 0) = 44, s(9, 0) = 54, s(10, 0) = 65$.

Je $s(1, 1) = 4, s(2, 2) = 12, \ldots, s(1, 2) = 7, s(2, 1) = 8$.

(ii) Je-li $a+b = v$, pak $t(a, b) = 2a+v^2+v$. Pro $a \geq 0, b > 0$ je $v \geq a \geq 0$. Nyní $v^2 + v < v^2 + v + 2 < \cdots < v^2 + 3v$ jsou právě všechna sudá čísla mezi

$v^2 + v$ a $v^2 + 3v$ (včetně). Číslo $(v+1)^2 + (v+1) = v^2 + 3v + 2$ je nejbližší další sudé číslo. Snadno uhodneme, že funkce t nabývá všech nezáporných sudých hodnot. Tedy funkce s nabývá všech nezáporných hodnot.

(iii) $s : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ je bijekce.

I.5 Mocniny prvočísel 2, 3, 5, 7, 11

I.5.1 Tabulka. Uveďme si trochu mocnin prvočísla 2. $2^0 = 1$. Dále následují:

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
n	11	12	13	14	15	16	17	18	19	20
2^n	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576

n	21	22	23	24	25
2^n	2097152	4194304	8388608	16777216	33554432
n	26	27	28	29	30
2^n	67108864	134217728	268435456	536870912	1073741824
n	31	32	33	34	35
2^n	2147483648	4294967296	8589934592	17179869184	34359738368
n	36	37	38	39	40
2^n	68719476736	137438953472	274877906944	549755813888	1099511627776

n	41	42	43	44
2^n	2199023255552	4398046511104	8796093022208	17592186044416
n	45	46	47	48
2^n	35184372088832	70368744177664	140737488355328	281474976710656
n	49	50	51	52
2^n	562949953421312	1125899906842624	2251799813685248	4503599627370496

n	53	54	55
2^n	9007199254740992	18014398509481984	36028797018963968
n	56	57	58
2^n	72057594037927936	144115188075855872	288230376151711744
n	59	60	61
2^n	576460752303423488	1152921504606846976	2305843009213693952
n	62	63	64
2^n	4611686018427387904	9223372036854775808	18446744073709551616
n	65	66	67
2^n	36893488147419103232	73786976294838206464	147573952589676412928
n	68	69	70
2^n	295147905179352825856	590295810358705651712	1180591620717411303424

n	71	72
2^n	2361183241434822606848	4722366482869645213696
n	73	74
2^n	9444732965739290427392	18889465931478580854784
2	75	76
2^n	37778931862957161709568	75557863725914323419136
n	77	78
2^n	151115727451828646838272	302231454903657293676544
n	79	80
2^n	604462909807314587353088	1208925819614629174706176
n	81	82
2^n	2417851639229258349412352	4835703278458516698824704
n	83	84
2^n	9671406556917033397649408	19342813113834066795298816
n	85	86
2^n	38685626227668133590597632	77371252455336267181195264
n	87	88
2^n	154742504910672534362390528	309485009821345068724781056
n	89	90
2^n	618970019642690137449562112	1237940039285380274899124224

A teď si všímejme různých zajímavostí:

Je $2^9 = 512$ a $5 + 1 + 2 = 8 = 2^3$, $3 \mid 9$. Ciferný součet mocniny 2^{36} je $64 = 2^6$, $6 \mid 36$. Ciferný součet mocniny 2^{85} je $128 = 2^7$, $7 \nmid 85$.

První mocninou, která obsahuje číslici 0 ve svém desítkovém zápise je $2^{10} = 1024$.

Mocnina $2^{86} = 77371252455336267181195264$ nemá číslici 0 ve svém zápise, i když všechny ostatní číslice $1, 2, 3, 4, 5, 6, 7, 8, 9$ jsou zastoupeny. Je domněnka, že jde o největší mocninu čísla 2, která nemá číslici 0 ve svém zápise v desítkové soustavě. Další mocniny, které nemají ve svém zápise číslici 0 jsou 2^l pro $l = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 13, 14, 15, 16, 18, 19, 24, 25, 27, 28, 31, 32, 33, 34, 35, 36, 37, 39, 49, 51, 67, 72, 76, 77, 81$. Společně s číslem 86 je to dohromady 36 exponentů.

První dvě mocniny, které obsahují číslici 1 jsou $2^0 = 1$ a $2^4 = 15$. Např. mocnina 2^{66} číslici 1 neobsahuje a mocnina 2^{73} také ne.

První dvě mocniny, které obsahují číslici 2 jsou 2^1 a $2^5 = 32$. Mocniny 2^{64}, 2^{74}, 2^{83} neobsahují číslici 2.

Mocnina $2^{68} = 295147905179352825856$ je první mocninou čísla 2, která obsahuje ve svém desítkovém zápise všechny číslice $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ (aspoň jednou). Všimněme si, že $68 = 2 \cdot 34$ a $86 = 2 \cdot 43$.

Mocnina $2^{51} = 2251799813685248$ je první, která obsahuje ve svém zápise všechny číslice $1, 2, 3, 4, 5, 6, 7, 8, 9$.

Je $2^{25} + 1 = 33554433 = 3 \cdot 111848111 = 3 \cdot 11 \cdot 251 \cdot 4051$ (prvočíselný rozklad).

První mocnina, v jejímž zápise je číslice 7 je $2^{15} = 32768$, ostatní číslice se vyskytují dříve.

Číslo $2^{64} - 1 = 18446744073709551615 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 6700417$ je tzv. šachové číslo.

Je $16^2 = 2^{24} = 16777216 = 8^8$, $2^{41} = 2199023255552$.

Je $8200 = 8 + 8192 = 2^3 + 2^{13}$. Takže $10 \cdot 820 + i = 820i = 2^{13} + 0 + i$ pro $0 \leq i \leq 9$ (zde $820i$ není součin, ale zápis v desítkové soustavě).

Je $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^7 = 128, 2^{10} = 1024, 2^{11} = 2048$ (a $2^{-\infty} = 0$).

I.5.2 Tabulka. A teď něco málo mocnin prvočísla 3.

n	0	1	2	3	4	5	6	7
3^n	1	3	9	27	81	243	729	2187
n	8	9	10	11	12	13	14	15
3^n	6561	19683	59049	177147	531441	1594323	4782969	14348907

n	16	17	18
3^n	43046721	129140163	387420489
n	19	20	21
3^n	1162261467	3486784401	10460353203
n	22	23	24
3^n	31381059609	94143178827	282429536481
n	25	26	27
3^n	847288609443	2541865828329	7625597484987
n	28	29	30
3^n	22876792454961	68630377364883	205891132094649
n	31	32	33
3^n	617673396283947	1853020188851841	5559060566555523
n	34	35	36
3^n	16677181699666569	50031545098999707	150094635296999121
n	37	38	39
3^n	450283905890997363	1350851717672992089	4052555153018976267

Povšimněme si, že v zápise mocniny 3^{34} chybí číslice 0 a v zápise mocniny 3^{43} chybí číslice 1 ($3^{43} = 328256967394537067627$).

Je $3^{16} = 43046721$ a $4+3+0+4+6+7+2+1 = 27 = 3^3$. Mezi námi uvedenými mocninami prvočísla 3 nalézáme 18 takových, že ciferný součet jejich dekadického zápisu je opět mocninou čísla 3. Jedná se o mocniny pro exponent $l = 0, 1, 2, 3, 4, 5, 9, 10, 11, 13, 16, 17, 21, 27, 31, 35, 36$ a 39.

Pro úplnost v následující tabulce uvádíme ciferné součty pro 3^l pro exponent $l = 0, \ldots, 99$:

exponent	0	1	2	3	4	5	6	7	8	9
ciferný součet	1	3	9	9	9	9	18	18	18	27
exponent	10	11	12	13	14	15	16	17	18	19
ciferný součet	27	27	18	27	45	36	27	27	45	36
exponent	20	21	22	23	24	25	26	27	28	29
ciferný součet	45	27	45	54	54	63	63	81	72	72
exponent	30	31	32	33	34	35	36	37	38	39
ciferný součet	63	81	63	72	99	81	81	90	90	81
exponent	40	41	42	43	44	45	46	47	48	49
ciferný součet	90	99	90	108	90	99	108	126	117	108
exponent	50	51	52	53	54	55	56	57	58	59
ciferný součet	144	117	117	135	108	90	90	108	126	117
exponent	60	61	62	63	64	65	66	67	68	69
ciferný součet	99	135	153	153	144	135	117	162	153	153
exponent	70	71	72	73	74	75	76	77	78	79
ciferný součet	144	180	162	153	171	180	153	162	153	189
exponent	80	81	82	83	84	85	86	87	88	89
ciferný součet	153	189	198	198	162	162	171	189	198	189
exponent	90	91	92	93	94	95	96	97	98	99
ciferný součet	216	171	171	198	198	180	198	216	225	207

Je $3^0+3^1 = 4$, $3^0+3^1+3^2 = 13$, $3^0+3^1+3^2+3^3 = 40$, $3^0+3^1+3^2+3^3+3^4 = 121 = 11^2$.

I.5.3 Tabulka. Přejděme k mocninám prvočísla 5.

n	0	1	2	3	4
5^n	1	5	25	125	625
n	5	6	7	8	9
5^n	3125	15625	78125	390625	1953125
n	10	11	12	13	14
5^n	9765625	48828125	244140625	1220703125	6103515625
n	15	16	17	18	19
5^n	30517578125	152587890625	762939453125	3814697265625	19073486328125

n	20	21	22
5^n	95367431640625	476837158203125	2384185791015625
n	23	24	25
	11920928955078125	59604644775390625	298023223876953125
n	26	27	28
5^n	1490116119384765625	7450580596923828125	37252902984619140625

Je $5^8 = 390625$ a $3 + 9 + 0 + 6 + 2 + 5 = 25 = 5^2$.
Je $5^9 = 1953125$ a $1 + 9 + 5 + 3 + 1 + 2 + 5 = 26 = 5^2 + 1$.
Je $5^{30} = 931322574615478515625$, v zápise tohoto čísla nenacházíme 0.

I.5.4 Tabulka. A nyní mocniny prvočísla 7.

n	0	1	2	3
7^n	1	7	49	343
n	4	5	6	7
7^n	2401	16807	117649	823543
n	8	9	10	11
7^n	5764801	40353607	282475249	1977326743
n	12	13	14	15
7^n	13841287201	96889010407	678223072849	4747561509943
n	16	17	18	19
5^n	33232930569601	232630513987207	1628413597910449	11398895185373143

Je $7^4 = 2401$ a $2 + 4 + 0 + 1 = 7$.
Je $7^0 + 7^1 + 7^2 + 7^3 = 20^2$.
Je $7^7 = 823543$ a $8 + 2 + 3 + 5 + 4 + 3 = 25 = 5^2$.
Je $7^{11} = 1977326743$ a $1 + 9 + 7 + 7 + 3 + 2 + 6 + 7 + 4 + 3 = 49 = 7^2$.

I.5.5 Tabulka. A na závěr něco mocnin prvočísla 11.

n	0	1	2	3
11^n	1	11	121	1331
n	4	5	6	7
11^n	14641	161051	1771561	19487171
n	8	9	10	11
11^n	214358881	2357947691	25937424601	285311670611
n	12	13	14	15
11^n	3138428376721	34522712143931	379749833583241	4177248169415651

Je $11^4 = 14641$ a $1 + 4 + 6 + 4 + 1 = 16 = 2^4$.

I.5.6 Věta. Nechť n je takové kladné číslo, že $n \neq 2^l$ pro každé $l \geq 0$. Potom existuje právě jedno $k \geq 1$ tak, že $n < 2^k < 2n$.

Důkaz. Existenci čísla k dokážeme indukcí podle n. Je-li $n = 3$, pak $k = 2$. Buď tedy $n > 3$. Je-li $n-1 = 2^l$ pro nějaké $l \geq 0$, pak $n < 2n-2 = 2^{l+1} < 2n$. Je-li $n-1 \neq 2^l$ pro každé $l \geq 0$, pak existuje $k \geq 1$ tak, že $n-1 < 2^k < 2n-2$ a to podle indukčního předpokladu. Nyní je $n < 2^k < 2n$. Tím je dokázaná existence čísla k.

Jednoznačnost je zřejmá. Je-li totiž $n < 2^k < 2n$, pak $2n < 2 \cdot 2^k = 2^{k+1}$. □

I.5.7 Poznámka. Z I.5.6 ihned plyne, že pro každé $n \geq 1$ existuje $k \geq 1$ tak, že $n \leq 2^k \leq 2n$. Je-li $n = 2^l$, pak $2^l = 2^l < 2^{l+1} = 2 \cdot 2^l$ a číslo $k(= l, l+1)$ není v tomto případě určeno jednoznačně.

I.6 Druhé mocniny

I.6.1 Tabulka. Vyrobme si tabulku druhých mocnin $n^2, 0 \leq n \leq 100$. Je $(n+1)^2 - n^2 = 2n+1$ pro každé $n \in \mathbb{Z}$. To nám říká, že následující druhou mocninu získáme z předchozí přičtením příslušného lichého čísla. Začneme od nuly ($0^2 = 0$) a budeme postupně přičítat lichá čísla tak, jak jdou za sebou.

1^2	2^2	3^2	4^2	5^2
$0+1=1$	$1+3=4$	$4+5=9$	$9+7=16$	$16+9=25$
6^2	7^2	8^2	9^2	10^2
$25+11=36$	$36+13=49$	$49+15=64$	$64+17=81$	$81+19=100$

Dále si uvedeme již jen druhé mocniny až po 100^2:

n	11	12	13	14	15	16	17	18	19	20
n^2	121	144	169	196	225	256	289	324	361	400
n	21	22	23	24	25	26	27	28	29	30
n^2	441	484	529	576	625	676	729	784	841	900
n	31	32	33	34	35	36	37	38	39	40
n^2	961	1024	1089	1156	1225	1296	1369	1444	1521	1600
n	41	42	43	44	45	46	47	48	49	50
n^2	1681	1764	1849	1936	2025	2116	2209	2304	2401	2500
n	51	52	53	54	55	56	57	58	59	60
n^2	2601	2704	2809	2916	3025	3136	3249	3364	3481	3600
n	61	62	63	64	65	66	67	68	69	70
n^2	3721	3844	3969	4096	4225	4356	4489	4624	4761	4900
n	71	72	73	74	75	76	77	78	79	80
n^2	5041	5184	5329	5476	5625	5776	5929	6084	6241	6400
n	81	82	83	84	85	86	87	88	89	90
n^2	6561	6724	6889	7056	7225	7396	7569	7744	7921	8100
n	91	92	93	94	95	96	97	98	99	100
n^2	8281	8464	8649	8836	9025	9216	9409	9604	9801	10000

Je-li $n \in \mathbb{Z}$, pak $n = 10m+k$, $m \in \mathbb{Z}$, $0 \leq k \leq 9$ a $n^2 = 100m^2+20mk+k^2$. Z tabulky (čísla k^2) vidíme, že dekadický zápis čísla n^2 bude končit některou z číslic $0, 1, 4, 5, 6, 9$ (chybí číslice $2, 3, 7, 8$).

Uvažujme ještě trochu dále. Je-li $n = \pm(100a+10b+c)$, kde $0 \leq a, b, c \leq 9$, pak dekadický zápis čísla n^2 bude mít poslední dvojčíslí (napravo) stejné,

jako dekadický zápis čísla $(10b + c)^2 = 100b^2 + 20bc + c^2$ (a vlastně též čísla $20bc + c^2$). Z tabulky vidíme, že přichází v úvahu pouze tato dvojčíslí: $00, 01, 04, 09, 16, 21, 24, 25, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96$, což je 21 dvojčíslí ze 100 možných.

Obecně, je-li $n \in \mathbb{N}$, pak lze psát $n = m + k$, kde $m, k \in \mathbb{N}_0$, 1000 dělí m a $0 \leq k \leq 1000$. Nyní $n^2 = m^2 + 2mk + k^2$, kde 1000 dělí m^2 a také $2mk$. Takže dekadický zápis čísla n^2 končí stejně stejně jako dekadický zápis čísla k^2. To je výše uvedených 21 dvojčíslí.

Je $6^2 = 36$ a $3 + 6 = 9 = 3^2$. Je $9^2 = 81$ a $8 + 1 = 9 = 3^2$. Je $11^2 = 121$ a $1 + 2 + 1 = 4 = 2^2$. Je $12^2 = 144$ a $1 + 4 + 4 = 9 = 3^2$. Je $13^2 = 169$ a $1 + 6 + 9 = 16 = 4^2$. Je $14^2 = 196$ a $1 + 9 + 6 = 16 = 4^2$. Je $31^2 = 961$ a $9 + 6 + 1 = 16 = 4^2$. Je $67^2 = 4489$ a $4 + 4 + 8 + 9 = 25 = 5^2$.

Je $19^2 = 361$, $1+9 = 10 = 3+6+1$, $19 = (1\cdot 9)+(1+9)$, $3\cdot 6\cdot 1 = 18 = 2\cdot 9$.

Je $9079 = 7 \cdot 1297$ a $9079^2 = 82428241 = 8242 \cdot 10^3 + 8241$. Je $69^2 = 4761$ a $69^3 = 328509$. Je $45624^2 = 2081549376$. Je $66276^2 = 4392508176$. Je $88^2 = 7744$. Je $149^2 = 22201$. Je $995^2 = 989025$. Je $996^2 = 992016$. Je $423^2 = 75686967$. Je $173^2 = 29929$. Je $27889^2 = 777796321$.

Je $5292 = 28 + 0 + 0 + 5264$ a $5293^2 = 28005264$. Je $1681 = 41^2, 16 = 4^2, 81 = 9^2$. Je $212^2 = 44944, 4 = 2^2, 9 = 3^2, 49 = 7^2$. Je $307^2 = 94249$. Je $367^2 = 134689$. Je $263^2 = 69169$. Je $2001^2 = 4004001$ a $2004^2 = 4016016$. Je $2810 = 2 \cdot 5 \cdot 281$, kde $2, 5, 281$ jsou prvočísla a $25281 = 159^2, 159 = 3 \cdot 53$. Je $264^2 = 69696 = 2^6 \cdot 3^2 \cdot 11^2$. Je $3242^2 = 10510564, 64 + (42 - 1) = 105 = 3 \cdot 5 \cdot 7, 64 = 8^2$. Je $3249 = 57^2, 324 = 18^2, 49 = 7^2, 9 = 3^2, 4 = 2^2, 32 = 2^5, 24 = 3 \cdot 2^3$.

Je $2867 = 47 \cdot 61$, kde 47 a 61 jsou prvočísla a $4761 = 69^2, 69 = 3 \cdot 2^3, 3 + 2 + 3 = 8 = 2^3, 2867 = 2869 - 2 = (4 \cdot 7) \cdot 10^2 + (61 + 6)$.

Je $(8 + 1)^2 = 9^2 = 81$. Je $164 = 10 \cdot 16 + 4 = 100 \cdot 1 + 64, 16 = 4^2, 100 = 10^2, 1 = 1^2, 64 = 8^2$.

Jak již jsme poznamenali, tak $(n + 1)^2 - n^2 = 2n + 1$ pro každé $n \in \mathbb{Z}$. Tedy každé liché číslo je rozdílem dvou druhých mocnin. Je-li $m = a^2 - b^2$, $a, b \in \mathbb{Z}$, sudé číslo, tak obě čísla a, b mají stejnou paritu (jsou obě buďto sudá, nebo lichá). Tedy, buďto $a = 2k+1, b = 2l+1$ a $m = 4(k^2+k-l^2-l)$ a nebo $a = 2k, b = 2l$ a $m = 4(k^2 - l^2$. V obou případech je číslo m dělitelné číslem 4. Naopak, je-li $m = 4t$, tak $m = (t + 1)^2 - (t - 1)^2$. Vidíme, že mezi sudými čísly jsou to právě násobky čísla 4, které jsou rozdílem dvou druhých mocnin. Takže, např., $2, 6 \neq a^2 - b^2$ pro všechna $a, b \in \mathbb{Z}$.

V souvislosti si ještě všimněme těchto dvou rovností: $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$ a $(a^2-b^2)(c^2-d^2) = (ac+bd)^2-(ad+bc)^2$. K tomuto se vrátíme později.

I.6.2 Hříčka. Je $5^2 = 25$, $6^2 = 36$, $76^2 = 5776$, $376^2 = 141376$, $1249^2 =$

1948441249, $890625^2 = 793212890625$. Čísla tohoto typu jsou známa jako čísla automorfní či okružní (cirkulární). To vše při základu 10.

Je $495475^2 = 245495475625$.

Máme také $50^2 = 2500$, $60^2 = 3600$, $10^2 = 100$, $100^2 = 10000$, $799^2 = 9801$, $999^2 = 998001$, $9999^2 = 99980001$. (A jak je to dál?)

I.6.3 Tabulka. Udělejme si tabulku součtů dvou druhých mocnin $n^2 + m^2$, kde $0 \leq n, m \leq 12$.

$n^2 + m^2$

n \ m	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
0	0	1	4	9	16	25	36	49	64	81	100	121	144
1	1	2	5	10	17	26	37	50	65	82	101	122	145
2	4	5	8	13	20	29	40	53	68	85	104	125	148
3	9	10	13	18	25	34	45	58	73	90	109	130	153
4	16	17	20	25	32	41	52	65	80	97	116	137	160
5	25	26	29	34	41	50	61	74	89	106	125	146	169
6	36	37	40	45	52	61	72	85	100	117	136	157	180
7	49	50	53	58	65	74	85	98	113	130	149	170	193
8	64	65	68	73	80	89	100	113	128	145	164	185	208
9	81	82	85	90	97	106	117	130	145	162	181	202	225
10	100	101	104	109	116	125	136	149	164	181	200	221	244
11	121	122	125	130	137	146	157	170	185	202	221	242	265
12	144	145	148	153	160	169	180	193	208	225	244	265	288

A teď trochu rovností. Je $(2n^2 + 2n)^2 + (2n + 1)^2 = (2n^2 + 2n + 1)^2$ pro každé $n \in \mathbb{Z}$. Např., $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$. Dále, $(2n^2m + 2nm)^2 + (2nm + m)^2 = (2n^2m + 2nm + m)^2$ pro všechna $n, m \in \mathbb{Z}$. Např., $6^2 + 8^2 = 10^2$, $9^2 + 12^2 = 15^2$. Platí také rovnost $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.

Všimněme si, že $a^2 + b^2 \neq 3, 6, 7, 11, 12, 15, 19$ a $a^2 + b^2 + c^2 \neq 7, 15, 28$ pro všechna $a, b, c \in \mathbb{Z}$.

Je $0^2 + 5^2 = 25 = 3^2 + 4^2$. Číslo 25 $(= 5^2)$ je nejmenší číslo, které lze (aspoň) dvěma způsoby napsat jako součet dvou druhých mocnin. Je $1^2 + 7^2 = 50 = 5^2 + 5^2$. Číslo 50 $(= 2 \cdot 5^2)$ je nejmenší číslo, které lze (aspoň) dvěma způsoby napsat jako součet dvou nenulových druhých mocnin.

Je $1^2 + 8^2 = 4^2 + 7^2 = 65 = 5 \cdot 13$, $2^2 + 11^2 = 5^2 + 10^2 = 125 = 5^3$, $3^2 + 11^2 = 7^2 + 9^2 = 130 = 2 \cdot 5 \cdot 13$, $4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2 = 1105 = 5 \cdot 13 \cdot 17$.

Je $119^2 + 120^2 = 14161 + 14400 = 28561 = 169^2 = 13^4$, $22^2 + 23 = 507 = 3 \cdot 13^2$. Je $232 = 6^2 + 14^2$, $233 = 8^2 + 13^2$, $234 = 3^2 + 15^2$. Je $588^2 + 2353^2 = 345744 + 5536609 = 5882353$ a $9412^2 + 2353^2 = 88585744 + 5536609 = 94122353$. Také je $8833 = 7744 + 1089 + 88^2 + 33^2$, $1^2 + 11^2 =$

$1 + 121 = 122 = 2 \cdot 61$, $2^2 + 22^2 = 4 + 484 = 488 = 8 \cdot 61$, $3^2 + 33^2 = 9 + 1089 = 1098 = 2 \cdot 9 \cdot 61$, $4^2 + 44^2 = 16 + 1936 = 1952 = 32 \cdot 61$ (je totiž $a^2 + (11a)^2 = a^2(1^2 + 11^2) = 2 \cdot 61 \cdot a^2$).

I.6.4 Zábavka. Je $9^2 = 81$, $9 = 1 + 8$ a $2 \cdot 9 = 18$. Podobně, $33^2 = 1089$ a $9801 = 297 \cdot 33$. Buď nyní n takové kladné celé číslo, že n^2 je trojciferné číslo; zřejmě je $10 \leq n \leq 32$. Nechť $n^2 = 100a + 10b + c$, $0 \leq b$, $c \leq 9$, $1 \leq a \leq 9$. Nechť $100c + 10b + a = kn$ pro nějaké $k \geq 0$. Potom n dělí rozdíl $100a + 10b + c - 100c - 10b - a = 99(a - c)$. Ovšem, $|a - c| \leq 9$. Čísla $1, 3, 9, 11, 33, 99$ jsou právě všichni kladní dělitelé čísla 99. Z těchto dělitelů připadá pro číslo n pouze hodnota $n = 11$. A hle! $11^2 = 121 = 11 \cdot 11$. Uvážíme-li nyní dělitele čísla $a - c$, tak vidíme, že musíme ještě prověřit $n = 12, 15, 18, 21, 22, 24, 27$. Je však $12^2 = 144$, $18^2 = 324$, $24^2 = 576$ a čísla $441, 423, 675$ jsou lichá. Tudy cesta nevede. Dále, $15^2 = 225$ a 5 nedělí 522, $21^2 = 441$ a 7 nedělí 144, $27^2 = 729$ a $927 = 9 \cdot 103$, 3 nedělí 103. Nakonec, $22^2 = 484 = 22 \cdot 22$. Řešením naší úlohy jsou čísla $n = 11, 22$. Všimněme si ještě, že $99^2 = 9801$ a $1089 = 11 \cdot 99$. Podobně, $66^2 = 4356$ a $6534 = 99 \cdot 66$.

I.6.5 Hříčka. Nechť $1 \leq a \leq 9$, $0 \leq b \leq 9$. Chceme ověřit, že $10a + b \neq a^2 + b^2$.

Nechť, naopak, $10 + b = a^2 + b^2$. Je $10a > 9a \geq a^2$ a máme $b(b - 1) = b^2 - b = 10a - a^2 = (10 - a)a > 0$. Snadno nahlédneme, že $(10 - a)a \geq 9$. Tedy $b \geq 4$ a $b(b - 1) \geq 12$. Pak ale $2 \leq a \leq 8$, $(10 - a)a \geq 16$, $b \geq 5$, $b(b - 1) \geq 20$. Pak ale $3 \leq a \leq 7$, $(10 - a)a \geq 21$, $b \geq 6$ a $b(b - 1) \geq 30$. Ovšem, $(10 - a)a \leq 25$, spor.

I.6.6 Zábavka. (i)Je $1^2+9^2 = 82$, $8^2+2^2 = 68$, $6^2+8^2 = 100$, $1^2+0^2+0^2 = 1$, $1^2 = 1$. Podobně, $1^2 + 3^2 = 10$, $1^2 + 0^2 = 1$, $1^2 = 1$. Podobně, $2^2 + 3^2 = 13$, $1^2 + 3^2 = 10$, $1^2 + 0^2 = 1$, $1^2 = 1$. Podobně, $6^2 + 8^2 = 100$, $1^2 + 0^2 + 0^2 = 1$, $1^2 = 1$.

Čísla $19, 91, 13, 31, 23, 32, 68, 86$ patří mezi tzv. šťastná čísla.

(ii) Je $91^2 = 8281$, $8^2 + 2^2 + 8^2 + 1^2 = 135$, $1^2 + 3^2 + 5^2 = 35$, $3^2 + 5^2 = 34$, $3^2 + 4^2 = 25$, $2^2 + 5^2 = 29$, $2^2 + 9^2 = 85$, $8^2 + 5^2 = 89$, $8^2 + 9^2 = 145$, $1^2 + 4^2 + 5^2 = 42$, $4^2 + 2^2 = 20$, $2^2 + 0^2 = 4$, $4^2 = 16$, $1^2 + 6^2 = 37$, $3^2 + 7^2 = 56$, $5^2 + 6^2 = 61$, $6^2 + 1^2 = 37$, $3^2 + 7^2 = 58$, $5^2 + 8^2 = 89$, $8^2 + 9^2 = 145$, $1^2 + 4^2 + 5^2 = 42$, $4^2 + 2^2 = 20$, atd.

I.6.7 Příklad. Nechť $a, b \in \mathbb{Z}, ab \neq 0, c = a^2 + b^2 (\geq 2)$. Buď $d \in \mathbb{Z}$ takové číslo, že d^2 dělí c. Je tedy $c = ed^2, e \geq 1$, a my položme $f = a^2e$ a $g = b^2e$. Nyní, $f + g = a^2e + b^2e = (a^2 + b^2)e = ce = d^2e^2 = (de)^2$ a $fg = a^2eb^2e = (abe)^2$.

Je-li $d = 1$, pak $e = c$, $f = a^4 + a^2b^2$, $g = b^4 + a^2b^2$, $f + g = (a^2 + b^2)^2$, $fg = (a^3b + ab^3)^2$.

Je-li $e = 1$ (t.j., $c = d^2$), pak $f = a^2$, $g = b^2$, $f + g = a^2 + b^2 = d^2$, $fg = (ab)^2$.

Je-li $a = 3, b = 6$, pak $c = 45$ a lze určit $d = 3$. Potom $e = 5, f = 45, g = 180, f + g = 225 = 15^2, fg = 8100 = 90^2$.

I.6.8 Věta. Nechť $n \geq 3$, $n \neq 4$. Potom existuje aspoň jedno $m \geq 2$ tak, že $n < m^2 < 2n$.

Důkaz. Zvolme k největší číslo takové, že $k^2 \leq n$. Jistě je $k \geq 1$ a $n < (k+1)^2$. Je-li $(k+1)^2 < 2n$, pak lze položit $m = k + 1$. Nechť tedy $2n \leq (k+1)^2 = k^2 + 2k + 1$. Ovšem, $2n \geq 2k^2$, takže $2k^2 \leq k^2 + 2k + 1$, $(k-1)^2 - 2 = k^2 - 2k - 1 \leq 0$, $(k-1)^2 \leq 2$, $|k-1| \leq 1$, $k = 1, 2$, $2n \leq (k+1)^2 \leq 3^2 = 9$, $n \leq 4$. Je-li $n = 3$, pak lze volit $k = 2$. □

I.6.9 Poznámka. (i) Máme $0 = 0^2 = 2 \cdot 0$, $1 = 1^2 < 2 \cdot 1$, $2 < 2^2 = 2 \cdot 2$, $4 = 2^2 < 2 \cdot 4$. Takže pro všechna $n \geq 0$ existuje $m \geq 0$ tak, že $n \leq m^2 \leq 2n$.

Je $13 < 4^2 < 5^2 < 26 = 2 \cdot 13$, $35 < 6^2 < 7^2 < 8^2 < 70 = 2 \cdot 35$.

(ii) A ještě tato úvaha: Nechť $n \geq 1$ je takové číslo, že pro nějaké $k \geq 1$ existují $a, b \in \mathbb{N}$ tak, že $nb^2 \leq a^2$ a $ka^2 \leq (k+4)nb^2$. Buď m nejmenší číslo takové, že $a \leq mb$. Zřejmě je $m \geq 1$, $(m-1)b < a$, $nb^2 \leq a^2 \leq m^2b^2$, $n \leq m^2$. Předpokládejme nyní, že $2n < m^2$. Pak $2k(m-1)^2b^2 < 2ka^2 \leq (k+4)2nb^2 < (k+4)m^2b^2$, $2km^2 - 4km + 2k = 2k(m-1)^2 < (k+4)m^2 = km^2 + 4m^2$, $(k-4)m^2 < 4km - 2k < 4km$, $(k-4)m < 4k$. Je-li $k = 5$, pak máme $m \leq 19$ a $n \leq m^2 \leq 19^2 = 361$. Pro $k = 7$ máme $m \leq 9$ a $n \leq m^2 \leq 9^2 = 81$. Pro $k = 8$ máme $m \leq 7$ a $n \leq m^2 \leq 7^2 = 49$. Pro $k = 9$ máme $m \leq 7$. Pro $k = 10$ máme $m \leq 6$ a $n \leq m^2 \leq 6^2 = 36$. Pro $k = 11$ máme $m \leq 6$. Pro $k = 12$ máme $m \leq 5$ a $n \leq m^2 = 5^2 = 25$. Pro $k = 13$ máme $m \leq 5$. Pro $k = 14$ máme $m \leq 5$. Pro $k = 16$ máme $m \leq 5$. Pro $k = 17$ máme $m \leq 5$. Pro $k = 18$ máme $m \leq 5$. Pro $k = 19$ máme $m \leq 5$. Pro $k = 20$ máme $m \leq 4$ a $n \leq m^2 \leq 4^2 = 16$.

Takže, je-li $n \geq 17$ a $k = 20$, pak $n \leq m^2 \leq 2n$. V tomto případě je však $20a^2 \leq 24nb^2$, takže $5a^2 \leq 6nb^2$ a naopak. Specielně, pro $n = 17, k = 20$ je $m = 5$. Pro $k = 15$ máme $m \leq 5$.

I.7 Další mocniny

I.7.1 Tabulka. Přicházejí na řadu třetí mocniny:

n	1	2	3	4	5	6	7	8	9
n^3	1	8	27	64	125	216	343	512	729
n	10	11	12	13	14	15	16	17	18
n^3	1000	1331	1728	2197	2744	3375	4096	4913	5832
n	19	20	21	22	23	24	25	26	27
n^3	6859	8000	9261	10648	12167	13824	15625	17576	19683
n	28	29	30	31	32	33	34	35	36
n^3	21952	24389	27000	29791	32768	35937	39304	42875	46656

Ihned vidíme, že $21^3 < 100^2 < 22^3$. Dále, $3^3 = 27$, $2 + 7 = 3^2$, $5^3 = 125$, $1+2+5 = 2^3$, $6^3 = 216$, $2+1+6 = 3^2$, $8^3 = 512$, $5+1+2 = 2^3$, $2^3+1 = 3^2$, $5^2 + 2 = 3^3$, $3^2 + 3^3 = 6^2$, $2^2 + 11^2 = 5^3$, $3^3 + 13^2 = 14^2$, $3^2 + 6^3 = 15^2$, $7^3 + 13^2 = 8^3$, $10^2 + 20^3 = 90^2$, $181^2 + 7 = 32^3$, $9^2 + 44 = 5^3$, $9^3 = 729$, $7+2+9 = 18$, $11^3 = 1331$, $1+3+3+1 = 2^3$, $12^3 = 1728$, $1+7+2+8 = 18$, $14^3 = 2744$, $2 + 7 + 4 + 7 = 17$, $15^3 = 3375$, $3 + 3 + 7 + 5 = 18$, $16^3 = 4096$, $4+0+9+6 = 19$, $17^3 = 4913$, $4+9+1+3 = 17$, $18^3 = 5832$, $5+8+3+2 = 18$, $21^3 = 9261$, $9+2+6+1 = 18$, $24^3 = 13824$, $1+3+8+2+4 = 18$, $27^3 = 19683$, $1 + 9 + 6 + 8 + 3 = 27$, $30^3 = 27000$, $2 + 7 + 0 + 0 + 0 = 9$, $33^3 = 35937$, $3 + 5 + 9 + 3 + 7 = 27$, $36^3 = 46656$, $4 + 6 + 6 + 5 + 6 = 27$.

Je $250 = 2 \cdot 125 = 2 \cdot 5^3$, $2 + 1 + 2 + 5 = 10 = 2 \cdot 5$. Je $22 \cdot 9954^3 = 17299^3 + 25469^3$. Je známo, že $a^3 + b^3 \neq c^3$ pro všechna $a, b, c \in \mathbb{Z}$ taková, že $abc \neq 0$.

I.7.2 Pozorování. Je $1^3+12^3 = 1729 = 9^3+10^3$. Číslo 1729 lze tedy (aspoň) dvěma způsoby napsat jako součet dvou třetích mocnin nezáporných celých čísel. Je to nejmenší kladné číslo s touto vlastností a je známo jako Hardyho-Ramanujanovo číslo. Anglický matematik Godfrey Harold Hardy (1877–1947) a indický matematik Srinivasa Ramanujan (1887–1920) se o tomto čísle bavili v roce 1917. Všiml si ho také francouzský matematik Frénicle de Bessy (1605–1675). Je $1729 = 7 \cdot 13 \cdot 19$, $1+2+7+9 = 19$, $7+13+19 = 39 = 3 \cdot 13$, $3 + 13 = 16 = 2^4$, $1 + 6 = 7$. Dále $3^3 + 4^3 = 91 = (-5)^3 + 6^3$. Opět, číslo $91(= 7 \cdot 13)$ je nejmenší kladné číslo, které lze (aspoň) dvěma způsoby napsat jako součet dvou třetích mocnin. Je ovšem $0^3 + 0^3 = 0 = (-1)^3 + 1^3$. Dále, $7 \cdot 19 = 133 = 2^3+5^3$. Tedy, $19(3^3+4^3) = 19((-5)^3+6^3) = 19 \cdot 91 = 9^3+10^3 = 1^3 + 12^3 = 13(2^3 + 5^3)$. Samozřejmě, $7 = 2^3 + (-1)^3$, $19 = 3^3 + (-2)^3$.

Teď si uvědomme, že $13 \neq a^3 + b^3$ pro všechna $a, b \in \mathbb{Z}$.

Nechť, naopak, $13 = a^3 + b^3$. Můžeme předpokládat, že $a \geq 1$. Je $1 + 0^3 = 1$, $1 + 1^3 = 2$, $1 + 2^3 = 9$, $1 + 3^3 = 28$, $8 + 0^3 = 8$, $8 + 1^3 = 9$, $8 + 2^3 = 16$. Tedy můžeme předpokládat, že $b \leq -1$. Je $13 + (-b)^3 = a^3$, takže $a \geq 3$, $-b \leq a - 1$, $13 + (a-1)^3 \geq a^3$. Odtud, $4a + 1 \geq a^2$, $5 \geq (a-2)^2$, $4 \geq a \geq 3$. Ovšem, $13 - 27 = -14$ a $13 - 64 = 51$. Dosáhli jsme sporu.

Je $8^3 = 512 = (5 + 1 + 2)^3$. Je $2 \cdot 999 = 1998 = 28 + 2 \cdot 729 + 512 = 1 + 9 + 9 + 8 + 9^3 + 9^3 + 8^3 = 1^3 + 3^3 + 8^3 + 9^3 + 9^3$. Je $3543^3 = 44474744007$.

I.7.3 Hříčka. Je $3^3 + 4^3 + 5^3 = 27 + 64 + 125 = 216 = 6^3$. Je $7353^3 = 397551775977$. Je $10^3 + 5^3 + 4^3 + 6^2 = 1225 = 10^3 + 6^3 + 2^3 + 1^3(1^2)$, $1225 = 5^2 \cdot 7^2$. Je $153 = 1 + 125 + 27 = 1^3 + 5^3 + 3^3$, $370 = 27 + 343 + 0 = 3^3 + 7^3 + 0^3$, $371 = 27 + 343 + 1 = 3^3 + 7^3 + 1^3$ (srovnej s I.6.5). Je $135 = 1 + 9 + 125 = 1^1 + 3^2 + 5^3$. Je $69^2 = 4761$ a $69^3 = 328509$. Je $31^2 = 961$, $31^3 = 29791$, $31^3 + 1^3 = 29792 = 32 \cdot 931 = (31 + 1)(31 + 900)$.

I.7.4 Tabulka. Čtvrté mocniny

n	1	2	3	4	5	6	7
n^4	1	16	81	256	625	1296	2401
n	8	9	10	11	12	13	14
n^4	4096	6561	10000	14641	20736	28561	38416
n	15	16	17	18	19	20	21
n^4	50625	65536	83521	104976	130321	160000	194481
n	22	23	24	25	26	27	28
n^4	234256	279841	331776	390625	456976	531441	614656
n	2229	30	31	32	33	34	35
n^4	707281	810000	923521	1048576	1185921	1336336	1500625

Všimněme si, že $9^4 < 100^2 = 10^4$. Dekadický zápis každé čtvrté mocniny končí na některou z číslic $0, 1, 5, 6$.

Je $4^4 + 6^4 + 8^4 + 9^4 + 14^4 = 256 + 1296 + 4096 + 6561 + 38416 = 50625 = 15^4$. Je $83^4 = 47458321$, $9350^4 = 764269350625000$. Je $3^4 + 4^3 = 9^2 + 4^3 = 1^2 + 12^2 = 145 = 5 \cdot 29$. Je $66^4 = 18974736 = 8712 \cdot 2178$.

Je $1^4 + 2^4 = 17$, $2^4 + 3^4 = 97$, $3^4 + 4^4 = 337$, $4^5 + 5^4 = 881$ a všechna tato čtyři čísla jsou prvočísla. Avšak, $5^4 + 6^4 = 1921 = 17 \cdot 113$ a $7^4 + 8^4 = 6497 = 73 \cdot 89$. Nicméně, $6^4 + 7^4 = 3697$ je opět prvočíslo.

I.7.5 Tabulka. Páté mocniny:

n	1	2	3	4	5	6
n^5	1	32	243	1024	3125	7776
n	7	8	9	10	11	12
n^5	16807	32768	59049	100000	161051	248832
n	13	14	15	16	17	18
n^5	371293	537824	759375	1048576	1419857	1889568
n	19	20	21	22	23	24
n^5	2476099	3200000	4084101	5153632	6436343	7962624
n	25	26	27	28	29	30
n^5	9765625	11881376	14348907	17210368	20511149	24300000

Je $6^5 < 100^2 < 7^5$. Je $4^5 + 5^5 + 6^5 + 7^5 + 9^5 + 11^5 = 1024 + 3125 + 7776 + 16807 + 59049 + 16051 = 248832 = 12^5$. Je $3435 = 27 + 256 + 27 + 3125 = 3^3 + 4^4 + 3^3 + 5^5$. Je $4^5 + 5^4 = 1639 = 38^2 + 14^2 + (-1)^3$, $1639 = 11 \cdot 149$, $149 = 7^2 + 10^2$, $13 = 2^2 + 3^2$. Je $2^5 + 7^2 = 3^4$ a $3^5 + 11^4 = 122^2$.

I.7.6 Tabulka. Šesté mocniny:

n	1	2	3	4	5	6
n^6	1	64	729	4096	15625	46656
n	7	8	9	10	11	12
n^6	117649	262144	531441	1000000	1771561	2985984
n	13	14	15	16	17	18
n^6	4826809	7529536	11390625	16777216	24137569	34012224
n	19	20	21	22	23	24
n^6	47045881	64000000	85766121	113379904	148035889	191102976
n	25	26	27	28	29	30
n^6	244140625	308915776	387420489	481890304	594823321	729000000

Je $4^6 < 100^2 < 5^6$. Dekadický zápis šesté mocniny končí na číslice $0, 1, 4, 5, 6, 9$. Je $16^6 = 16777216$. Je $(3^1)^6 = 729$, $3 \cdot 1 \cdot 6 = 18 = 7 + 2 + 9$, $316 = 4 \cdot 79 = 2^2 \cdot 79$. Číslě 613 a 631 jsta prvočíslě. Ovšem, $361 = 19^2$.

I.7.7 Tabulka. Sedmé mocniny:

n	1	2	3	4	5
n^7	1	128	2187	16384	78125
n	6	7	8	9	10
n^7	279936	823543	2097152	4782969	10000000
n	11	12	13	14	15
n^7	19487171	35831808	62748517	105413504	170859375
n	16	17	18	19	20
n^7	268435456	410338673	612220032	893871739	1280000000
n	21	22	23	24	25
n^7	1801088541	2494357888	3404825447	4586471424	6103515625

Je $3^7 < 100^2 < 4^7$. Dekadický zápis sedmé mocniny končí na některou z číslic $0, 1, 3, 4, 5, 6, 7, 8$. Je $6^7 = 2779936$, $2+7+7+9+9+3+6 = 36 = 6^2$, $2 \cdot 7 \cdot 7 \cdot 9 \cdot 9 \cdot 3 \cdot 6 = 200492 = 2^2 \cdot 3^6 \cdot 7$.

I.7.8 Tabulka. Osmé mocniny:

n	1	2	3	4
n^8	1	256	6561	65536
n	5	6	7	8
n^8	390625	1679616	5764801	16777216
n	9	10	11	12
n^8	43046721	100000000	214358881	429981696
n	13	14	15	16
n^8	815730721	1475789056	2562890625	4294967296
n	17	18	19	20
n^8	6975757441	11019960576	16983563041	25600000000
n	21	22	23	24
n^8	37822859361	54875873536	78310985281	110075314176

Je $3^8 < 100^2 < 4^8$. Dekadický zápis osmé mocniny končí na některou z číslic $0, 1, 5, 6$. Je $2^2 + 2^8 + 3^8 = 4 + 512 + 6561 = 7077 = 7 \cdot 1011 = 3 \cdot 7 \cdot 337$.

I.7.9 Tabulka. Deváté mocniny:

n	1	2	3	4
n^9	1	512	19683	262144
n	5	6	7	8
n^9	1953125	10077696	40353607	134217728
n	9	10	11	12
n^9	387420489	1000000000	2357947691	5159780352
n	13	14	15	16
n^9	10604499373	20661046784	38443359375	68719476736
n	17	18	19	20
n^9	118587876497	198359290368	322687697779	512000000000

Je $2^9 < 100^2 < 3^9$. Rovněž tak $2^k < 100^2 < 3^k$ pro $10 \leq k \leq 13$. Ovšem, $100^2 = 10000 < 16384 = 2^{14}$. Je $2^9 = 13^2 + 7^3$. Je $6^6 + 6^7 + 6^8 + 6^9 = 46656 + 279936 + 1679616 + 10077696 = 12083904$, $6 \cdot 7 \cdot 8 \cdot 9 = 3024$ a $(6^6 + 6^7 + 6^8 + 6^9)/(6 \cdot 7 \cdot 8 \cdot 9) = 3996$.

I.7.10 Procvičování. Nechť $a \in \mathbb{Z}$, $a \neq 0$, $b, c, d \in \mathbb{N}_0$ jsou taková čísla, že $a^b + a^c = a^d$. Bez újmy na obecnosti lze předpokládat, že $b \leq c$. Pak $a^b(1 + a^{c-b}) = a^d$.

(i) Buď $b \geq d$. Potom $a^{b-d}(1 + a^{c-b}) = 1$, $1 + a^{c-b} = \pm 1$, $a^{b-d} = \pm 1$. Je-li $1 + a^{c-b} = 1$, pak $a^{c-b} = 0$, $a = 0$, spor. Je-li $1 + a^{c-b} = -1$, pak $a^{c-b} = -2$, $a = -2$, $c - b = 1$, $c = b + 1$, $(-2)^{b-d} = a^{b-d} = \pm 1$, $b - d = 1$, $d = b - 1$, $b \geq 1$. Máme tedy $(-2)^b + (-2)^{b+1} = a^b + a^c = a^d = (-2)^{b-1}$. Odtud, $2 \cdot (-2)^{b-1} = (-2)^{b-1}(-2 + 4) = (-2)^b + (-2)^{b+1} = (-2)^{b-1}$, $2 = 1$, opět spor.

(ii) Buď $b < d$. Potom $1 + a^{c-b} = a^{d-b}$. Je-li $a = 1$, tak $1 + a^{c-b} = 2 \neq 1 = a^{d-b}$. Je-li $a = -1$, tak $1 + a^{c-b} \in \{0, 2\}$, $a^{d-b} \in \{1, -1\}$. Vidíme, že $a \neq \pm 1$. Je-li $c > b$, pak a dělí 1, což nelze. Tedy $c = b$, $2 = 1 + a^0 = 1 + a^{c-b} = a^{d-b}$, $a = 2$, $d - b = 1$, $d = b + 1$.

(iii) Zjistili jsme, že $a = 2$, $b = c$, $d = b + 1$. Samozřejmě, platí i opak. Je $2^b + 2^b = 2 \cdot 2^b = 2^{b+1}$ pro každé $b \geq 0$.

„Opačná“ rovnost $b^a + c^a = d^a$ dá mnohem více práce.

I.7.11 Procvičování. Nechť a, b, c, d, e jsou taková kladná čísla, že $a^b + a^c + a^d = a^e$. Bez újmy na obecnosti lze předpokládat, že $b \leq c \leq d < e$. Také je zřejmé, že $a \geq 2$.

(i) Buď $a = 2$. Pak $1 + 2^{c-b} + 2^{d-b} = 2^{e-b}$. Tedy číslo nalevo je sudé, a tak $c = b$. Odtud, $2 + 2^{d-b} = 2^{e-b}, d > b, 1 + 2^{d-b-1} = 2^{e-b-1}, d - b - 1 = 0, d = e + 1, e - b - 1 = 1, e = b + 2$. Takže $c = b, d = b + 1, e = b + 2$. A samozřejmě, $2^b + 2^b + 2^{b+1} = 2^{b+1} + 2^{b+1} = 2^{b+2}$.

(ii) Nechť $a \geq 3$. Je $1+a^{c-b}+a^{d-b} = a^{e-b}$, a nedělí 1, $c = b$, $2+a^{d-b} = a^{e-b}$, a nedělí 2, $d = b$, $3 = a^{e-b}$, $a = 3$, $e = b+1$. Zjistili jsme, že $a = 3$, $b = c = d$, $e = b + 1$. Samozřejmě, $3^b + 3^b + 3^b = 3 \cdot 3^b = 3^{b+1}$.

(iii) Je $4^b + 4^b + 4^b + 4^b = 4 \cdot 4^b = 4^{b+1}$, $5^b + 5^b + 5^b + 5^b + 5^b = 5^{b+1}$, atd. Podobně, $3^b + 3^b + 3^b + 3^{b+1} + 3^{b+1} = 3^{b+2}$, atd.

I.7.12 Věta. (Srovnej s I.6.8.) Následující podmínky jsou ekvivalentní pro $n \geq 0$:

(i) Existuje $m \geq 0$ tak, že $n < m^3 < 2n$.

(ii) $n \geq 33$ a nebo $n = 5, 6, 7, 14, 15, \ldots, 25, 26$.

(Tedy buďto $n \geq 33$, nebo $14 \leq n \leq 26$ a nebo $5 \leq n \leq 7$.)

Důkaz. Množinu nezáporných celých čísel splňujících podmínku (i) označme A. Zřejmě $0, 1, 2, 3, 4, 8, \ldots, 13 \notin A$, $5, 6, 7, 14, \ldots, 26 \in A$, $27, 28, 29, 30, 31, 32 \notin A$. Je-li $33 \leq n \leq 63$, pak $n \leq 63 < 64 = 4^3 < 66 \leq 2n$, čili $n \in A$.

Nechť $n \geq 64$ a nechť k je největší číslo takové, že $k^3 \leq n$; zřejmě je $k \geq 4$. Nyní, $n < (k+1)^3$ a, je-li $(k+1)^3 < 2n$, pak lze položit $m = k + 1$ a dostáváme $n \in A$. Předpokládejme tedy, že $2n \leq (k+1)^3$. Odtud, $2k^3 \leq 2n \leq (k+1)^3 = k^3 + 3k^2 + 3k + 1$, $k^3 \leq 3k^2 + 3k + 1$. Je-li $k^3 = 3k^2 + 3k + 1$, pak k dělí 1 a $k = 1$, spor, neb víme, že $k \geq 4$. Tedy $k^3 \leq 3k^2 + 3k$, z čehož plyne $k^2 \leq 3k + 3$. Je-li $k^2 = 3k + i$, $i = 1, 2, 3$, pak k dělí i, spor s tím, že $k \geq 4$. Takže $k^2 \leq 3k$, $k \leq 3$, poslední spor. □

I.7.13 Poznámka. Je $0 = 0^3 = 2 \cdot 0$, $1 = 1^3 < 2 \cdot 1$, $4 < 2^3 = 2 \cdot 4$, $8 = 2^3 < 2 \cdot 8$, $27 = 3^3 < 2 \cdot 27$, $32 < 4^3 = 2 \cdot 32$. Tedy pro každé $n \geq 0$, $n \neq 2, 3, 9, 10, 11, 12, 13, 28, 29, 30, 31$ existuje $m \geq 0$ tak, že $n \leq m^3 \leq 2n$.

I.7.14 Kolikerka. Pro každé $k \geq 0$ označme symbolem $\omega(k)$ největší celé číslo n takové, že pro $m \in \mathbb{Z}$ je buďto $m^k \leq n$ či $2n \leq m^k$. Ihned vidíme, že $\omega(0)$ neexistuje a $\omega(1) = 1$. V I.6.8 jsme zjistili, že $\omega(2) = 4$. V I.7.12 jsme zjistili, že $\omega(3) = 32$. A kolik je $\omega(4)$? Existuje vůbec? Možná že je $\omega(4) = 648$ $(= 2^3 \cdot 3^4)$. Anebo ne?

I.8 Rozdíly a součty mocnin

I.8.1 Cvičení. S případným použitím tabulek I.6.1, I.7.1, I.7.4, I.7.5, I.7.6, I.7.7, I.7.8, I.7.9, si seřadíme mocniny n^k, $n \geq 0$, $k \geq 2$, $n^k \leq 10000$, tak, jak jdou za sebou. Dostaneme $125 (= 5^3)$ čísel: 0, 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343, 361, 400, 441, 484, 512, 529, 576, 625, 676, 729, 784, 841, 900, 951, 1000, 1024, 1089, 1156, 1225, 1296, 1331, 1369, 1444, 1521, 1600, 1681, 1728, 1764, 1849, 1936, 2025, 2048, 2116, 2187, 2197, 2209, 2304, 2401, 2500, 2601, 2704, 2724, 2809, 2916, 3025, 3136, 3249, 3364, 3375, 3481, 3600, 3721, 3844, 3969, 4096, 4225, 4356, 4489, 4624, 4761, 4900, 4913, 5041, 5184, 5329, 5476, 5625, 5776, 5832, 5929, 6084, 6171, 6400, 6561, 6724, 6859, 6889, 7056, 7225, 7396, 7569, 7744, 7776, 7921, 8000, 8100, 8192, 8282, 8464, 8649, 8836, 9025, 9216, 9261, 9409, 9604, 9801, 10000.

A nyní si postupně uděláme rozdíly po sobě jdoucích mocnin a tyto rozdíly seřadíme podle velikosti. Dostaneme posloupnost: 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 27, 28, 30, 32, 33, 35, 36, 38, 39, 41, 43, 45, 47, 49, 51, 53, 55, 56, 57, 59, 61, 65, 67, 68, 69, 71, 75, 77, 79, 81, 85, 87, 89, 92, 95, 97, 99, 100, 101, 103, 106, 107, 109, 111, 113, 115, 119, 121, 123, 125, 127, 128, 129, 131, 133, 135, 137, 139, 143, 145, 147, 148, 149, 151, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 183, 185, 187, 189, 191, 195, 197, 199. Z lichých čísel (do 199) chybí 29, 31, 37, 63, 73, 83, 91, 93, 105, 117, 141, 153, 177, 179, 181, 193 a ze sudých chybí 6, 8, 14, 22, 26, 34, 40, 42, 44, 46, 48, 50, 52, 54, 58, 60, 62, 64, 66, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 94, 94, 98, 102, 104, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 130, 132, 134, 136, 138, 140, 142, 144, 146, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198.

I.8.2 Poznámka. (i) $2n + 1 = (n + 1)^2 - n^2$ pro každé $n \in \mathbb{Z}$. Tedy každé liché číslo lze získat jako rozdíl dvou druhých mocnin.

(ii) $4n = (n + 1)^2 - (n - 1)^2$. Tedy každé číslo dělitelné 4 lze získat jako rozdíl dvou druhých mocnin.

(iii) Je $2 = 27 - 25 = 3^3 - 5^2$.

(iv) Je $(-1)^3 + 1 = 0^2$, $0^2 + 1 = 1^2$, $2^3 + 1 = 3^2$. Tedy $1 = 0^2 - (-1)^3 = 1^2 - 0^2 = 3^2 - 2^3$. Je známo, že pro $a \neq -1, 0, 8$ vždy aspoň jedno z čísel $a, a + 1$ není druhou či vyšší mocninou jakéhokoliv celého čísla. Bohužel, elementární důkaz tohoto zajímavého faktu nemáme k dispozici.

(v) Pro každé $a \in \mathbb{Z}, a \neq -1$, aspoň jedno z čísel $a, a + 1, a + 2$ není druhou či vyšší mocninou. Ani toto slabší tvrzení zatím neumíme dokázat elementárně.

I.8.3 Cvičení. (i) Nechť $a, b, c \in \mathbb{Z}, n, m \in \mathbb{N}, n \geq 2, m \geq 2$, jsou taková čísla, že $a = b^n$ a $a + 2 = c^m$ (např. $a = 5^2, a + 2 = 3^3$). Zajisté, číslo a je sudé právě když číslo b je sudé a rovněž právě když číslo c je sudé. V tomto případě však číslo 4 dělí obě čísla b^n, c^m a tedy 4 dělí obě čísla $a, a+2$. Potom 4 dělí i rozdíl $a+2-a = 2$, což neplatí. Nahlížíme, že čísla a, b, c jsou vesměs lichá.

(ii) Nechť $a \in \mathbb{Z}$ je sudé číslo, $a = b^n$, $b \in \mathbb{Z}$, $n \geq 2$. Z (i) plyne, že $a + 2 \neq c^m$ pro všechna $c \in \mathbb{Z}$ a $m \geq 2$.

(iii) Nechť $a \in \mathbb{Z}$ je liché číslo, $a + 1 = b^n$, $b \in \mathbb{Z}$, $n \geq 2$. Číslo $a + 1$ je sudé, a proto $a + 3 \neq c^m$ pro všechna $c \in \mathbb{Z}$ a $m \geq 2$ podle (ii).

(iv) Nechť $a \in \mathbb{Z}$. Z (ii) a (iii) plyne, že ze čtyř (po sobě jdoucích) čísel $a, a + 1, a + 2, a + 3$ aspoň jedno není druhou či vyšší mocninou celého čísla.

I.8.4 Úloha. (i) Která čísla n lze získat ve tvaru $n = a^k - b^l$, kde $a, b, k, l \geq 2$, $a^k \geq b^l$?

Samozřejmě $0 = 2^2 - 2^2$, $1 = 3^2 - 2^3$, $2 = 3^3 - 5^2$, $3 = 2^7 - 5^3$, $4 = 2^3 - 2^2 = 5^3 - 11^2 = 6^2 - 2^5$, $5 = 3^2 - 2^2 = 2^5 - 3^3$, $7 = 2^4 - 3^2 = 2^5 - 5^2 = 2^7 - 11^2$, $8 = 2^4 - 2^3$, $9 = 5^2 - 2^4 = 6^2 - 3^3 = 15^2 - 6^3$, $10 = 13^3 - 3^7$. Tedy určitě čísla 1, 2, 3, 4, 5, 7, 8, 9, 10 (chybí 6).

Je-li $n \geq 5$ liché číslo, pak $(n-1)/2 \geq 2$ a $n = ((n+1)/2)^2 - ((n-1)/2)^2$. Je-li $n \geq 2$ sudé, 4 dělí n, pak $(n-4)/4 \geq 2$ a $n = ((n+4)/4)^2 - ((n-4)/4)^2$. Zbývají čísla $n = 4k+2$, $k \geq 0$. Již jsme si všimli, že $2 = 3^3 - 5^2$, $10 = 13^3 - 3^7$. Je také $18 = 19^2 - 7^3 = 3^5 - 15^2$. A co čísla 6 a 14?

(ii) K číslům z (i) přidejme ještě čísla tvaru $a^k - 1 (= a^k - 1^2)$, kde $a \geq 2$, $k \geq 2$. Tedy čísla 3, 7, 8, 15, 26, 31, 63, 80, ...

Je-li a sudé číslo, pak $a^k - 1 \geq 3$ je liché číslo a je tedy typu (i). Je-li $a = 4l + 1, l \geq 1$, liché číslo, pak 4 dělí $a^k - 1$ a tedy $a^k - 1$ je opět typu (i). Je-li $a = 4l + 3, l \geq 1, k$ sudé, pak opět 4 dělí $a^k - 1$ a tedy $a^k - 1$ je typu (i). Zbývají čísla $(4l + 3)^k - 1$, kde $l \geq 1$, $k \geq 3$, k liché. Nejmenší z nich je $7^3 - 1 = 342 (= 2 \cdot 3^2 \cdot 19)$.

(iii) A teď čísla $a^k (= a^k - 0^2)$, $a \geq 2, k \geq 2$. Tedy čísla 4, 8, 9, 16, 25, 27, 32, 49, 64, 81, ... Tato čísla jsou buď lichá ≥ 9 a nebo sudá a dělitelná číslem 4. Tedy jsou vesměs typu (i). Např. $9 = 5^2 - 4^2, 16 = 5^2 - 3^2$.

I.8.5 Cvičení. (i) A teď zkusme sčítat mocniny z I.8.1, od 4 výše a vždy po dvou. Dostáváme čísla $4 + 4 = 8$, $4 + 8 = 12$, $4 + 9 = 13$, 20, 29, 31, 36, 40, 53, 68, 85, 104, 1 25, 129, 131, 148, 173, 200, 220, 229, 247, 260, 293, ... a další. Dále, $8 + 8 = 16$, $8 + 9 = 17$, $8 + 16 = 24$, 33, 35, 40, 44, 57, 72, 89, 108, 129, 133, 136, 152, 177, 204, 224, 233, 251, 264, 297, ... a další. Dále, $9 + 9 = 18$, $9 + 16 = 25$, $9 + 25 = 34$, 36, 41, 45, 58, 73, 90, 109, 130, 134, 137, 153, 178, 205, 22 5, 234, 252, 265, 298, ... a další. Dále, $16 + 16 = 32$, $16 + 25 = 41$, $16 + 27 = 43$, $16 + 32 = 48$, $16 + 36 = 52$,

$16+49=65$, $16+64=80$, $16+81=97$, $16+100=116$, $16+121=137$, $16+125=141$, $16+128=144$, $16+169=185$, $16+196=212$, $16+216=232$, $16+225=241$, $16+243=259$, $16+256=272$, $16+289=305$, ... a další. Dále, $25+25=50$, $25+27=52$, $25+32=57$, $25+36=61$, $25+49=74$, $25+64=89$, $25+81=106$, $25+100=125$, $25+121=146$, $25+125=150$, $25+128=153$, $25+144=169$, $25+169=194$, $25+196=221$, $25+225=250$, $25+243=268$, $25+268=293$, $25+256=281$, $25+289=314$ a další. Dále, $27+27=54$, $27+32=59$, $27+36=63$, $27+49=76$, $27+64=91$, $27+81=108$, $27+100=127$, $27+121=148$, $27+125=152$, $27+128=155$, $27+144=171$, $27+169=196$, $27+196=223$, $27+216=243$, $27+225=252$, $27+243=270$, $27+256=283$, $27+289=316$, ... a další. Dále, $32+32=64$, $32+36=68$, $32+49=81$, $32+64=96$, $32+81=113$, $32+100=132$, $32+121=153$, $32+125=157$, $32+128=160$, $32+144=176$, $32+176=208$, $32+169=201$, $32+196=228$, $32+216=248$, $32+225=257$, $32+243=275$, $32+256=288$, $32+289=321$, ... a další. Dále, $36+36=72$, $36+49=85$, $36+64=100$, $36+81=117$, $36+100=136$, $36+121=157$, $36+125=161$, $36+128=164$, $36+144=180$, $36+169=205$, $36+216=252$, $36+225=261$, $36+243=279$, $36+256=292$, ... a další. Dále, $49+49=98$, $49+64=113$, $49+81=130$, $49+100=149$, $49+121=170$, $49+125=174$, $49+128=177$, $49+144=193$, $49+169=218$, $49+196=245$, $49+216=265$, $49+225=274$, $49+243=292$, ... a další. Dále, $64+64=128$, $64+81=145$, $64+100=164$, $64+121=185$, $64+125=189$, $64+128=192$, $64+144=208$, $64+169=233$, $64+196=260$, $64+216=280$, $64+225=289$, $64+243=307$, ... a další. Dále, $81+81=162$, $81+100=181$, $81+121=202$, $81+125=206$, $81+128=209$, $81+144=225$, $81+169=250$, $81+196=277$, $81+225=306$, ... a další. Dále, $100+100=200$, $100+121=221$, $100+125=225$, $100+128=228$, $100+144=244$, $100+169=269$, $100+196=296$, ... a další. Dále, $121+100=221$, $121+125=246$, $121+128=249$, $121+144=265$, $121+169=290$, $121+196=317$, ... a další. Dále $125+125=250$, $125+128=253$, $125+144=272$, $125+169=294$, ... a další. Dále, $128+128=256$, $128+144=272$, $128+169=297$, ... a další. Dále $144+144=288$, $144+169=313$, ... a další. Dále, $169+169=338$, ... a další.

Získaná čísla, která jsme napsali, si seřadíme podle velikosti. Bude to posloupnost (α): 8, 12, 13, 16, 17, 18, 20, 21, 22, 24, 23, 29, 31, 32, 33, 34, 35, 36, 40, 41, 43, 44, 45, 48, 50, 52, 53, 54, 57, 58, 59, 61, 63, 64, 65, 68, 72, 73, 74, 76, 80, 81, 85, 89, 90, 91, 96, 97, 98, 100, 104, 106, 108, 109, 113, 116, 117, 125, 127, 128, 129, 130, 132, 133, 134, 136, 137, 141, 144, 145, 146, 148, 149, 150, 152, 153, 155, 157, 160, 161, 162, 164, 169, 170, 171, 174, 176, 177, 178, 180, 181, 185, 189, 192, 193, 194, 196, 200, 201, 202, 204, 206, 209, 212, 218, 220, 221, 223, 224, 225, 228, 229, 232, 233, 234, 241, 242, 243, 244,

245, 246, 247, 248, 249, 250, 251, 252, 253, 256, 257, 259, 260, 261, 264, 265, 268, 269, 270, 272, 274, 275, 277, 279, 280, 281, 283, 288, 289, 290, 292, 293, 294, 296, 297, 305, 306, 307, 313, 314, 316, 317, 321, 338.

(ii) Zbývající čísla v intervalu $1, \ldots, 338$ tvoří posloupnost (β): 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 25, 26, 27, 28, 30, 37, 38, 39, 42, 46, 47, 49, 51, 55, 56, 60, 62, 66, 67, 69, 70, 71, 75, 77, 78, 79, 83, 84, 86, 87, 88, 92, 93, 94, 95, 99, 101, 102, 103, 105, 107, 110, 111, 112, 114, 115, 118, 119, 120, 121, 122, 123, 124, 126, 131, 135, 138, 139, 140, 142, 143, 147, 151, 154, 156, 158, 159, 163, 165, 166, 167, 168, 172, 173, 175, 179, 182, 183, 184, 186, 187, 188, 190, 191, 195, 197, 198, 199, 203, 205, 207, 208, 210, 211, 213, 214, 215, 216, 217, 219, 222, 226, 227, 230, 231, 235, 236, 237, 238, 239, 240, 254, 255, 258, 262, 263, 266, 267, 271, 273, 276, 278, 282, 284, 285, 286, 287, 291, 295, 298, 299, 300, 301, 302, 303, 304, 308, 309, 310, 311, 312, 315, 318, 319, 320, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337.

(iii) Ke každému číslu z posloupnosti (α) přičteme číslo 4 a uveďmě zde posloupnost (γ) tvořenou získanými čísly, ale jen těmi, co nejsou v posloupnosti (α) obsažené: 21, 22, 28, 37, 38, 39, 47, 49, 56, 62, 67, 69, 77, 78, 84, 93, 94, 95, 101, 102, 110, 112, 120, 121, 131, 138, 140, 154, 156, 159, 165, 166, 168, 175, 182, 184, 197, 198, 210, 213, 216, 222, 227, 236, 237, 238, 254, 255, 263, 273, 276, 278, 284, 285, 287, 298, 300, 301, 309, 310, 311, 318, 320, 325, 342.

(iv) Vyhoďme z posloupnosti (β) čísla obsažená v posloupnosti (γ) a získejme velmi levně posloupnost (δ): 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 23, 26, 27, 29, 30, 42, 46, 51, 55, 60, 66, 70, 71, 75, 79, 82, 83, 86, 87, 88, 92, 96, 99, 103, 105, 107, 111, 114, 115, 118, 119, 122, 123, 124, 126, 135, 139, 142, 143, 147, 151, 158, 163, 167, 172, 179, 183, 186, 187, 188, 190, 191, 195, 199, 203, 205, 207, 210, 211, 214, 215, 217, 219, 226, 230, 231, 235, 239, 240, 255, 258, 262, 266, 267, 271, 282, 286, 291, 295, 299, 302, 303, 304, 308, 312, 315, 319, 322, 323, 324, 326, ..., 337.

(v) Ke každému číslu z posloupnosti (α) přičtěme číslo 8 a získaná čísla vyhoďme z posloupnosti (δ) – ovšem jen ta čísla, co se v (δ) vyskytují. Získáme tak posloupnost (ϵ): 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 23, 27, 29, 30, 46, 55, 70, 75, 79, 83, 86, 87, 92, 96, 103, 107, 111, 115, 118, 119, 122, 123, 126, 139, 143, 147, 151, 167, 183, 187, 190, 191, 195, 199, 203, 207, 211, 215, 219, 230, 235, 239, 262, 266, 271, 286, 295, 299, 303, 308, 312, 319, 323, 326, 327, 328, 330, ..., 337.

(vi) Ke každému číslu z posloupnosti (α) přičtěme číslo 9 a získaná čísla vyhoďme z posloupnosti (ϵ) – ovšem jen ta, co se v (ϵ) vyskytují. Získáme tak posloupnost (ϕ): 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 23, 30, 46, 55, 75, 79, 86, 87, 92, 96, 103, 111, 119, 123, 147, 151, 167, 191, 195, 199, 203, 207, 219, 235, 239, 271, 295, 308, 312, 319, 327, 328, 331, ..., 337.

(vii) Pokračujeme pilně dále. Ke každému číslu z (α) přičtěme 16 a opět získaná čísla vyhoďme z posloupnosti (ϕ). Vzniká nová posloupnost (ψ). Z (ϕ) v tomto bodu vyřadíme čísla 75, 92, 96, 295, 308, 312, 332, 333, 337.

(viii) A nyní přičítejme 25 k posloupnosti (α). Z ϕ budeme vyřazovat čísla 79, 86, 123, 195, 199, 203, 219, 308, 319, 331. A získáme posloupnost ξ: 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 23, 30, 46, 55, 87, 103, 111, 119, 147, 151, 167, 191, 207, 235, 271, 327, 328, 334, 335, 336.

(ix) A přičítáme 27. Z posloupnosti ξ vyřadíme čísla 103, 191, 207, 235, 271 a 334. Získáme novou posloupnost (ζ).

(x) A přičítáme 36. Z posloupnosti (ζ) vyřadíme čísla 151, 328 a dostaneme posloupnost (ρ).

(xi) A přičítáme 49. Z posloupnosti (ρ) vyřadíme číslo 147. Vznikla posloupnost (λ): 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 19, 23, 30, 46, 55, 87, 111, 119, 327, 335, 336.

(xii) Z posloupnosti (λ) vyřadíme $336 = 272 + 64$. Dále, $327 = 248 + 81$. Dále, $335 = 4 + 25 + 81 + 225$. Dále, $167 = 4 + 8 + 27 + 128$. Dále, $119 = 4+9+25+81$. Dále, $111 = 4+8+9+9+81$. Dále, $87 = 4+9+25+49$. Dále, $55 = 4+8+16+27$. Dále, $46 = 4+8+9+25$. Dále, $30 = 4+8+9+9$. A úplně nakonec je $9 = 3^2$ a $4 = 2^2$. Po vyřazení těchto čísel nám zbyde posloupnost (κ): 1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23, což je 12 čísel, $(23 + 1)/2 = 12$.

I.8.6 Poučení. Označme A množinu všech součtů tvaru $a_1^{k_1} + \cdots + a_n^{k_n}$, kde $n \geq 1$, $a_i \geq 2$, $k_i \geq 2$. Nejmenší číslo z množiny A je zřejmě $2^2 = 4$, a tak $A \subseteq \mathbb{N} \setminus \{1, 2, 3\}$. Další čísla z množiny A jsou zřejmě $2^2 + 2^2 = 4$, $3^2 = 9$, $2^2 + 2^2 + 2^2 = 12$, $2^2 + 3^2 = 13$, $4^2 = 2^2 + 2^2 + 2^2 + 2^2 = 16$, $2^2+2^2+3^2 = 17$, $3^2+3^2 = 18$, $2^2+2^2+2^2+2^2+2^2 = 20$, $2^2+2^2+2^2+3^2 = 21$, $2^2 + 3^2 + 3^2 = 22$. Takže $A \subseteq \mathbb{N} \setminus \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19\}$. Ovšem, $5^2 = 25 > 23$, $23 - 4^2 = 23 - 16 = 7 \notin A$, $23 - 3^2 = 23 - 9 = 14 \notin A$, $23 - 2^2 = 23 - 4 = 19 \notin A$. Nahlížíme, že též $23 \notin A$. Na druhé straně, $24 = 4^2 + 2^3$, $25 = 5^2$, $26 = 2^3 + 3^2 + 3^2$, $27 = 3^3$. Tedy $24, 25, 26, 27 \in A$.

Dokážeme si, že $A = \mathbb{N} \setminus \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23\}$ (takže 23 je největší kladné číslo, které není obsaženo v množině A).

Nechť, naopak, m je nejmenší takové číslo, že $m \notin A$ a $24 \leq m$. Je potom $28 \leq m$, $24 \leq m - 4 < m$, $m - 4 \in A$ a $m = (m - 4) + 2^2 \in A$, což je spor. Důkaz je hotov.

Všimněme si, že $2 + 3 = 5 = 6 - 1$, $6 = 2 \cdot 3$. Dále si všimněme, že $2^2 + 3^2 = 13$, $2^3 + 3^3 = 35$, $2^2 + 3^3 = 31$, $2^3 + 3^2 = 17$, přičemž $1 + 3 = 4$, $3 + 5 = 8 = 1 + 7$ a čísla $13, 17, 31, 53, 71$ jsou prvočísla. Ovšem, $35 = 5 \cdot 7$ a $5 + 7 = 12 = 3 \cdot 2^2$.

I.8.7 Cvičení. Označme S množinu všech součtů $a_1^2 + \cdots + a_n^2, n \geq 1$, $a_i \in \{2, 3\}$. Chceme ověřit, že $S = \{4, 8, 9, 12, 13, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, \dots\}$ (tedy, že $\mathbb{N} \setminus S = \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23\}$.

Zřejmě 4 je nejmenší číslo z S. Dále, $9 \in S$, $8 = 4+4 \in S$, $12 = 4+4+4 \in S$, $13 = 4+9 \in S$, $16 = 4+4+4+4 \in S$, $17 = 4+4+9 \in S$, $18 = 9+9 \in S$, $20 = 4+4+4+4+4+4 \in S$, $21 = 4+4+4+9 \in S$, $22 = 4+9+9 \in S$. Tedy $\{4, 8, 9, 12, 13, 16, 17, 18, 20, 21, 22\} \subseteq S$.

Nechť $m \geq 24$, $m = 4t+3, t \geq 6, 0 \leq r \leq 3$. Je-li $r = 0$, tak $m = t \cdot 4 \in S$. Je-li $r = 1$, tak $m = (t-2) \cdot 4+9 \in S$. Je-li $r = 2$, pak $m = (t-4) \cdot 4+9+9 \in S$. Je-li $r = 3$, pak $m = (t-6) \cdot 4 + 9 + 9 + 9 \in S$. Zjistili jsme, že $m \in S$.

Na druhé straně, zřejmě $S \subseteq A$, kde A je množina definovaná v I.8.6. Tedy $\{1, 2, 3, 5, 6, 7, 10, 11, 14, 19, 23\} = \mathbb{N} \setminus A \subseteq \mathbb{N} \setminus S$ a nyní je jasné, že $S = A$.

I.8.8 Příklad. (i) Nechť $n \geq 0$, $m \in \mathbb{Z}$, $a = 1 + m^n$, $b = ma (= m + m^{n+1})$. Potom je $a^n + b^n = a^n + m^n a^n = a^n(1+m^n) = a^{n+1}$. Tedy také $a^{n+1} - b^n = a^n$.

Např., pro $n = 0$ je $a = 2$, $b = 2m$. Pro $n = 1$ je $a = 1 + m$, $b = m + m^2$. Pro $m = 0 \neq n$ je $a = 1$, $b = 0$ Pro $m = 1$ je $a = 2 = b$. Pro $n = 2 = m$ je $a = 5$, $b = 10$. Pro $n = 2$, $m = 3$ je $a = 10$, $b = 30$. Pro $n = 3$, $m = 2$ je $a = 9$, $b = 18$. Pro $n = 3 = m$ je $a = 28$, $b = 84$.

(ii) Nechť $n \geq 2$, $m \in \mathbb{Z}$, $a = (1 + m^n)^{n-2}$, $b = ma (= m(1 + m^n)^{n-2})$. Potom je $a^n + b^n = a^n + m^n a^n = a^n(1 + m^n) = (1 + m^n)^{n-2n+1} = ((1 + m^n)^{n-1})^{n-1} = c^{n-1}$, $c = (1 + m^n)^{n-1}$. Tedy také $c^{n-1} - a^n = b^n$.

Např., pro $n = 2$ je $a = 1$, $b = m$ a $c = 1 + m^2$. Pro $n = 3$ je $a = 1 + m^3$, $b = m + m^4$ a $c = 1 + 2m^3 + m^6$. Pro $n = 3$, $m = 2$ je $a = 9$, $b = 18$ a $c = 81$.

I.8.9 Počítání. (i) Označme (jen místně) A množinu všech součtů $a^k + b^k$, kde $a, b \in \mathbb{N}$, $k \geq 2$. Je $-9 = (-2)^3 + (-1)^3$, $-8 = (-2)^3 + 0^3$, $-7 = (-2)^3 + 1^3$, $-2 = (-1)^3 + (-1)^3$, $-1 = (-1)^3 + 0^3$, $0 = 0^2 + 0^2 = (-1)^3 + 1^3$, $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $7 = 2^3 + (-1)^3$, $8 = 2^3 + 0^3$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$.

Tedy $-9, -8, -7, -2, 0, 1, 2, 4, 5, 7, 8, 9, 10 \in A$. Je také $2 \cdot 13 = 26 = 3^3 + (-1)^3 \in A$.

(ii) Nechť $n = a^k + b^k$, kde $a, b \in \mathbb{N}$, $a > 0$, $b < 0$, $k \geq 3$, k liché. Položme $c = -b$. Tudíž $c > 0$, $n = a^k - c^k = (a - c)d$, kde $d = a^{k-1} + a^{k-2}c + \cdots + ac^{k-2} + c^{k-1} \geq k$.

Je-li $d = k$, pak $a = 1 = c$, $b = -1, n = 0$.

Je-li $n > 0$, pak $a > c$, z čehož plyne $a \geq 2$ a $d \geq 2^{k-1} + 2^{k-2} + \cdots + 2 + 1 = 2^k - 1 \geq 7$, $n \geq 7$.

Je-li $n = 7$, pak $k = 3$, $a = 2$, $c = 1$, $b = -1$.

Je-li $n = 0$, pak $a = c = -b$.

Je-li $n < 0$, pak $a < c$, z čehož plyne $c \geq 2$ a $d \geq 7$, $n \leq -7$.

Je-li $n = -7$, pak $k = 3$, $a = 1$, $c = 2$, $b = -2$.

(iii) Pomocí (ii) se není těžké přesvědčit o tom, že $-10, -6, -3, 3, 6 \notin A$.

(iv) Je ovšem $3 = 2^7 + (-5)^3$, $5 = 2^5 + (-3)^3$, $13 = 2^8 + (-3)^5$, $15 = 2^6 + (-7)^2$, $-3 = 5^3 + (-2)^7$.

(v) Je $6 \neq a^k + b^l$ pro všechna $a, b \in \mathbb{N}_0$, $k \geq 2, l \geq 2$.

I.8.10 Počítání. (i) Označme (jen místně) B množinu všech rozdílů $a^k - b^k$, kde $a, b \in \mathbb{Z}$, $k \geq 2$. Jak jsme si všimli v I.6.1, tak množina B obsahuje všechna lichá čísla a také všechny násobky čísla 4 (neboť to jsou všechna čísla, která jsou rozdílem druhých mocnin).

(ii) Je-li $k = 2l$, tedy sudé, pak $a^k - b^k = (a^l)^2 - (b^l)^2$ (viz (i)).

(iii) Je-li k liché, pak $a^k - b^k = a^k + (-b)^k \in A$ (I.8.9).

(iv) Z předchozího plyne, že $6, -6 \notin A \cup B$.

I.9 Dělení se zbytkem

V celých číslech nejde neomezeně dělit, avšak:

I.9.1 Věta. Nechť n, m jsou celá nezáporná čísla, $n \neq 0$. Potom existují jednoznačně určená celá nezáporná čísla r, s tak, že $m = rn + s$, přičemž $0 \leq s < n$.

Důkaz. Nejdříve dokážeme existenci čísel r a s. Budeme přitom postupovat indukcí podle $m \geq 0$. Je-li $m = 0$, volíme $r = 0 = s$. Je-li nyní $m \geq 0$ a $m = rn + s$, $r \geq 0$, $0 \leq s < n$, pak $m + 1 = rn + s + 1$, kde $1 \leq s + 1 \leq n$, a jsme hotovi pro $s + 1 < n$. Je-li však $s + 1 = n$, pak $s = n - 1$, $m = rn + s = (r + 1)n - 1$ a $m + 1 = (r + 1)n$. Tím je indukční krok završen.

Nyní ověříme jednoznačnost čísel r a s. Nechť $r_1 n + s_1 = m = r_2 n + s_2$, kde $r_1, r_2, s_1, s_2 \in \mathbb{N}_0$, $0 \leq s_1 < n$, $0 \leq s_2 < n$. Bez újmy na obecnosti lze předpokládat, že $s_1 \geq s_2$. Pak je $(r_2 - r_1)n = s_1 - s_2 \geq 0$, čili $r_2 \geq r_1$. Ovšem, $0 \leq s_1 - s_2 < n - s_2 \leq n$, čili $n > s_1 - s_2$. Je-li však $r_2 > r_1$, pak $s_1 - s_2 = (r_2 - r_1)n \geq n \geq n$, což je nyní spor. Tedy $r_2 = r_1$ a $s_1 = s_2$. □

I.9.2 Poznamenání. V důkazu předchozí věty jsme mohli postupovat také takto: Je-li $m < n$, volíme $r = 0$ a $s = m$. Je-li $m = n$, volíme $r = 1$ a $s = 0$. Nechť tedy $n < m$. Pak je $n < 2n < 3n < \ldots$ a existuje $r \geq 1$ tak, že $rn \leq m$ a $m < (r + 1)n$. Nyní $0 \leq s = m - rn < n$.

I.9.3 Věta. Nechť n, m jsou celá čísla, $n \neq 0$. Potom existují jednoznačně určená celá čísla r a s tak, že $m = rn + s$, přičemž $0 \leq s < |n|$.

Důkaz. Opět nejdříve dokážeme existenci čísel r a s s danými vlastnostmi.

Nejprve předpokládejme, že $n \geq 1$. Mezi čísly $m - rn$, $r \in \mathbb{Z}$, jsou jistě některá nezáporná a zvolíme $r_0 \in \mathbb{Z}$ tak, aby číslo $s_0 = m - r_0 n$ bylo nejmenší možné mezi těmi nezápornými. Tedy $0 \leq s_0$. Je-li však $n \leq s_0$, pak $m - (r_0 - 1)n = s_0 - n$ je opět nezáporné číslo a tak $s_0 - n \geq s_0$ a $n \leq 0$, což je spor. Tím jsme dokázali, že $0 \leq s_0 < n = |n|$.

Je-li nyní $n \leq -1$, pak podle předchozího zjištění existují čísla r_1 a s_1 tak, že $m = r_1(-n) + s_1$, kde $0 \leq s_1$, kde $0 \leq s_1 < -n = |n|$. Nyní však $m = (-r_1)n + s_1$. Existence čísel r a s je dokázána.

A teď jednoznačnost. Je-li $r_2 n + s_2 = m = r_3 n + s_3$, kde $0 \leq s_2 < |n|$, $0 \leq s_3 < |n|$, $s_2 \geq s_3$, pakj $|n|$ dělí $s_2 - s_3$, $s_2 - s_3 \geq 0$. Odtud, buďto $s_2 = s_3$ (a $r_2 = r_3$) a nebo $|n| \leq s_2 - s_3 < |n| - s_3 \leq |n|$, což není možné. □

I.9.4 Důležité značení. Nechť $n \in \mathbb{Z}, n \neq 0$. Je-li $m \in \mathbb{Z}$ a $m = rn + s$, kde $r, s \in \mathbb{Z}$, $0 \leq s < |n|$ (viz I.9.3), pak píšeme $s = [m]_n$. Tedy n dělí

$m - [m]_n$ a (nezáporné) číslo $[m]_n$ je standartní zbytek po dělení čísla m číslem n. Číslo n zde vystupuje jako tzv. modulus.

Zřejmě $[m]_n = 0$ právě když n dělí m.

I.9.5 Proposice. Nechť $n, m \in \mathbb{Z}$, $n \neq 0$. Potom:

(i) $[0]_n = 0$.
(ii) n dělí m právě když $[m]_n = 0$.
(iii) $[m]_n = [m]_{-n} = [m]_{|n|}$.
(iv) Jestliže n nedělí m, pak $[-m]_n = |n| - [m]_n$ (neboli $[m]_n + [-m]_n = |n|$).
(v) Je-li $0 \leq m < |n|$, pak $[m]_n = m$.
(vi) Je-li $|m| < |n|$, $m < 0$, $n \nmid m$, pak $[m]_n = |n| - |m|$ (neboli $[m]_n + |m| = |n|$).

Důkaz. (i) Je $0 = 0 \cdot n + 0$.
(ii) Toto je zřejmé.
(iii) Je $m = (-r)(-n) + [m]_n$.
(iv) Vzhledem k (iii) lze předpokládat, že $n \geq 1$. Pak $n \geq 2$ (neboť n nedělí m) a $-n = (-r-1)n + n - [m]_n$, kde $1 \leq n - [m]_n = n - [m]_n$.
(v) Toto je zřejmé (použije se (iii) pro $n < 0$).
(vi) Plyne z (v) a (iv).

□

I.9.6 Lemma. Nechť n, a, b, c jsou taková čísla, že $a \geq 0$, $0 \leq c < |n|$, $a = bn + c$. Potom:

(i) $n \neq 0$.
(ii) $|b| \leq |a|$.
(iii) $|b| = |a|$ právě když buďto $a = b = c = 0$ nebo $c = 0$, $n = \pm 1$.

Důkaz. Předně, $n \neq 0$, neboť $c < |n|$. Dále, je-li $a = 0$, pak $b = c = 0$ plyne z I.9.3 (jednoznačnost). Nechť tedy $a \geq 1$. Budeme postupovat indukcí podle $c \geq 0$.

Je-li $c = 0$, pak $a = bn$, čili $a = |a| = |b| \cdot |n| \geq |b|$. Navíc, $|a| = |b|$ právě když $|n| = 1$. Nechť tedy $c \geq 1$. Pak $a - 1 = bn + c - 1$, kde $0 \leq c - 1 < |n|$. Je-li $a \geq 2$, potom $|b| \leq |a - 1| = a - 1 < a = |a|$ podle indukčního předpokladu. Je-li však $a = 1$, pak $|n| > c > c - 1 = |c - 1| = |b| \cdot |n|$, čili $b = 0$ a $|b| = 0 < 1 = a = |a|$. □

I.9.7 Lemma. Nechť n, a, b, c jsou taková čísla, že $a \leq -1$, $0 \leq c < n$, $a = bn + c$. Potom:

(i) $n \geq 1$.
(ii) $|b| \leq |a|$.
(iii) $|b| = |a|$ právě když buďto $c = 0$, $n = 1$ anebo $a = b = -1$, $c = n - 1$.

Důkaz. Opět, $n \geq 1$, neb $c < n$. Je-li $c = 0$, pak $|a| = |b| \cdot |n|$ a vše je jasné. Dále indukcí podle $c \geq 1$. Je $a - 1 = bn + c - 1$, kde $0 \leq c - 1 < n$, takže $|b| \leq |a - 1| = |a| + 1$ podle indukčního předpokladu. Je-li $|b| = |a| + 1$, pak z indukčního předpokladu (a toho, že $c \geq 1$) plyne $a = b = -1$, $c - 1 = n - 1$, $c = n$, což je spor. Takže $|b| \leq |a|$. Nakonec, je-li $|a| = |b|$, pak buďto $a = an + c$ a nebo $a = -an + c$.

Teď, nechť $a = an + c$. Tudíž $a(1 - n) = c$, $(n - 1) \cdot |a| = |a(1 - n)| = |c| = c < n$, $n \cdot |a| < n + |a|$ a, jelikož $n \geq 2$ ($n > c \geq 1$), tak $|a| = 1$ (viz I.3.1). Odtud, $a = -1$, $-1 = -n + c$, $c = n - 1$.

A nyní buď $a = -an + c$. Opět, $c = a(1 + n) < 0$, což je poslední spor. □

I.9.8 Lemma. Nechť n, a, b, c jsou taková celá čísla, že $a \leq -1$, $0 \leq c < -n$, $a = bn + c$. Potom:

(i) $n \leq -1$.
(ii) $|b| \leq |a|$.
(iii) $|b| = |a|$ právě když buďto $c = 0$, $n = -1$ anebo $a = -1$, $b = 1$, $c = -n - 1$.

Důkaz. Je $a = (-b)(-n) + c$ a z I.9.7 plyne $-n \geq 1$ (čili $n \leq -1$) a $|b| = |-b| \leq |a|$. Je-li $|a| = |b|$, pak z I.9.7(iii) plyne, že buďto $c = 0$, $n = -1$ a nebo $a = -b = -1$, $c = -n - 1$. □

I.9.9 Proposice. Nechť n, a, b, c jsou taková celá čísla, že $a = bn + c$, přičemž $0 \leq c < |n|$. Potom $n \neq 0$ a $|b| \leq |a|$. Navíc, rovnost $|a| \leq |b|$ nastává právě když je splněna aspoň (a potom pouze) jedna z následujících pěti podmínek:

(1) $a = b = c = 0$;
(2) $n = 1$, $c = 0$, $a = b \neq 0$;
(3) $n = -1$, $c = 0$, $a = -b \neq 0$;
(4) $n \geq 2$, $c = n - 1$, $a = b = -1$;
(5) $n \leq -2$, $c = -n - 1$, $a = -1$, $b = 1$.

Důkaz. Stačí zkombinovat předchozí tři lemmata. □

I.9.10 Proposice. Nechť $n = 2k + 1$, $k \geq 1$. Potom pro každé $m \geq 0$ existují jednoznačně určená celá čísla r a s taková, že $m = rn + s$, přičemž $r \geq 0$ a $-k \leq s \leq k$.

Důkaz. Podle I.9.1 existují nezáporná r_1 a s_1 tak, že $m = r_1 n + s_1$, $0 \leq s_1 < n$. Je-li $k + 1 \leq s_1$, pak $-k \leq s_1 - n = s < 0$ a $m = (r_1 + 1)n + s$. Tím je dokázána existence čísel r a s s danými vlastnostmi. Jednoznačnost čísel r, s se snadno ověří. □

I.9.11 Proposice. Nechť $n = 2k + 1$, $k \geq 1$. Potom pro každé $m \leq 0$ existují jednoznačně určená celá čísla r a s taková, že $m = rn + s$, přičemž $r \leq 0$ a $-k \leq s \leq k$.

Důkaz. Tvrzení plyne snadno z I.9.10, kde uvážíme celé číslo $-m$. □

I.9.12 Poznámka. Nechť $n = 2k - 1$, $k \leq -1$. Potom pro každé $m \in \mathbb{Z}$ existují jednoznačně určená čísla r a s taková, že $m = rn + s$, přičemž $k \leq s \leq -k$. Pro $m \geq 0$ je $r \leq 0$ a pro $m \leq 0$ je $r \geq 0$. (Použije se I.9.10, I.9.11, pro základ $-n = 2(-k) + 1$.)

I.9.13 Proposice. Nechť $n = 2k$, $k \geq 1$. Potom pro každé $m \geq 0$ existují jednoznačně určená celá čísla r a s taková, že $m = rn + s$, přičemž $r \geq 0$ a $-k + 1 \leq s \leq k$.

Důkaz. Podle I.9.1 existují nezáporná r_1 a s_1 tak, že $m = r_1 n + s_1$, $0 \leq s_1 < n$. Je-li $k + 1 \leq s_1$, pak $-k + 1 \leq s_1 - n = s < 0$ a $m = (r_1 + 1)n + s$. Tím je pak dokázána existence čísel r a s s danými vlastnostmi. Jednoznačnost čísel r, s se snadno ověří. □

I.9.14 Proposice. Nechť $n = 2k$, $k \geq 1$. Potom pro každé $m \leq 0$ existují jednoznačně určená čísla r a s taková, že $m = rn + s$, přičemž $r \leq 0$ a $-k \leq s \leq k + 1$.

Důkaz. Tvrzení plyne snadno z I.9.13, kde uvážíme číslo $-m$. □

I.9.15 Úloha. (i) Nechť $a, b, c, n \in \mathbb{Z}$, $n \geq 4$. Nalezneme číslo m takové, že $0 \leq m < n$, přičemž n nedělí žádné z čísel $a + m$, $b + m$, $c + m$.

Nechť $r_1 = [-a]_n$, $r_2 = [-b]_n$ a $r_3 = [-c]_n$ (I.9.4). Víme, že $0 \leq r_i \leq n-1$. Jelikož $3 \leq n - 1$, tak existuje m, $0 \leq m \leq n - 1$ a $m \neq r_1, r_2, r_3$. Nechť n dělí $a + m$. Potom n dělí $m - r_1$, neboť n dělí $-a - r_1$. Ovšem, $1 \leq |m - r_1|$, takže dostáváme spor. Tedy n nedělí $a + m$ a, symetricky, n nedělí $b + m$, n nedělí $c + m$. Navíc, je-li $k \geq 0$, pak n nedělí žádné z čísel $a + m + kn$, $b + m + kn$, $c + m + kn$. Čísel $m + kn$ je nekonečně mnoho.

(ii) Pro každé $m \in \mathbb{Z}$ platí, že 3 (popř. 2, 1) dělí aspoň jedno z čísel $1+m$, $2 + m$, $3 + m$.

(iii) Pro každé $m \in \mathbb{Z}$ platí, že číslo 4 dělí aspoň jedno z čísel $1 + m, 2 + m, 3 + m, 4 + m$.

I.9.16 Úloha. (i)Nechť $m \geq 2$ a $n \in \mathbb{Z}$. Dokážeme, že m dělí právě jedno z m po sobě jdoucích čísel $n, n + 1, \cdots, n + m - 1$.

Je to tak. Položme $s_i = [n + i]_m$ pro každé $i = 0, \cdots, m - 1$ (viz I.9.4). Je tedy $0 \leq s_i \leq m - 1$. Bylo-li by $s_i = s_j$, kde $0 \leq i \leq j \leq m - 1$, pak by $m|(n + j) - (n + i) = j - i$, kde $0 \leq s_i \leq m - 1$. Jelikož $m \geq 2$, pak $j - i = 0$, $j = i$. Nalezli jsme, že čísla $s_0, s_1, \cdots, s_{m-1}$ jsou vesměs různá. Je to m různých čísel z intervalu $0, 1, \ldots, m - 1$. Nebývá než to, že jedno z nich je rovno 0.

(ii) Předchozí tvrzení triviálně platí pro $m = 1$.

I.10 Trochu součtových vzorců

I.10.1 Pouze pro účely této zde přítomné sekce položíme $\alpha_k(n) = \sum_{i=1}^{n} i^k$ $(= \sum_{i=0}^{n} i^k)$ pro všechna $k \geq 1$ a $n \geq 1$. Pro úplnost ještě buď $\alpha_0(n) = \sum_{i=1}^{n} 1 = n$, $\alpha_k(0) = 0$ a $\alpha_0(0) = 0$.

Přímo z definice vidíme, že $\alpha_k(n+1) = \alpha_k(n) + (n+1)^k$ pro všechna $k \geq 0$, $n \geq 0$. Je také $\alpha_k(1) = 1$.

Není těžké vyrobit tuto tabulku:

n	1	2	3	4	5	6	7	8	9
$\alpha_1(n)$	1	3	6	10	15	21	28	36	45
$\alpha_2(n)$	1	5	14	30	55	91	140	204	285
$\alpha_3(n)$	1	9	36	100	225	441	784	1296	2025
$\alpha_4(n)$	1	17	98	354	979	2275	4676	8772	15333
$\alpha_5(n)$	1	33	276	1300	4425	12201	29008	61776	120825
$\alpha_6(n)$	1	65	794	4890	20515	67171	184820	446964	978405
$\alpha_7(n)$	1	129	2316	18700	96825	376761	1200304	3297456	8080425
$\alpha_8(n)$	1	257	6818	72354	462979	2142595	7907396	24684612	67731333

Všimněme si, že $\alpha_1(8) = 36 = 6^2 = \alpha_1(3)^2 = \alpha_3(3)$, $\alpha_1(2) + \alpha_1(2) = 6 = \alpha_1(3)$, $\alpha_1(4) + \alpha_1(9) = 55 = \alpha_1(10) = \alpha_2(5)$, $\alpha_1(5) + \alpha_1(14) = 120 = \alpha_1(15)$, $\alpha_2(24) = 4900 = 70^2$.

Z tabulky též vidíme, že $\alpha_3(n) = \alpha_1(n)^2$ pro všechna naše čísla $0 < n < 10$.

I.10.2 Věta. $\alpha_1(n) = \sum_{i=1}^{n} i = n(n+1)/2$ pro každé $n \geq 1 (\alpha_1(0) = 0 = 0 \cdot 1/2)$.

Důkaz. Aspoň jedno z čísel n, $n+1$ je sudé, takže 2 dělí $n(n+1)$ a $n(n+1)/2$ je celé číslo. Náš vzorec platí zcela zřejmě pro $n = 0, 1$ a dále postupujeme indukcí podle n.

Je $\alpha_1(n+1) = n+1+\alpha_1(n) = (2(n+1)+n(n+1))/2 = (n+2)(n+1)/2$ a je to! □

I.10.3 Pozorování. Chceme objevit vzorec pro čísla $\alpha_2(n)$. Čerpajíce poučení z I.10.2, hledejme tento vzorec ve tvaru $d\alpha_2(n) = an^3 + bn^2 + cn$, kde $a, b, c, d \in \mathbb{Z}$. Dosadíme-li $n = 1, 2, 3, 4$, pak dostaneme tyto čtyři rovnosti:

$$
\begin{aligned}
d &= a + b + c \\
5d &= 8a + 4b + 2c \\
14d &= 27a + 9b + 3c \\
30d &= 64a + 16b + 4c
\end{aligned}
$$

Postupným odečítáním zjistíme:

$$
\begin{aligned}
4d &= 7a + 3b + c \\
9d &= 19a + 5b + c \\
16d &= 37a + 7b + c \\
2d &= 6a \\
d &= 3a
\end{aligned}
$$

Po dosazení $3a$ za d do první čtyř rovností dostaneme:

$$
\begin{aligned}
2a &= b + c \\
7a &= 4b + 2c \\
15a &= 9b + 3c \\
26a &= 16b + c
\end{aligned}
$$

A opět odečítáme:

$$
\begin{aligned}
5a &= 3b + c \\
8a &= 5b + c \\
11a &= 7b + c \\
3a &= 2b \\
10b &= 15a = 9b + 3c \\
b &= 3c \\
a &= 2c
\end{aligned}
$$

Takže $d = 6c$, $a = 2c$, $b = 3c$. Odtud, $6c\alpha_2(n) = 2cn^3 + 3cn^2 + cn$. Pro $c \neq 0$ to znamená $6\alpha_2(n) = 2n^3 + 3n^2 + n = n(n+1)(2n+1)$.

I.10.4 Věta. $\alpha_2(n) = \sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$ pro každé $n \geq 1$ ($\alpha_2(0) = 0 = 0 \cdot 1 \cdot 1/6$).

Důkaz. Předně, aspoň jedno číslo z $n, n+1$ je sudé. Jestliže 3 nedělí n, 3 nedělí $n+1$, pak 3 dělí $n+2$, 3 dělí $2(n+2)-3 = 2n+1$. Tedy 6 dělí $n(n+1)(2n+1)$.

Vzorec jistě platí pro $n = 0, 1$. Dále indukcí podle n. Je $\alpha_2(n+1) = (n+1)^2+\alpha_2(n) = (6(n+1)^2+n(n+1)(2n+1))/6 = (n+1)(6n+6+2n^2+n)/6 = (n+1)(2n^2+7n+6)/6 = (n+1)(n+2)(2n+3)/6$ a je to! □

I.10.5 Věta. $\alpha_3(n) = \sum_{i=1}^{n} i^3 = n^2(n+1)^2/4 = \alpha_1(n)^2$ pro každé $n \geq 1$ ($\alpha_3(0) = \alpha_1(0) = 0$) .

Důkaz. Vzorec je inspirován tabulkou z I.10.1 a zřejmě platí pro $n = 0, 1$. Dále indukcí. Je $\alpha_3(n+1) = (n+1)^3 + \alpha_3(n) = (4(n+1)^3 + n^2(n+1)^2)/4 = (n+1)^2(4n+4+n^2)/4 = (n+1)^2(n+2)^2/4$. A je to! □

I.10.6 Pro $n \geq 1$ a $k \geq 1$ buď $\beta_k(n) = \sum_{i=1}^{n}(\sum_{j=1}^{i} j^k) = \sum_{i=1}^{n} \alpha_k(i)$ (opět značení pouze lokální). Pro úplnost buď $\beta_0(n) = n(n+1)/2 (= \alpha_1(n))$, $n \geq 1, \beta_k(0) = 0 = \beta_0(0), k \geq 1$).

I.10.7 Proposice. $\beta_k(n) = \sum_{i=0}^{n-1}(n-i)(i+1)^k$ pro všechna $n \geqq 1$ a $k \geq 0$.

Důkaz. Je-li $k = 0$, pak $\beta_0(n) = n(n+1)/2 = \sum_{i=1}^{n} i = \sum_{i=0}^{n-1}(n-i) = \sum_{i=0}^{n-1}(n-i)(i+1)^0$ (I.10.2). Je-li $n = 1$, pak $\beta_k(n) = \beta_k(1) = 1 = \sum_{i=0}^{0} 1 \cdot 1^k$. Buď tedy $n \geq 2$, $k \geq 1$. Pak $\beta_k(n) = \sum_{i=1}^{n}(1^k + 2^k + \cdots + i^k) = n1^k + (n-1)2^k + \cdots + 2(n-1)^k + n^k = \sum_{i=0}^{n-1}(n-i)(i+1)^k$. □

I.10.8 Proposice. $(n+1)\alpha_k(n) = \alpha_{k+1}(n) + \beta_k(n)$ pro všechna $n \geq 0$ a $k \geq 0$.

Důkaz. Snadno se přesvědčíme, že uvedený vzorec platí pro $n = 0, 1$. Nechť je $n \geq 2$. Podle I.10.7 je $\alpha_{k+1}(n) + \beta_k(n) = \sum_{i=0}^{n-1}(i+1)(i+1)^k + \sum_{i=0}^{n-1}(n-i)(i+1)^k = \sum_{i=0}^{n-1}(n+1)(i+1)^k = (n+1)\sum_{i=1}^{n} i^k = (n+1)\alpha_k(n)$. □

I.10.9 Proposice. $\beta_1(n) = n(n+1)(n+2)/6$ pro všechna $n \geq 0$.

Důkaz. Vzorec platí pro $n = 0$. Nechť $n \geq 1$. Je $\alpha_1(n) = n(n+1)/2$ a $\alpha_2(n) = n(n+1)(2n+1)/6$ podle I.10.2 a I.10.4. Z I.10.8 nyní máme $6\beta_1(n) = 3n(n+1)^2 - n(n+1)(2n+1) = n(n+1)(3n+3-2n-1) = n(n+1)(n+2)$. □

I.10.10 Proposice. $\beta_2(n) = n(n+1)^2(n+2)/12 (= (n+1)\beta_1(n)/2)$ pro každé $n \geq 0$.

Důkaz. Vzorec platí pro $n = 0$. Nechť $n \geq 1$. Z I.10.8, I.10.4 a I.10.5 plyne $12\beta_2(n) = 12(n+1)\alpha_2(n) - 12\alpha_3(n) = 2n(n+1)^2(2n+1) - 3n^2(n+1)^2 = n(n+1)^2(4n+2-3n) = n(n+1)^2(n+2)$. □

I.10.11 Poznámka. Čísla $\alpha_1(n)$ jsou známá pod názvem trojúhelníková čísla (nebo triangulární čísla). Čísla $\beta_1(n)$ pak můžeme nazývat čtyřstěnná (tetrahedrální).

Všimněme si, že $\beta_1(2) = 4 = 2^2$, $\beta_1(48) = 19600 = 140^2$, $\alpha_1(1) = 1 = \beta(1)$, $\alpha_1(4) = 10 = \beta_1(3)$, $\alpha_1(15) = 120 = \beta_1(8)$, $\alpha_1(55) = 1540 = \beta_1(20)$, $\alpha_1(119) = 7140 = \beta_1(34)$.

I.10.12 Cvičení. Nechť $n \geq 2$. Uvažme součet všech sudých čísel mezi 2 a n (včetně). Je-li n sudé, pak tento součet je $\sum_{i=1}^{n/2} 2i = 2\sum_{i=1}^{n/2} i = 2\alpha_1(n/2) = (n/2)((n/2)+1) = n(n+2)/4$ podle I.10.2. Je-li n liché, pak tento součet je $\sum_{i=1}^{(n-1)/2} 2i = 2\sum_{i=1}^{(n-1)/2} i = 2\alpha((n-1)/2) = ((n-1)/2)((n-1)/2)+1) = (n-1)(n+4)/4$.

I.10.13 Cvičení. Nechť $n \geq 1$. Uvažme součet všech lichých čísel mezi 1 a n (včetně). Je-li n liché, pak tento součet je $\sum_{i=0}^{(n-1)/2}(2i+1) = 2\sum_{i=0}^{(n-1)/2} i + \sum_{i=0}^{(n-1)/2} 1 = 2\alpha_1((n-1)/2)+(n+1)/2 = ((n-1)/2)((n+1)/2)+(n+1)/2 = (n+1)^2/4$. Je-li n sudé, pak tento součet je $\sum_{i=0}^{(n-2)/2}(2i+1) = 2\sum_{i=0}^{(n-2)/2} i + \sum_{i=0}^{(n-2)/2} 1 = 2\alpha((n-2)/2) + n/2 = (n-2)/2)(n/2) + (n/2) = n^2/4$.

I.10.14 Cvičení. Nechť $n \geq 1$. Součet prvních n kladných sudých čísel je $\sum_{i=1}^{n} 2i = n(n+1)$. Součet prvních n kladných lichých čísel je $\sum_{i=0}^{n-1}(2i+1) = n^2$.

I.10.15 Lemma. Nechť $m \geq 0$. Pro každé $n \in \mathbb{Z}$ platí:

(i) $n-1$ dělí $n^{m+1}-1$.
(ii) Je-li $n \neq 1$, pak $\sum_{i=0}^{m} n^i = (n^{m+1}-1)/(n-1)$.
(iii) Je-li $n \neq 1$, pak $\sum_{i=1}^{m} n^i = (n^{m+1}-n)/(n-1)$.
(iv) Je-li $n = 1$, pak $\sum_{i=0}^{m} n^i = m+1$ a $\sum_{i=1}^{m} n^i = m$.

Důkaz. Předně, $n^{m+1}-1 = (n-1)a$, $a = 1+n+\cdots+n^m$. Je-li $n \neq 1$, tak $b = n-1 \neq 0$, $c = (n^{m+1}-1)/b \in \mathbb{Z}$, $bc = ba$, $c = a$. Zbytek je jasný. □

I.10.16 Cvičení. (i) Nechť $n \geq 2$. Uvažme součet všech druhých mocnin sudých čísel mezi 2 a n (včetně).

Je-li n sudé, pak tento součet je $\sum_{i=0}^{n/2}(2i)^2 = 4\sum_{i=0}^{n/2} i^2 = 4\alpha_2(n/2) = 4(n/2)(((n+2)/2)(n+1))/6 = n(n+1)(n+1)/6$.

Je-li n liché, pak je tento součet $(n-1)n(n+2)/6$ (což plyne snadno z předchozího).

(ii) Nechť $n \geq 1$. Součet druhých mocnin prvních n kladných sudých čísel je $2n(n+1)(2n+1)/3$.

I.10.17 Cvičení. (i) Nechť $n \geq 1$. Uvažme součet všech druhých mocnin lichých čísel mezi 1 a n (včetně).

Je-li n liché, pak je tento součet $(n(n+1)(2n+1) - (n-1)n(n+1))/6 = n(n+1)(n+2)/6$.

Je-li n sudé, pak je tento součet $(n-1)n(n+1)/6$.

(ii) Nechť $n \geq 1$. Součet druhých mocnin prvních n kladných lichých čísel je $n(2n-1)(2n+1)/3$.

I.10.18 Cvičení. (i) Nechť $n \geq 2$. Uvažme součet všech třetích mocnin sudých čísel mezi 2 a n (včetně).

Je-li n sudé, pak tento součet je $\sum_{i=0}^{n/2}(2i)^3 = 8\sum_{i=0}^{n/2} i^3 = 4\alpha_1(n/2)^2 = n^2(n+2)^2/8$.

Je-li n liché, pak je tento součet je $(n-1)^2(n+1)^2/8$.

(ii) Nechť $n \geq 1$. Součet třetích mocnin prvních n kladných sudých čísel je $2n^2(n+1)^2$.

I.10.19 Cvičení. (i) Nechť $n \geq 1$. Uvažme součet všech třetích mocnin lichých čísel mezi 1 a n (včetně).

Je-li n liché, pak je tento součet $n^2(n+1)^2/4 - (n-1)^2(n+1)^2/8 = (n+1)^2(n^2+2n-1)/8$.

Je-li n sudé, pak tento součet je $n^2(n^2-2)/8$.

(ii) Nechť $n \geq 1$. Součet třetích mocnin prvních n kladných lichých čísel je $n^2(2n^2-1) = 2n^4 - n^2$. Je však $2n^4 - n^2 = 2n^2(2n^2-1)/2 = \alpha_1(2n^2-1)$, což je trojúhelníkové číslo (I.10.11).

I.11 Jeden rozdílový vzorec

I.11.1 Pro účely této sekce definujme čísla $\alpha_m(a,n)$, $n,m \in \mathbb{N}_0$, $a \in \mathbb{Z}$. A sice následujícím rekurentním způsobem: $\alpha_0(a,n) = a^n$ a $\alpha_{m+1}(a,n) = \alpha_m(a+1,n) - \alpha_m(a,n)$ pro každé $m \geq 0$.

Ihned vidíme, že $\alpha_1(a,n) = (a+1)^n - a^n$, $\alpha_2(a,n) = (a+2)^n - 2(a+1)^n + a^n$.

I.11.2 Lemma. $\alpha_{m+1}(a,n+1) = (a+m+1)\alpha_{m+1}(a,n) + (m+1)\alpha_m(a,n)$.

Důkaz. Postupujeme indukcí podle $m \geq 0$. Pro $m = 0$ je $\alpha_1(a,n+1) = (a+1)^{n+1} - a^{n+1} = (a+1)^n(a+1) - a^n(a+1) + a^n = (a+1)((a+1)^n - a^n)) + a^n = (a+1)\alpha_1(a,n) + \alpha_0(a,n)$. Dále pak je $\alpha_{m+2}(a,n+1) = \alpha_{m+1}(a+1,n+1) - \alpha_{m+1}(a,n+1) = (a+m+2)\alpha_{m+1}(a+1,n) + (m+1)\alpha_m(a+1,n) - (a+m+1)\alpha_{m+1}(a,n) - (m+1)\alpha_m(a,n) = (a+m+2)(\alpha_{m+1}(a+1,n) - \alpha_{m+1}(a,n)) - \alpha_{m+1}(a,n) + (m+1)(\alpha_m(a+1,n) - \alpha_m(a,n)) = (a+m+2)\alpha_{m+2}(a,n) + (m+2)\alpha_{m+1}(a,n)$.

Při tomto výpočtu jsme použili indukční krok a definici čísel $\alpha_m(a,n)$. □

I.11.3 Věta. Pro všechna $n \in \mathbb{N}_0$, $a \in \mathbb{Z}$ je $\alpha_n(a,n) = n!$ a $\alpha_{n+1}(a,n) = 0$.

Důkaz. S použitím I.11.2 budeme postupovat indukcí podle $n \geq 0$. Pro $n = 0$ je zřejmě $\alpha_0(a,0) = a^0 = 1 = 0!$ a $\alpha_1(a,0) = (a+1)^0 - a^0 = 1 - 1 = 0$. Dále pak $\alpha_{n+1}(a,n+1) = (a+n+1)\alpha_{n+1}(a,n) + (n+1)\alpha_n(a,n) = (n+1)n! = (n+1)!$ podle I.11.2 a indukčního předpokladu. Podobně $\alpha_{n+2}(a,n+1) = \alpha_{n+1}(a+1,n+1) - \alpha_{n+1}(a,n+1) = (n+1)! - (n+1)! = 0$. □

I.11.4 Lemma. Nechť $t,n \in \mathbb{N}$, $a,b \in \mathbb{Z}$ jsou taková čísla, že t dělí $(a+i)^n + b$ pro všechna $i = 0,1,\ldots,n$. Potom t dělí $n!$. Navíc, je-li t prvočíslo, pak $t \leq n$.

Důkaz. Tvrzení je snadno nahlédnutelné pro $n = 1$, takže předpokládejme, že $n \geq 2$.

Nejdříve si všimněme, že $\alpha_1(a+i,n) = (a+i+1)^n - (a+i)^n = ((a+i+1)^n + b) - ((a+i)^n + b)$, čili t dělí $\alpha_1(a+i,n)$ pro $i = 0,1,\ldots,n-1$. Buď nyní j takové, že $1 \leq j < n$ a t dělí $\alpha_j(a+i,n)$ pro $i = 0,1,\ldots n-j$. Opět, $\alpha_{j+1}(a+i,n) = \alpha_j(a+i+1,n) - \alpha_j(a+i,n)$ pro $0 \leq i \leq n-j-1$. Tímto postupem se dostaneme až k $j = n-1$, a tak t dělí $\alpha_n(a,n) = n!$ (I.11.3). □

I.11.5 Pozorování. Nechť $t,n \in \mathbb{N}$ jsou taková čísla, že $n \geq 2$ a t dělí všechna čísla $2^n - 1$, $3^n - 1, \ldots, (n+1)^n - 1$. Samozřejmě t dělí $0 = 1^n - 1$ a z I.11.4 plyne, že t dělí $n!$. Je-li navíc t prvočíslo, pak $t \leq n$. Ve skutečnosti $t < n$, neboť p nedělí $2^p - 1$ pro žádné prvočíslo p.

Jako příklad na tuto situaci zvolme $t = p$, p prvočíslo, $p \geq 5$, $2 \leq n \leq p-2$. Potom $p \not\leq n$, čili p nedělí $k^n - 1$ pro aspoň jedno k, $2 \leq k \leq n+1 (\leq p-1)$. Kdybychom zvolili $n = p-1$, pak sice $p \not\leq n$, avšak ihned vidíme, že p nedělí $k^n - 1$ pro $k = p = n+1$. Ovšem p dělí $k^{p-1} = k^n - 1$ pro $1 \leq k \leq p-1 = n$.

I.12 Rozmanité užitečné (algebraické) rovnosti

V této sekci shromáždíme bez ladu a skladu různé algebraické rovnosti platné v oboru $\mathbb{Z}$ celých čísel. Všechny tyto rovnosti se ověří snadným přímým výpočtem.

I.12.1 První skupina rovností.

(1) $a^2 - b^2 = (a-b)(a+b)$;
(2) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$, $n \geq 2$;
(3) $a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n)$, $n \geq 0$;
(4) $a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n})$, $n \geq 1$.

Kombinací rovnosti (2) a (3) dostaneme:

(5) $a^{2n} - b^{2n} = (a-b)(a^n + b^n)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$ pro $n \geq 2$.

Kombinací (5) a (4) dostaneme:

(6) $a^{4n+2} - b^{4n+2} = (a-b)(a+b)(a^{2n} + a^{2n-1}b + \cdots + ab^{2n-1} + b^{2n})(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n})$ pro $n \geq 1$.

Zvolíme-li $n = 1$, pak z (6) plyne:

(7) $a^6 - b^6 = (a-b)(a+b)(a^2 + ab + b^2)(a^2 - ab + b^2)$.

Např. pro $a = 101$, $b = 96$ dostaneme rozklad $101^6 - 96^6 = 5 \cdot 197 \cdot 29113 \cdot 9721 (= 5 \cdot 7 \cdot 197 \cdot 4159 \cdot 9721$, což je prvočíselný rozklad); je $101^6 - 96^6 = 278762360905$. Pro $a = 14$, $b = 11$ dostaneme $14^6 - 11^6 = 3 \cdot 25 \cdot 471 \cdot 163 (= 3^2 \cdot 5^2 \cdot 157 \cdot 163$, což je prvočíselný rozklad).

I.12.2 Druhá skupina rovností.

V rovnostech z I.12.1 položme $b = 1$. Dostaneme:

(1) $a^2 - 1 = (a-1)(a+1)$;
(2) $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, $n \geq 2$;
(3) $a^{2n} - 1 = (a^n - 1)(a^n + 1)$, $n \geq 0$;
(4) $a^{2n+1} + 1 = (a+1)(a^{2n} - a^{2n-1} + \ldots - a + 1)$;
(5) $a^{2n} - 1 = (a-1)(a^n + 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, $n \geq 1$;
(6) $a^{4n+2} - 1 = (a-1)(a+1)(a^{2n} + a^{2n-1} + \cdots + a + 1)(a^{2n} - a^{2n-1} + \ldots - a + 1)$ pro $n \geq 1$;
(7) $a^6 - 1 = (a-1)(a+1)(a^2 + a + 1)(a^2 - a + 1)$.

Například pro $a = 101$ dostaneme rozklad $101^6 - 1 = 100 \cdot 102 \cdot 10303 \cdot 10101 (= 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 37 \cdot 10303$, což je prvočíselný rozklad). Je $101^6 - 1 = 10161520150600$.

I.12.3 Třetí skupina rovností. A nyní budiž $a = 2$ a $b = 1$. Potom:

(1) $3 = 2^2 - 1 = (2-1)(2+1)$;
(2) $2^n - 1 = 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 = \sum_{i=0}^{n-1} 2^i$ pro $n \geq 1$;
(3) $2^{2n} - 1 = (2^n - 1)(2^n + 1)$ pro $n \geq 0$;

(4) $2^{2n+1}+1 = 3(2^{2n}-2^{2n-1}+\cdots+4-2+1) = 3(2^{2n-1}+2^{2n-3}+\cdots+2+1)$ pro $n \geq 0$;
(5) $2^{2n}-1 = (2^n+1)(2^{n-1}+2^{n-2}+\cdots+2+1)$ pro $n \geq 1$;
(6) $2^{4n+2}-1 = 3(2^{2n}+2^{2n-1}+\cdots+2+1)(2^{2n}-2^{2n-1}+\ldots-2+1) = 3(2^{2n+1}-1)(2^{2n-1}+2^{2n-3}+\cdots+2+1)$ pro $n \geq 1$;
(7) $(63 =)2^6-1 = 3\cdot 7\cdot 3$.

Rovnost (2) můžeme přepsat takto:
(2a) $2^n = 2+\sum_{i=1}^{n-1} 2^i$, $n \geq 1$;
(2b) $2(2^n-1) = \sum_{i=1}^{n} 2^i$, $n \geq 0$.

Z (6) plyne, že $2^{58}-1 = 3(2^{29}-1)m$, $m = 2^{27}+2^{25}+2^{23}+\cdots+2^5+2^3+1 = 5(2^{25}+2^{21}+2^{17}+2^{13}+2^9+2^5+2)+1 = 5\cdot 17(2^{21}+2^{13}+2^5)+11 = 5\cdot 17\cdot 257\cdot 2^{13}+5\cdot 17\cdot 32+11 = 2720(257\cdot 256+1)+11 = 2720(2^{16}+257)+11 = 2720\cdot 65793+11 = 178956971$. Tedy $2^{58}-1 = 3\cdot 536870911\cdot 178956971 (= 288230376151711743)$. Je $2^{58}-1 = 3\cdot 59\cdot 73\cdot 233\cdot 1103\cdot 2089\cdot 4153$ (prvočíselný rozklad).

I.12.4 Příklad. (i) Každé (prvo)číslo p lze psát triviálně ve tvaru $p = (p+1)-1$ a $p = (p-1)+1$, tedy ve tvaru $a-b$ a $c+d$, kde a, b, c, d jsou kladná celá čísla.

(ii) Každé liché (prvo)číslo $p = 2k+1$ lze psát triviálně ve tvaru $p = (k+1)^2-k^2$, tedy ve tvaru a^2-b^2, kde a, b jsou kladná celá čísla ($a = 1, b = 0$ pro $k = 0$). Na druhé straně, $2 \neq a^2-b^2$ pro všechna $a, b \in \mathbb{Z}$ (plyne snadno z I.12.1(1)). Otázkou, která prvočísla p lze psát ve tvaru $p = a^2+b^2$ se budeme zabývat později. Například $3 \neq a^2+b^2$ pro všechna $a, b \in \mathbb{Z}$, $2 = 1^2+1^2$, $5 = 1^2+2^2$.

(iii) Z I.12.1(2) (pro $n = 3$) snadno plyne, že je-li $p = a^3-b^3$ prvočíslo pro nějaká $a, b \in \mathbb{N}_0$, pak $b \geq 1$, $a = b+1$ a $p = 3b^2+3b+1$. Pro $b = 1$ dostáváme $p = 7$, pro $b = 2$ je $p = 19$, pro $b = 3$ je $p = 37$, pro $b = 4$ je $p = 61$ a čísla $7, 19, 37, 61$ jsou vskutku prvočísla. Ovšem $3\cdot 5^2+3\cdot 5+1 = 91 = 7\cdot 13$ již prvočíslo není. Zato však $3\cdot 6^2+3\cdot 6+1 = 127$ je opět prvočíslo.

(iv) Nechť $a, b \in \mathbb{N}_0$ jsou taková čísla, že $p = a^3+b^3$ je prvočíslo. Je ihned patrné, že $a \neq 0 \neq b$. Je-li $a = b$, pak $p = 2a^3$, a tedy $a = 1$, $p = 2 = 1^3+1^3$. Předpokládejme nyní, že $a > b$. Je $a^2-ab+b^2 = a(a-b)+b^2 \geq a+b^2 \geq 2$ a z I.12.1(4) (kde $n = 1$) plyne, že $a+b = 1$, což není možné. Takže jediné prvočíslo p tvaru a^3+b^3, $a, b \in \mathbb{N}_0$ je $p = 2 = 1^3+1^3$. Samozřejmě, $7 = 2^3+(-1)^3$ (viz též (iii)).

(v) Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $p = a^4-b^4$ je prvočíslo. Můžeme předpokládat, že a, b jsou kladná čísla, $a > b$. Je $p = (a-b)(a+b)(a^2+b^2)$, a tak $a = b+1$, $a+b = 2b+1 \geq 3$, $a^2+b^2 \geq 5$. Závěr je, že $p \neq a^4-b^4$ pro všechna prvočísla p, $a, b \in \mathbb{Z}$ (např. $2^4-1^4 = 15 = 3\cdot 5$).

(vi) $2 = 1^4+1^4$, $17 = 1^4+2^4$, $257 = 1^4+4^4$, $1297 = 1^4+6^4$, $4097 = 1^4+8^4$

(2, 17 , 1297 jsou prvočísla a $4097 = 17 \cdot 241$). Dále $17 = 2^4+1^4$, $97 = 2^4+3^4$, $641 = 2^4+5^4$, $2417 = 2^4+7^4$, $6577 = 2^4+9^4$, $14657 = 2^4+11^4$ jsou prvočísla. Ovšem $2^4 + 13^4 = 28577 = 17 \cdot 41^2$.

(vii) $31 = 2^5 - 1^5$ je prvočíslo a $3 \cdot 341 = 1023 = 4^5 - 1^5$ je prvočíslo. $211 = 3^5 - 2^5$ je prvočíslo.

(viii) Stejným postupem jako v (iv) zjistíme, že jediné prvočíslo p tvaru $p = a^5 + b^5$, kde $a, b \in \mathbb{N}_0$, je $p = 2 = 1^5 + 2^5$. Ovšem, $31 = 2^5 + (-1)^5$ je prvočíslo (viz též (vii)).

(ix) Z I.12.1(7) plyne, že $p \neq a^6 - b^6$ pro všechna prvočísla p, $a, b \in \mathbb{Z}$.

I.12.5 Z I.12.2(2) ihned plyne, že:

(1) $a^{mn} - 1 = (a^m - 1)(a^{m(n-1)} + a^{m(n-2)} + \cdots + a^m + 1)$;

(2) $a^{mn} - 1 = (a^n - 1)(a^{n(m-1)} + a^{n(m-2)} + \cdots + a^1 + 1)$ pro všechna $a \in \mathbb{Z}$, $m, n \in \mathbb{N}_0$.

Například pro $m = 2$, $m = 5$ dostaneme $a^{10} - 1 = (a^2 - 1)(a^8 + a^6 + a^4 + a^2 + 1)(= (a+1)(a-1)(a^8 + a^6 + a^4 + a^2 + 1))$, $a^{10} - 1 = (a^5 - 1)(a^5 + 1)$. Pro $a = 4$ máme $2^{20} - 1 = 3 \cdot 69905$ a $2^{20} - 1 = 1023 \cdot 1025$. Snadno nalezneme, že $2^{20} - 1 = 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41 (= 1048575)$ je prvočíselný rozklad.

I.12.6 Z I.12.2(4) ihned plyne, že:

(1) $a^{2nm+m} + 1 = (a^m + 1)(a^{2nm} - a^{(2n-1)m} + \ldots - a^m + 1)$, $n \geq 1$, $m \geq 0$;

(2) $a^{4mn+2m+2n+1} + 1 = (a + 1)(a^{2m} - a^{2m-1} + \ldots - a + 1)(a^{4mn+2n} - a^{4mn+2n-2m-1} + a^{4mn+2n-4m-2} - \ldots - a^{2m+1} + 1)$, $n \geq 1$, $m \geq 0$.

Rovnost (2) jsme odvodili z rovnosti (1), kde místo m se napíše $2m + 1$ a rozloží se výraz $a^{2m+1} + 1$. Všimněme si, že ve výrazu $a^{4nm+2n-2m-1}$ je role čísel n a m symetrická.

Zvolme $n = 1 = m$. Z (2) plyne rozklad $a^9 + 1 = (a + 1)(a^2 - a + 1)(a^6 - a^3 + 1)$. Je-li $a = 32 = 2^5$, pak $2^{45} + 1 = 33 \cdot 993 \cdot 1073709057 = 3^3 \cdot 11 \cdot 19 \cdot 331 \cdot 18837001$ (jde o prvočíselný rozklad).

A teď buď $n = m = a = 2$. Pak $2^{25} + 1 = 3 \cdot 11 \cdot (2^{20} - 2^{15} + 2^{10} - 2^5 + 1)$
$= 3 \cdot 11 \cdot (2^{15}(2^5 - 1) + 2^5(2^5 - 1) + 1)$
$= 3 \cdot 11 \cdot ((2^5 - 1)(2^{15} + 2^5) + 1)$
$= 3 \cdot 11 \cdot (31 \cdot (2^{15} + 2^5) + 1)$
$= 3 \cdot 11 \cdot (31 \cdot 32 \cdot (2^{10} + 1) + 1)$
$= 3 \cdot 11 \cdot (31 \cdot 32 \cdot 1025 + 1)$
$= 3 \cdot 11 \cdot 10168001 = 3 \cdot 11 \cdot 251 \cdot 4051$ (prvočíselný rozklad).
Je $33554433 = 11 \cdot 101 \cdot 30203$ (opět prvočíselný rozklad).

I.12.7 Následující rovnosti jsou velmi podnětné:

(1) $a^4 + 4 = (a^2 + 2a + 2)(a^2 - 2a + 2)$;

(2) $a^{4n} + 4 = (a^{2n} + 2a^n + 2)(a^{2n} - 2a^n + 2)$, $n \geq 0$;

(3) $a^{4n} + 4b^{4n} = (a^{2n} + 2a^n b^n + 2b^{2n})(a^{2n} - 2a^n b^n + 2b^{2n})$, $n \geq 0$;

(4) $a^{4n} + 2^{4n+2} = (a^{2n} + 2^{n+1}a^n + 2^{2n+1})(a^{2n} - 2^{n+1}a^n + 2^{2n+1})$, $n \geq 0$;
(5) $a^4 + 64 = (a^2 + 4a + 8)(a^2 - 4a + 8)$;
(6) $a^8 + 1024 = (a^4 + 8a^2 + 32)(a^4 - 8a^2 + 32)$;
(7) $4a^{4n} + 1 = (2a^{2n} + 2a^n + 1)(2a^{2n} - 2a^n + 1)$, $n \geq 0$;
(8) $2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1)$, $n \geq 0$;
(9) $a^{4n+2} + (2-a)a^{2n+1} + 1 = (a^{2n+1} + a^{n+1} + 1)(a^{2n+1} - 2^{n+1} + 1)$, $n \geq 0$;
(10) $3^{4n+2} - 3^{2n+1} + 1 = (3^{2n+1} + 1 = (3^{2n+1} + 3^{n+1} + 1)(3^{2n+1} - 3^{n+1} + 1)$, $n \geq 0$.

Rovnost (7) plyne z (3) pro $a = 1$. Uveďme si několik příkladů. V (1) buď $a = 9$. Tedy $3^8 + 4 = 65 \cdot 101 = 5 \cdot 13 \cdot 101 (= 6565)$. Podobně, $3(3^{15} + 1) + 1 = 3^{16} + 4 = 6725 \cdot 6401 = 5^2 \cdot 269 \cdot 6401 = 5^2 \cdot 269 \cdot 6401 = 5^2 \cdot 37 \cdot 173 \cdot 269 (= 43046725)$. V (4) volme $a = 3$ a $n = 2$. Pak $3^8 + 2^{10} = (81 + 72 + 32)(81 - 72 + 32) = 185 \cdot 41 = 5 \cdot 37 \cdot 41 (= 7585)$. Podle (10) je $3^{15}(3^{15} - 1) + 1 = 3^{30} - 3^{15} + 1 = (3^{15} + 3^8 + 1)(3^{15} - 3^8 + 1) = 14413469 \cdot 14400347 = 7 \cdot 13 \cdot 19 \cdot 173 \cdot 337 \cdot 3359$ (prvočíselný rozklad). Podle (8) je $2^{58} + 1 = (2^{29} + 2^{15} + 1)(2^{29} - 2^{15} + 1) = 536903681 \cdot 536838145 = 5 \cdot 107367629 \cdot 536903681$ (prvočíselný rozklad).
(11) $(3ab^2 - a^3)^2 + (3a^2b - b^3)^2 = (a^2 + b^2)^3 (= 3a^2b^4 + 3a^4b^2 + a^6 + b^6)$;
(12) $(2a^2 + 2a)^2 + (2a + 1)^2 = (2a^2 + 2a + 1)^2$;
(13) $((8a^4 - 1)^2 - 1)^2 + (2a)^{12} = ((8a^4 + 1)^2 - 1)^2$;
(14) $(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$;
(15) $(8a^3 - 32a)^2 + (a^4 - 24a^2 + 16)^2 = (a^2 + 4)^4$;
(16) $(a + b + c)^3 = 3(a + b)(a + c)(b + c) + a^3 + b^3 + c^3$;
(17) $(9a^4)^3 + (9a^3 + 1)^3 = (9a^4 + 3a)^3 + 1 (= 3^6a^{12} + 3^6a^9 + 3^5a^6 + 3^3a^3 + 1)$; např. $9^3 + 10^3 = 1729 = 12^3 + 1^3$ a $144^3 + 73^3 = 160^3 + 1^3 = 12^6 + 73^3$).

I.12.8 Příklad. Nechť $a \in \mathbb{Z}$, $n \geq 0$ jsou taková čísla, že $p = a^{4n} + 4$ je prvočíslo. Je jistě $a \neq 0$ a můžeme předpokládat, že $a \geq 1$. Pro $a = 1$ dostáváme $p = 5$. Pro $n = 0$ dostáváme opět $p = 5$. Nechť tedy $a \geq 2$ a $n \geq 1$. Podle I.12.7(2) je $p = (a^{2n} + 2a^n + 2)(a^{2n} - 2a^n + 2)$. Je $a^{2n} - 2a^n + 2 \geq 10$, čili $a^{2n} - 2a^n + 2 = 1$, $a^{2n} - 2a^n + 1 = 0$, $a^n(a^n - 2) = -1$, což je ve sporu s $a \geq 2$. Takže jediné prvočíslo p tvaru $p = a^{4n} + 4$ je $p = 5$.

I.12.9 A teď další rovnosti.
(1) $a^{20} - a^{10} + 1 = (a^4 - a^2 + 1)(a^{16} + a^{14} - a^{10} - a^8 - a^6 + a^2 + 1)$;
(2) $a^n(a^n - 1) - 2 = (a^n - 2)(a^n + 1) = a^{2n} - a^n - 2, n \geq 0$;
(3) $a^{20} - a^{10} - 2 = (a^{10} - 2)(a^{10} + 1)$;
(4) $a^n(a^n + 1) - 2 = (a^n + 2)(a^n - 1) = a^{2n} + a^n - 2, n \geq 0$;
(5) $a^{20} + a^{10} - 2 = (a^{10} + 2)(a^{10} - 1)$;
(6) $((2a^2+2a)^2-1)^2+((2a+1)^2-1)^2 = ((2a^2+2a)^2+1)^2$; je-li $b = 2a^2+2a$, pak $2b = (2a + 1)^2 - 1, (b^2 - 1)^2 + 4b^2 = (b^2 + 1)^2$;

(7) $(a^2+b^2+c^2)^3 = a^2(3c^2-a^2-b^2)^2+b^2(3c^2-a^2-b^2)^2+c^2(c^2-3a^2-3b^2)^2 = a^2(a^2+b^2-3c^2)^2+b^2(a^2+b^2-3c^2)^2+c^2(3a^2+3b^2-c^2)^2$ (tato rovnost se nazývá Catalanova rovnost).

I.12.10 Legendreova identita (či rovnost).

(1) $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$;

(2) $(a^2+nb^2)(c^2+nd^2) = (ac+nbd)^2+n(ad-bc)^2$ pro všechna $n \in \mathbb{Z}$.

I.12.11 Eulerova identita.

(1) $(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2+(a_1b_3-a_3b_1+a_4b_2-a_2b_4)^2+(a_1b_4-a_4b_1+a_2b_3-a_3b_2)^2$.

Roznásobíme-li levou stranu rovnosti, získáme součet $\sum a_i^2b_j^2$, $1 \le i,j \le 4$, což je součet 16 sčítanců. Všechny tyto sčítance se objeví na straně pravé. Mimo to však na pravé straně se vyskytuje 36 sčítanců tvaru $\pm 2a_ia_jb_kb_l$, $i < j$. $k < l$. Upevníme-li na chvíli indexy i,j a vytkneme-li výraz $\pm 2a_ia_j$ před závorku, dostaneme výrazy $\pm 2a_1a_2(b_1b_2-b_2b_1-b_3b_4+b_4b_3)$, $\pm 2a_1a_3(b_1b_3+b_2b_4-b_3b_1-b_4b_2)$, $\pm 2a_1a_4(b_1b_4-b_2b_3+b_3b_2-b_4b_1)$, $\pm 2a_2a_3(b_2b_3-b_1b_4+b_1b_4-b_3b_2)$, $\pm 2a_2a_4(b_2b_4+b_1b_3-b_2b_4-b_1b_3)$, $\pm 2a_3a_4(b_3b_4-b_4b_3-b_1b_2+b_1b_2)$. Ve všech těchto případech ovšem získáváme pouze číslo 0.

I.12.12 Degenova identita.

(1) $(a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2+a_8^2)(b_1^2+b_2^2+b_3^2+b_4^2+b_5^2+b_6^2+b_7^2+b_8^2) = (a_1b_1-a_2b_2-a_3b_3-a_4b_4-a_5b_5-a_6b_6-a_7b_7-a_8b_8)^2+(a_1b_2+a_2b_1+a_3b_4-a_4b_3+a_5b_6-a_6b_5-a_7b_8+a_8b_7)^2+(a_1b_3-a_2b_4+a_3b_1+a_4b_2-a_5b_7+a_6b_8-a_7b_5-a_8b_6)^2+(a_1b_4+a_2b_3-a_3b_2+a_4b_1+a_5b_8-a_6b_7+a_7b_6-a_8b_5)^2+(a_1b_5-a_2b_6-a_3b_7-a_4b_8+a_5b_1+a_6b_2+a_7b_3+a_8b_4)^2+(a_1b_6+a_2b_5-a_3b_8+a_4b_7-a_5b_2+a_6b_1-a_7b_4+a_8b_3)^2+(a_1b_7+a_2b_8+a_3b_5-a_4b_6-a_5b_3+a_6b_4+a_7b_1-a_8b_2)^2+(a_1b_8-a_2b_7+a_3b_6+a_4b_5-a_5b_4-a_6b_3+a_7b_2+a_8b_1)^2$.

Tuto rovnost objevil dánský matematik Carl Ferdinand Degen (1766–1825) okolo roku 1818. Německý matematik Adolf Hurwitz (1859–1919) dokázal roku 1898, že podobné rovnosti neexistují pro jiný počet druhých mocnin nežli 1, 2, 4 a 8 ($a^2b^2 = (ab)^2$, I.12.10(1), I.12.11(1), I.12.12(1)).

Kapitola II

Dělitelnost

II.1 Relace dělitelnosti

II.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 binární relace je to vlastně množina příslušných dvojic celých čísel. Tato relace má řadu vlastností.

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

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

Je $1, 2, 4, 7, 8, 53, 56 \mid 5936$, neb $5936 = 2^4 \cdot 7 \cdot 53$. Ovšem $0, 3, 5, 6, 9, 59 \nmid 5936$.

II.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. □

II.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) $n = 1 \cdot n = (-1) \cdot (-n)$. □

II.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 $n \mid 1$ anebo $n \mid -1$ pak $n = \pm 1$.

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

II.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 $n = m$ anebo $n = -m$ (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 $m = n$, anebo $k = -1$ 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 $n \mid\mid m$. □

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

II.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 $n \mid m$. □

II.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 $n = -1$.

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

II.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 II.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 $\mid$ 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 $(1 =)n^0, (n =)n^1, n^2, n^3, \ldots$ je ostře rostoucí v obou uspořádáních $\mid$ 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 $\{0, 2, 3, \ldots\} = \mathbb{N}_0 \setminus 1$ existuje mnoho. Říkáme jim prvočísla.

II.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 II.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 I.9.3 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 $m = 1m = rm = (a_1q + b_1n)m = a_1mq + b_1nm$. 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 $t = \pm 1$. □

II.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 II.1.11(iv) předpokládat, že $q \neq 0$.

II.1.13 Definice. Celé číslo q nazveme (multiplikativně) nerozložitelné, neboli ireducibilní, jestliže $q \neq \pm 1$ a q splňuje ekvivalentní podmínky II.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 $2, 3, 5, 7 \in \mathbb{P}$ a $0, 1, 4, 6, 8, 9 \notin \mathbb{P}$.

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.

II.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 $1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4$.

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

II.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 $333333331 = 17 \cdot 19607843$ 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.

Čísla $1481, 1483, 1487, 1489, 1493$ jsou prvočísla. Čísla $1479, 1486, 1491$ nejsou prvočísla.

Čísla $3, 7, 37, 73, 337, 373, 733, 773, 3373, 3733, 7333$ jsou vesměs prvočísla.

II.1.16 Věta. Nechť p je prvočíslo a nechť $n_1, \dots, n_k$, $k \geq 1$ 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 II.1.11(iv). □

II.1.17 Příklad. Nechť $k \in \mathbb{Z}$, $a = 36k + 14$ 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 jsme, 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 $a = -22, b = 77$.

II.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).

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 $n \in \{-3, -2, 0, 1\}$ (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 $n \in \{-1, 0, 2, 3\}$.

II.2 Tabulka malých prvočísel

II.2.1 Tabulka. A zde uvidíme tabulku malých prvočísel. Prvních 1236 prvočísel v pořadí, jak jdou za sebou. Jsou to prvočísla $\mathbf{p}(1), \ldots, \mathbf{p}(1236)$, (např.$\mathbf{p}(74) = 373$).

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 $\mathbf{p}(1) = 2, \mathbf{p}(10) = 29, \mathbf{p}(100) = 541, \mathbf{p}(1000) = 7919$ a dále $\mathbf{p}(10000) = 104729$, $\mathbf{p}(100000) = 1299709$ a $\mathbf{p}(1000000) = 15485863$.

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

Posloupnost $\mathbf{p}(i) - i$, 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

$4, 5, 8, 9, 12, 13, 15, 16, \ldots$.

Je $\mathbf{p}(680) = 4831, \mathbf{p}(681) = 4861, \mathbf{p}(682) = 4871$. Tedy 3 po sobě jdoucí prvočísla, jejichž dekadické zápisy končí stejnou číslicí. Je to první trojice tohoto druhu (srovnej se čtveřicí $11, 13, 17, 19$).

Čísla $1117, 2221, 3331, 4111, 4441, 5557, 7333, 8887$ jsou prvočísla.

II.2.2 Eratosthenovo síto. Čísla 2,3,5,7,11 představují 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 $pq \mid n$. 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, která jsou menší než 150.

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

II.2.3 Cvičení. Označme $A = \{n^2 + q | n \geq 0, q \in \{0, 1\} \cup \mathbb{P}\}$.

(i) Spočtěme si, která čísla m, $m \leq 100$, patří do A. Všechna čísla z A jsou nezáporná a $0 = 0^2 + 0$, $100 = 10^2 + 0$. Tedy $0, 100 \in A$. Dále, je-li $n^2 + q \leq 100$, pak $n \leq 10$, $q \leq 97$. Další počty si vepíšeme do následujících 3 tabulek. Tyto jsou vymyšleny tak, že sloupce jsou ozačeny postupně čísly q, $q \in \{0, 1\} \cup \mathbb{P}, q \leq 97$, a řádky čísly $m = 0, 1, \ldots, 99$. V okénku nalézajícím se na průsečíku řádku označeného číslem m a sloupce označeného (nahoře) číslem q se objeví rozdíl $m - q$ za předpokladu, že tento rozdíl je druhou mocninou (pak totiž $m \in A$). Není-li tento rozdíl druhou mocninou, pak ve zmíněném okénku není nic.

m	0	1	2	3	5	7	11	13	17	19	23	29	31	37
0	0													
1	1	0												
2		1	0											
3			1	0										
4	4			1										
5		4			0									
6			4		1									
7				4		0								
8						1								
9	9				4									
10		9												
11			9			4	0							
12				9			1							
13								0						
14					9			1						
15							4							
16	16					9								
17		16						4	0					
18			16						1					
19				16						0				
20							9			1				
21					16				4					
22								9						
23						16				4	0			
24											1			
25	25													
26		25							9					
27			25				16				4			
28				25						9				
29								16				0		
30					25							1		
31													0	
32						25					9		1	
33									16			4		
34														
35										16			4	
36	36						25							
37		36												0
38			36					25				9		1
39				36							16			
40													9	
41					36									4
42									25					
43						36								
44										25				
45												16		
46														9
47							36						16	
48											25			
49	49							36						
50		49												

m	0	1	2	3	5	7	11	13	17	19	23	29	31	37
51			49											
52				49										
53									36					16
54					49							25		
55										36				
56						49							25	
57														
58														
59											36			
60							49							
61														
62								49						25
63														
64	64													
65		64										36		
66			64						49					
67				64									36	
68										49				
69					64									
70														
71						64								
72											49			
73														36
74														
75							64							
76														
77								64						
78												49		
79														
80													49	
81	81								64					
82		81												
83			81							64				
84				81										
85														
86					81									49
87											64			
88						81								
89														
90														
91														
92							81							
93												64		
94								81						
95													64	
96														
97														
98									81					

m	41	43	47	53	59	61	67	71	73	79	83	89	97
41	0												
42	1												
43		0											
44		1											
45	4												
46													
47		4	0										
48			1										
49													
50	9												
51			4										
52		9											
53				0									
54				1									
55													
56			9										
57	16			4									
58													
59		16			0								
60					1								
61						0							
62				9		1							
63			16		4								
64													
65						4							
66	25												
67							0						
68		25			9		1						
69				16									
70						9							
71							4	0					
72			25					1					
73									0				
74									1				
75					16			4					
76							9						
77	36					16			4				
78				25									
79		36								0			
80								9		1			
81													
82									9				
83			36				16			4	0		
84					25						1		
85													
86						25							
87								16			4		
88										9			
89				36					16			0	
90	49											1	
91													
92		49					25				9		
93												4	
94													
95					36					16			
96			49					25					
97						36							0
98									25			9	1
99											16		

Je $100 = 10^2 + 0 = 9^2 + 19$ (jiných rozkladů čísla 100 není).

(ii) Prohlédneme-li pečlivě předchozí tabulky, tu si uvědomíme, že v řádcích označených čísly 34, 58, 85 nic není. Naopak, v ostatních řádcích něco je. Takže $\{1, 2, \ldots, 33, 35, 36, \ldots, 57, 58, 59, \ldots, 84, 86, 87, \ldots, 100\} \subseteq A$, $34, 58, 85 \notin A$. Číslo 34 je nejmenší nezáporné celé číslo nepatřící do A a číslo 85 je nejmenší liché nezáporné celé číslo nepatřící do A.

Je $(2\cdot 17 =)34 = 2^5+2 = 3^3+7$, $(2\cdot 29 =)58 = 3^3+3$, $(5\cdot 17 =)85 = 2^5+53$. Je $3 + 4 = 7$, $5 + 8 = 13 = 8 + 5$.

(iii) Ještě označme $B = \{n^2 + p | n \geq 1, p \in \mathbb{P}\}$. Z tabulek vidíme, že $\{3, 4, 6, 7, 8, 9, 11, 12, 14, 15, \ldots, 24, 26, 27, \ldots, 33, 35, 36, \ldots, 57, 59, 60, 61, 62, 63, 65, 66, \ldots, 84, 86, 87, \ldots, 90, 92, 93, \ldots, 100\} \subseteq B$ a $0, 1, 2, 5, 10, 13, 25, 34, 58, 61, 64, 85, 91 \notin B$. Zde $0, 1, 25, 64$ jsou druhé mocniny a $2, 5, 13, 61$ jsou prvočísla. Ovšem, $10 = 2 \cdot 5$, $34 = 2 \cdot 17$, $58 = 2 \cdot 29$, $85 = 5 \cdot 17$, $91 = 7 \cdot 13$.

II.2.4 Cvičení. Je $0 = 0+0$, $1 = 0+1 = 2^0+0$, $2 = 0+2 = 2^0+1 = 2^1+0$, $3 = 0+3 = 2^0+2 = 2^1+1$, $4 = 2^0+3 = 2^2+0$, $5 = 0+5 = 2^0+4 = 2^1+3 = 2^2+1$, $6 = 2^0+5 = 2^2+2$, $7 = 0+7 = 2^1+5 = 2^2+3$, $8 = 2^0+7 = 2^3+0$, $9 = 2^1+7 = 2^2+5 = 2^3+1$, $10 = 2^3+2$, $11 = 0+11 = 2^2+7 = 2^3+3$, $12 = 2^0+11$, $13 = 2^1+11 = 2^2+7 = 2^3+5$, $14 = 2^0+13$, $15 = 2^1+13 = 2^2+11 = 2^3+7$, $16 = 2^4+0$, $17 = 0+17 = 2^1+17 = 2^2+13 = 2^4+1$, $18 = 2^0+17 = 2^4+2$, $19 = 0+19 = 2^1+11 = 2^3+11 = 2^4+3$, $20 = 2^0+19$, $21 = 2^1+19 = 2^2+17 = 2^3+13 = 2^4+5$. Ale $22-0 = 2\cdot 11, 22-1 = 3\cdot 7, 22-2 = 4\cdot 5, 22-4 = 2\cdot 9, 22-8 = 2\cdot 7, 22-16 = 2\cdot 3, 22-32 = -2\cdot 5$.

Označíme-li nyní $C = \{0\} \cup \mathbb{P} \cup \{2^k + q \mid k \geq 0, q \in \mathbb{P} \cup \{0, 1\}$, pak snadno vidíme, že $0, 1, 2, \ldots, 21 \in C, 22 \notin C$. (Je ovšem $22 = 3^1 + 19 = 3^2 + 13 = 5^1 + 17 = 11^1 + 1 = 17^1 + 5 = 19^1 + 3$.)

Je $959 - 0 = 959 = 7 \cdot 137, 959 - 1 = 958 = 2 \cdot 474, 959 - 2 = 957 = 3 \cdot 11 \cdot 29, 959 - 4 = 955 = 5 \cdot 191, 959 - 8 = 951 = 3 \cdot 317, 959 - 16 = 943 = 23 \cdot 41, 959 - 32 = 927 = 3 \cdot 3 \cdot 103, 959 - 64 = 895 = 5 \cdot 179, 959 - 128 = 831 = 3 \cdot 277, 959 - 256 = 703 = 19 \cdot 37, 959 - 512 = 447 = 3 \cdot 149, 959 - 1024 = -65 = -5 \cdot 13$ (vesměs prvočíselné rozklady). Tedy $959 \notin C$.

Dobrým cvičením je přesvědčit se o tom, že 959 je nejmenší liché číslo, které nepatří do množiny C. Ještě si všimněme tohoto: pro každé liché prvočíslo p a každé $k \geq 0$ je číslo $959 - p^k$ sudé. Snadno usuzujeme, že $959 \neq p^k + q$ pro všechna $p \in \mathbb{P}, k \geq 0, q \in \{0, 1, \} \cup \mathbb{P}$. Nicméně, $959 = 10^2 + 859$, kde 859 je již prvočíslo. Je $9+5+9 = 23, 2+3 = 6, 9\cdot 5\cdot 9 = 405, 4+0+5 = 9$.

II.3 Základní věta aritmetiky

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

Důkaz. Je $p \geq 2$. Jestliže $q \geq 1$ 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 $p \in \mathbb{P}$. □

II.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 II.3.1 existuje $p \in \mathbb{P}$ tak, že $p \mid |n|$. Samozřejmě $p \mid n$. □

II.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 $(2 =)\mathbf{p}(1) < (3 =)\mathbf{p}(2) < (5 =)\mathbf{p}(3) < \cdots < \mathbf{p}(n) = p$, $n \geq 5$, je posloupnost všech prvočísel menších či rovných našemu prvočíslu p.

Položme $m = (\mathbf{p}(1)\mathbf{p}(2)\cdots\mathbf{p}(n)) + 1$. Jistě je $m \geq 2$ (ve skutečnosti je $m > 1609$) a podle II.3.2 existuje prvočíslo q takové, že $q \mid m$. Ovšem, $q \nmid 1$, čili $q \nmid m - \mathbf{p}(1)\mathbf{p}(2)\cdots\mathbf{p}(n)$, pročež $q \neq \mathbf{p}(i)$, pro všechna $i = 1, 2, \ldots, n$. Pak ale $q > p$.

Nepatrně obměněný důkaz: Existuje prvočíslo q tak, že $q \mid p! + 1$. Zřejmě je $q > p$. □

II.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 $\{p_1, p_2, \ldots, p_s\}$ obsahující s vesměs různých prvočísel a jednoznačně určené exponenty $r_1, r_2, \ldots r_s \geq 1$ takové, že $n = \pm p_1^{r_1} \ldots p_s^{r_s}$.

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 II.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 $p_1^{r_1} \ldots p_s^{r_s} = n = q_1^{u_1} \ldots q_v^{u_v}$ 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 II.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 II.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. □

II.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 $r = \mathrm{cont}_p(n)$ 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 $\mathrm{cont}_p(0) = +\infty$.

II.3.6 Věta. $\mathrm{cont}_p(nm) = \mathrm{cont}_p(n) + \mathrm{cont}_p(m)$ 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 $a = \mathrm{cont}_p(n)$, $b = \mathrm{cont}_p(m)$, $c = \mathrm{cont}_p(nm)$, $p \nmid n_1, m_1, k$. Odtud $p^c \cdot k = nm = p^{a+b} n_1 m_1$. Z II.1.11(iv) plyne, že $p \nmid n_1 m_1$ a tedy $a + b = c$. □

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

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

II.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) $\mathrm{cont}_{p_i}(n) = r_i$ pro každé $1 \leq i \leq s$.
(ii) $\mathrm{cont}_p(n) = 0$ pro každé $p \in \mathbb{P}$, $p \notin \{p_1, \dots, p_s\}$

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

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

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

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

Důkaz. Jestliže $n \mid m$, pak nerovnost $\mathrm{cont}_p(n) \leq \mathrm{cont}_p(m)$ plyne ihned z II.3.5. Jestliže $r = \mathrm{cont}_p(n) \leq \mathrm{cont}_p(m) = s \leq +\infty$, 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 II.3.9 □

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

Důkaz. Tvrzení plyne snadno z II.3.10. □

II.3.12 Proposice. Nechť $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$, $n \neq 0 \neq m$, $n \neq -m$. Potom:
(i) $\mathrm{cont}_p(n+m) \geq \min(\mathrm{cont}_p(n), \mathrm{cont}_p(m))$.
(ii) Je-li $\mathrm{cont}_p(n) \neq \mathrm{cont}_p(m)$, pak $\mathrm{cont}_p(n+m) = \min(\mathrm{cont}_p(n), \mathrm{cont}_p(m))$.
(iii) Je-li $\mathrm{cont}_2(n) = \mathrm{cont}_2(m)$, pak $\mathrm{cont}_2(n+m) > \mathrm{cont}_2(n)$.

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 $p = 2 \mid k$. □

II.3.13 Proposice. Nechť $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$, $n \neq 1 \neq m$. Potom $\mathrm{cont}_p(nm-1) \geq \max(\mathrm{cont}_p(n-1), \mathrm{cont}_p(m-1))$.

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

II.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 $\mathrm{cont}_p(n_1 \cdots n_k - 1) \geq \min(\mathrm{cont}_p(n_i - 1) \mid 1 \leq i \leq k)$.

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

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

Důkaz. Podle II.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 II.3.14 máme $\mathrm{cont}_p(n-1) \geq \min(\mathrm{cont}_p(p_i-1))$. □

II.3.16 Poznámka. (i) Základní věta aritmetiky nás poučuje o tom, že multiplikativní pologrupa $\mathbb{N}'(\cdot)$, kde $\mathbb{N}' = \{n \mid n \geq 2\}$ 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: $(2 =)\mathbf{p}(1) < (3 =)\mathbf{p}(2) < \dots$. Pro každé $n \in \mathbb{Z}$ sestrojíme nekonečnou posloupnost $\alpha(n) = (\ \mathrm{cont}_{\mathbf{p}(1)}(n),\ \mathrm{cont}_{\mathbf{p}(2)}(n),\ \mathrm{cont}_{\mathbf{p}(3)}(n), \dots)$ Je-li $n \neq 0$, pak $\alpha(n)$ je nekonečná posloupnost nezáporných celých čísel, kde ovšem jen konečně mnoho čísel je nenulových. Např. $\alpha(1) = \alpha(-1) = (0, 0, 0, \dots)$, $\alpha(\mathbf{p}(i)) = (0, 0, \dots, 0, 1, 0 \dots)$, 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 II.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.

II.3.17 Příklad. (i) 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.

(ii) Je $405 = 3^4 \cdot 5, 2 \cdot 405 = 810$ a čísla $809, 811$ jsou prvočísla. Je $4 \cdot 405 = 1620$ a čísla $1619, 1621$ jsou prvočísla. Je $6 \cdot 405 = 2430$ a žádné z čísel 2429,2431 není prvočíslo. Je $8 \cdot 405 = 3240$ a žádné z čísel 3239,3241 není prvočíslo. Je $10 \cdot 405 = 4050$ a obě čísla $4049, 4051$ jsou prvočísla. Je $12 \cdot 405 = 4860$, 4859 není prvočíslo a 4861 je prvočíslo. Je $14 \cdot 405 = 5670$, 5669 je prvočíslo a 5671 není prvočíslo. Je $16 \cdot 405 = 6480$, 6479 není prvočíslo a 6481 je prvočíslo.

(iii) Je $1375 = 5^3 \cdot 11, 1376 = 2^5 \cdot 43$ a $1377 = 3^4 \cdot 17$.

(iv) $101, 1009, 10007$ jsou prvočísla. $11, 211, 311, 811, 911, 1511, 1811, 2011, 2111, 2311, 2411, 2711, 3011$ jsou také prvočísla.

II.3.18 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 $432 = 2^4 \cdot 3^3 = 4 \cdot 3^3 \cdot 2^2$

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

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

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

II.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 $2 + 11 + 19 = 32 = 4 \cdot 1 \cdot 8$.

II.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 $m \mid n^l$, $\underline{P}(m) \subseteq \underline{P}(n)$. □

II.3.22 Příklad. (i) Je $1919 = 19 \cdot 101$, $1920 = 2^7 \cdot 3 \cdot 5$, $1921 = 17 \cdot 113$ (prvočíselné rozklady). Je $19 + 101 = 120$ a $17 + 113 = 130$.

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

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

(iv) Je $5561 = 67 \cdot 83$ (prvočíselný rozklad) a $5 \cdot 5 \cdot 6 \cdot 1 = 150 = 67 + 83$.

(v) Je $6277 = 6277$, $6278 = 2{\cdot}43{\cdot}73$, $6279 = 3{\cdot}7{\cdot}13{\cdot}23$, $6280 = 2{\cdot}2{\cdot}2{\cdot}5{\cdot}157$, $6281 = 11 \cdot 571$ (prvočíselné rozklady) a $6+2+7+7 = 22, 2+4+3+7+3 = 19 = 3+7+1+3+2+3, 2+2+2+5+1+5 = 24, 1+1+5+7+1 = 15$.

(vi) Je $1948 = 2 \cdot 2 \cdot 487$ (prvočíselný rozklad), $1+9+4+8 = 22, 2+2+4+8+7 = 23$, $1 \cdot 9 \cdot 4 \cdot 8 = 288, 2 \cdot 2 \cdot 4 \cdot 8 \cdot 7 = 896, 2+8+8 = 18, 4+8+7 = 19, 8+9+6 = 23$.

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

Důkaz. Podle II.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 $q < |n|$, pak $q \leq |n/q|$ a $q^2 \leq |n| \cdot |n/q| = |n|$. □

II.3.24 Lemma. Nechť $n, m \in \mathbb{Z}$ a $k \in \mathbb{N}$ jsou taková čísla, že $n^k \mid m^k$. 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 $k \operatorname{cont}_p(n) = \operatorname{cont}_p(n^k) \leq \operatorname{cont}_p(m^k) = k \operatorname{cont}_p(m)$ a tedy $\operatorname{cont}_p(n) \leq \operatorname{cont}_p(m)$. Podle II.3.10 máme $n \mid m$. □

II.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 II.3.24. Nakonec, $n^k \mid m^l = n^{tl} \cdot u^l$ a $n^{k-tl} \mid u^l$. □

II.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, $m \mid p_1 - 1$, $m \mid p_1 p_2 - p_2$, $m \mid p_2 - 1$, $m \mid (p_1 p_2 - p_2) + (p_2) - 1 = p_1 p_2 - 1$, $m \mid p_1 p_2 p_3 - p_3$, $m \mid p_3 - 1$, $m \mid p_1 p_2 p_3 - 1$, $\dots$, $m \mid p_1 p_2 \dots p_s - 1$. □

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

Důkaz. Pro každé $p \in \underline{P}(n)$ je $\mathrm{cont}_q(p-1) = r(p)$ 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 II.3.26. □

II.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 $s_i = \mathrm{cont}_q(p_i + 1)$. 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 $\mathrm{cont}_q(n-1) \geq z$. Je-li r liché, tak $q^z \mid n + 1$ a $\mathrm{cont}_q(n+1) \geq z$.

II.3.29 Sdělení. Číslo $n = pq, p, q \in \mathbb{P}$, se občas nazývá poloprvočíslo. Zde může být $p = q$,či $p \neq q$. Ve druhém případě se n nazývá diskrétní poloprvočíslo.

Posloupnost poloprvočísel začíná takto: $4, 6, 9, 10, 14, 15, 21, 22, 25, \dots$ a posloupnost diskrétních poloprvočísel takto: $6, 10, 14, 15, 21, 22, 26, 33, 35, \dots$.

II.4 Příklady

II.4.1 Příklad. Je $\underline{P}(1) = \emptyset$, $\underline{P}(2) = \{2\}$, $\underline{P}(3) = \{3\}$, $\underline{P}(4) = \{2\}$, $\underline{P}(5) = \{5\}$, $\underline{P}(6) = \{2, 3\}$, $\underline{P}(7) = \{7\}$, $\underline{P}(8) = \{2\}$, $\underline{P}(9) = \{3\}$, $\underline{P}(10) = \{2, 5\}$.

Je $\underline{P}(33) = \{3, 11\}$, $\underline{P}(34) = \{2, 17\}$, $\underline{P}(35) = \{5, 7\}$, $\underline{P}(36) = \{2, 3\}$, $33 = 3 \cdot 11, 34 = 2 \cdot 17, 35 = 5 \cdot 7, 36 = 4 \cdot 9$.

Nyní si ukážeme, že pro každé číslo $n \geq 4, n \neq 7$, aspoň jedna z množin $\underline{P}(n), \underline{P}(n+1), \underline{P}(n+2)$ má aspoň 2 prvky.

Můžeme předpokládat, že $n \geq 11$. Nechť naopak $\underline{P}(n) = \{p_1\}$, $\underline{P}(n+1) = \{p_2\}$ a $\underline{P}(n+2) = \{p_3\}$ jsou jednoprvkové množiny. Specielně $6 \nmid n, 6 \nmid n+1, 6 \nmid n+2$ a tudíž $n = 6k + l, k \geq 2, 1 \leq l \leq 3$.

Nejprve, nechť $l = 1$. Číslo $n+1 = 6k+2$ je sudé a tak $p_2 = 2$ a $n+1 = 2^b$ pro $b \geq 4$. Dále, $n+2 = 6k+3$ tedy $3 \mid n+2, p_3 = 3$ a $n+2 = 3^a$ pro $a \geq 3$. Nyní $3^a - 2^b = n + 2 - n - 1 = 1$ čili $2^b = 3^a - 1$.

Nechť $a = 2c, c \geq 2$, je sudé číslo. Je $3^a - 1 = (3^c - 1)(3^c + 1)$ a tak $3^c - 1 = 2^u$ a $3^c + 1 - 2^v$, $u \geq 3, v \geq 4$. Pak ale $8 = 2^3 \mid (3^c + 1) - (3^c - 1) = 2$, což nelze. Nahlédli jsme, že $a \geq 3$ je liché číslo. Pak ale $3^a - 1 = (3 - 1)(3^{a-1} + 3^{a-2} + \cdots + 3 + 1) = 2w$, kde $w = 3^{a-1} + 3^{a-2} + \cdots + 3 + 1$. A, jelikož $4 \mid 3^a - 1$, tak $2 \mid w$. Jelikož a je liché, tak w je součtem lichého počtu lichých čísel. Tedy w je liché, což je spor.

Nyní nechť $l = 2$. Pak $p_1 = 2, n = 2^a, a \geq 4, n+1 = 6k+3, p_2 = 3, n+1 = 3^b, b \geq 3, 2^2 = 3^b - 1$ a situace je stejná jako před chvílí. Zde ovšem je také $n + 2 = 2^c, c \geq 5, 2 = n + 2 - n = 2^c - 2^a = 2^a(2^{c-a} - 1), 2 = 2^a = n$, což také nejde.

Nakonec, nechť $n = 6k+3$. Pak $p_1 = 3, n = 3^b, b \geq 3, n+1 = 6k+4, p_2 = 2, n + 1 = 2^a, a \geq 4$. Takže $1 = n + 1 - n = 2^a - 3^b, 1 + 3^b = 2^a, 2^a - 1 = 3^b$.

Nechť $a = 2c, c \geq 2$, je sudé číslo. Je $2^a - 1 = (2^c - 1)(2^c + 1)$ a tak $2^c - 1 = 3^u, 2^c + 1 = 3^v, u \geq 1, v \geq 2$. Pak ale $3 \mid (2^c + 1) - (2^c - 1) = 2$, což nelze.

Nahlédli jsme, že $a \geq 5$ je liché číslo. Je $2^3 = 8 = 3 \cdot 2 + 2$. Je-li nyní $k \geq 3$ takové číslo, že $2^k = 3l + 2$, pak $2^{k+2} = 12l + 8 = 3(4l + 2) + 2$. Z této úvahy plyne, že $3^b + 1 = 2^a = 3m + 2$. Pak ale $3 \mid 2 - 1 = 1$, spor.

Alternativní důkaz

Alespoň jedno ze zkoumaných čísel $n, n+1, n+2$ je sudé, a protože musí být mocninou 2, je ve tvaru 2^a. Další takové číslo, lišící se od něj o 2, již mezi uvedenými čísly být nemůže, takže $n + 1 = 2^a$. Dokážeme, že, je-li a sudé, pak n je dělitelné 3 a současně není mocninou 3; je-li a liché, pak $n+2$ je dělitelné 3 a není mocninou 3.

(a) Je $a = 2k$ a tedy $n = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$. Činitelé jsou lichými čísly a liší se o 2 a tedy jeden z nich je dělitelný 3 a druhý nikoli a tedy ani

nemůže být mocninou 3.

(b) Je $a = 2k+1$ a tedy $n+2 = 2^{2k+1}+1-3+3 = 2^{2k+1}-2+3 = 2(2^k-1)(2^k+1)+3$. Opět buď (2^k-1) nebo (2^k+1) je dělitelné 3 a tím i celý výraz. Nechť je tedy $n+2 = 3^a$ a $2^{2k+1} = 3^a - 1$. Opět rozlišme 2 případy: $a = 2l, a = 2l+1$. V prvním je $3^a - 1 = (3^l-1)(3^l+1)$. 2 činitelé lišící se o 2 nemohou být současně mocninou 2. Ve druhém případě dostáváme $3^a - 1 = (3-1)(3^{2l} + 3^{2l-1} + \cdots + 3 + 1)$, ale druhý činitel je součtem lichého $(2l+1)$ počtu lichých sčítanců a tedy nemůže být mocninou 2.

Poznámka: Tvrzení, že ze tří po sobě jdoucích čísel je právě jedno dělitelné 3, je triviální. Netriviální ovšem je, že v našem případě není $2^k \pm 1$ mocninou 3.

Dokázali jsme žádané. Tedy: Je-li $n \geq 4, n \neq 7$, pak alespoň jedno z čísel $n, n+1, n+2$ není mocninou žádného prvočísla. Samozřejmě čísla $1, 2, 3, 4, 5, 7, 8, 9$ jsou mocninami prvočísel.

II.4.2 Příklad. (i) Nechť $p \in \mathbb{P}$ a $n \in \mathbb{N}$. Pro každé $m, 1 \leq m \leq np$, máme $m = p^{a(m)} \cdot b(m)$, kde $a(m) = \mathrm{cont}_p(m) \geq 1$, $b(m) \geq 1$, $p \nmid b(m)$. Je-li $a(m) \geq 1$, pak $1 \leq b(m) \leq n$. Dále je zřejmé, že po dvou různá čísla $p, 2p, \ldots, np$ jsou právě všechna ta čísla m taková, že $1 \leq m \leq np$ a $a(m) \geq 1$. Těchto čísel je právě n a ostatních čísel mezi 1 a np včetně je právě $np - n = n(p-1)$.

Nechť nyní $m_1, \ldots, m_k$, kde $k \geq n(p-1)+1$, jsou po dvou různá čísla taková, že $1 \leq m_i \leq np$ pro každé $i = 1, 2, \ldots, k$. Je $1 \leq b(m_i) \leq np$ a $p \nmid b(m_i)$. Jak jsme si před chvílí všimli, tak pro čísla $b(m_i)$ máme nejvýše (ve skutečnosti právě) $n(p-1)$ možností. To znamená, že existují indexy $1 \leq t, l \leq k$ takové, že $l \neq t$ a $b(m_t) = b(m_l)$. Je-li $m_t < m_l$, pak nutně $m_t \mid m_l$ a naopak.

(ii) Buď $p = 2$ a $n \in \mathbb{N}$. Vybereme-li $n+1$ různých čísel mezi 1 a $2n$ včetně, pak alespoň jedno vybrané číslo dělí nějaké jiné z vybraných čísel. To znamená, že tato vybraná čísla nejsou nesrovnatelná v uspořádání daném dělitelností v $\mathbb{N}$ (viz II.1.10).

Na druhé straně, $n+1, n+2, \ldots, 2n$ je n různých čísel (mezi 1 a 2n) a žádné z těchto čísel nedělí žádné druhé z nich.

II.4.3 Hříčka. Pro $n \geq 1$ budiž $q_n = 10^{n-1} + 10^{n-2} + \cdots + 10 + 1$. Tedy $q_1 = 1, q_2 = 11, q_3 = 111, q_4 = 1111$, atd. Číslo q_n je tedy liché a má v desítkové soustavě tvaru $11\ldots1$, kde číslice 1 se vyskytuje právě n-krát. Číslo q_n bychom mohli nazvat "n-krát opakovaná jednička, či kratšeji opička" (samozřejmě při základu 10).

(i) Zřejmě je $9 \cdot q_n + 1 = 10^n$ a dále $5 \nmid q_n$ (dekadický zápis lichých násobků 5 končí opět na 5). Specielně, čísla q_n a 10 nemají jiné společné dělitele nežli čísla $1, -1$.

(ii) Je $q_{n+1} = 10^n + q_n = 10 \cdot q_n + 1$, $q_{n+m} = 10^m \cdot q_n + q_m = 10^n \cdot q_m + q_n, n \geq 1, m \geq 1$.

(iii) Ověříme, že $q_n \mid q_m$ právě když $n \mid m$.

Jestliže $q_n \mid q_m$, tak $n \leq m$ (neboť $q_n \leq q_m$) a budeme postupovat indukcí podle $m - n$. Je-li $m - n = 0$, tak $m = n$ a $n \mid m$. Je-li $m \geq n$, tak $q_m = 10^n \cdot q_{m-n} + q_n$ dle (ii), čili $q_n \mid q_{m-n}, n \mid m - n$ podle indukčního předpokladu, a tak $n \mid m$.

Nyní naopak, nechť $n \mid m$, $m = kn, k \geq 2$. Pak $q_m = 10^{(k-1)n} \cdot q_n + q_{(k-1)n}$ a opět indukcí podle k dokážeme, že $q_n \mid q_m$.

(iv) Je-li číslo q_n prvočíslo, tak z (iii) plyne, že i n je prvočíslo. Samozřejmě, $q_2 = 11$ je prvočíslo a je známo, že i čísla q_{19}, q_{23}, q_{317} a q_{1031} jsou prvočísla. Na druhé straně, $q_3 = 3 \cdot 37, q_4 = 11 \cdot 101, q_5 = 41 \cdot 271, q_6 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 71$, $q_7 = 239 \cdot 4649$, $q_8 = 11 \cdot 73 \cdot 101 \cdot 137$, $q_9 = 3^2 \cdot 37 \cdot 333667$, $q_{10} = 11 \cdot 41 \cdot 271 \cdot 9091$ a $q_{11} = 21649 \cdot 513239$ prvočísly nejsou (jsou uvedeny jejich prvočíselné rozklady).

Všimněme si, že $q_9 = 9 \cdot 12345679$.

(v) Nechť $a \in \mathbb{Z}$, $a \mid q_n, a \mid q_{n+1}$. Pak z (ii) plyne, že $a \mid 10^n$, čili $a = \pm 2^b \cdot 5^c, b \geq 0, c \geq 0$. Pak ale $a = \pm 1$ (viz (i)).

(vi) Je $10^n - 1 = 9 \cdot q_n$. Takže $n \mid 10^n - 1$ právě když buďto $n \mid q_n$ nebo $n = 3 \cdot n_1, n_1 \mid q_n$ anebo $n = 9 \cdot n_2, n_2 \mid q_n$.

(vii) Nahlédneme, že $3^k \mid q_{3^k}$ pro každé $k \geq 0$.

Zajisté, $3^0 = 1 \mid 1 = q_1$ a $3^1 = 3 \mid 111 = 3 \cdot 37 = q_3$. Dále pak $q_{3^{k+1}} = q_{3^k} \cdot w$ kde $w = 10^6 + 10^3 + 1 = 1001001 = 3 \cdot 333667$ (prvočíselný rozklad). Takže $3^{k+1} \mid q_{3^{k+1}}$ (indukce).

(viii) Z (vii) a (iii) plyne, že $q_{3^k} \mid q_{q_{3^k}}$. Speciálně, 111 dělí $111\ldots111$ (stojedenáct 1), což je ovšem ihned vidět z toho, že v dlouhém čísle se trojčíslí 111 opakuje sedmatřicetkrát.

II.4.4 Cvičení. (i) $1^2 + 2^2 = 5$, $2^2 + 3^2 = 13$, $4^2 + 5^2 = 41$, $5^2 + 6^2 = 61$, $7^2 + 8^2 = 113$, $9^2 + 10^2 = 181$, $12^2 + 13^2 = 313$, $14^2 + 15^2 = 421$, $17^2 + 18^2 = 613$, $19^2 + 20^2 = 761$ jsou prvočísla.

Naproti tomu $0^2 + 1^2 = 1$, $3^2 + 4^2 = 25$, $6^2 + 7^2 = 85 = 5 \cdot 17$, $8^2 + 9^2 = 145 = 5 \cdot 29$, $10^2 + 11^2 = 221 = 13 \cdot 17$, $11^2 + 12^2 = 265 = 5 \cdot 5^3$, $13^2 + 14^2 = 365 = 5 \cdot 73$, $15^2 + 16^2 = 481 = 13 \cdot 37$, $16^2 + 17^2 = 545 = 5 \cdot 109$, $18^2 + 19^2 = 685 = 5 \cdot 137$ prvočísla nejsou (uvádíme prvočíselné rozklady).

(ii) Nechť $n \geq 1$ je takové číslo, že $p = n^2 + (n+1)^2 (= 2n^2 + 2n + 1)$ je prvočíslo. Potom p je liché a $2p = (2n+1)^2 + 1$.

(iii) Nechť p je liché prvočíslo takové, že $2p = m^2 + 1$ pro nějaké $p \geq 0$. Zřejmě, $m \geq 3$, m je liché, $m = 2n + 1$, $n \geq 1$, $p = n^2 + (n+1)^2$.

(iv) Nechť dekadický zápis čísla $n \geq 1$ končí (vpravo) na jednu z číslic 1,3,6,8. Potom zápis čísla n^2 končí na 1,9,6,4, číslo $(n+1)^2$ pak na 4,6,9,1 a

čísla $t = n^2 + (n+1)^2$ končí na 5. Čili $5 \mid t$ a t není prvočíslo.

(v) $2^2 + 3^2 = 13$, $12^2 + 13^2 = 313$, $22^2 + 23^2 = 1013$, $32^2 + 33^2 = 2113$,$42^2+43^2 = 3613$ jsou vesměs prvočísla. Avšak $52^2+53^2 = 5513 = 37\cdot149$ (prvočíselný rozklad) prvočíslem není.

$4^2 + 5^2 = 41$,$14^2 + 15^2 = 421$,$24^2 + 25^2 = 1201$,$34^2 + 35^2 = 2381$ jsou prvočísla. Avšak $44^2+45^2 = 3961 = 17\cdot233$ (prvočíselný rozklad) prvočíslem není.

$5^2 + 6^2 = 61$ je prvočíslo. Avšak $15^2 + 16^2 = 481 = 13 \cdot 37$ (prvočíselný rozklad) prvočíslem není.

$7^2 + 8^2 = 113$, $17^2 + 18^2 = 613$ jsou prvočísla. Avšak $27^2 + 28^2 = 1513 = 17 \cdot 89$ (prvočíselný rozklad) prvočíslem není.

$9^2 + 10^2 = 181$, $19^2 + 20^2 = 761$, $29^2 + 30^2 = 1741$, $39^2 + 40^2 = 3121$ jsou prvočísla. Avšak $49^2+50^2 = 4901 = 13^2\cdot29$ (prvočíselný rozklad) prvočíslem není.

Nakonec, $0^2 + 1^2 = 1$,$10^2 + 11^2 = 221 = 13 \cdot 17$, $20^2 + 21^2 = 841 = 29^2$ prvočísla nejsou. Avšak $30^2 + 31^2 = 1861$ již prvočíslo je.

II.4.5 Cvičení. Je $|\underline{P}(n)| \leq 2$ pro všechna $1 \leq n \leq 29$ a $|\underline{P}(30)| = 3$ neboť $30 = 2 \cdot 3 \cdot 5$. Je $6 + 23 = 29$.

Nechť $n \geq 7$. Ověříme, že existuje aspoň jedno m takové, že $n \leq m \leq 23$, přičemž $|\underline{P}(m)| \geq 3$. $(n, n+1, \ldots, n+23$ je 24 po sobě jdoucích čísel.)

Vskutku. Buď $k \geq 1$. Pak $2, 3 \nmid 6k+1, 6k+1 \geq 7$ a tak $|\underline{P}(6(6k+1))| \geq 3$.

Zcela obdobně, $|\underline{P}(6(6k+5))| \geq 3$. Je $6(6k+1) = 36k+6$ a $6(6k+5) = 6k+30$.

A teď! Je-li $7 \leq n \leq 30$, lze volit $m = 30$. Buď tedy $n \geq 31$ a buď r největší nezáporné číslo takové, že $36r + 30 < n$. Takže $n \leq 36r + 66$. Je $36(r+1) + 6 = 36r + 42 < n + 12 < n + 23$ a můžeme položit $m = 36(r+1) + 6 (= 6(6(r+1)+1))$, je-li $n \leq 36r + 42$. V opačném případě, jestliže $36r + 42 < n$, pak je $36r + 66 \leq n + 23$ a položíme $m = 36r + 66 = 36(r+1) + 30 = 6(6(r+1) + 5)$. Jsme hotovi.

II.4.6 Příklad. Nechť $p \in \mathbb{P}$, $p \geq 2^{k-1} \cdot k$, $k \geq 2$. Buď $a = 2^k$, $b = 2p$. Prvočíslo p je liché a $k \geq 2$. Snadno vidíme, že $a \nmid b$. Avšak $a^a = 2^{k\cdot 2^k}$ a $b^b = (2p)^{2p} = 2^{2p} \cdot p^{2p}$. Jelikož $2p > 2^k \cdot k$, tak $a^a \mid b^b$.

II.4.7 Příklad. (i) Je $0^2 - 3 = -2$, $2^2 - 3 = 1$, $3^2 - 3 = 2 \cdot 3$, $3^2 - 3 = 2 \cdot 3$, $4^2 - 3 = 13$, $5^2 - 3 = 2 \cdot 11$, $6^2 - 3 = 3 \cdot 11$, $7^2 - 3 = 2 \cdot 23$, $8^2 - 3 = 61$, $9^2-3 = 2\cdot3\cdot13$, $10^2-3 = 97$, $11^2-3 = 2\cdot59$, $12^2-3 = 3\cdot47$, $13^2-3 = 2\cdot83$, $14^2 - 3 = 193$, $15^2 - 3 = 2 \cdot 3 \cdot 37$, $16^2 - 3 = 11 \cdot 23$, $17^2 - 3 = 2 \cdot 11 \cdot 13$, $18^2 - 3 = 3 \cdot 107$, $19^2 - 3 = 2 \cdot 197$, $20^2 - 3 = 397$, $21^2 - 3 = 2 \cdot 3 \cdot 73$, $22^2 - 3 = 13 \cdot 37$, $23^2 - 3 = 2 \cdot 263$, $24^2 - 3 = 3 \cdot 191$, $25^2 - 3 = 2 \cdot 311$, $26^2 - 3 = 673$, $27^2 - 3 = 2 \cdot 3 \cdot 11^2$ (jedná se o prvočíselné rozklady).

Zjistili jsme, že 27 je nejmenší nezáporné číslo n takové, že $p^2 \mid (n^2-3)$ aspoň pro jedno $p \in \mathbb{P}$ $(27-3=2^3\cdot 3)$.

(ii) Je $(27+121\cdot k)^2 = 27^2+2\cdot 27\cdot 11^2\cdot k+11^4\cdot k^2$. Jelikož $11^2 \mid 27^2-3$, tak $11^2 \mid (27+121\cdot k)^2-3$ pro každé $k \geq 0$.

(iii) Je $0^2-2=-2$, $1^2-2=-1$, $2^2-2=2$, $2^2-2=2$, $3^2-2=7$, $4^2-2=2\cdot 7$, $5^2-2=23$, $6^2-2=2\cdot 17$, $7^2-2=47$, $8^2-2=2\cdot 31$, $9^2-2=79$, $10^2-2=2\cdot 7^2$.

(iv) Je $0^2-1=-1$, $1^2-1=0$, $2^2-1=3$, $3^2-1=2^3$.

(v) Je $0^2-5=-4$, $1^2-5=-2^2$, $2^2-5=-1^2$, $3^2-5=2^2$. Je $4^2-7=3^2$ a $6^2-11=5^2$.

(vi) Je $0^2+1=1$, $1^2+1=2$, $2^2+1=5$, $3^2+1=2\cdot$, $4^2+1=17$, $5^2+1=2\cdot 13$, $6^2+1=37$, $7^2+1=2\cdot 5^2$, $7+1=2^3$.

(vii) Je $0^2+2=2$, $1^2+2=3$, $2^2+2=2\cdot 3$, $3^2+2=11$, $4^2+2=2\cdot 9$, $5^2+2=3^3$.

(viii) Je $0^2+3=3$, $1^2+3=2^2$, $2^2+3=7$, $3^2+3=2^2\cdot 3$.

(ix) Je $0^2+5=5$, $1^2+5=2\cdot 3$, $2^2+5=3^2$ a $1^2+7=2^3$. Je $3^2+11=2^2\cdot 5$.

(x) Je $1^4+1^4=2$, $1^4+2^4=17$, $2^4+3^4=97$, $1^4+4^4=257$, $2^4+5^4=641$, přičemž 2, 17, 97, 257 a 641 jsou prvočísla.

II.4.8 Příklad. Je $22=2\cdot 11$, $2+2=4=2+1+1$, $378=2\cdot 3\cdot 3\cdot 3\cdot 7$, $3+7+8=18=2+3+3+3+7$, $4937775=3\cdot 5\cdot 5\cdot 65837$ (prvočíselný rozklad) $4+9+3+7+7+7+5=42=3+5+5+6+5+8+3+7$, $2954=2\cdot 2\cdot 3\cdot 13\cdot 19$, $2+9+5+4=21=2+2+3+1+3+1+9$.

Čísla tohoto typu jsou známa jako Smithova čísla (srovnej s II.3.22 (iv),(v)).

II.4.9 Příklad. Je $25662=2\cdot 3\cdot 7\cdot 13\cdot 47$ a $2\cdot 5\cdot 6\cdot 6\cdot 2=720=10\cdot 72=10\cdot(2+3+7+13+47)$, $1568=2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 7\cdot 7$ a $1\cdot 5\cdot 6\cdot 8=240=10\cdot 24=10\cdot(2+2+2+2+2+7+7)$. Čísla tohoto typu jsou známa jako Rhondina čísla (při základu 10).

II.4.10 Příklad. (i) Nechť $k\geq 1$, $n=2^k-2=2(2^{k-1}-1)$ a $m=2^k(2^k-2)=2^{k+1}(2^{k-1}-1)$. Zřejmě je $\underline{P}(n)=\{2\}\cup\underline{P}(2^{k-1}-1)=\underline{P}(m)$. A nyní je $n+1=2^k-1$ a $m+1=2^{2k}-2^{k+1}+1=(2^k-1)^2$. Tedy $\underline{P}(n+1)=\underline{P}(2^k-1)=\underline{P}(m+1)$. Čísla n,m jsou sudá a čísla n+1, m+1 lichá.

Pro $k=1$ je $n=0=m$, $n+1=1=m+1$. Pro $k=2$ je $n=2$, $m=8$, $n+1=3$, $m+1=9$. Pro $k=3$ je $n=6$, $m=48$, $n+1=7$, $m+1=49$. Pro $k=4$ je $n=14$, $m=224$, $n+1=15$, $m+1=225$.

(ii) Buď $n=75=3\cdot 5^2$ a $m=1215=3^5\cdot 5$. Je tedy $\underline{P}(n)=\{3,5\}=\underline{P}(m)$. Ovšem, $n+1=76=2^2\cdot 19$ a $m+1=1216=2^6\cdot 19$. Tedy také $\underline{P}(n+1)=\{2,19\}=\underline{P}(m+1)$. Zde jsou čísla n,m lichá a $n+1, m+1$ sudá.

II.4.11 Cvičení. (Srovnej s II.2.3) Nechť $n \geq 1$. Dokážeme si, že $(3n+2)^2 \neq m^2 + p$ pro každé $m \in \mathbb{Z}$ a $p \in \mathbb{P} \cup \{1\}$.

Nechť naopak $(3n+2)^2 = m^2 + p$, $m \in \mathbb{Z}$. Je $3n+2 \geq 5$, takže $m \neq 0$ a můžeme brát $m \geq 1$. Dále $p = (3n+2)^2 - m^2 = (3n+2-m)(3n+2+m)$. Samozřejmě $3n+2 > m$, takže $1 = 3n+2-m$ a $p = 3n+2+m$, $p+1 = 6n+4$, $p = 6n+3 = 3(2n+1)$, spor.

Je $1 = 0^2 + 1$, $2^2 = 4 = 1^2 + 3$, $3^2 = 9 = 2^2 + 5$, $4^2 = 16 = 3^2 + 7$. Avšak $5^2 \neq m^2 + p$. No, ale $6^2 = 36 = 5^2 + 11$, $7^2 = 49 = 6^2 + 1$. A opět $8^2 \neq m^2 + p$.

Je $5777, 5993 \neq m^2 + p$ pro všechna $m \in \mathbb{N}$ a $p \in \mathbb{P} \cup \{1\}$.

II.5 Složená čísla

II.5.1 Definice. Celé číslo, které není nerozložitelné ve smyslu II.1.13 se nazývá (multiplikativně) rozložitelné. Nenulové rozložitelné číslo se nazývá složené.

II.5.2 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 II.1.13, II.3.4 a II.5.1. □

II.5.3 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, $(n+1)!+m > m \geq 2$. Takže číslo $(n+1)!+m$ je složené (viz II.5.2). 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, 724, 725, 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 II.2.1).

II.5.4 Poučení. Uvažujme nenulová čísla n taková, že $p^2|n$ kdykoliv $p \in \mathbb{P}$, $p|n$ (t.j., $\mathrm{cont}_p(n) \geq 2$ kdykoliv $\mathrm{cont}_p(n) > 0$). Těmto číslům se někdy říká mocná, či plnočtvercová. Nám se více zamlouvá jim říkat vydatná.

(i) Samozřejmě, pro každé $n \neq 0$ a pro každé $k \geq 2$ je mocnina n^k vydatné číslo.

(ii) Čísla 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 72, 81, 100, 108, 121, 125, 128, 144, 169, 196, 200, 216, 225, 243, 256, 288, 289, 324, 343, 361, 392, 400,

432, 441, 484, 500, 512, 529, 576, 625, 648, 675, 676, 729, 784, 800, 841, 864, 900, 961, 968, 972, 1000 jsou všechna vydatná čísla n, $1 \leq n \leq 1000$. Je to 54 čísel. Z nich pak čísla 72, 108, 200, 288, 392, 432, 500, 648, 675, 800, 864, 968, 972 nejsou mocninami (je to 13 čísel).

Postupné rozdíly výše uvedených vydatných čísel jsou 3, 4, 1, 7, 9, 2, 5, 4, 13, 15, 8, 9, 19, 8, 13, 4, 3, 16, 25, 27, 4, 16, 9, 18, 13, 32, 1, 35, 19, 18, 31, 8, 32, 9, 43, 16, 12, 17, 47, 49, 23, 27, 1, 53, 55, 16, 41, 23, 36, 61, 7, 4, 28. Seřadíme-li tyto rozdíly podle velikosti, dostaneme posloupnost 1, 2, 3, 4, 5, 7, 8, 9, 12, 13, 15, 17, 18, 19, 23, 25, 27, 28, 31, 32, 35, 36, 41, 43, 47, 49, 53, 55, 61.

(iii) Vydatná čísla jsou zřejmě uzavřená na součiny.

(iv) Nechť n, m jsou taková čísla, že součin mn je také vydatné číslo, přičemž $\mathrm{nsd}(n, m) = 1$. Zřejmě obě čísla n, m jsou vydatná.

(v) Předchozí bod lze také zobecnit: Nechť n, m jsou taková čísla, že součin mn i největší společný dělitel $\mathrm{nsd}(n, m)$ jsou vydatná čísla. Pak obě čísla n, m jsou vydatná.

(vi) Nechť $n \in \mathbb{Z}$ je takové číslo, že $n(n+1) = 2m$, kde m je vydatné číslo. Je $\mathrm{psd}(n, n+1) = 1$.

Je-li n sudé, pak čísla $n/2$ a $n+1$ jsou vydatná. Jestliže navíc $4|n$, pak i číslo n je vydatné.

Je-li n liché, pak čísla n a $(n+1)/2$ jsou vydatná. Jestliže navíc $4|n+1$ ($n \equiv_4 3$), pak i číslo $n+1$ je vydatné.

V obou případech je $(4n^2+4n)(4n^2+4n+1) = 2 \cdot 2n(n+1)(2n+1)^2 = 2 \cdot (2m(2n+1))^2$, kde $(2m(2n+1))^2$ je jistě vydatné a $4|4n^2+4n$. Samozřejmě, $4n^2+4n (= 4n(n+1) = 8m)$ a $4n^2+4n+1 (= (2n^2+1)^2)$ jsou po sobě jdoucí vydatná čísla.

(vii) Je $1 \cdot 2 = 2 \cdot 1$, kde 1 je vydatné. Z (vi) dostáváme postupně dvojice po sobě jdoucích vydatných čísel. $8 (= 2^3)$, $9 (= 3^2)$, $288 (= 2^5 \cdot 3^2)$, $289 (= 17^2)$, $332928 (= 2^7 \cdot 3^2 \cdot 17^2)$, $332929 (= 577^2)$, ... Dostáváme takto nekonečně mnoho dvojic.

(viii) Je $49 \cdot 50 = 2 \cdot 35^2$. I zde dostaneme nekonečně mnoho dvojic po sobě jdoucích vydatných čísel. První je $9800 (= 2^3 \cdot 5^7 \cdot 7^2)$, $9801 (= 99^2 \cdot 3^4 \cdot 11^2)$.

(ix) $675 (= 3^3 \cdot 5^2)$, $676 (= 26^2 = 2^2 \cdot 13^2)$ a $12167 (= 23^2)$, $12168 (= 2^3 \cdot 3^2 \cdot 13^2)$ jsou dvojice po sobě jdoucích vydatných čísel.

(x) Nechť $n \in \mathbb{N}$, přičemž n i $n+2$ jsou vydatná čísla, $n \neq -1$. Pak $n(n+2)$ je vydatné číslo. Samozřejmě, $(n+1)^2$ je vydatné číslo. Avšak $(n+1)^2 - n(n+2) = 1$. Tedy $n(n+2)$ a $(n+1)^2$ je dvojice po sobě jdoucích vydatných čísel. Například $25 (= 5^2)$ a $27 (= 3^3)$ skýtají dvojici 675, 676.

(xi) Nechť $n \in \mathbb{Z}$ přičemž n i $n+4$ jsou vydatná čísla (je $n \neq -4$). Samozřejmě, $n(n+4)$ a $(n+2)^2$ jsou vydatná čísla. Je $(n+2)^2 - n(n+4) = 4$.

Například, $4(=2^2)$, $8(=2^3)$ skýtají vydatná čísla $32(=2^5)$ a $36(=6^2=2^3\cdot 3^2)$, $36-32=4$. Dále pak $1152(=2^7\cdot 3^2)$ a $1156(=34^2=2^2\cdot 17^2)$.

Je také $125-121=4$, kde $121=11^2$ a $125=5^3$.

(xii) Čísla $214369(=463^2)$ a $214375(=5^4\cdot 7^3)$ jsou vydatná a $214375-214369=6$ (srovnej s I.8.4 (i)).

(xiii) Není známo, zda existují tři po sobě jdoucí vydatná čísla $n, n+1, n+2$.

(xiv) Je-li n sudé číslo, pak i $n+2$ je sudé a buďto $4\nmid n$ a nebo $4\nmid n+2$. Tedy alespoň jedno z čísel $n, n+2$ není vydatné.

(xv) Z (xiv) plyne, že neexistují čtyři po sobě jdoucí vydatná čísla.

(xvi) Je-li n liché číslo, přičemž $n+1$ je vydatné číslo, pak $n+3$ není vydatné.

II.5.5 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 sudá, 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 $a=p_1^{(r_1-3)/2}\dots p_s^{(r_s-3)/2}$, $b=p_1\cdots p_s$. 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 $a=p_1^{r_1/2}\cdots p_t^{r_t/2}p_{t+1}^{(r_{t+1}-3)/2}\dots p_s^{(r_s-3)/2}$ a $b=p_{t+1}\cdots p_s$.

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

II.5.6 Poznámka. Kladné vydatné číslo, které není druhou, či vyšší mocninou, je známo jako Achillovo číslo.

Čísla $72=2^3\cdot 3^2$, $108=2^2\cdot 3^3$ a $200=2^3\cdot 3^2$ jsou nejmenší tři Achillova čísla. Číslo $5000=2^35^4$ je také Achillovo. Říká se, že $5425069447=7^341^297^2$ a $5425069448=2^3\cdot 26041^2$ je nejmenší dvojice po sobě jdoucích Achillových čísel.

Nejmenší liché Achillovo číslo je $675=3^35^2$. Pro každé $p\in\mathbb{P}$, $p\geq 5$ a každé $k\geq 3$, k liché, jsou čísla $2^k\cdot p^2$ a $3^k\cdot p^2$ Achillova. To je nekonečně mnoho různých čísel, sudých i lichých.

II.5.7 Proposice. Nechť n je složené číslo. Potom existuje alespoň jedno prvočíslo p takové, že $p\mid n$, přičemž $p^2\leq |n|$.

Důkaz. Viz II.3.23. □

II.6 Bezčtvercová čísla

II.6.1 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 kladných 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, 33, 34, 35. Je známo, že existuje nekonečně mnoho čísel $k \geq 1$ takových, že $4k+1, 4k+2, 4k+3$ jsou bezčtvercová ($k = 1, 3, 4, 5, 7, 8, 9, 10, 14, 16, \dots$). Čísla 8, 9 nejsou bezčtvercová a 48, 49, 50 je první trojice po sobě jdoucích kladných čísel, která nejsou bezčtvercová.

Později (IV.6.2) si dokážeme, že pro každé $n \geq 2$ existuje n po sobě jdoucích čísel takových, že žádné z nich není bezčtvercové (srovnej s II.5.3).

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

II.6.2 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 II.3.4.

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

II.6.3 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. Lze předpokládat $n \geq 1$. Je-li $n = 1$, pak volíme $m = 1 = k$. Buď tedy $n \geq 2$. Podle II.3.4 je $n = p_1^{r_1} \cdots p_s^{r_s}$, kde $s, r_i \geq 1$ a $p_1, \dots, p_s$ jsou po dvou různá prvočísla.

Jsou-li všechna čísla r_i sudá, pak volíme $m = 1$ a $k = p_1^{r_1/2} \cdots p_s^{r_s/2}$.

Jsou-li všechna čísla r_i lichá, pak volíme $m = p_1 \cdots p_s$ a $k = p_1^{(r_1-1)/2} \cdots p_s^{(r_s-1)/2}$.

Nenastává-li ani jeden z předchozích případů, pak je $s \geq 2$ 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 $r_{t+1}, \dots, r_s$ lichá. Nyní volíme $m = p_{t+1} \cdots p_s$ a $k = p_1^{r_1/2} \cdots p_t^{r_t/2} \cdot p_{t+1}^{(r_{t+1}-1)/2} \cdots p_s^{(r_s-1)/2}$.

Dokázali jsme existenci čísel m a k. Teď je potřeba dokázat jejich jednoznačnost. Budeme postupovat indukcí podle n. Případ pro $n = 1, 2$ je jasný. Buď $n \geq 3$ a $n = m_1 k_1^2 = m_2 k_2^2$, 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 $p | m_1$. Jestliže $p | m_2$, pak $m_3 k_1^2 = m_4 k_2^2$, kde $m_3 = m_1/p$ a $m_4 = m_2/p$. Čísla m_3, m_4 jsou bezčtvercová a použijeme indukční předpoklad. Dostaneme $m_3 = m_4$ a $k_1 = k_2$. Pak ovšem také $m_1 = m_2$. Jestliže však $p \nmid m_2$ tak $p \mid k_2$. Nyní, $1 + 2\mathrm{cont}_p(n) = 2\mathrm{cont}_p(k_2)$, což nelze.

Zbytek je jasný. □

II.6.4 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 $\mathrm{cont}_p(r) + k\ \mathrm{cont}_p(n) = \mathrm{cont}_p(t) + k\ \mathrm{cont}_p(m) \leq 1 + k\ \mathrm{cont}_p(m)$ a $k(\ \mathrm{cont}_p(n) - \mathrm{cont}_p(m)) = \mathrm{cont}_p(t) - \mathrm{cont}_p(r) \leq 1$. Odtud, $\mathrm{cont}_p(n) - \mathrm{cont}_p(m) \leq 0$ a $\mathrm{cont}_p(n) \leq \mathrm{cont}_p(m)$. Podle II.3.10 je $n \mid m$. □

II.6.5 Věta. Nechť $n \in \mathbb{Z}$, $n \neq 0$. Potom existují jednonačně určená čísla $m \in \mathbb{Z}$ a $w \in \mathbb{N}$ taková, že $n = mw$, přičemž číslo m je bezčtvercové a $\underline{P}(m) \cap \underline{P}(w) = \emptyset$.

Důkaz. Lze předpokládat, že $n \geq 1$ a n není vydatné. Pak $n \geq 2$ a píšeme $n = p_1 \cdots p_k \cdot w$, kde $p_1, \dots, p_k$ jsou různá prvočísla, w je vydatné číslo a $p_i \nmid w$. Položíme $m = p_1 \cdots p_k$. □

II.6.6 Věta. Nechť $n \in \mathbb{Z}$, $n \neq 0, r \geq 2$. Potom existují jednoznačně určená čísla $m \in \mathbb{Z}$ a $k \in \mathbb{N}$ taková, že $n = m \cdot k^r$, přičemž $p^r \nmid m$ pro každé prvočíslo p.

Důkaz. Lze předpokládat, že $n \geq 1$. Máme $n = p_1^{s_1} \cdots p_t^{s_t}$, kde $t, s_i \in \mathbb{N}$ a p_i jsou po dvou různá prvočísla. Máme $s_i = ru_i + v_i$, kde $0 \leq v_i < r$. Nyní stačí položit $m = p_1^{v_1} \cdots p_t^{v_t}$ a $k = p_1^{u_1} \cdots p_t^{u_t}$. □

II.6.7 Poznámka. Věta II.6.3 snadno plyne z předcházející věty.

II.6.8 Úloha. Nechť $a, b, c \in \mathbb{N}$, $k \geq 2$, jsou taková čísla, že $a + b = c^k$. (i) Položme $r = \mathrm{nsd}(a, b)$, $r \geq 1$. Máme $a = ra_1$, $b = rb_1$, $a_1, b_1 \in \mathbb{N}$, $\mathrm{nsd}(a_1, b_1) = 1$. Je $r(a_1 + b_1) = a + b = c^k, r^2 a_1 b_1 = ab$.

(ii) Jistě $1^k \mid r$ a my si vezmeme největší kladné číslo s takové, že $s^k \mid r$. Je $r = ts^k, t \geq 1$, $\mathrm{cont}_p(t) \leq k-1$ pro každé $p \in \mathbb{P}$. Dále, $(a_1+b_1)ts^k = (a_1+b_1)r = a+b = c^k$, $a_1b_1(ts^k)^2 = ab$.

(iii) Nechť $p \in \mathbb{P}$. Je $\mathrm{cont}_p(a_1+b_1) + \mathrm{cont}_p(t) + k\,\mathrm{cont}_p(s) = k\mathit{cont}_p(c)$, z čehož plyne $0 \leq \mathrm{cont}_p(s) \leq \mathrm{cont}_p(c)$. Toto platí pro každé prvočíslo p, takže $s \mid c, c = vs, v \geq 1$. Je pak $(a_1+b_1)ts^k = c^k = v^k s^k$, z cehož dostáváme $(a_1+b_1)t = v^k$.

A teď, $\mathrm{cont}_p(a_1+b_1) + k - 1 \geq \mathrm{cont}_p(a_1+b_1) + \mathrm{cont}_p(t) = k\,\mathrm{cont}_p(v)$. Je-li $\mathrm{cont}_p(v) \geq 1$, potom $\mathrm{cont}_p(a_1+b_1) \geq 1$. Odtud, $\underline{P}(a_1+b_1) \subseteq \underline{P}(v)$. Samozřejmě $\underline{P}(t) \subseteq \underline{P}(v)$, takže $\underline{P}(t) \subseteq \underline{P}(a_1+b_1)$.

(iv) Nechť $p \in \underline{P}(a_1)$, přičemž $\mathrm{cont}_p(ab)$ je sudé číslo. Je $\mathrm{cont}_p(b_1) = 0$, takže $\mathrm{cont}_p(ab) = \mathrm{cont}_p(a) + \mathrm{cont}_p(b) = \mathrm{cont}_p(a_1) + 2\,\mathrm{cont}_p(ts^k)$. Odtud $\mathrm{cont}_p(a_1)$ je sudé číslo.

(v) Nechť $ab = d^2, d \geq 1$. Pak $\mathrm{cont}_p(a_1)$ je sudé číslo pro každé $p \in \mathbb{P}$. Tedy $a_1 = a_2^2$ pro nějaké $a_2 \geq 1$. Z důvodu symetrie je také $b_1 = b_2^2$ pro nějaké $b_2 \geq 1$. Celkově, $d^2 = ab = r^2a_1a_2 = (ra_2b_2)^2, ra_2b_2 = d$.

(vi) Nechť t je bezčtvercové číslo. Pak $t \mid v, t \mid a_1+b_1, v = wt, w \geq 1, c = wts, a_1+b_1 = w^kt^{k-1} = wv^{k-1}$.

(vii) Nechť a_1+b_1 je bezčtvercové číslo. Pak $a_1+b_1 \mid v, v = u(a_1+b_1), u \geq 1$. Dále, $(a_1+b_1)t = v^k = u^k(a_1+b_1)^k, t = u^k(a_1+b_1)^{k-1}$ a nutně $u = 1$ (neboť $u^k \mid t$). Je tedy $v = a_1+b_1, t = (a_1+b_1)^{k-1}, r = (a_1+b_1)^{k-1}s^k, c = (a_1+b_1)s, r = sc^{k-1}, a = a_1(a_1+b_1)^{k-1}s^k = a_1v^{k-1}s^k$, $b = b_1(a_1+b_1)^{k-1}s^k = b_1v^{k-1}s^k, ab = a_1b_1(v^{k-1}s^k)^2$.

II.6.9 Úloha. Nechť $a, b, c \in \mathbb{N}$ jsou taková čísla, že $a+b = c^2$. Navažme na předchozí úlohu, kde zvolíme $k = 2$ a použijeme stejné značení.

Pro $k = 2$ je t bezčtvercové číslo a podle II.6.8 (vi) je $v = wt, c = wts, a_1+b_1 = tw^2 = tv$. Dále $r = ts^2, a = ts^2a_1, b = ts^2b_1, ab = a_1b_1(ts^2)^2$.

A teď předpokládejme, že $ab = d^2, d \geq 1$. Z II.6.8 (v) víme, že $a_1 = a_2^2, b_1 = b_2^2, d = ra_2b_2 = ts^2a_2b_2$. Je také $a = t(sa_2)^2, b = t(sb_2)^2$. Je $(sa_2)^2 + (sb_2)^2 = s^2(a_2^2+b_2^2) = s^2(a_1+b_1)$. Je $w^2t^2s^2 = c^2 = a+b = ts^2(a_1+b_1), w^2t = a_1+b_1 = a_2^2+b_2^2$. Jelikož t je bezčtvercové, tak w je největší číslo takové, že $w \mid a_1+b_1$ $(= a_2^2+b_2^2)$. Rovněž také, ws je největší číslo, jehož druhá mocnina dělí součet $(sa_2)^2 + (sb_2)^2$.

II.6.10 Úloha. Obraťme úvahy činěné v předchozí úloze.

Zvolme $x, y \in \mathbb{N}$ libovolně a buď z největší číslo takové, že $z^2 \mid x^2+y^2$. Je $x^2+y^2 = qz^2$, kde q je bezčtvercové číslo. Teď položíme $a = qx^2, b = qy^2$. Je $a+b = q(x^2+y^2) = qz^2$ a $ab = qx^2qy^2 = (qxy)^2$.

A teď se vraťme k předchozí úloze. Předně, $c = qz$ a $d = qxy$. Buď $g = \mathrm{nsd}(x,y)$, $x = gx_1, y = gy_1, \mathrm{nsd}(x_1,y_1) = 1$. Máme $qg^2 = \mathrm{nsd}(a,b) = r, q =$

$t, g = s, qz = c = wts = wqg, z = wg = ws$. Dále, $a = t(sa_2)^2 = q(sa_2)^2 = qx^2, x = sa_2$ a podobně $y = sb_2$. Je pak $x_1 = a_2, y_1 = b_2, x_1^2 = a_1, y_1^2 = b_1$.

II.6.11 Příklad. Pro $x = 1, y = 1$ dostaneme $a = 2 = b$. Pro $x = 1, y = 2$ dostaneme $a = 5, b = 20$. Pro $x = 1, y = 3$ dostaneme $a = 10, b = 90$. Pro $x = 1, y = 4$ dostaneme $a = 17, b = 272$. Pro $x = 2, y = 2$ dostaneme $a = 8 = b$. Pro $x = 2, y = 3$ dostaneme $a = 52, b = 117$. Pro $x = 2, y = 4$ dostaneme $a = 20, b = 80$.

Namátková kontrola: $17 + 272 = 289 = 17^2, 17 \cdot 272 = 4624 = 2^4 \cdot 17^2 = 68^2$.

Všimněme si, že $4 + 4 = 2^3, 4 \cdot 4 = 4^2, 16 \cdot 16 = 2^5, 16 \cdot 16 = 16^2$, atd. Je také $9 + 27 = 6^2, 9 \cdot 27 = 3^5$.

II.7 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 "předrozkladu" lze někdy vyjít.

II.7.1 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 $4c^2 - 4d^2 = (a+b)^2 - (a-b)^2 = a^2 + 2ab + b^2 - a^2 + 2ab - b^2 = 4ab = 4n$, $n = ab = c^2 - d^2 = (c-d)(c+d)$, $c^2 = n + d^2$ a $d^2 = c^2 - n$. Samozřejmě, $c^2 \geq n$.

Je-li $b \geq 5$, tak $n + 1 > 4c$ podle I.3.3. Je-li $a \geq 7$, $b \geq 3$, tak $n + 1 > 4c$ podle I.3.4. Je-li $a = 5$, $b = 3$, tak $n = 15$, $c = 4$, $n + 1 = 16 = 4c$. Je-li $a = 3 = b$, 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 $m^2 \geq n$. Je-li $m^2 = n$, jsme hotovi. Je-li $m^2 > n$, pak pátráme, zda $m^2 - n = k_0^2$ pro nějaké $k_0 \geq 1$, $m > k_0$. Není-li tomu tak, pak nás bude zajímat rovnice $(m+1)^2 - n = k_1^2$, $k_1 \geq 1$, $m+1 > k_1$. Obecně pak rovnice $(m+l)^2 - n = k_l^2$, $k_l \geq 1$, $m + l > k_l$. 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).

II.7.2 Příklad. Buď $n = 21$. Potom $m = 5$, $5^2 = 25$, $25 - n = 4 = 2^2$, $n = 5^2 - 2^2 = (5-2)(5+2) = 3 \cdot 7$.

II.7.3 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 $n = 52^2 - 21^2 = (52 - 21)(52 + 21) = 31 \cdot 73$.

II.7.4 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 $6077 = 81^2 - 22^2 = (81 - 22)(81 + 22) = 59 \cdot 103$.

II.7.5 Příklad. Buď $n = 2027651281$. Je $m = 45030$, $m^2 = 2027700900$ a $2m = 90060$. A nyní píšeme

$$\begin{aligned}
m^2 - n = \quad & 2027700900 - 2027651281 = & 49619 \\
& 2m + 1 = & 90061 \\
(m+1)^2 - n = \quad & m^2 - n + 2m + 1 = & 139680 \\
& 2m + 3 = & 90063 \\
(m+2)^2 - n = \quad & (m+1)^2 - n + 2m + 3 = & 229743 \\
& 2m + 5 = & 90065 \\
(m+3)^2 - n = \quad & (m+2)^2 - n + 2m + 5 = & 319808 \\
& 2m + 7 = & 90067 \\
(m+4)^2 - n = \quad & (m+3)^2 - n + 2m + 7 = & 40872 \\
& 2m + 9 = & 90069 \\
(m+5)^2 - n = \quad & (m+4)^2 - n + 2m + 9 = & 499944 \\
& 2m + 11 = & 90071 \\
(m+6)^2 - n = \quad & (m+5)^2 - n + 2m + 11 = & 590015 \\
& 2m + 13 = & 90073 \\
(m+7)^2 - n = \quad & (m+6)^2 - n + 2m + 13 = & 680088 \\
& 2m + 15 = & 90075 \\
(m+8)^2 - n = \quad & (m+7)^2 - n + 2m + 15 = & 770163 \\
& 2m + 17 = & 90077 \\
(m+9)^2 - n = \quad & (m+8)^2 - n + 2m + 17 = & 860240 \\
& 2m + 19 = & 90079 \\
(m+10)^2 - n = \quad & (m+9)^2 - n + 2m + 19 = & 950319 \\
& 2m + 21 = & 90081 \\
(m+11)^2 - n = \quad & (m+10)^2 - n + 2m + 21 = & 1040400
\end{aligned}$$

což je 1020^2.

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

Tento příklad je poučný. Předně jsme použili vztahu $(m+i+1)^2 - n = (m+i)^2 - n + 2m + 2i + 1$ 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 (viz I.6.1).

Z toho plyne, že v našem příkladě zjišťujeme pouze, zda čísla 499944 a 1040400 jsou druhými mocninami. Ovšem, $499944 = 8 \cdot 62493$. Je tedy $\mathrm{cont}_2(499944) = 3$ a 499944 není druhou mocninou. Oproti tomu, $1040400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 17^2 = (2^2 \cdot 3 \cdot 5 \cdot 17)^2 = 1020^2$.

II.7.6 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.

II.8 Cvičení

II.8.1 Cvičení. Za účelem rekreačního cvičení si sestavme tabulku prvočíselných rozklaů čísel n^2-1 pro $1 \leq n \leq 49$. Není to tak těžké, neboť $n^2-1 = (n+1)(n-1)$ a je-li p takové prvočíslo, že $p \mid (n-1)$ a $p \mid (n+1)$, pak $p = 2$. Navíc se občas přihodí, že aspoň jedno z čísel $n-1$, $n+1$ je již prvočíslo.

n	1	2	3	4	5	6	7
n^2-1	0	3	8	15	24	35	48
Πp	–	3	2^3	$3 \cdot 5$	$2^3 \cdot 3$	$5 \cdot 7$	$2^4 \cdot 3$
n	8	9	10	11	12	13	14
n^2-1	63	80	91	120	143	168	195
Πp	$3^2 \cdot 7$	$2^4 \cdot 5$	$3^2 \cdot 11$	$2 \cdot 3 \cdot 5$	$11 \cdot 13$	$2^3 \cdot 3 \cdot 7$	$3 \cdot 5 \cdot 13$
n	15	16	17	18	19	20	21
n^2-1	224	255	288	323	360	399	440
Πp	$2^5 \cdot 7$	$3 \cdot 5 \cdot 17$	$2^5 \cdot 3^2$	$17 \cdot 19$	$2^3 \cdot 3^2 \cdot 5$	$3 \cdot 7 \cdot 19$	$2^3 \cdot 5 \cdot 11$
ni	22	23	24	25	26	27	28
n^2-1	483	528	575	624	675	728	783
Πp	$3 \cdot 7 \cdot 23$	$2^4 \cdot 3 \cdot 11$	$5^2 \cdot 23$	$2^4 \cdot 3 \cdot 13$	$3^2 \cdot 5^2$	$2^2 \cdot 7 \cdot 13$	$3^3 \cdot 29$
n	29	30	31	32	33	34	35
n^2-1	840	899	960	1023	1088	1155	1224
Πp	$2^3 \cdot 3 \cdot 5 \cdot 7$	$29 \cdot 31$	$2^6 \cdot 3 \cdot 5$	$3 \cdot 11 \cdot 31$	$2^6 \cdot 17$	$3 \cdot 5 \cdot 7 \cdot 11$	$2^3 \cdot 3^2 \cdot 17$
n	36	37	38	39	40	41	42
n^2-1	1295	1368	1443	1520	1599	1680	1763
Πp	$3 \cdot 5 \cdot 37$	$2^3 \cdot 3^2 \cdot 19$	$3 \cdot 13 \cdot 37$	$2^4 \cdot 5 \cdot 11$	$3 \cdot 13 \cdot 41$	$2^4 \cdot 3 \cdot 5 \cdot 7$	$41 \cdot 43$
n	43	44	45	46	47	48	49
n^2-1	1848	1935	2024	2115	2208	2303	2400
Πp	$2^3 \cdot 3 \cdot 7 \cdot 11$	$3^2 \cdot 5 \cdot 43$	$2^3 \cdot 11 \cdot 23$	$3^2 \cdot 5 \cdot 47$	$2^5 \cdot 3 \cdot 23$	$7^2 \cdot 47$	$2^5 \cdot 3 \cdot 5^2$

Je $(n+1)^2 - 1 = (n^2-1) + (2n+1)$. Pro $n \in \mathbb{Z}$ je n^2-1 prvočíslo pouze pro $n = \pm 2$ a potom $n^2-1 = 3$. Pro $n \in \mathbb{Z}$ je $n^2-1 = m^k, m \geq 2, k \geq 2$, pouze pro $n = \pm 3$ a potom $n^2-1 = 8 = 2^3$. Je-li p takové prvočíslo, že i $p+2$ je prvočíslo, pak $(p+1)^2 - 1 = p(p+2)$ je prvočíselný rozklad a číslo $(p+1)^2-1$ je bezčtvercové. Číslo $17^2 - 1 = 2^5 \cdot 3^2$ je Achillovo (viz II.5.6). Pro každé $n \in \mathbb{Z}$ je $n \mid n(n+2) = (n+1)^2 - 1$.

Je-li n sudé, pak n^2-1 je liché. Je-li n liché, pak $n-1, n+1$ jsou sudá čísla a tak $4 \mid n^2-1$. Jestliže navíc $8 \nmid n^2-1$, pak $n-1 = 2k$, $n+1 = 2l$, kde k, l jsou lichá čísla. Odtud, $2k+1 = n = 2l-1, 2l = 2k+2, l = k+1, l$ je sudé, spor. Zjistili jsme, že $8 \mid n^2-1$ pro n liché. Je také zřejmé, $3 \mid n^2-1$ právě když $3 \nmid n$.

II.8.2 Cvičení. A teď prvočíselné rozklady čísel n^2+1 pro $1 \leq n \leq 49$.

n	1	2	3	4	5	6	7
n^2+1	2	5	10	17	26	37	50
Πp	2	5	$2 \cdot 5$	17	$2 \cdot 13$	37	$2 \cdot 5^2$
n	8	9	10	11	12	13	14
n^2+1	65	82	101	122	145	170	197
Πp	$5 \cdot 13$	$2 \cdot 41$	101	$2 \cdot 61$	$5 \cdot 29$	$2 \cdot 5 \cdot 17$	197
n	15	16	17	18	19	20	21
n^2+1	226	257	290	325	362	401	442
Πp	$2 \cdot 113$	257	$2 \cdot 5 \cdot 29$	$5^2 \cdot 13$	$2 \cdot 181$	401	$2 \cdot 13 \cdot 17$
ni	22	23	24	25	26	27	28
n^2+1	485	530	577	626	677	730	785
Πp	$5 \cdot 97$	$2 \cdot 5 \cdot 53$	577	$2 \cdot 313$	677	$2 \cdot 5 \cdot 73$	$5 \cdot 157$
n	29	30	31	32	33	34	35
n^2+1	842	901	962	1025	1090	1157	1226
Πp	$2 \cdot 421$	$17 \cdot 53$	$2 \cdot 13 \cdot 37$	$5^2 \cdot 41$	$2 \cdot 5 \cdot 109$	$13 \cdot 89$	$2 \cdot 613$
n	36	37	38	39	40	41	42
n^2+1	1297	1370	1445	1522	1601	1682	1765
Πp	1297	$2 \cdot 5 \cdot 137$	$5 \cdot 17^2$	$2 \cdot 761$	1601	$2 \cdot 29^2$	$5 \cdot 353$
n	43	44	45	46	47	48	49
n^2+1	1850	1937	2026	2117	2210	2305	2402
Πp	$2 \cdot 5^2 \cdot 37$	$13 \cdot 149$	$2 \cdot 1013$	$29 \cdot 73$	$2 \cdot 5 \cdot 13 \cdot 17$	$5 \cdot 461$	$2 \cdot 1201$

Je-li $n = 2k+1, k \geq 0$ pak $2 \mid n^2+1 = 4k^2+4k+2$ a $4 \nmid n^2+1$. Tedy pro liché $n \geq 3$ není n^2+1 prvočíslem. Jestliže dekadický zápis čísla n končí na některou z číslic $2, 3, 7, 8$, pak $5 \mid n^2+1$ a tedy n^2+1 není prvočíslem pro $n \geq 3$. Takže, jestliže n^2+1 je prvočíslo, pak buďto $n = 1, 2$ a nebo $n \geq 4$ je sudé a dekadický zápis čísla n končí na 0,4 nebo 6 (například $n = 4, 6, 10, 14, 16, 20, 24, 26, 36, 40$). Není známo, zda existuje nekonečně mnoho prvočísel tvaru n^2+1.

II.8.3 Cvičení. (i) Všimněme si, že číslo n^2-2 je prvočíslem pro $n = 2, 3, 5, 7, 13, 15, 19, 21, 27, 29, \ldots$.

(ii) Všimněme si, že číslo n^2+2 je prvočíslem pro $0, 1, 3, 9, 15, 21, \ldots$

(iii) Všimněme si, že číslo n^2-3 je prvočíslem pro $4, 8, 10, 14, 20, \ldots$.

(ii) Všimněme si, že číslo n^2+3 je prvočíslem pro $2, 4, 8, 10, 14, 22, \ldots$.

(v) Je $23^3+1 = 2^3 \cdot 3^2 \cdot 13^2$ (a $2^3+1 = 3^2$).

II.8.4 Cvičení. Prvočíselné rozklady čísel $2^n - n$ pro $1 \leq n \leq 12$:

n	1	2	3	4	5	6
2^n-n	1	2	5	12	27	58
Πp	–	2	5	$2^2 \cdot 3$	3^3	$2 \cdot 29$
n	7	8	9	10	11	12
n^2-n	121	248	413	1014	2037	4084
Πp	11^2	$2^3 \cdot 31$	$7 \cdot 59$	$2 \cdot 3 \cdot 13^2$	$3 \cdot 679$	$2^2 \cdot 1021$

II.8.5 Cvičení. Prvočíselné rozklady čísel $2^n + n$ pro $1 \leq n \leq 12$:

n	1	2	3	4	5	6
$2^n + n$	3	6	11	20	37	70
Πp	3	$2 \cdot 3$	11	$2^2 \cdot 5$	37	$2 \cdot 5 \cdot 7$
n	7	8	9	10	11	12
$n^2 + n$	135	264	521	1034	2059	4108
Πp	$3^3 \cdot 5$	$2^2 \cdot 3 \cdot 11$	521	$2 \cdot 11 \cdot 47$	$29 \cdot 71$	$2^2 \cdot 13 \cdot 79$

II.8.6 Cvičení. (i) Je $100 = 10^2 = (7+3)^2 = 7^2+2(7\cdot 3)+3^2 = 49+42+9$, $121 = 11^2 = (10+1)^2 = 49+63+9 = 7^2+3(3\cdot 7)+3^3$, Je $4 = (-2)^2 = (1+(-3))^2 = 1-6+9 = 1^2+2(1\cdot(-3))+(-3)^2$.

(ii) Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $(a+b+1)^2 = a^2+3ab+b^2$. Je pak $a^2+2ab+b^2+2a+2b = a^2+3ab+b^2$, $1+2a+2b = ab$, $a(b-2) = 2b+1 = 2(b-2)+5$, $(a-2)(b-2) = 5$, $a-2, b-2 \in \{1,-1,5,-5\}$ a $(a,b) = (3,7),(7,3),(1,-3)(-3,1)$.

II.9 Zábavné nerovnosti

II.9.1 Zábavka. Nechť $n \geq 1$ a nechť $a_1, \ldots, a_n$ jsou libovolně vybraná celá čísla. Buď I libovolná (prázdná či neprázdná) část intervalu $\{1, \ldots, n\}$ kladných čísel (od 1 do n). Položme $\alpha(I) = \sum_{i=1}^{n} a_i^2 + 2\sum_{i\in I} a_i$ (označení jen pro tuto sekci). Je jistě $\alpha(I) = \sum_{i\notin I} a_i^2 + 2\sum_{i\in I}(a_i^2 + 2a_i) = \sum_{i\notin I} a_i^2 + 2\sum_{i\in I}(a_i+1)^2 - |I|$. Zajímejme se o to, kdy je číslo $\alpha(I)$ kladné, nulové či záporné.

Položme $K_1 = \{i \mid 1 \leq i \leq n, a_i \neq 0\}$ a $I_1 = \{i \mid i \in I, a_i \neq 0\}$. Jistě je $I_1 = I \cap K_1$. Jelikož $0^2 = 0 = 0^2 + 2\cdot 0$, tak vidíme, že $\alpha(I) = \sum_{i\in K_1} a_i^2 + 2\sum_{i\in I_1} a_i$.

Položme $L_1 = \{i \mid i \in I_1, a_i = -2\}$, $K_2 = K_1 \backslash L_1$,$I_2 = I_1 \backslash L_1$. Je $K_2 = \{i \mid 1 \leq i \leq n, a_i \neq 0, -2$ nebo $a_i = -2, i \notin I\}$, $I_2 = \{i \mid I, a_i \neq 0, -2\}$ a $I_2 \subseteq K_2$. Jelikož $(-2)^2 + 2(-2) = 0$, tak vidíme, že $\alpha(I) = \sum_{i\in K_2} a_i^2 + 2\sum_{i\in I_2} a_i$.

Položme $L_2 = \{i \mid i \in I, a_i = -1\}$, $m = |L_2|$, $K_3 = K_2 \setminus L_2$ a $I_3 = I_2 \setminus L_2$. Je $K_3 = \{i \mid 1 \leq i \leq n, a_i \neq 0, -1, -2$, nebo $a_i = -1, i \notin I$ nebo $a_i = -2, i \notin I\}$, $I_3 = \{i \mid i \in I, a_i \neq 0, -1, -2\}$ a $I_3 \subseteq K_3$. Jelikož $(-1)^2 + 2(-1) = -1$, tak vidíme, že $\alpha(I) = -m + \sum_{i\in K_3} a_i^2 + 2\sum_{i\in I_3} a_i$.

Buď $i \in I_3$. Je-li $a_i > 0$, pak $a_i^2 + 2a_i \geq 3a_i = 3|a_i| > |a_i|$. Je-li $a_i \leq 0$, pak $a_i \leq -3$ a $a_i^2 + 2a_i \geq |a_i|$ (v poslední nerovnosti nastane rovnost pouze pro $a_i = -3$). Je tedy $\alpha(I) \geq -m + \sum_{i\in K_3} |a_i|$.

(i) Zjistili jsme, že $\alpha(I) \geq 0$ za předpokladu, že $\sum_{i\in K_3} |a_i| \geq m$.

(ii) Snadno nahlédneme, že $L_3 = \{i \mid 1 \leq i \leq n, a_i \geq 1\} \subseteq K_3$. Je jistě $\sum_{i\in L_3} a_i \geq \sum_{i=1}^{n} a_i$. Takže $\alpha(I) \geq -m + \sum_{i\in K_3} |a_i| \geq -m + \sum_{i\in L_3} a_i = \sum_{i\in L_4} a_i$, kde $L_4 = L_2 \cup L_3$ $(= \{i \mid 1 \leq i \leq n, a_i \geq 1$ nebo $i \in I, a_i = -1\}$).

(iii) Zjistili jsme, že $\alpha(I) \geq 0$ za předpokladu, že $\sum_{i\in L_4} a_i \geq 0$.

(iv) Je zjevné, že $\sum_{i\in L_4} a_i \geq \sum_{i=1}^{n} a_i$. Takže $\alpha(I) \geq 0$ za předpokladu $\sum_{i=1}^{n} a_i \geq 0$.

(v) Předpokládejme, že $\alpha(I) = -m + \sum_{i\in K_3} |a_i|$. Jelikož $a_i^2 + 2a_i \geq 3|a_i|$ pro $i \in I, a_i \geq 1$, tak je nutně $a_i \leq 0$ pro každé $i \in I$. Dále $a_i^2 + 2a_i > |a_i|$ pro $i \in I, a_i \leq -4$. Tedy $a_i \in \{0, -1, -2, -3\}$ pro každé $i \in I$. Je pak $\sum_{i\in I_3}(a_i^2 + 2a_i) = 3k$, kde $k = |\{i \mid i \in I, a_i = -3\}|$. Odtud $\alpha(I) = -m + \sum_{i\in K_3} a_i^2 + 2\sum_{i\in I_3} a_i = -m + 3k + \sum_{i\in K_3\setminus I} a_i^2$, čili $\sum_{i\in K_3} |a_i| = 3k + \sum_{i\in K_3\setminus I} a_i^2$. Ovšem $\sum_{i\in K_3} |a_i| = 3k + \sum_{i\in K_3\setminus I} |a_i|$ takže $\sum_{i\in K_3\setminus I} |a_i| = \sum_{i\in K_3\setminus I} a_i^2$, z čehož plyne $a_i^2 = |a_i|$ a $a_i \in \{-1, 1\}$ pro každé $i \in K_3 \setminus I$. Celkově dostáváme $a_i \in \{-1, 0, 1\}$ pro každé $i \notin I$, $a_i \in \{0, 1, -1, -2, -3\}$ pro každé $i = 1, \ldots, n$.

(vi) Úvahu činěnou v (v) nyní obraťme. Nechť je tedy $a_i \in \{0, 1, -1, -2, -3\}$ pro každé $i \in I$ a $a_i \in \{-1, 0, 1\}$ pro každé $i \notin I$. Je pak $\alpha(I) = -m + 3k + u + v$, kde $u = |\{i \mid i \notin I, a_i = 1\}|$ a $v = |\{i \mid i \notin I, a_i = -1\}|$. Je dále $\sum_{i\in K_3} |a_i| = 3k + u + v$. Tedy $\alpha(I) = -m + \sum_{i\in K_3} |a_i|$. Navíc platí

$\sum_{i=1}^n a_i = -m - 3k - 2w - v - u$, kde $w = |\{i \mid i \in I, a_i = -2\}|$. Je tedy $\sum_{i=1}^n a_i \geq 0$ právě když $u \geq m + 3k + 2w + v$.

(vii) Z (v) a (vi) plyne, že $\alpha(I) = -m + \sum_{i\in K_3} |a_i|$ právě když $a_i \in \{0, -1, -2, -3\}$ pro $i \in I$ a $a_i \in \{1, 0, -1\}$ pro $i \notin I$.

(viii) V (ii) a (iv) jsme objevili, že $\alpha(I) \geq -m + \sum_{i\in K_3} |a_i| \geq \sum_{i\in L_4} a_i \geq \sum_{i=1}^n a_i$. Z (vii) nyní plyne, že $\alpha(I) = \sum_{i\in L_4} a_i$ právě tehdy, když jsou splněny ekvivalentní podmínky z (vi) a navíc $K_3 = L_3$. To jest, $a_i \in \{0, -1, -2\}$ pro $i \in I$ a $a_i \in \{1, 0\}$ pro $i \notin I$. Je pak $\sum_{i=1}^n a_i = -m - 2w + u$.

(ix) Z (viii) plyne, že $\alpha(I) = \sum_{i=1}^n a_i$ právě když $a_i \in \{0, -1\}$ pro $i \in I$ a $a_i \in \{1, 0\}$ pro $i \notin I$. Je pak $\sum_{i=1}^n a_i = u - m$.

II.9.2 Proposice. Nechť $n \geq 1$ a $a_1, \ldots, a_n$ jsou celá čísla. Buď I libovolná část celočíselného intervalu $\{1, \ldots, n\}$. Potom:

(i) $\sum_{i=1}^n a_i^2 + 2\sum_{i\in I} a_i \geq \sum_{i=1}^n a_i$.

(ii) Rovnost platí právě když $a_i \in \{0, -1\}$ pro $i \in I$ a $a_i \in \{1, 0\}$ pro $i \notin I$

Důkaz. Vše je podrobně rozebráno v II.9.1. Nicméně si uveďme velmi rychlý důkaz. Máme $\sum_{i=1}^n a_i^2 + 2\sum_{i\in I} a_i - \sum_{i=1}^n a_i = u + v$, kde $u = \sum_{i\in I}(a_i^2 + a_i)$, $v = \sum_{i\notin I}(a_i^2 - a_i)$. Pro každé $a \in \mathbb{Z}$ je $a^2 + a \geq 0$, přičemž rovnost nastává pouze pro $a = 0, -1$. Pro každé $a \in \mathbb{Z}$ je $a^2 - a \geq 0$, přičemž rovnost nastává pouze pro $a = 0, 1$. Zbytek je zjevný. □

II.9.3 Příklad. (i) Buď $n = 2$, $I = \{1\}$, $a_1 = -1$, $a_2 = 0$. Je $a_1 + a_2 = -1$, $a_1^2 + 2a_1 + a_2^2 = -1$.

(ii) Buď $n = 3$, $I = \{1, 2\}$, $a_1 = -2$, $a_2 = -1$, $a_3 = 1$. Je $a_1 + a_2 + a_3 = -2$, $a_1^2 + 2a_1 + a_2^2 + 2a_2 + 2a_3 = 0$.

(iii) Buď $n = 4$, $I = \{1, 2, 3, 4\}$, $a_1 = -3$, $a_2 = -1$, $a_3 = -1$, $a_4 = -1$. Je $a_1 + a_2 + a_3 + a_4 = -6$, $a_1^2 + 2a_1 + a_2^2 + 2a_2 + a_3^2 + 2a_3 + a_4^2 + 2a_4 = 0$.

(iv) Buď $n = 2$, $I = \{1, 2\}$, $a_1 = -2$, $a_2 = 1$. Je $a_1 + a_2 = -1$, $a_1^2 + 2a_1 + a_2^2 + 2a_2 = 3$.

II.9.4 Proposice. Nechť $n \geq 1$ a nechť $a_1, \ldots, a_n$ jsou taková celá čísla, že $\sum_{i=1}^n |a_i| \geq n$. Označme z počet těch indexů i, pro něž je $a_i = 0$. Potom:

(i) $\sum_{i=1}^n (a_i^2 - a_i) \geq 2z$.

(ii) Rovnost platí tehdy a jen tehdy, jestliže $a_i \in \{0, 1, 2\}$ pro každé $i, 1 \leq i \leq n$, a $\sum_{i=1}^n a_i = n$ (potom $z = |\{i \mid 1 \leq i \leq n, a_i = 2\}|$ a $n - 2z = |\{i \mid 1 \leq i \leq n, a_i = 1\}|$).

Důkaz. Je $\sum_{i=1}^n a_i^2 - \sum_{i=1}^n a_i - 2z \geq \sum_{i=1}^n |a_i|^2 - \sum_{i=1}^n |a_i| - 2z \geq \sum_{i=1}^n |a_i|^2 - 2\sum_{i=1}^n |a_i| + n - 2z = \sum_{i=1}^n (|a_i| - 1)^2 - 2z$ (je totiž $n - \sum_{i=1}^n |a_i| \leq 0$). Položme $b_i = |a_i| - 1$ pro každé i. Je $\sum_{i=1}^n b_i = \sum_{i=1}^n |a_i| - n \geq 0$ a $|I| = z = -\sum_{i\in I} b_i$,

kde $I = \{i \in 1 \le i \le n, a_i = 0\}$. Nyní $\sum_{i=1}^n (a_i^2 - a_i) - 2z \ge \sum_{i=1}^n b_i^2 + 2\sum_{i\in I} b_i \ge \sum_{i=1}^n b_i \ge 0$ (použije se II.2.9 (i)).

A teď, nechť $\sum_{i=1}^n (a_i^2 - a_i) = 2z$. Potom $\sum_{i=1}^n (a_i^2 - a_i) - 2z = \sum_{i=1}^n b_i^2 + 2\sum_{i\in I} b_i = \sum_{i=1}^n b_i = 0$. Z II.2.9 (ii) nyní plyne $b_i \in \{-1, 0\}$ pro $i \in I$ a $b_i \in \{0, 1\}$ pro $i \notin I$. Jinak napsáno, $a_i \in \{0, \mp 1, \mp 2\}$. Dále $\sum_{i=1}^n b_i = 0$ implikuje $\sum_{i=1}^n |a_i| = n$. Máme ovšem $\sum_{i=1}^n (a_i^2 - a_i) - 2z \ge \sum_{i=1}^n (a_i^2 - |a_i|) - 2z \ge 0$. Tedy $\sum_{i=1}^n a_i = \sum_{i=1}^n |a_i| - n$. Odtud $a_i \ge 0$ pro každé i. Takže $a_i \in \{0, 1, 2\}$. Naopak, je-li $a_i \in \{0, 1, 2\}$ a $\sum_{i=1}^n a_i = n$, pak $\sum_{i=1}^n a_i^2 - \sum_{i=1}^n a_i - 2z = 4v + u - n - 2z$, kde $v = |\{i \in a_i = 2\}|$ a $u = |\{i \in a_i = 1\}|$. Jelikož $n = u + v + z$, tak $4v + u - n - 2z = 3v - 3z$. Jelikož $n = \sum_{i=1}^n a_i = 2v + u$, tak $2v = n - u = v + z$, $v = z$ a $3v - 3z = 0$. □

II.9.5 Proposice. Nechť $n \ge 1$ a nechť $a_1, \dots, a_n, b_1, \dots, b_n$ jsou taková celá čísla, že $\sum_{i=1}^n a_i \ge n$ a $\sum_{i=1}^n b_i \ge n$. Označme z_1 (popř. z_2) počet těch indexů, pro něž $a_i = 0$ (popř. $b_i = 0$) a vezměme si libovolnou část I celočíselného intervalu $\{1, \dots, n\}$ (ať prázdnou či neprázdnou). Buď ještě $m = |I|$, $0 \le m \le n$. Potom:

(i) $2\sum_{i=1}^n (a_i^2 + b_i^2 + a_i b_i) + 4m \ge 3\sum_{i=1}^n (a_i + b_i) + 2\sum_{i\in I} (a_i + b_i) + 2z_1 + 2z_2$
$= \sum_{i=1}^n (a_i + b_i) + 2(\sum_{i=1}^n (a_i + b_i) + \sum_{i\in I} (a_i + b_i) + z_1 + z_2)$
$= 5\sum_{i\in I} (a_i + b_i) + 3\sum_{i\notin I} (a_i + b_i) + 2(z_1 + z_2)$.

(ii) Rovnost platí právě když

(a) $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$,

(b) $a_i, b_i \in \{0, 1, 2\}$ pro každé $i = 1, \dots, n$,

(c) $a_i + b_i \in \{2, 3\}$ pro každé $i \in I$,

(d) $a_i + b_i \in \{1, 2\}$ pro každé $i \notin I$.

Důkaz. (i) Buď $J = \{1, \dots, n\} \setminus I$ a $c_i = a_i + b_i - 2$ pro každé $i = 1, \dots, n$. Je $\sum_{i=1}^n c_i = -2n + \sum_{i=1}^n a_i + \sum_{i=1}^n b_i \ge 0$. A teď už počítejme. Je $2\sum_{i=1}^n (a_i^2 + b_i^2 + a_i b_i) + 4m - 3\sum_{i=1}^n (a_i + b_i) - 2\sum_{i\in I} (a_i + b_i) - 2z_1 - 2z_2 = u + v + w$ kde $u = \sum_{i=1}^n a_i^2 - \sum_{i=1}^n a_i - 2z_1$, $v = \sum_{i=1}^n b_i^2 - \sum_{i=1}^n b_i - 2z_2$ a $w = \sum_{i=1}^n a_i^2 + \sum_{i=1}^n b_i^2 + 2\sum_{i=1}^n a_i b_i + 4m - 2\sum_{i=1}^n a_i - 2\sum_{i=1}^n b_i - 2\sum_{i\in I} a_i - 2\sum_{i\in I} b_i$
$= \sum_{i=1}^n (a_i + b_i)^2 - 4\sum_{i=1}^n (a_i + b_i) + 4n + 2\sum_{i=1}^n (a_i + b_i) - 2\sum_{i\in I} (a_i + b_i) - 4n + 4m$
$= \sum_{i=1}^n c_i^2 + 2\sum_{i\in J} (a_i + b_i) - 4(n - m) = \sum_{i=1}^n c_i^2 + 2\sum_{i\in J} c_i$, neboť $n - m = |J|$. Nyní $w \ge 0$ podle II.9.1 a $u \ge 0, v \ge 0$ podle II.9.4.

(ii) Z předchozího vidíme, že rovnost platí, právě když je $u = v = w = 0$. Nyní, podle II.9.4 (ii), $u = 0 = v$ tehdy a jen tehdy, jestliže $\sum_{i=1}^n a_i = n = \sum_{i=1}^n b_i$ a $a_i, b_i \in \{0, 1, 2\}$. Tedy právě když je splněno (ii a,b). Podle II.9.2 (ii) je $w = 0$ právě když $a_i + b_i \in \{1, 2\}$ pro $i \notin I$ a $a_i + b_i \in \{2, 3\}$ pro $i \in I$ a $\sum_{i=1}^n (a_i + b_i) = 2n$. □

Kapitola III

Největší společný dělitel a nejmenší společný násobek

III.1 Největší společný dělitel

III.1.1 Nechť M je nějaká množina celých čísel (konečná či nekonečná, prázdná či neprázdná). Označme $\mathrm{sd}(M)$ množinu všech společných dělitelů čísel z množiny M. To jest, $n \in \mathrm{sd}(M)$ právě tehdy když $n \in \mathbb{Z}$ a $n \mid m$ pro každé $m \in M$. Množina $\mathrm{sd}(M)$ je neprázdná, neboť $1 \in \mathrm{sd}(M)$ a $-1 \in \mathrm{sd}(M)$ v každém případě.

Zřejmě je $\mathrm{sd}(\emptyset) = \mathbb{Z} = \mathrm{sd}(\{0\})$ a $\mathrm{sd}(\mathbb{Z}) = \{1, -1\} = \mathrm{sd}(\mathbb{N}) = \mathrm{sd}(\mathbb{N}_0)$. Dále, $\mathrm{sd}(M_1 \cup M_2) = \mathrm{sd}(M_1) \cap \mathrm{sd}(M_2)$ a $\mathrm{sd}(M_1) \cup \mathrm{sd}(M_2) \subseteq \mathrm{sd}(M_1 \cap M_2)$. Je-li $M_1 \subseteq M_2$, pak $\mathrm{sd}(M_2) \subseteq \mathrm{sd}(M_1)$.

Je-li $p \in \mathbb{P}$, pak $\mathrm{sd}(\{p\}) = \{1, -1, p, -p\} = \mathrm{sd}(\{-p\})$.

Je-li $\pm 1 \in M$, pak $\mathrm{sd}(M) = \{1, -1\}$.

Je-li $n \in \mathrm{sd}(M)$, pak $-n \in \mathrm{sd}(M)$.

III.1.2 Proposice. Nechť množina M obsahuje aspoň jedno nenulové číslo. Potom množina $\mathrm{sd}(M)$ je konečná.

Důkaz. Buď $m \in M$, $m \neq 0$. Je $\mathrm{sd}(M) \subseteq \mathrm{sd}(\{m\})$ a $n \in \mathrm{sd}(\{m\})$ právě tehdy když $n \mid m$. Pak ale $|n| \leq |m|$. Odtud naše tvrzení. □

III.1.3 Důležitá definice. Nechť množina M obsahuje alespoň jedno nenulové číslo. Podle III.1.1 a III.1.2 je množina $\mathrm{sd}(M)$ neprázdná a konečná. Označme symbolem $\mathrm{nsd}(M)$ největší číslo z množiny $\mathrm{sd}(M)$. Toto číslo je kladné, je jednoznačně určené množinou M a nazývá se největší společný dělitel množiny M.

Jestliže množina $M = \{m_1, \ldots, m_k\}$, $k \geq 1$, je konečná, pak mluvíme o největším společném děliteli čísel $m_1, \ldots, m_k$ a píšeme $\mathrm{nsd}(M) = \mathrm{nsd}(m_1, \ldots, m_k)$.

Zbývají dva případy: $M = \emptyset$ a $M = \{0\}$. Pro úplnost položíme $\mathrm{nsd}(\emptyset) = 0 = \mathrm{nsd}(\{0\})$.

III.1.4 Proposice. Nechť $m \in \mathbb{Z}$. Potom $\mathrm{nsd}(m) = \mathrm{nsd}(\{m\}) = |m|$.

Důkaz. Můžeme předpokládat $m \neq 0$. Jestliže $n \in \mathbb{Z}$ a $n \mid m$, pak $1 \leq |n| \leq |m|$ a $n \leq |m|$. Ovšem, $|m| \mid m$. Zbytek je jasný. □

III.1.5 Věta. Nechť $m_1, \ldots, m_k \in \mathbb{Z}$, $k \geq 1$, a nechť $r = \mathrm{nsd}(m_1, \ldots, m_k)$. Potom:

(i) $r = a_1 m_1 + \cdots + a_k m_k$ pro nějaká celá čísla $a_1, \ldots, a_k$.

(ii) $n \mid r$ pro každé $n \in \mathrm{sd}(m_1, \ldots, m_k)$.

Důkaz. Je-li $m_1 = \cdots = m_k = 0$, pak obě tvrzení jsou zřejmá, neboť $sd(0) = \mathbb{Z}$ a $r = 0$. Předpokládejme tudíž, že aspoň jedno z čísel $m_1, \ldots, m_k$ je nenulové. Tak $r \geq 1$ a množina $A = \{b_1 m_1 + \cdots + b_k m_k \mid b_i \in \mathbb{Z}\}$ obsahuje aspoň jedno kladné celé číslo. Buď nyní t nejmenší kladné číslo z množiny A. Speciálně, $t = a_1 m_1 + \cdots + a_k m_k$ pro vhodná čísla a_i. Buď $d_i = [m_i]_t$. Tedy $0 \leq d_i < t$ a $m_i = c_i t + d_i$, $c_i \in \mathbb{Z}$ (I.9.3, I.9.4). Je $c_i t = c_i a_1 m_1 + \cdots + c_i a_k m_k \in A$ a, ovšem, $m_i \in A$. Snadno nahlédneme, že i $d_i = m_i - c_i t \in A$.

Z minimality kladného čísla t plynou rovnosti $d_i = 0$. Tedy $t \mid m_i$ pro všechna i a $t \in \mathrm{sd}(m_1, \ldots, m_k)$.

Buď nyní $n \in \mathrm{sd}(m_1, \ldots, m_k)$. Tedy $n \mid m_i$, z čehož ihned plyne, že n dělí každé číslo z množiny A. Speciálně, $n \mid t$ a $r \mid t$. Ovšem, $r \geq 1$, čili $r \leq t$. Z maximality největšího společného dělitele plyne rovnost $r = t$. □

III.1.6 Věta. Nechť M je nějaká množina celých čísel a $r = \mathrm{nsd}(M)$. Potom:

(i) Je-li $M \neq \emptyset$, pak existují po dvou různá čísla $m_1, \ldots, m_k \in M$, $k \geq 1$, a nenulová čísla $a_1, \ldots, a_k$ taková, že $r = a_1 m_1 + \cdots + a_k m_k = \mathrm{nsd}(M)$.

(ii) $n \mid r$ pro každé $n \in \mathrm{sd}(M)$.

Důkaz. Je-li $M = \emptyset$ či $M = \{0\}$, pak $r = 0$ a obě tvrzení jsou zřejmá.

Předpokládejme tedy, že M obsahuje aspoň jedno nenulové číslo, takže $r \geq 1$, opět uvážíme množinu $A = \{b_1 m_1 + \cdots + b_l m_l \mid l \geq 1, b_i \in \mathbb{Z}, m_i \in M\}$ a vezmeme nejmenší kladné číslo z A, budiž to $t \geq 1$. Je snadno viděti, že lze psát $t = a_1 m_1 + \cdots + a_k m_k$, $k_i \geq 1$, $a_i \in \mathbb{Z} \setminus \{0\}$, m_i po dvou různá čísla z A. Dále, pro každé $m \in M$ existují čísla c, d taková, že $m = ct + d$, přičemž $0 \leq d < t$. Potom $d = m - ct \in A$, čili $d = 0$ a $t \mid m$. Tím jsme ověřili, že $t \in \mathrm{sd}(M)$. Je-li $n \in \mathrm{sd}(M)$, pak $n \mid m_i$, tedy $n \mid t$ a, specielně, $r \mid t$. Pak ale $r = t$. Rovnost $r = \mathrm{nsd}(m_1, \ldots, m_k)$ je nyní zřejmá. □

III.1.7 Poznámka. Nechť M je nějaká množina celých čísel obsahující alespoň jedno nenulové celé číslo. Buď $r = \mathrm{nsd}(M)$. Je $r \geq 1$ a r je vskutku největší společný dělitel čísel z M a to ve smyslu obvyklého uspořádání celých čísel. Z III.1.6 (ii) ovšem plyne, že r je současně největší společný dělitel čísel z M a to ve smyslu uspořádání nezáporných celých čísel daném relací dělitelnosti – viz II.1.10.

Je-li $M = \{0\}$ či $M = \emptyset$, pak $\mathrm{nsd}(M) = 0$, což sice není největší číslo v množině společných dělitelů (a tou je celé $\mathbb{Z}$ v tomto případě) v obvyklém uspořádání, ale je to největší číslo z $\mathbb{N}_0$ v uspořádání daném dělitelností.

III.1.8 Věta. Nechť M je nějaká množina celých čísel obsahující aspoň jedno nenulové číslo. Pro každé $p \in \mathbb{P}$ buď $a(p) = \min\{\ \mathrm{cont}_p(m), m \in M\}$. Potom $a(p) \neq 0$ jen pro konečně mnoho $p \in \mathbb{P}$ a $\mathrm{nsd}(M) = \prod_{p\in\mathbb{P}} p^{a(p)}$ a $\mathrm{cont}_p(\ \mathrm{nsd}(M)) = a(p)$.

Důkaz. Je $r = \mathrm{nsd}(M) \geq 1$. Položme $s = \prod p^{a(p)}$. Je-li $m \in M$, pak $a(p) \leq \mathrm{cont}_p(m) = b(m)$, tedy $p^{a(m)} \mid m$. Je $m = \prod p^{b(p)}$, z čehož plyne $s \mid m$. Tedy $s \in \mathrm{sd}(M)$ a $s \mid r$ podle III.1.6 (ii).

Naopak, je-li $p \in \mathbb{P}$, pak existuje $m_{(p)} \in M$ takové číslo, že $a(p) = \mathrm{cont}_p(m_{(p)})$. Ovšem $r \mid m_{(p)}$ a tak $\mathrm{cont}_p(r) \leq a(p)$. Odtud, $r \mid s$. □

III.1.9 Proposice. $\mathrm{nsd}(M_1 \cup M_2) = \mathrm{nsd}(\ \mathrm{nsd}(M_1), \mathrm{nsd}(M_2))$ pro libovolné podmnožiny M_1 a M_2 množiny všech celých čísel.

Důkaz. Nechť $r = \mathrm{nsd}(M_1 \cup M_2)$, $u = \mathrm{nsd}(M_1)$, $v = \mathrm{nsd}(M_2)$ a $w = \mathrm{nsd}(u, v)$. Je $r \in \mathrm{sd}(M_1) \cap \mathrm{sd}(M_2)$, či-li $r \mid u$ a $r \mid v$. Pak ale $r \mid w$. Naopak, $w \mid u$, $w \mid v$, či-li $w \in \mathrm{sd}(M_1) \cap \mathrm{sd}(M_2) = \mathrm{sd}(M_1 \cup M_2)$ a $w \mid r$. Takže $r = w$. □

III.1.10 Proposice. $\mathrm{nsd}(a, \mathrm{nsd}(b, c)) = \mathrm{nsd}(a, b, c) = \mathrm{nsd}(\ \mathrm{nsd}(a, b), c)$ pro všechna $a, b, c \in \mathbb{Z}$.

Důkaz. Toto tvrzení plyne snadno z III.1.9. □

III.1.11 Proposice. $\mathrm{nsd}(aM) = a \cdot \mathrm{nsd}(M)$ pro každé $a \in \mathbb{N}_0$.

Důkaz. Můžeme předpokládat, že $a \neq 0$ a množina M obsahuje aspoň jedno nenulové celé číslo. Buď $r = \mathrm{nsd}(M)$ a $s = \mathrm{nsd}(aM)$. Podle III.1.6 (i) je $r = a_1 m_1 + \cdots + a_k m_k$, $k \geq 1$, $m_i \in M$, $a_i \in \mathbb{Z}$. Tedy $ar = aa_1 m_1 + \cdots + aa_k m_k$ a $s \mid ar$. Odtud, $s = ar$. □

III.1.12 Poznámka. Na množině $\mathbb{N}_0$ můžeme definovat binární operaci $\wedge$ předpisem $a \wedge b = \mathrm{nsd}(a, b)$. Z definice největšího společného dělitele (III.1.3) a z III.1.4 a III.1.10 je vidět, že tato operace je idempotentní, komutativní a asociativní (t.j., $a \wedge a = a$, $a \wedge b = b \wedge a$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. Tedy je to polosvaz. Navíc, $a(b \wedge c) = (ab) \wedge (ac)$ (III.1.11).

III.1.13 Věta. Nechť M je neprázdná množina celých čísel a $r = \mathrm{nsd}(M)$. Potom pro každé $m \in M$ existuje $a(m) \in \mathbb{Z}$ tak, že $m = ra(m)$. Navíc, $\mathrm{nsd}(\{a(m), m \in M\}) = 1$ $(a(0) = 1)$.

Důkaz. Je $r \in \mathrm{sd}(M)$, takže lze psát $m = ra(m)$, kde pro $m = 0$ volíme $a(0) = 1$.

Je-li $t \in \mathrm{sd}(\{a(m)\})$, pak $rt \in \mathrm{sd}(M)$, $rt \mid r$, $r = rts$. Pro $r \neq 0$ dostáváme $|t| = 1$. Pro $r = 0$ je $M = \{0\}$ a opět $|t| = 1$. □

III.1.14 Úkol. (i) Nechť $n, m \in \mathbb{Z}, k \in \mathbb{N}_0, r = \mathrm{nsd}(n, m)$. Máme za úkol zjistit, že $\mathrm{nsd}(n^k, m^k) = r^k$ (nebo-li $n^k \wedge m^k = (n \wedge m)^k$).

Předně, rovnost je zřejmá pro $k = 0$, neb potom $n^k = 1 = m^k$ a $r^k = 1$. Rovnost je také zřejmá pro $k = 1$. Buď tedy $k = 2$. Je-li $n = 0$, pak $r = |m|$ a $r^k = |m|^k = |m^k| = \mathrm{nsd}(0, m^k)$. Podobně, je-li $m = 0$. Nechť je tedy $m \neq 0 \neq n$. Jistě, $r^k \mid n^k$, $r^k \mid m^k$ a tedy $r^k \mid s = \mathrm{nsd}(n^k, m^k)$. Buď $p \in \mathbb{P}$ a $a = \mathrm{cont}_p(n)$, $b = \mathrm{cont}_p(m)$. Je tedy $ka = \mathrm{cont}_p(n^k)$, $bk = \mathrm{cont}_p(m^k)$, $\mathrm{cont}_p(r) = \min(a, b)$, $\mathrm{cont}_p(r^k) = k \cdot \min(a, b) = \min(ka, kb) = \min(\ \mathrm{cont}_p(n^k), \mathrm{cont}_p(m^k)) = k \cdot \min(a, b) = \min(ka, kb) = \min(\ \mathrm{cont}_p(n^k), \mathrm{cont}_p(m^k))$. Z III.1.8 plyne rovnost $s = r^k$.

(ii) Je $\mathrm{nsd}(2, 3) = 1 = \mathrm{nsd}(3, 2)$, avšak $\mathrm{nsd}(2 \cdot 3, 3 \cdot 2) = 6$. Tedy $(2 \wedge 3)(3 \wedge 2) = 1 \neq 6 = (2 \cdot 3) \wedge (3 \cdot 2)$ (viz III.1.12).

III.2 Nesoudělná čísla

III.2.1 Definice. Množina M celých čísel se nazývá nesoudělná, jestliže $\mathrm{nsd}(M) = 1$.

Je-li M nesoudělná množina, pak $M \neq \emptyset$ a M obsahuje alespoň jedno nenulové číslo (viz III.1.3).

Je-li $M = \{m\}$ jednoprvková množina, pak M je nesoudělná právě když $m = \pm 1$ (viz III.1.4).

Množina M je nesoudělná, jestliže $1 \in M$ či $-1 \in M$.

III.2.2 Poznámka. Nechť $m_1, \ldots, m_k$, $k \geq 1$, jsou celá čísla. Tato čísla nazveme nesoudělná, jestliže nesoudělnou je množina $\{m_1, \ldots, m_k\}$. To jest, $\mathrm{nsd}(m_1, \ldots, m_k) = 1$.

III.2.3 Věta. M je nesoudělná právě když existují $k \geq 1$, $m_1, \ldots, m_k \in M$ a $a_1, \ldots, a_k \in \mathbb{Z}$ tak, že $a_1 m_1 + \cdots + a_k m_k = 1$.

Důkaz. Je-li M nesoudělná, pak $M \neq \emptyset$ a naše tvrzení plyne z III.1.6 (i). Naopak, je-li $r = \mathrm{nsd}(M)$, pak $r \mid m_i$, a tedy $r \mid a_1 m_1 + \cdots + a_k m_k = 1$. Tedy $r = 1$. □

III.2.4 Lemma. Nechť n, m jsou nesoudělná kladná čísla. Potom existují kladná čísla u, v tak, že $un - vm = 1$.

Důkaz. Podle III.2.3 je $an + bm = 1$ pro nějaké $a, b \in \mathbb{Z}$. Jistě existuje $c \in \mathbb{N}$ takové číslo, že $cm > -a$, $cn > b$. Pak $u = cm + a > 0$, $v = cn - b > 0$ a $un - vm = (cm+a)n - (cn-b)m = cmn + an - cnb + bm = an + bm = 1$. □

III.2.5 Poznámka. (i) Nechť n, m jsou nesoudělná záporná čísla. Podle III.2.4 je $1 = v(-m) - u(-n) = un - vm$ pro nějaká $u, v \in \mathbb{N}$.

(ii) Nechť $n > 0$ a $m < 0$, n, m nesoudělná. Podle III.2.4 je $1 = un - v(-m) = un + vm$ pro nějaká $u, v \in \mathbb{N}$.

(iii) Jsou-li n, m nesoudělná celá čísla, přičemž $m = 0$, pak $n = \pm 1$.

III.2.6 Proposice. Nechť n, m jsou nesoudělná kladná čísla. Potom:

(i) Pro každé $k > nm$ existují kladná čísla x, y tak, že $k = xn + ym$.

(ii) $nm \neq xn + ym$ pro všechna kladná čísla x, y.

(iii) $nm = mn + 0m = 0n + 0$.

Důkaz. (i) Podle III.2.4 je $1 = un - vm$ pro $u, v \in \mathbb{N}$. Pak také $ukn - vkm = k > nm$, $ukn > nm + vkm$. Je $uk > m$ a označme l největší číslo takové, že $uk > lm$. Zřejmě $l \geq 1$. Je-li $vkm \geq lnm$, pak $ukn > nm + vkm \geq nm + lnm = (l+1)nm$, $uk > (l+1)m$, spor s maximalitou čísla l.Takže

$vkm < lnm$, $vk < ln$, $x = uk - lm > 0$, $y = ln - vk > 0$. Nakonec, $xn + ym = ukn - lnm + lnm - vkm = k$.

(ii) Je-li $nm = xn + ym$,pak $xn = (n - y)m$, $an + bm = 1$ (III.2.3), $x = axm + bxm = a(n-y)m + bxm = (a(n-y) + bx)m$. Tedy $m \mid x$, $m \leq x$ a $nm = xn + ym \geq mn + ym > nm$, spor.

(iii) Zřejmé. □

III.2.7 Proposice. Nechť a, b, c jsou taková celá čísla, že $a \mid bc$ a čísla a, b jsou nesoudělná. Potom $a \mid c$.

Důkaz. Je $bc = da$, $d \in \mathbb{Z}$. Jelikož $\mathrm{nsd}(a, b) = 1$, tak $ea + fb = 1$ pro $e, f \in \mathbb{Z}$ (III.2.3). Nyní, $c = c1 = cea + cfb = cea + fda = a(ce + fd)$. Tedy $a \mid c$. □

III.2.8 Proposice. Nechť M je neprázdná množina celých čísel taková, že $0 \notin M$. Nechť $r = \mathrm{nsd}(M)$. Pro každé $m \in M$ existuje jednoznačně určené celé číslo $a(m)$ tak, že $m = ra(m)$. Množina čísel $\{a(m), m \in M\}$ je nesoudělná.

Důkaz. Plyne z III.1.13. □

III.2.9 Věta. Nech+t M je nějaká množina celých čísel. Potom M je nesoudělná, jestliže pro každé prvočíslo p existuje aspoň jedno číslo $m \in M$ takové, že $p \nmid m$ (neboli $\cap_{m \in M} P(m) = \emptyset$).

Důkaz. Je-li M nesoudělná, tak $\mathrm{nsd}(M) = 1$. To znamená, že $p \notin \mathrm{sd}(M)$ a existuje $m \in M$, $p \nmid m$.

Nyní opak. Buď $r = \mathrm{nsd}(M)$. Je-li $p \in \mathbb{P}$, pak p nedělí aspoň jedno číslo z množiny M a, jelikož $r \in \mathrm{sd}(M)$, tak $p \nmid r$. Číslo r není dělitelné žádným prvočíslem. Takže $r = 1$. □

III.2.10 Poznámka. III.2.9 říká, že množin M celých čísel je soudělná (t.j., $\mathrm{nsd}(M) > 1$) právě tehdy když existuje aspoň jedno prvočíslo p dělící všechna čísla z M.

III.2.11 Příklad. Nechť $n, m \in \mathbb{Z}$ a $k = \mathrm{nsd}(n + m, nm)$. Je-li $n = 0$, pak $k = |m|$. Je-li $m = 0$, pak $k = |n|$.

(i) Nechť $p \in \underline{P}(k)$. Pak $p \mid nm$ a tedy $p \mid n$ či $p \mid m$. Ovšem také $p \mid n + m$. Tudíž $p \mid n$ a $p \mid m$, neboli $p \in \underline{P}(n) \cap \underline{P}(m)$.

Nalezli jsme, že $\underline{P}(k) = \underline{P}(n) \cap \underline{P}(m) = \underline{P}(n) \cap \underline{P}(n+m) = \underline{P}(m) \cap \underline{P}(n+m)$.

(ii) Z (i) a III.2.9 plyne, že čísla nm a $n + m$ jsou nesoudělná (t.j. $k = 1$) tehdy a jen tehdy, jestliže čísla n, m jsou nesoudělná.

(iii) Nechť $k \geq 2$, $p \in \underline{P}(k)$, $r = \mathrm{cont}_p(k)$, $s = \mathrm{cont}_p(n)$, $t = \mathrm{cont}_p(m)$. Zřejmě je $\mathrm{cont}_p(nm) = s + t \geq r$. Dále, $\mathrm{cont}_p(n+m) \geq r \geq \min(s,t)$.

Je-li $s \neq t$, tak $r = \min(s,t)$.

Je-li $s = t$, tak $2s \geq r \geq s$.

(iv) Je-li $n = m$, pak $k = |n|$ pro n liché a $k = |2n|$ pro n sudé.

III.2.12 Proposice. Nechť $n, m \in \mathbb{Z}$. Potom $nm \mid n+m$ právě tehdy když buďto $n = -m$ nebo $n = 1 = m$ nebo $n = -1 = m$ nebo $n = 2 = m$ nebo $n = -2 = m$.

Důkaz. Je $n(-n) = -n^2 \mid 0 = n + (-n)$, $1 \cdot 1 = 1 \mid 2 = 1 + 1$, $(-1) \cdot (-1) = 1 \mid -2 = -1 + (-1)$, $2 \cdot 2 = 4 \mid 4 = 2 + 2$, $(-2) \cdot (-2) = 4 \mid -4 = (-2) + (-2)$.

Nyní naopak. Nechť $nm \mid n + m$. Je-li $n = 0$, pak $m = 0$ a naopak. Můžeme tedy předpokládat $n \neq 0 \neq m$ a $n \neq -m$.

Je-li $|n| = 1$, pak $nm = \pm m$ dělí $n + m$, $m \mid n$, $m \mid 1$ a $|m| = 1$. Máme $m = \pm 1$, $n = \pm 1$. Zcela obdobně postupujeme, jestliže $|m| = 1$. Předpokládejme tedy na konec, že $|n| \geq 2$ a $|m| \geq 2$.

Jestliže $nm \mid n + m$, tak $\underline{P}(n) \cup \underline{P}(m) = \underline{P}(nm) \subseteq \underline{P}(n+m)$. Navíc, $|nm| \geq 4$ a $|nm| = \mathrm{nsd}(nm, n+m)$. Z III.2.11(i) plyne rovnost $\underline{P}(n) = \underline{P}(m)$.

Nechť $p \in \underline{P}(n)$. Jelikož $nm \mid n + m$ a $n + m \neq 0$, tak $\mathrm{cont}_p(n) + \mathrm{cont}_p(m) = \mathrm{cont}_p(nm) \leq \mathrm{cont}_p(n+m)$. Máme $n = p^s \cdot n_1$, $m = p^t \cdot m_1$, $s = \mathrm{cont}_p(n)$, $t = \mathrm{cont}_p(m)$, $p \nmid n_1$, $p \nmid m_1$. Buď, pro určitost $s \leq t$. Potom $n + m = p^s(n_1 + p^{t-s} \cdot m_1) = p^s \cdot w$, $w = n_1 + p^{t-s} \cdot m_1$. Je-li $t > s$, pak $p \nmid w$, $s = \mathrm{cont}_p(n+m)$ a $s + t = \mathrm{cont}_p(nm) \leq s = \mathrm{cont}_p(n+m)$. Odtud $s = 0 = t$.

Zjistili jsme, že $\mathrm{cont}_p(n) = \mathrm{cont}_p(m)$ pro každé $p \in \underline{P}(n) = \underline{P}(m)$. To ale znamená, že $|n| = |m|$. Předpokládali jsme však, že $n \neq -m$. Takže $n = m$, $nm = n^2$, $n + m = 2n$, $n^2 \mid 2n$ a $n = 2 = m$ či $n = -2 = m$. □

III.2.13 Proposice. Nechť $n, m \in \mathbb{Z}$. Potom $|nm| = |n + m|$ právě když $(n, m) \in \{(0,0), (2,2), (-2,-2)\}$.

Důkaz. Je-li $|nm| = |n + m|$, pak $nm \mid n + m$ a vše snadno plyne z III.2.12. □

III.2.14 Proposice. Nechť $n, m \in \mathbb{Z}$. Potom $n + m \mid nm$ právě když $n = a(b+c)b$, $m = a(b+c)c$ pro nějaká $a, b, c \in \mathbb{Z}$.

Důkaz. Předně, $a(b+c)b + a(b+c)c = a(b+c)^2 \mid a^2bc(b+c)^2 = a(+bc)b \cdot a(b+c)c$.

Nyní naopak. Nechť $n + m \mid nm$ a $k = \mathrm{nsd}(n, m)$. Je-li $k = 0$, pak $n = 0 = m$ a lze volit $a = 0$, b, c libovolně. Předpokládejme tedy, že $k \geq 1$. Máme $n = kb$, $m = kc$ pro nějaká $b, c \in \mathbb{Z}$ a dostáváme $n + m = k(b+c)$.

Takže číslo $k(b+c)$ dělí číslo $nm = k^2bc$ a, jelikož $k \neq 0$, tak $b+c \mid kbc$. Aspoň jedno z čísel n, m je nenulové a tak $\mathrm{nsd}(b, c) = 1$ (viz III.1.13). V III.2.11 (ii) jsme zjistili, že následně je $\mathrm{nsd}(b+c, bc) = 1$. Takže, z III.2.7 plyne $b+c \mid k$, $k = a(b+c)$. Nyní, $n = a(b+c)b$ a $m = a(b+c)c$, co jsme chtěli dokázat. □

III.2.15 Poznámka. (i) Nechť $n, m \in \mathbb{Z}$. Z III.2.14 snadno plyne, že $\mathrm{nsd}(n, m) = 1$ a $n+m \mid nm$ tehdy a jen tehdy, jestliže $m = 1-n$ $(n = 1-m)$ a nebo $m = -1-n$ $(n = -1-m)$.

(ii) Z III.2.12 plyne, že $\mathrm{nsd}(n, m) = 1$ a $nm \mid n+m$ tehdy a jen tehdy, jestliže $(n, m) \in \{(1, 1), (-1, -1), (1, -1), (-1, 1)\}$.

III.2.16 Poznámka. V I.4.11 jsme zpozorovali, že pro $n, m \in \mathbb{N}_0$ je $nm = n^m$ právě tehdy když $m = 1$ nebo $n = 0$, $m \geq 1$, a nebo $n = 2 = m$. Pro úplnost, zkoumejme, kdy $nm = n^m$ pro $n \in \mathbb{N}^-$, $m \in \mathbb{N}_0$.

Jistě je $m \geq 1$, $nm \leq -1$, z čehož plyne, že m je liché. Potom $(-n)m = (-1)^m \cdot n^m = (-n)^m$, $-n \geq 1$. Z toho, co již víme, nyní plyne rovnost $m = 1$.

III.2.17 Poznámka. V I.4.12 jsme postřehli, že pro $n, m \in \mathbb{N}_0$ je $n+m = n^m$ pouze pro $(n, m) = (1, 0)$, či $(2, 2)$. Pro úplnost zkoumejme, kdy $n+m = n^m$ pro $n \in \mathbb{N}^-$, $m \in \mathbb{N}_0$.

Jistě je $m \geq 1$. Pro $m = 1$ dostáváme $n+1 = n$, což není možné. Takže $m \geq 2$. Je-li $n = -1$, pak $m-1 = (-1)^m$, m sudé, $m-1 = 1$, $m = 2$. Buď tedy $n \leq -2$. Je-li m sudé, pak $n+m < n < (-n)^m$. Tedy $m \geq 3$ je liché a $n^m \leq -8$. Odtud, $3 \leq m \leq -8-n$, $n \leq -11$. Ostatně, $n+m > n > n^m$.

Zjistili jsme, že $(n, m) = (-1, 2)$.

III.2.18 Poznámka. Z III.2.16 a III.2.17 plyne, že pro $n \in \mathbb{Z}$ a $m \in \mathbb{N}_0$ je $n+m = nm = n^m$ pouze pro $n = 2 = m$.

III.2.19 Věta. Následující podmínky jsou ekvivalentní pro $a, b \in \mathbb{Z}$:

(i) Čísla a, b jsou nesoudělná.

(ii) Existuje $k \geq 1$ tak, že $b \mid a^k - 1$.

(iii) Existuje $l \geq 1$ tak, že $a \mid b^l - 1$.

Důkaz. (i) implikuje (ii) Je-li $b = 0$, pak $a = \pm 1$. Pak pro $a = 1$ volíme $k = 1$ a pro $a = -1$ volíme $k = 2$. Nechť je $b \neq 0$. Pro každé $n \geq 1$ existují $r(n), s(n) \in \mathbb{Z}$ tak, že $a^n - 1 = r(n)b + s(n)$, $0 \leq s(n) < |b|$ (I.9.3). Možných čísel $s(n)$ je jen konečně mnoho a tak se přihodí, že $s(n) = s(m)$, kde $1 \leq n < m$. Odkud, $a^n(a^{m-n} - 1) = a^m - a^n = (a^m - 1) - (a^n - 1) = r(m)b + s(m) - r(n)b - s(n) = (r(m) - r(n))b$. Tedy $b \mid a^n(a^{m-n} - 1)$. Je $\mathrm{nsd}(b, a) = 1$ a tedy opakovaným využitím III.2.7 dostáváme $b \mid a^k - 1$, kde $k = m - n$.

(ii) implikuje (i). Je-li $p \in \mathbb{P}$, přičemž $p \mid b$, pak $p \mid a^k - 1$ a tak $p \nmid a^k$. Odtud, $p \nmid a$. Z III.2.9 nyní plyne, že $\mathrm{nsd}(a, b) = 1$. □

III.2.20 Lemma. Následující podmínky jsou ekvivalentní pro $n \in \mathbb{N}_0$:
(i) $n = ab$, kde $a \geq 2$, $b \geq 2$ a $\mathrm{nsd}(a, b) = 1$.
(ii) $n \geq 6$ a $n \neq \pm p^k$ pro všechna $p \in \mathbb{P}$ a $k \geq 1$.

Důkaz. (i) implikuje (ii). Je $n = ab \geq 4$. Snadno vidíme, že $n \neq 4, 5$, takže $n \geq 6$. Nechť $p_1, p_2 \in \mathbb{P}$ jsou taková prvočísla, že $p_1 \mid a$ a $p_2 \mid b$. Potom $p_1 p_2 \mid ab = n$ a $p_1 \neq p_2$, neb $\mathrm{nsd}(a, b) = 1$. Zbytek je jasný.

(ii) implikuje (i). Je $|\underline{P}(n)| \geq 2$ a tak $n = p_1^{r_1} \dots p_s^{r_s}$, kde $s \geq 2$, $r_i \geq 1$ a p_i jsou po dvou různá prvočísla. Nyní lze rozložit $a = p_1^{r_1}$ a $b = p_2^{r_2} \dots p_s^{r_s}$. □

III.2.21 Lemma. Následující podmínky jsou ekvivalentní pro $n \in \mathbb{Z}$:
(i) $n = ab$, kde $|a| \geq 2$, $|b| \geq 2$ a $\mathrm{nsd}(a, b) = 1$.
(ii) $|n| \geq 6$ a $n \neq \pm p^k$ pro všechna $p \in \mathbb{P}$ a $k \geq 1$.

Důkaz. Tvrzení snadno plyne z III.2.20 □

III.2.22 Lemma. Nechť $a, a_1, \dots, a_k$, $k \geq 1$, jsou taková celá čísla, že $\mathrm{nsd}(a, a_i) = 1$ pro všechna i, $1 \leq i \leq k$. Potom $\mathrm{nsd}(a, a_1 \cdots a_k) = 1$.

Důkaz. Buď $r = \mathrm{nsd}(a, a_1 \cdots a_k)$. Je-li $r \geq 2$, pak $p \mid r$ pro aspoň jedno $p \in \mathbb{P}$. Potom $p \mid a$, $p \mid a_1 \cdots a_k$ a tak $p \mid a_i$ pro aspoň jedno i. Takže $p \mid \mathrm{nsd}(a, a_i) = 1$, spor. □

III.2.23 Lemma. Nechť $a, b, c \in \mathbb{Z}$, $\mathrm{nsd}(a, b) = 1$. Jestliže $a \mid c$, $b \mid c$, pak $ab \mid c$.

Důkaz. Je $ra = c = sb$ a $1 = ua + vb$ (III.1.5(i)). Takže $c = cua + cvb = sbua + ravb = ab(su + rv)$. □

III.2.24 Lemma. Nechť $a_1, \dots, a_k$, $k \geq 1$, $a \in \mathbb{Z}$ jsou taková čísla, že $a_i \mid a$ pro každé i a čísla $a_1, \dots, a_k$ jsou po dvou nesoudělná. Potom $a_1 \cdots a_k \mid a$.

Důkaz. Tvrzení je zřejmé pro $k = 1$ a je dokázáno v III.2.23 pro $k = 2$. Dále postupujeme indukcí. Buď $k \geq 2$ a $b = a_1 \cdots a_{k-1}$. Z indukčního předpokladu víme, že $b \mid a$. Z III.2.22 víme, že $\mathrm{nsd}(a_k, b) = 1$. Tedy $a_1 \cdots a_k = ba_k \mid a$ podle III.2.23. □

III.2.25 Cvičení. Nechť n je sudé celé číslo.
(i) Nechť $n = 4k$, $k \geq 2$. Máme $n = (2k-1) + (2k+1)$, kde $3 \leq 2k-1 < 2k+1$ a $\mathrm{nsd}(2k-1, 2k+1) = 1$.
(ii) Nechť $n = 4k+2$, $k \geq 2$. Máme $n = (2k-1) + (2k+3)$, kde $3 \leq 2k-1 < 2k+3$ a $\mathrm{nsd}(2k-1, 2k+3) = 1$.
(iii) Nechť $n = 6k$, $k \geq 2$. Máme $n = 2 + 3 + (6k-5)$, $6k-5 \geq 7$, $\mathrm{nsd}(2, 3) = \mathrm{nsd}(2, 6k-5) = \mathrm{nsd}(3, 6k-5) = 1$.

(iv) Nechť $n = 6k + 2$, $k \geq 2$. Máme $n = 3 + 4 + (6k - 5)$, $6k - 5 \geq 7$, $\mathrm{nsd}(3, 4) = \mathrm{nsd}(3, 6k - 5) = \mathrm{nsd}(4, 6k - 5) = 1$.

(iv) Nechť $n = 6k + 4$, $k \geq 1$. Máme $n = 2 + 3 + (6k - 1)$, $6k - 1 \geq 5$, $\mathrm{nsd}(2, 3) = \mathrm{nsd}(2, 6k - 1) = \mathrm{nsd}(3, 6k - 1) = 1$.

III.2.26 Cvičení. Nechť n je liché číslo.

(i) Nechť $n \geq 5$. Máme $n = 2 + (n - 2)$, $n - 2 \geq 3$, $\mathrm{nsd}(2, n - 2) = 1$.

(ii) Nechť $n = 12k + 1$, $k \geq 2$. Máme $n = (6k - 7) + (6k - 1) + 9$, $5 \leq 6k-7 < 6k-1$, $\mathrm{nsd}(6k-7, 6k-1) = \mathrm{nsd}(6k-7, 9) = \mathrm{nsd}(6k-1, 9) = 1$.

(iii) Nechť $n = 12k + 3$, $k \geq 2$. Máme $n = (6k - 1) + (6k + 1) + 3$, $11 \leq 6k-1 < 6k+1$, $\mathrm{nsd}(6k-1, 6k+1) = \mathrm{nsd}(6k-1, 3) = \mathrm{nsd}(6k+1, 3) = 1$.

(iv) Nechť $n = 12k + 5$, $k \geq 2$. Máme $n = (6k - 5) + (6k + 1) + 9$, $7 \leq 6k-5 < 6k+1$, $\mathrm{nsd}(6k-5, 6k+1) = \mathrm{nsd}(6k-5, 9) = \mathrm{nsd}(6k+1, 9) = 1$.

(v) Nechť $n = 12k + 7$, $k \geq 1$. Máme $n = (6k - 1) + (6k + 5) + 3$, $5 \leq 6k-1 < 6k+5$, $\mathrm{nsd}(6k-1, 6k+5) = \mathrm{nsd}(6k-1, 3) = \mathrm{nsd}(6k+5, 3) = 1$.

(vi) Nechť $n = 12k + 9$, $k \geq 1$. Máme $n = (6k - 1) + (6k + 1) + 9$, $5 \leq 6k-1 < 6k+1$, $\mathrm{nsd}(6k-1, 6k+1) = \mathrm{nsd}(6k-1, 9) = \mathrm{nsd}(6k+1, 9) = 1$.

(vii) Nechť $n = 12k + 11$, $k \geq 1$. Máme $n = (6k + 1) + (6k + 7) + 3$, $7 \leq 6k+1 < 6k+7$, $\mathrm{nsd}(6k+1, 6k+7) = \mathrm{nsd}(6k+1, 3) = \mathrm{nsd}(6k+7, 3) = 1$.

III.2.27 Poučení. (i) Z III.2.25(i), (ii) a III.2.26(i) plyne toto: Buď $n \geq 5$, $n \neq 6$. Potom existují $a \geq 2$, $b \geq 2$ tak, že $n = a + b$, $\mathrm{nsd}(a, b) = 1$.

Samozřejmě, $2 + 2 = 4$, $\mathrm{nsd}(2, 2) = 2$, $3 + 3 = 6$, $\mathrm{nsd}(3, 3) = 3$.

(ii) Z III.2.25(iii) a III.2.26(ii),...,(vii) plyne toto: Nechť $n \geq 10$, $n \neq 11, 13, 15, 17$. Potom existují $a \geq 2$, $b \geq 2$, $c \geq 2$ tak, že $n = a + b + c$ a $\mathrm{nsd}(a, b) = \mathrm{nsd}(a, c) = \mathrm{nsd}(b, c) = 1$.

Samozřejmě, $3 + 5 + 7 = 15$, $\mathrm{nsd}(3, 5) = \mathrm{nsd}(3, 7) = \mathrm{nsd}(5, 7) = 1$.

(iii) Nechť $a \geq 2$, $b \geq 2$, $c \geq 2$ jsou po dvou nesoudělná čísla. Můžeme předpokládat, že $2 \leq a < b < c$. Tedy $3 \leq b$, $5 \leq c$ a $a + b + c \geq 10$. Je-li součet $a + b + c$ liché číslo, pak všechna tři čísla a, b, c jsou lichá, $3 \leq a$, $5 \leq b$, $7 \leq c$ a $a + b + c \geq 15$. Je-li $a = 3$, pak buďto $a + b + c = 15$ a nebo $a+b+c \geq 19$. Je-li $a \geq 5$, pak $a+b+c \geq 21$. Každopádně je $a+b+c \neq 17$.

(iv) Z (ii) a (iii) plyne toto: Nechť $n \in \mathbb{Z}$. Potom existují po dvou nesoudělná čísla a, b, c taková, že $a \geq 2$, $b \geq 2$, $c \geq 2$ a $n = a + b + c$ právě když $n \geq 10$ a $n \neq 11, 13, 17$.

(v) Je $17 = 2 + 3 + 5 + 7$ (prvočísla $2, 3, 5, 7$ jsou po dvou nesoudělná).

III.2.28 Lemma. Následující podmínky jsou ekvivalentní pro každé $n \geq 1$:

(i) $n^2 \mid n!$.

(ii) $n \mid (n - 1)!$.

(iii) $n \neq 4$ a n není prvočíslo (čili buďto $n = 1$ a nebo $n \geq 6$ je složené číslo).

Důkaz. $n! = (n-1)!\cdot n$. Takže první dvě podmínky jsou zřejmě ekvivalentní. Jestliže $p \in \mathbb{P}$, pak $p \mid (n-1)!$ právě když $p < n$. Odtud snadno plyne, že (ii) implikuje (iii) ($4 \nmid 6 = 3!$).

Teď buď $n \geq 6$, přičemž n není mocnina žádného prvočísla. Podle III.2.21 je $n = ab$, kde $a \geq 2$, $b \geq 2$ a $\mathrm{nsd}(a,b) = 1$. Je $a \leq n-1$, $b \leq n-1$, $a \mid (n-1)!$, $b \mid (n-1)! = ac$, $b \mid c$ (neboť $\mathrm{nsd}(a,b) = 1$), a nakonec, $n = ab \mid (n-1)!$.

Takže, buď $n = p^k$, kde $p \in \mathbb{P}$, $k \geq 2$. Je-li $k \geq 3$, pak $1 < p < p^{k-1} \leq n-1$, či-li $n = p^k = p \cdot p^{k-1} \mid (n-1)!$. Je-li $k = 2$ a $p = 3$, pak $1 < p < 2p \leq n-1$ a opět $n = p^2 \mid 2p^2 \mid (n-1)!$. □

III.2.29 Věta. Nechť p je prvočíslo. Pro každé $n \in \mathbb{Z}$ takové, že $p \nmid n$ existuje jednoznačně určené číslo m tak, že $p \mid nm-1$ přičemž $1 \leq m \leq p-1$.

Důkaz. Jelikož $p \nmid n$, tak $\mathrm{nsd}(p,n) = 1$ a podle II.2.3 existují celá čísla a, b s tím, že $ap + bn = 1$. Tedy $p \mid nb - 1$. Buď $m = [b]_p$. Je $0 \leq m \leq p$ a $p \mid b - m$. Odtud, $p \mid (nb - nm) + (1 - nb) = 1 - nm$. Zřejmě, $m \neq 0$ a také jednoznačnost čísla m je zřejmá.

Lze ovšem uvažovat také takto: Buď $1 \leq n \leq p-1$. Je-li $1 \leq i \leq j \leq p-1$, přičemž $p \mid (nj-ni) = n(j-i)$, pak $p \mid j-i$, čili $j = i$. Tím zjišťujeme, že čísla $[n1]_p, [n2]_p, \ldots, [n(p-1)]_p$ jsou po dvou různá. Je jich dohromady $p-1$. Jsou to čísla $1, 2, \ldots, p-1$, třebas i jinak seřazená. Musí existovat m tak, že $1 \leq m \leq p-1$ a $[nm]_p = 1$.

III.2.30 Úvaha. Nechť n, m jsou nesoudělná kladná čísla. Položme $K = \mathbb{N}n+\mathbb{N}m$ a $L = \mathbb{N}_0 n+\mathbb{N}_0 m$. Zřejmě $K \subseteq L$, $K+K \subseteq K \subseteq \mathbb{N}$, $L+L \subseteq L \subseteq \mathbb{N}_0$, $K + L = K$ a $\mathbb{N}_0 n \cup \mathbb{N}_0 m \subseteq L$. Nejmenší číslo z množiny K je $n + m$ a v množině L je nejmenší číslo 0. Nejmenší kladné číslo z L je pak $\min(n,m)$.

(i) Je-li $n = 1$ (popř. $m = 1$), pak $K = \mathbb{N}+\mathbb{N}m = \{m+1, m+2, m+3, \ldots\}$ (popř. $K = \mathbb{N}n + \mathbb{N} = \{n+1, n+2, n+3, \ldots\}$) a $L = \mathbb{N}_0$.

(ii) Je-li $m = n$, pak $n = 1 = m$ a $K = \{2, 3, 4, ...\}$.

(iii) Nechť $l \geq (n-1)(m-1)$. Dokážeme, že $l \in L$.

Vskutku. Podle III.2.4 existují kladná čísla u, v tak, že $1 = un - vm$. Podle I.9.1 je $lu = rm + s, r, s \in \mathbb{N}_0, 0 \leq s \leq m$. Buď $t = rn - lv$ ($\in \mathbb{Z}$). Máme $sn + tm = sn + rnm - lvm = l(un - vm) = l \geq (m-1)(n-1) = nm-m-n+1$. Odtud $tm \geq n(m-s-1)-m+1$ a $(t+1)m \geq n(m-s-1)+1$. Jelikož $s + 1 \leq m$, tak $(t+1)m \geq 1$. A protože $m \geq 1$, tak $t \geq 0$. Je $l = sn + tm$, kde $s, t \in \mathbb{N}_0$. Neboli $l \in L$.

(vi) Dokážeme, že $(n-1)(m-1) - 1 \notin L$.

Vskutku. Nechť $(n-1)(m-1) - 1 = nm - n - m = an + bm$ pro nějaká $a, b \in \mathbb{Z}$. Jelikož $\mathrm{nsd}(n,m) = 1$, tak $n \mid b + 1$ a $m \mid n - a - 1$. Tedy $b + 1 = cn, m - a - 1 = dm, c, d \in \mathbb{Z}$. Odtud $ndm = cnm$. Je-li $c = 0$ či $d = 0$, pak $c = 0 = d$, $b = -1 = a$. Je-li $c \neq 0$ či $d \neq 0$, pak

$c \neq 0 \neq d, c = d, b = cn - 1, a = (1 - c)m - 1$. Je-li navíc $c \geq 1$, pak $a \leq -1$. Je-li však $c < 0$, pak $b \leq -1$.

Zjistili jsme, že buďto $a < 0$ a nebo $b < 0$. Takže $(n-1)(m-1) - 1 \notin L$.

(v) Označme l_1 nejmenší celé číslo takové, že $\{l_1, l_1 + 1, l_1 + 2, \dots\} \subseteq L$. Z (iii) a (iv) plyne, že $l_1 = (n-1)(m-1)$ $(= nm - n - m + 1)$.

Například, pro $n = 2, m = 9$ je $l_1 = 8$. Zde máme $L = \{0,\ 2,\ 4,\ 6,\ 8,\ 9,\ 10,\ 11,\ 12,\ \dots\}$.

(vi) Je-li $a > m$, pak $an \in K$, neb $an = (a - m)n + nm$. Symetricky, je-li $b > n$, pak $bm \in K$.

(vii) Nechť $k > nm$. Dokážeme, že $k \in K$.

Vskutku. Podle (iii) je $k \in L$. Tedy $k = an + bm, a, b \in \mathbb{N}_0$. Je-li $a \leq 0 \leq b$, pak $k \in K$. Je-li $b = 0$, pak $am = k > nm, a > m, k \in K$ podle (vi). Podobně, je-li $b = 0$.

(viii) Nechť $a, b \in \mathbb{Z}$ jsou taková čísla, že $nm = an + bm$. Potom $(n - 1)(m - 1) = (a - 1)n + (b - 1)m$ a z (iv) plyne, že buďto $a - 1 < 0, a \leq 0$ či $b - 1 < 0, b \leq 0$. Tím jsme zjistili, že $nm \notin K$.

(ix) Označme k_1 nejmenší celé číslo takové, že $\{k_1, k_1+1, k_1+2, \dots\} \subseteq K$. Z (vii) a (viii) plyne, že $k_1 = nm + 1$.

Například, pro $n = 2, m = 9$ je $k_1 = 19$. Zde máme $K = \{11,\ 13,\ 15,\ 17,\ 19,\ 20,\ 21,\ \dots\}$.

(x) Je $k_1 - l_1 = n + m$.

III.3 Příklady, úklady a cvičení

III.3.1 Pozorování. Nechť $n \in \mathbb{Z}$. Potom

(1) $\text{nsd}(n, n+1) = 1$;

(2) $\text{nsd}(n+1, n) = \text{nsd}(n+1, n+2) = 1$;

(3) Je-li n liché, pak $\text{nsd}(n+2, n) = \text{nsd}(n+2, n+1) = \text{nsd}(n+2, n+3) = 1$;

(4) Je-li n sudé, pak $\text{nsd}(n+1, n) = \text{nsd}(n+1, n+2) = \text{nsd}(n+1, n+3) = 1$;

(5) Je-li n liché, pak $\text{nsd}(n+2, n) = \text{nsd}(n+2, n+1) = \text{nsd}(n+2, n+3) = \text{nsd}(n+2, n+4) = 1$;

(6) Je-li n sudé a $3 \nmid n$, pak $\text{nsd}(n, n+1) = \text{nsd}(n, n+2) = \text{nsd}(n, n+3) = \text{nsd}(n, n+4) = 1$;

(7) Je-li n liché a $3 \mid n$, pak $\text{nsd}(n+1, n) = \text{nsd}(n+1, n+2) = \text{nsd}(n+1, n+3) = \text{nsd}(n+1, n+4) = 1$;

III.3.2 Definice. Kladné číslo m nazveme japné (pouze pro místní účely), jestliže platí: Pro každé $n \in \mathbb{Z}$ existuje $0 \leq j \leq m-1$ tak, že $\text{nsd}(n+j, n+i) = 1$ pro všechna $0 \leq i \leq m-1$, $i \neq j$. To jest, máme-li m po sobě jdoucích celých čísel, pak alespoň jedno z nich je nesoudělné s každým ze zbývajících $m-1$ čísel (všimněme si, že pro $m \geq 3$ musí být toto nesoudělné číslo vždy liché).

V III.3.1 jsme zpozorovali, že čísla $1, 2, 3, 4, 5$ jsou japná. V literatuře se lze dočíst, byť i s obtížemi, že japná čísla jsou právě jen čísla $1, 2, 3, \ldots, 16$. Zabývejme se tím trochu.

III.3.3 Příklad. Přesvědčme se o tom, že 17 není japné číslo.

Máme tyto prvočíselné rozklady: $2183 = 37 \cdot 59$, $2184 = 2^3 \cdot 3 \cdot 7 \cdot 13$, $2185 = 5 \cdot 19 \cdot 23$, $2186 = 2 \cdot 1093$, $2187 = 3^7$, $2188 = 2^2 \cdot 547$, $2189 = 11 \cdot 199$, $2190 = 2 \cdot 3 \cdot 5 \cdot 73$, $2191 = 7 \cdot 313$, $2192 = 2^4 \cdot 137$, $2193 = 3 \cdot 17 \cdot 43$, $2194 = 2 \cdot 1097$, $2195 = 5 \cdot 439$, $2196 = 2^3 \cdot 3^2 \cdot 61$, $2197 = 13^3$, $2198 = 2 \cdot 7 \cdot 157$, $2199 = 3 \cdot 733$, $2200 = 2^3 \cdot 5^2 \cdot 11$, $2201 = 31 \cdot 71$.

Čísla $2184, 2186, \ldots, 2200$ jsou sudá. Dále pak $3 \mid 2184, 2187, 2190, 2193, 2196, 2199$, $5 \mid 2185, 2190, 2195, 2200$, $7 \mid 2184, 2191, 2198$, $11 \mid 2189, 2200$, $13 \mid 2184, 2197$, $17 \mid 2197$, $19 \mid 2185$, $23 \mid 2185$, $31 \mid 2201$, $37 \mid 2183$, $43 \mid 2193$. Prvočísla 29 a 41 nedělí žádné z 19 čísel $2183, \ldots, 2201$.

$2184, 2185, \ldots, 2200$ je právě 17 po sobě jdoucích čísel. Navíc $\text{nsd}(2185, 2195) = 5$, $\text{nsd}(2187, 2193) = 3$, $\text{nsd}(2189, 2200) = 11$, $\text{nsd}(2191, 2184) = 17$, $\text{nsd}(2197, 2184) = 13$, $\text{nsd}(2199, 2187) = 3$. Takže pro každé a, $2184 \leq a \leq 2200$ existuje alespoň jedno b, $b \neq a$, $2184 \leq b \leq 2200$, kdy $\text{nsd}(a, b) > 1$. To znamená, že číslo 17 není japné.

Ještě si připomeňme, že $13^3 - 3^7 = 2197 - 2187 = 10$.

III.3.4 Počítání. A teď si spočtěme, že číslo 16 je japné.

Postupujme sporem. Nechť, právě naopak, není. Potom existuje $n \in \mathbb{Z}$ tak, že pro každé $0 \leq i \leq 15$ máme čísla $\alpha(i)$, $0 \leq \alpha(i) \leq 15, \alpha(i) \neq i$, $\mathrm{nsd}(n+i, n+\alpha(i)) > 1$. Pak ale existuje prvočíslo $\beta(i)$ (aspoň jedno) takové, že $\beta(i) \mid n+i$ a $\beta(i) \mid n+\alpha(i)$ (tedy $\beta(i) \mid i-\alpha(i)$). Tímto způsobem získáváme zobrazení $\beta : \{0, 1, \ldots, 15\} \to \mathbb{P}$.

(i) $\beta : \{0, 1, \ldots, 15\} \to \{2, 3, 5, 7, 11, 13\}$.

Vskutku. Jelikož $\beta(i) \mid n+i, n+\alpha(i)$, tak $\beta(i) \mid i-\alpha(i)$, kde $1 \leq |i-\alpha(i)| \leq 15$.

(ii) $\beta(3), \beta(4), \beta(11), \beta(12) \leq 11$.

Vskutku. Máme $\beta(3) \mid 3-\alpha(3)$ a $3 \leq |3-\alpha(3)| \leq 12$. Tedy $\beta(3) \leq 11$. Podobně i další případy.

(iii) $\beta(5), \beta(6), \beta(7), \beta(8), \beta(9), \beta(10) \leq 7$.

Vskutku. Máme $\beta(5) \mid 5-\alpha(5)$ a $5 \leq |5-\alpha(5)|$. Tedy $\beta(5) \leq 7$. Podobně i další případy.

(iv) $\beta(i) \neq \beta(i+1)$ pro $0 \leq i \leq 14$.

Vskutku. Bylo-li by $\beta(i) = p = \beta(i+1)$, tak by $p \mid (n+i+1)-(n+i) = 1$, spor.

(v) Nechť $0 \leq i < j \leq 15$ a $\beta(i) = \beta(j)$. Potom $\beta(i) \mid j-i$.

Vskutku. Je $j-i = (n+j)-(n+i)$.

(vi) Označme ρ jadernou ekvivalenci zobrazení β. To jest, pro $0 \leq i < j \leq 15$ je $(i, j) \in \rho$ právě když $\beta(i) = \beta(j)$. Zřejmě má ekvivalence ρ nejvýše 6 bloků.

(vii) Nechť A je blok ekvivalence ρ a nechť $p = \beta(A)$. Potom $p \cdot (|A|-1) \leq 15$.

Vskutku. Je-li $|A| = a \geq 2$, $A = \{i_1, i_2, \ldots, i_a\}, i_1 < \cdots < i_a$, pak $i_1 + p, \leq i_2, i_2 + p \leq i_3, \ldots, i_{a-1} + p \leq i_a$ podle (v). Tedy $p \cdot (a-1) \leq i_1 + (a-1)p \leq i_a \leq 15$.

(viii) Nechť A je blok ekvivalence ρ. Je-li $\beta(A) = 11, 13$, pak $|A| = 1$. Je-li $\beta(A) = 7$, pak $|A| \leq 3$. Je-li $\beta(A) = 5$, pak $|A| \leq 4$. Je-li $\beta(A) = 3$, pak $|A| \leq 6$. Je-li $\beta(A) = 2$, pak $|A| \leq 8$.

Vskutku. Všechny nerovnosti snadno plynou z (vii).

(ix) Je-li n liché číslo, tak čísla $0, 1, 2$ leží každé v jiném bloku ekvivalence ρ. Je-li n sudé číslo, tak totéž platí pro čísla $1, 2, 3$. Tedy ekvivalence ρ má alespoň 3 a nejvýše 6 bloků.

(x) Bez újmy na obecnosti můžeme předpokládat, že $\alpha(i) = i+2$ pro každé $0 \leq i \leq 13$ takové, že $n+i$ je sudé. Je pak $\beta(i) = 2$. Je-li n sudé, pak lze klást $\alpha(14) = 2$ a $\beta(14) = 2$. Je-li n liché, pak lze klást $\alpha(15) = 13$ a $\beta(15) = 2$. Toto vše tedy budeme předpokládat v dalším.

(xi) Nechť n je liché. Potom $\beta(A) = 2$, kde $A = \{1, 3, 5, 7, 9, 11, 13, 15\}$ je osmiprvkový blok ekvivalence ρ (viz (x)). Zbývajících 8 sudých čísel $\{0, 2, 4, 6, 8, 10, 12, 14\}$ je rozděleno do nejvýše 5 bloků.

Čísla $6, 8, 10$ patří do různých bloků B, C, D. Tedy $6 \in B, 8 \in C, 10 \in D$. Z (iii) víme, že $\{\beta(b), \beta(C), \beta(D)\} = \{3, 5, 7\}$. Zbývá rozdělit do bloků čísla

$0, 2, 4, 12, 14$.

Nechť $4 \notin B \cup C \cup D$. Z (ii) plyne, že $\beta(4) = 11$ a ihned vidíme, že $\{4\}$ je jednoprvkový blok ekvivalence ρ. Je také $\beta(12) \leq 11$, čili $\beta(12) \leq 7$ a $12 \in B \cup C \cup D$. Pak ale $12 \in B$, $\beta(6) = \beta(12) = 3$ a můžeme předpokládat, že též $\beta(0) = 3$. Takže $B = \{0, 6, 12\}$. Navíc, $\{14\}$ je též jednoprvkový blok $(14 - 8 = 6, 14 - 10 = 2, 14 - 2 = 12)$. Nakonec, $2 \notin C$ a $2 \notin D$. Takže i $\{2\}$ je jednoprvkový blok. Celkem máme sudá čísla rozdělena do 6 bloků, což neplatí.

Zjistili jsme, že $4 \in B \cup C \cup D$. Pak ale $4 \in D, 10 - 4 = 6$, čili $\beta(4) = \beta(10) = 3$ a $D = \{4, 10\}$. Je $\beta(3) = \beta(6) = 7$, čili nutně $B = \{6\}$ a, podobně $C = \{8\}$. Tím jsme rozdělili čísla $4, 5, 8, 10$ do tří bloků a zbývá rozdělit čísla $\{0, 2, 12, 14\}$ do nejvýše dvou bloků. To ale nepůjde. Zbývají totiž pouze prvočísla 11 a 13 pro hodnoty β.

(xii) Nechť n je sudé. Potom $\beta(A) = 2$, kde $a = \{0, 2, 4, 6, 8, 10, 12, 14\}$ je osmiprvkový blok (viz (x)). Zbývajících 8 lichých čísel $1, 3, 5, 7, 9, 11, 13, 15$ je rozděleno nejvýše do 5 bloků.

Čísla $5, 7, 9$ patří do různých bloků B, C, D. Tedy $5 \in B, 7 \in C, 9 \in D$. Z (iii) víme, že $\{\beta(B), \beta(C), \beta(D)\} = \{3, 5, 7\}$. Zbývá rozdělit do bloků čísla $1, 3, 11, 13, 15$.

Nechť $3 \notin B \cup C \cup D$. Z (ii) plyne, že $\beta(3) = 11$ a ihned vidíme, že $\{3\}$ je jednoprvkový blok. Je také $\beta(11) \leq 11$, čili $\beta(11) \leq 7, 11 \in B \cup C \cup D$. Pak ale $11 \in B$, $\beta(5) = \beta(11) = 3$ a máme $B = \{5, 11\}$.

Snadno nahlédneme, že všechny další bloky jsou už jednoprvkové. Předpoklad, že lichá čísla máme rozdělena do 7 bloků, už neplatí.

Vidíme, že $3 \in B \cup C \cup D$. Takže $3 \in D, D = \{3, 9, 15\}, \beta(D) = 3$. Zbývají čísla $1, 5, 7, 11, 13$. Tato čísla vytvářejí jednoprvkové bloky. Dohromady máme lichá čísla rozdělena do 6 bloků, spor.

III.3.5 Počítání. Nechť $n \geq 1$ je liché číslo. Uvažme 10 po sobě jdoucích lichých čísel počínaje číslem n. Jsou to čísla $n, n+2, n+4, \ldots, n+18$. Tedy čísla $n + 2i, 0 \leq i \leq 9$. Předpokládejme, že pro každé takové i existuje (aspoň jedno) číslo $\alpha(i)$ takové, že $0 \leq \alpha(i) \leq 18, \alpha(i) \neq 2i$ a $\mathrm{nsd}(n + 2i, n + \alpha(i)) \geq 2$. Potom ovšem existuje (aspoň jedno) prvočíslo $\beta(i)$ takové, že $\beta(i) \mid n + 2i, \beta(i) \mid n + \alpha(i)$. Tímto způsobem získáváme zobrazení $\beta : \{0, 1, \ldots, 9\} \to \mathbb{P}$.

(i) $\beta : \{0, 1, \ldots, 9\} \to \{3, 5, 7, 11, 13, 17\}$.

Vskutku. Jelikož $\beta(i)$ dělí liché číslo $n + 2i$, tak $\beta(i)$ je liché prvočíslo. Jelikož $\beta(i) \mid (n + 2i) - (n + \alpha(i)) = 2i - \alpha(i)$ a $1 \leq |2i - \alpha(i)| \leq 18$, tak $\beta(i) \leq 17$. Odtud naše tvrzení.

(ii) $\beta(1), \beta(2), \beta(8) \leq 13$, $\beta(3), \beta(6) \leq 11$, $\beta(4), \beta(5) \leq 7$.

Vskutku. Máme $\beta(1) \mid \alpha(1) - 2$, $-2 \leq \alpha(1) - 2 \leq 16$. Podobně $\beta(2) \mid$

$\alpha(2)-4,\ -4 \le \alpha(2)-4 \le 14,\ \beta(3) \mid \alpha(3)-6,\ -6 \le \alpha(3)-6 \le 12,$ $\beta(4) \mid \alpha(4)-8,\ -8 \le \alpha(4)-8 \le 10,\ \beta(5) \mid \alpha(5)-10,\ -10 \le \alpha(5)-10 \le 8,$ $\beta(6) \mid \alpha(6)-12,\ -12 \le \alpha(6)-12 \le 6,\ \beta(7) \mid \alpha(7)-14,\ -14 \le \alpha(7)-14 \le 4,$ $\beta(8) \mid \alpha(8)-16,\ -16 \le \alpha(8)-16 \le 2.$

(iii) Na intervalu $\{0,1,\ldots,9\}$ uvažujme jadernou ekvivalenci ρ zobrazení β. Ta je definována tak, že $(i,j) \in \rho$ právě když $\beta(i) = \beta(j)$. Množina obrazů zobrazení β je podmnožinou v $\{3,5,7,11,13,17\}$ a tudíž ekvivalence ρ má nejvýše 6 bloků. Na druhé straně má ekvivalence ρ alespoň 3 bloky. To plyne z následujícího zjištění: Je $(n+10)-(n+8) = 2 = (n+12)-(n+10), (n+12)-(n+8) = 4$. Čísla 2 a 4 jsou kladné mocniny prvočísla 2 a nejsou dělena žádným lichým prvočíslem. Tedy prvočísla $\beta(4)$, $\beta(5)$ a $\beta(6)$ jsou různá čísla a čísla $4,5,6$ patří do různých bloků.

(vi) Nechť A je blok ekvivalence ρ, přičemž $|A| \ge 3$. Potom $4 \ge |A|$ a $\beta(A) = \{3\}$.

Vskutku. Máme $i,j,k \in A$, kde $0 \le i < j < k \le 9$, $\beta(i) = \beta(j) = \beta(k) = p, p \in \mathbb{P}, 3 \le p \le 17$. Nyní, $p \mid (n+2j)-(n+2i) = 2(j-i)$, $p \mid j-i, i+p \le j$. Podobně, $j+p \le k$, takže $6 \le i+2p \le k \le 9$. Odtud $2p \le 9$ a $p = 3$. Jelikož $9 = 0+3\cdot 3$, tak $|A| \le 4$.

(v) Nechť A je takový blok, že $|A| = 2$. Potom $\beta(A) \in \{3,5,7\}$.

Vskutku. Máme $A = \{i,j\}$, $0 < i < j \le 9$, $\beta(i = \beta(j) = p$, $3 \le p \le i+p \le j \le 9$, $p = 3,5,7$.

(vi) Ekvivalence ρ má alespoň 5 bloků. Z (iii) víme, že ρ má alespoň 3 bloky. Z (vi) víme, že každý blok obsahuje nejvýše 4 čísla, přičemž existuje nejvýše jeden blok, který obsahuje 3 či 4 čísla. Z (v) víme, že existují nejvýše 3 bloky obsahující právě 2 čísla.

Je-li A blok takový, že $|A| \ge 3$, pak $4 \ge |A|$ a $\beta(A) = 3$. Z (v) plyne, že existují 2 dvouprvkové bloky. Tedy existují aspoň 2 jednoprvkové bloky. Jestliže $|A| \le 2$ pro každý blok A, pak z (v) plyne, že existují aspoň 4 jednoprvkové bloky. V každém případě máme alespoň 2 jednoprvkové bloky.

(vii) Nechť $A = \{i,j,k,l | 0 \le i < j < k < l \le 9\}$ je čtyřprvkový blok. Z (iv) již víme, že $\beta(A) = 3$. Dále $i+9 \le l \le 9$, takže $i = 0, l = 9$. Ovšem, $i+6 = 6 \le k, i+3 = 3 \le j$, $3 \mid j, 3 \mid k$ a je nutně $j = 3, k = 6$. Zjistili jsme, že $A = \{0,3,6,9\}$.

Dle (iii) a (vi) má ekvivalence ρ 5 či 6 bloků. Blok A už máme vyřešen a zbývají čísla $1,2,4,5,7,8$, která máme rozdělit do 4 či 5 bloků. To znamená, že máme 1 či 2 dvouprvkové bloky a 4 či 2 jednoprvkové bloky. Kdyby ovšem ρ měla 6 bloků, tak by zobrazení β bylo na celou množinu prvočísel $\{3,5,7,11,13,17\}$ a tedy obrazem by bylo i prvočíslo 17. Z (ii) by plynulo, že $17 = \beta(0)$ a nebo $17 = \beta(9)$. Ale my máme $0,9 \in A$, což by vedlo ke sporu. Takže ρ má právě 5 bloků a má tak právě 3 dvojprvkové bloky. A sice B, C, kde $\beta(B) = 5$ a $\beta(C) = 7$ (plyne z (v)).

Buď $B = \{u, v\}$, $C = \{w, z\}$, $1 \leq u < v \leq 8$, $1 \leq w < z \leq 8$ (neboť $0, 9 \in A$). Je $w + 7 \leq z \leq 8$, čili $w = 1, z = 8, C = \{1, 8\}$. Podobně, $u + 5 \leq w \leq 7$ (neboť $8 \in C$) a $u \leq 2$ a tedy $u = 2$ (neboť $1 \in C$), $v = 7$, $B = \{2, 7\}$.

Zbývají 2 jednoprvkové bloky a sice $\{4\}$ a $\{5\}$. Z (ii) víme, že $\beta(4) \leq 7$ a $\beta(5) \leq 7$. Ale prvočísla $3, 5, 7$ jsou již obsazena. Dostali jsme spor.

(viii) V předchozím bodě jsme se přesvědčili o tom, že žádný čtyřprvový blok není. Jelikož $3+2+2 = 7$ a $10-7 = 3$, tak ρ musí mít jeden tříprvkový blok A, 2 dvojprvkové bloky B a C a 3 tříprvkové bloky. Tedy ρ má 6 bloků, každé prvočíslo $3, 5, 7, 11, 13, 17$ je obrazem a z (ii) plyne, že buďto $\beta(0) = 17$ či $\beta(9) = 17$.

Z (iv) je známo, že $\beta(A) = 3$. Je $A = \{i, j, k\}$, kde $0 \leq i < j < k \leq 9$, $3 \mid j - i$, $3 \mid k - j$. Jsou tedy čtyři možnosti: $A = \{0, 3, 6\}$, $A = \{1, 4, 7\}$, $A = \{2, 5, 8\}$, $A = \{3, 6, 9\}$.

Dále, $B = \{u, v\}, \beta(B) = 5$, $0 \leq u < v \leq 9$, $5 \mid v - u$, $C = \{w, z\}, \beta(C) = 7$, $0 \leq w < z \leq 9$, $7 \mid w - z$. Odtud, $B = \{0, 5\}, \{1, 6\}, \ldots, \{4, 9\}$ a $C = \{0, 7\}, \{1, 8\}, \{2, 9\}$. Z (ii) plyne $\{4, 5\} \subseteq A \cup B \cup C$. Rozeberme si různé možnosti.

(viii 1) Nechť $A = \{0, 3, 6\}$. Pak $B = \{2, 7\}, \{4, 9\}$ a $C = \{1, 8\}, \{2, 9\}$. To je ale spor s tím, že $5 \in A \cup B \cup C$.

(viii 2) Nechť $A = \{1, 4, 7\}$. Pak $B = \{0, 5\}, \{3, 8\}$ a $C = \{2, 9\}$. Dále $\beta(9) = 7$, čili $\beta(0) = 17$ a $B = \{3, 8\}$. To je ale spor s tím, že $5 \in A \cup B \cup C$.

(viii 3) Nechť $A = \{2, 5, 8\}$. Pak $B = \{1, 6\}, \{4, 9\}$ a $C = \{0, 7\}$. Tedy $\beta(0) = 7$, $\beta(9) = 17$ a $B = \{1, 6\}$. To je ale spor s tím, že $4 \in A \cup B \cup C$.

(viii 4) Nechť $A = \{3, 6, 9\}$. Pak $B = \{0, 5\}, \{2, 7\}$ a $C = \{0, 7\}, \{1, 8\}$. To je ale spor s tím, že $4 \in A \cup B \cup C$.

(ix) Ve všech bodech jsme dospěli ke sporu. Počáteční předpoklady našeho počítání nemohou být splněny. To znamená: Máme-li liché celé číslo n a uvážíme-li devatenáct po sobě jdoucích čísel $n, n+1, n+2, \ldots, n+18$ (z nichž je právě deset čísel lichých), potom existuje mezi nimi alespoň jedno liché číslo takové, že je nesoudělné se všemi zbývajícími osmnácti čísly (z intervalu $n, \ldots, n + 18$).

(x) Nechť n je takové sudé číslo, že pro každé $a, n \leq a \leq 19$, existuje $b, n \leq b \leq 19$, $a \neq b$, $\mathrm{nsd}(a, b) > 1$. Podle (ix) existuje liché číslo c tak, že $n + 1 \leq c \leq n + 19$ a $\mathrm{nsd}(c, d) = 1$ pro každé d, $n + 1 \leq d \leq n + 19$, $d \neq c$. Dále, jakž jsme předpokládali, existuje e, $n \leq e \leq n + 19$, $e \neq c$, $\mathrm{nsd}(e, c) > 1$. Pak ale musí být $e = n$. Tedy čísla n a c jsou soudělná. Je $c = n+i$, kde $3 \leq i \leq 19$, i liché. Dále, existuje prvočíslo p tak, že $p \mid n, p \mid c$. Tedy $p \mid i$ a $p \in \{3, 5, 7, 11, 13, 17, 19\}$.

III.3.6 Poznámka. Z III.3.4 víme, že 16 je japné číslo. A teď mějme patnáct po sobě jdoucích čísel $n, n+1, \ldots, n+14$ takových že každé z nich je soudělné s nějakým dalším. Protože číslo 16 je japné, tak číslo $n-1$ je nesoudělné se všemi čísly $n, n+1, \ldots, n+14$ a tedy n je sudé a $3, 5, 7, 11, 13 \nmid n-1$. Podobně, $n+15$ je nesoudělné se všemi čísly $n, n+1, \ldots, n+14$, $3, 5 \nmid n$, $7 \nmid n+1$, $11 \nmid n+4$, $13 \nmid n+2$. V podobných úvahách lze pokračovat ještě dlouho.

III.3.7 Úloha. Nechť p je liché prvočíslo, $p = 2n+1$. $n \geq 1$, $n = (p-1)/2$. Pro místní účely této úlohy si zavedeme následující označení: Pro každé $k, 1 \leq k \leq p-1$ nechť $\alpha(k)$ je to jednoznačně určené číslo takové, že $1 \leq \alpha(k) \leq p-1$ a $p \mid k \cdot \alpha(k) - 1$, (viz III.2.29)

Buď $w = \sum_{k=1}^{p-1}(k+\alpha(k))$, $u = \sum_{k=1}^{p-1}(k+\alpha(k))^2$, $v = \sum_{k=1}^{p-1}(k^2+\alpha(k)^2)$, $t = \sum_{k=1}^{p-1} 2k\alpha(k)$.

III.3.7.1 Tabulka Uveďme si hodnoty čísel w, u, v, t pro malá p:

p	3	5	7	11
w	6	20	42	110
u	20	118	348	1472
v	10	60	182	770
t	10	58	166	702

Pokud bychom definovali obdobná čísla i pro $p = 2$, pak bychom dostali $w = 2, u = 4, v = 2, t = 2$.

III.3.7.2 Lemma Zobrazení α je involuce intervalu $\{1, 2, \ldots, p-1\}$.

Důkaz. Stačí ukázat, že zobrazení α je prosté. Je-li však $\alpha(k) = \alpha(l)$, pak $p \mid (k\alpha(k)-1) - (l\alpha(l)-1) = (k-l)\alpha(k)$, $p \mid (k-l)$ a $k = l$. □

III.3.7.3 Lemma $w = p(p-1)$.

Důkaz. Vzhledem k III.7.2 je $\sum_{k=1}^{p-1} k = \sum_{k=1}^{p-1} \alpha(k)$ a tak $w = 2\sum_{k=1}^{p-1} k = p(p-1)$ (I.10.2). □

III.3.7.4 Lemma $v = (p-1)p(p+1)$.

Důkaz. Vzhledem k III.7.2 je $\sum_{k=1}^{p-1} k^2 = \sum_{k=1}^{p-1} \alpha(k)^2$ a tak $v = 2\sum_{k=1}^{p-1} k^2 = (p-1)p(p+1)$ (I.10.4). □

III.3.7.5 Lemma $u = v + t$.

Důkaz. Je $(k+\alpha(k))^2 = k^2 + \alpha(k)^2 + 2k\alpha(k)$. □

III.3.7.6 Lemma (i) $p \mid w$.
(ii) $p \mid t+2$.
(iii) $p \mid v$ pro $p \geq 5$ ($p \nmid v$ pro $p = 3$).
(iv) $p \mid u+2$ pro $p \geq 5$ ($p \nmid u+2$ pro $p = 3$).

Důkaz. (i) Toto plyne ihned z III.3.7.3.
(ii) Pro každé $k, 1 \leq k \leq p-1$ je $p \mid k\alpha(k) - 1$, takže $p \mid 2k\alpha(k) - 2$.
(iii) Toto plyne snadno z III.3.7.4 (je $v = 10$ pro $p = 3$).
(iv) Je $u + 2 = v + t + 2$ podle III.3.7.5 a tvrzení plyne z (ii) a (iii) (je $u + 2 = 22$ pro $p = 3$). □

III.3.7.7 Pro každé $k, 1 \leq k \leq p-1$, existuje jednoznačně určené číslo $\beta(k)$ takové, že $1 \leq \beta(k) \leq p-1$ a $p \mid k^2 - \beta(k)$.
Zřejmě je $\beta(1) = 1 = \beta(p-1)$.

III.3.7.8 Lemma Nechť $1 \leq k < l \leq p-1$. Potom $\beta(k) = \beta(l)$ právě tehdy, když $k + l = p$ (pak $1 \leq k \leq n < n+1 \leq l \leq p-1$).

Důkaz. Jestliže $\beta(k) = \beta(l)$, pak $p \mid l^2 - k^2 = (l+k)(l-k)$, $1 \leq l-k \leq p-2$, a nutně $p \mid l + k$. Ovšem $3 \leq l + k \leq 2p - 3 < p$. Tedy $k + l = p$.
Naopak, je-li $k+l = p$, pak $p \mid l^2 - k^2$, $p \mid (l^2 - k^2) + (k^2 - \beta(k)) + (\beta(l) - l^2) = \beta(l) - \beta(k)$. A tedy $\beta(l) = \beta(k)$. □

III.3.7.9 Lemma Nechť $p \leq 5$. Potom $p \mid \sum_{k=1}^{n} \beta(k)$.

Důkaz. Víme, že $p \mid \sum_{k=1}^{n}(k^2 - \beta(k)) = \sum_{k=1}^{n} k^2 - \sum_{k=1}^{n} \beta(k) = pn(n+1)/6 - \sum_{k=1}^{n} \beta(k)$ (I.10.4). Odtud $p \mid \sum_{k=1}^{n} \beta(k)$. □

III.3.7.10 Lemma Nechť $p \geq 5$. Potom $p \mid \sum_{k=1}^{n} \alpha(k)^2$.

Důkaz. Nejdříve si ověříme, že čísla $\beta\alpha(1), \ldots, \beta\alpha(n)$ jsou po dvou různá. Vskutku, je-li $1 \leq k < l \leq n$, přičemž $\beta\alpha(k) = \beta\alpha(l)$, pak z III.3.7.2 a III.3.7.8 plyne, že $\alpha(k) + \alpha(l) = p$. Tedy $p \mid k\alpha(k) + k\alpha(l)$, $p \mid k\alpha(k) + k\alpha(l) - k\alpha(k) + 1 = k\alpha(l) + 1$, $p \mid k\alpha(l) + 1 + l\alpha(l) - 1 = k\alpha(l) + l\alpha(l) = (k+l)\alpha(l)$, kde $2 \leq k + l \leq 2n - 1 < p$ a $1 \leq \alpha(l) < p$, což je spor.
Čísel $\beta\alpha(1), \ldots, \beta\alpha(n)$ je právě n. Z III.3.7.8 snadno plyne, že tato čísla jsou vlastně čísla $\beta(1), \ldots, \beta(n)$ i když třeba v jiném pořadí. Speciálně $\sum_{k=1}^{n} \beta(k) = \sum_{k=1}^{n} \beta\alpha(k)$ a $p \mid \sum_{k=1}^{n} \beta\alpha(k)$ podle III.3.7.9.
Víme, že $p \mid \sum_{k=1}^{n} \alpha(k)^2 - \beta\alpha(k)$ takže $p \mid \sum_{k=1}^{n}(\alpha(k)^2 - \beta\alpha(k)) - \sum_{k=1}^{n} \beta\alpha(k) = \sum_{k=1}^{n} \alpha(k)^2$. □

III.3.7.11 Tabulka Položme $z = \sum_{k=1}^{n} \alpha(k)^2$.

p	3	5	7	11
z	1	$10(2 \cdot 5)$	$42(2 \cdot 5 \cdot 7)$	$143(11 \cdot 13)$

III.3.7.12 Lemma $\sum_{k=1}^{p-1} \beta(k) = 2 \sum_{k=1}^{n} \beta(k)$.

Důkaz. Je $2n = p-1$. Z III.3.7.8 plyne, že čísla $\beta(1), \ldots, \beta(n)$ jsou po dvou různá. Je $1 + 2n = 2 + (2n-1) = \cdots = n + (n+1) = p$. Z III.3.7.8 nyní plyne, že čísla $\beta(n+1), \ldots, \beta(2n)$ jsou tatáž jako $\beta(1), \ldots, \beta(n)$ jen v jiném pořadí. Tedy vše je jasné. □

III.3.7.13 Lemma Nechť $p \geq 5$. Potom $p \mid \sum_{k=1}^{p-1} \beta(k)$.

Důkaz. Toto tvrzení plyne ihned z III.3.7.12 a III.3.7.9. Můžeme ovšem použít též rovnost $\sum_{k=1}^{p-1} k^2 = (p-1)p(2p-1)/6$. □

III.3.7.14 Lemma Nechť $p \geq 5$. Potom $p \mid \sum_{k=1}^{p-1} \alpha(k)^2$.

Důkaz. Z III.3.7.2 dostáváme rovnost $\sum_{k=1}^{p-1} \alpha(k) = \sum_{k=1}^{p-1} k^2 = (p-1)p(2p-1)/6$ a vše je jasné. □

III.3.7.15 Tabulka Položme $z1 = \sum_{k=1}^{p-1} \alpha(k)^2$.

p	3	5	7	11
$z1$	5	$30(2 \cdot 3 \cdot 5)$	$91(7 \cdot 13)$	$385(5 \cdot 7 \cdot 11)$

III.4 Nejmenší společný násobek

III.4.1 Nechť M je nějaká množina celých čísel. Označme $\mathrm{sn}(M)$ množinu všech společných násobků čísel z množiny M. To jest, $n \in \mathrm{sn}(M)$ právě tehdy když $n \in \mathbb{Z}$ a $m \mid n$ pro každé $m \in M$. Množina $\mathrm{sn}(M)$ je neprázdná, neboť $0 \in \mathrm{sn}(M)$ v každém případě.

Zřejmě je $\mathrm{sn}(\emptyset) = \mathbb{Z} = \mathrm{sn}(\{1\}) = \mathrm{sn}(\{-1\}) = \mathrm{sn}(\{1,-1\})$ a $\mathrm{sn}(\{0\}) = \{0\}$. Obecněji, je-li $0 \in M$ pak $\mathrm{sn}(\{M\}) = \{0\}$. Dále, $\mathrm{sn}(M_1 \cup M_2) = \mathrm{sn}(M_1) \cap \mathrm{sn}(M_2)$ a $\mathrm{sn}(M_1 \cap M_2) \subseteq \mathrm{sn}(M_1) \cup \mathrm{sn}(M_2)$. Je-li $M_1 \subseteq M_2$, pak $\mathrm{sn}(M_2) \subseteq \mathrm{sn}(M_1)$.

Je-li $n \in \mathrm{sn}(M)$, pak $-n \in \mathrm{sn}(M)$ a naopak.

Je $nm \in \mathrm{sn}(\{n,m\})$ pro všechna $n, m \in \mathbb{Z}$. Obecněji, je $n_1 \cdots n_k \in \mathrm{sn}(\{n_1, \ldots, n_k\})$ pro všechna $k \geq 1$, $n_1, \ldots, n_k \in \mathbb{Z}$.

III.4.2 Proposice. Nechť M je nějaká nekonečná množina celých čísel. Potom $\mathrm{sn}(M) = \{0\}$.

Důkaz. Nechť, naopak, $n \in \mathrm{sn}(M)$, $n \neq 0$. Potom $-n \in \mathrm{sn}(M)$ a my můžeme předpokládat, že $n \geq 1$. Je-li $m \in M$, pak $m \mid n$, čili $1 \leq |m| \leq n$ a tedy $m \in \{-n, \ldots, -1, 0, 1, \ldots, n\}$. Tato množina je však konečná. □

III.4.3 Proposice. Nechť $M = \{m_1, \cdots, , m_k\}$ $k \geq 1$ je konečná množina nenulových celých čísel. Potom:

(i) Množina $\mathrm{sn}(M)$ je nekonečná.

(ii) $lm_1 \cdots m_k \in \mathrm{sn}(M)$ pro každé $l \in \mathbb{Z}$.

Důkaz. Vše je jasné. □

III.4.4 Důležitá definice. Nechť M je neprázdná konečná množina celých nenulových čísel. Z III.4.3 plyne, že množina $\mathrm{sn}(M)$ je neprázdná, tedy obsahuje aspoň jedno kladné číslo. Symbolem $\mathrm{nsn}(M)$ značme nejmenší kladné číslo z množiny $\mathrm{sn}(M)$. Toto číslo je kladné, je jednoznačně určené a nazývá se nejmenší společný násobek množiny M.

Je-li $M = \{m_1, \ldots, m_k\}$, $k \geq 1$, pak mluvíme také o nejmenším společném násobku čísel $m_1, \ldots, m_k$ a píšeme $\mathrm{nsn}(M) = \mathrm{nsn}(m_1, \ldots, m_k)$.

Zbývají tři případy. Je-li M nějaká množina celých čísel, která je nekonečná či která je konečná, avšak $0 \in M$, pak $\mathrm{nsn}(M) = 0$ (je totiž $\mathrm{sn}(M) = \{0\}$). Je-li $M = \emptyset$, pak $\mathrm{sn}(M) = \mathbb{Z}$ a $\mathrm{nsn}(M) = 1$ (zde opět nejmenší kladné číslo z $\mathrm{sn}(M)$).

III.4.5 Proposice. Nechť $m \in \mathbb{Z}$. Potom $\mathrm{nsn}(m) = \mathrm{nsn}(\{m\}) = |m|$.

Důkaz. Je $\mathrm{nsn}(0) = 0$. Je-li $m \neq 0$ a $m \mid n$, pak $|m| \leq |n|$. Jelikož $m \mid |m|$, dostáváme $\mathrm{nsn}(m) = |m|$. □

III.4.6 Věta. Nechť M je nějaká množina celých čísel. Potom $\mathrm{nsn}(M) \mid n$ pro každé $n \in \mathrm{sn}(M)$.

Důkaz. Je-li $0 \in M$, či M je nekonečná, pak $\mathrm{nsn}(M) = 0$ a $\mathrm{sn}(M) = \{0\}$ (viz III.4.2). Je-li $M = \emptyset$, pak $\mathrm{nsn}(M) = 1$ a $\mathrm{sn}(M) = \mathbb{Z}$. Nechť, tedy, $M = \{m_1, \ldots, m_k\}$, $k \geq 1$, $m_i \neq 0$, $s = \mathrm{nsn}(M)$ a $n \in \mathrm{sn}(M)$. Podle I.9.3 je $n = as + b$, $a \in \mathbb{Z}$, $0 \leq b < s$. Víme, že $m_i \mid n$ a $m_i \mid s$. Takže $m_i \mid b$ pro $i = 1, \ldots, k$. Odtud, $b \in \mathrm{sn}(M)$ a $b = 0$ vzhledem k minimalitě čísla s. Tedy $s \mid n$. □

III.4.7 Proposice. Nechť $m_1, \ldots, m_k \in \mathbb{Z}$, $k \geq 1$. Potom $\mathrm{nsn}(m_1, \ldots, m_k) \mid m_1 \cdots m_k$.

Důkaz. Je $m_1 \cdots m_k \in \mathrm{sn}(m_1, \ldots m_k)$ a použije se III.4.6. □

III.4.8 Poznámka. Nechť M je konečná množina celých čísel taková, že $0 \notin M$. Buď $s = \mathrm{nsn}(M)$. Potom $s \geq 1$ a s je nejmenší kladný společný násobek čísel z M ve smyslu obvyklého uspořádání celých čísel.

Z III.4.6 plyne, že s je současně nejmenší kladný(nezáporný) společný násobek čísel z M a to ve smyslu uspořádání nezáporných celých čísel daném relací dělitelnosti - viz II.1.10.

Je-li $0 \in M$ či M je nekonečná množina, pak $\mathrm{nsn}(M) = 0$ je jediný společný násobek čísel z M a tedy je také nejmenší v obou uspořádáních. Nakonec, je-li $M = \emptyset$, pak $\mathrm{nsn}(M) = 1$ je opět nejmenší kladný společný násobek v obou uspořádáních (nejmenší nezáporný v uspořádání daném dělitelností).

III.4.9 Věta. Nechť M je neprázdná konečná množina nenulových celých čísel. Pro každé $p \in \mathbb{P}$ buď $b(p) = \max\{ \mathrm{cont}_p(m) | m \in M\}$. Potom:

(i) $b(p) \neq 0$ jen pro konečný počet prvočísel p.

(i) $\mathrm{nsn}(M) = \prod_{p \in \mathbb{P}} p^{b(p)}$.

Důkaz. Buď $P = \{p \in \mathbb{P} | b(p) \geq 1\}$. Je-li $p \in P$, pak existuje $m \in M$ tak, že $p \mid m$ a tedy $p \in \underline{P}(m)$. Je tak $P = \cup \underline{P}(m), m \in M$, z čehož plyne, že množina prvočísel P je konečná.

Položme $s = \mathrm{nsn}(M)$ a $r = \prod_{p \in \mathbb{P}} p^{b(p)}$. Je $\mathrm{cont}_p(m) \leq b(p)$ pro všechna $m \in M$ a $p \in \mathbb{P}$. Ovšem, $m = \prod_{p \in \mathbb{P}} p^{\mathrm{cont}_p(m)}$, z čehož plyne $m \mid r$. Pak ale $r \in \mathrm{sn}(M)$ a $s \mid r$ podle III.4.6. Zbývá dokázat, že $r \mid s$.

Pro každé $p \in \mathbb{P}$ existuje $m_p \in M$ takové číslo, že $b(p) = \mathrm{cont}_p(m_p)$. Tedy $p^{b(p)} \mid m \mid s$ a $b(p) \leq \mathrm{cont}_p(s)$. Jelikož $s = \prod p^{\mathrm{cont}_p(s)}$, je také $r \mid s$. □

III.4.10 Proposice. $\mathrm{nsn}(M_1 \cup M_2) = \mathrm{nsn}(\ \mathrm{nsn}(M_1), \mathrm{nsn}(M_2))$ pro libovolné podmnožiny M_1 a M_2 množiny všech celých čísel.

Důkaz. Nechť $s = \mathrm{nsn}(M_1 \cup M_2)$, $u = \mathrm{nsn}(M_1)$, $v = \mathrm{nsn}(M_2)$ a $w = \mathrm{nsn}(u, v)$. Je $s \in \mathrm{sn}(M_1) \cap \mathrm{sn}(M_2)$, čili $u \mid s$ a $v \mid s$ plyne z III.4.6. Pak ale $w \mid s$. Naopak, $u \mid w$ a $v \mid w$, z čehož vidíme, že $w \in \mathrm{sn}(M_1) \cap \mathrm{sn}(M_2) = \mathrm{sn}(M_1 \cup M_2)$. Odtud, $s \mid w$. Takže $s = w$. □

III.4.11 Proposice. $\mathrm{nsn}(a, \mathrm{nsn}(b, c)) = \mathrm{nsn}(a, b, c) = \mathrm{nsn}(\mathrm{nsn}(a, b), c)$ pro všechna $a, b, c \in \mathbb{Z}$.

Důkaz. Toto tvrzení plyne snadno z III.4.10. □

III.4.12 Proposice. Nechť $M \neq \emptyset$. Potom $\mathrm{nsn}(aM) = a \cdot \mathrm{nsn}(M)$ pro každé $a \in \mathbb{N}_0$.

Důkaz. Je-li $a = 0$, pak $\mathrm{nsn}(aM) = \mathrm{nsn}(0) = 0 = 0 \cdot \mathrm{nsn}(M)$. Je-li $0 \in M$, pak $0 \in aM$ a $\mathrm{nsn}(aM) = 0 = a \cdot 0 = a \cdot \mathrm{nsn}(M)$. Je-li M nekonečná množina, pak $\mathrm{nsn}(aM) = 0 = a \cdot \mathrm{nsn}(M)$ (pro $a \neq 0$ i pro $a = 0$). Můžeme tedy předpokládat, že množina M je konečná, neprázdná, a že $0 \notin M$. Buď $s = \mathrm{nsn}(M)$ a $r = \mathrm{nsn}(aM)$. Je $as \in \mathrm{sn}(aM)$, čili $r \mid as$ podle III.4.6. Je třeba dokázat, že $as \mid r$. My ale rovnou dokážeme, že $r = as$.

Podle III.4.9 je $r = \prod_{p \in \mathbb{P}} p^{b(p)}$, kde $b(p) = \max\{ \mathrm{cont}_p(am) | m \in M\}$. Ovšem, $\mathrm{cont}_p(am) = \mathrm{cont}_p(a) + \mathrm{cont}_p(m)$. Tedy $b(p) = \mathrm{cont}_p(a) + a(p)$, $a(p) = \max\{ \mathrm{cont}_p(m) | m \in M\}$. Tudíž $r = \prod p^{b(p)} = \prod p^{\mathrm{cont}_p(a)} \cdot \prod p^{a(p)} = as$. □

III.4.13 Poznámka. Je $a \cdot \emptyset = \emptyset$ pro každé $a \in \mathbb{Z}$. Takže $\mathrm{nsn}(a \cdot \emptyset) = \mathrm{nsn}(\emptyset) = 1$ a $a \cdot \mathrm{nsn}(\emptyset) = a \cdot 1 = a$. To znamená, že $\mathrm{nsn}(a \cdot \emptyset) = a \cdot \mathrm{nsn}(\emptyset)$ pouze pro $a = 1$ (srovnej s III.4.12).

III.4.14 Proposice. Nechť $m_1, \ldots, m_k$, $k \geq 1$, jsou nenulová čísla. Potom $\mathrm{nsn}(m_1, \ldots, m_k) = |m_1 \cdots m_k| (= |m_1| \cdots |m_k|)$ právě když $m_1, \ldots, m_k$ jsou po dvou nesoudělná.

Důkaz. Je-li $k = 1$, pak není co dokazovat (III.4.5). Buď tedy $k \geq 2$, $s = \mathrm{nsn}(m_1, \ldots, m_k)$ a $m = |m_1 \cdots m_k|$. Pro každé $p \in \mathbb{P}$ je $\mathrm{cont}_p(m) = \sum \mathrm{cont}_p(m_i)$ a $\mathrm{cont}_p(s) = \max\{ \mathrm{cont}_p(m_i)\}$. Samozřejmě, $s \mid m$. Je-li nyní $s = m$, pak pro každé $p \in \underline{P}(m) (= \cup \underline{P}(m_i))$ existuje právě jeden index $i(p)$, $1 \leq i(p) \leq k$, tak, že $p \mid m_{i(p)}$. Odtud snadno plyne, že čísla $m_1, \ldots, m_k$ jsou po dvou nesoudělná. Tuto úvahu můžeme snadno obrátit a důkaz je dokončen. □

III.4.15 Poznámka. Na množině $\mathbb{N}_0$ můžeme definovat binární operaci $\vee$ předpisem $a \vee b = \mathrm{nsn}(a, b)$. Z III.4.4, III.4.5 a III.4.11 je vidět, že tato operace je idempotentní, komutativní a asociativní. Jde tedy o polosvaz. Navíc, $a(b \vee c) = (ab) \vee (ac)$ podle III.4.12.

III.4.16 Příklad. Nechť $s \geq 1$, $n_1, \ldots, n_s \in \mathbb{N}$, $2 \leq n_1 \leq n_2 \leq \cdots \leq n_s$, $u = (n_1 - 1) \cdots (n_s - 1)$, $v = \mathrm{nsn}(n_1 - 1, \ldots, n_s - 1)$ a $w = n_1 \ldots n_s$.

(i) Je $w \geq 2^s$, $u \geq 1$, $v \geq 1$, $v \mid u$.

(ii) Jsou-li všechna čísla $n_1, \ldots, n_s$ lichá, pak $2^s \mid u$, $2 \mid v$, w je liché, $u \nmid w$, $v \nmid w$.

(iii) Je-li $s \geq 2$, aspoň jedno z čísel n_i je liché a aspoň jedno je sudé, pak u, v, w jsou vesměs sudá čísla a tak $u \nmid w - 1$, $u \nmid w + 1$, $v \nmid w - 1$, $v \nmid w + 1$.

(iv) Jsou-li všechna čísla $n_1, \ldots, n_s$ sudá, pak $2^s \mid w$ a u, v jsou lichá čísla.

(v) Je-li $s \geq 3$, $n_1 = 2$, $n_2, \ldots, n_s$ lichá, pak $4 \mid u$, $4 \nmid w$, $u \nmid w$.

(vi) Nechť $s = 2$. Potom $w = u + n_1 + n_2 - 1$, $w - 1 = u + (n_1 - 1) + (n_2 - 1)$, $w + 1 = u + n_1 + n_2$.

(vii) Nechť $s = 2$ a $v \mid w$. Z (vi) plyne, že $n_2 - 1 \mid n_1$ a, jelikož $n_1 \leq n_2$, tak $n_2 \in \{n_1, n_1 + 1\}$.

Je-li $n_1 = n_2$, tak $v = n_1 - 1$, $w = n_1^2$, $nsd(v, w) = 1$. Takže, nyní, $v \mid w$ implikuje $v = 1$, $n_1 = 2 = n_2$. Je-li $n_1 + 1 = n_2$, tak $w = n_1(n_1 + 1)$, $v = \mathrm{nsn}(n_1 - 1, n_1) = n_1(n_1 - 1)$. Jelikož $v \mid w$, tak $n_1 - 1 \mid n_1 + 1$, $2(n_1 - 1) \leq n_1 + 1$, $n_1 \leq 3$. Je-li $n_1 = 2$, pak $n_2 = 3$. Je-li $n_1 = 3$, pak $n_2 = 4$.

Zjistili jsem, že $(n_1, n_2) = (2, 2), (2, 3), (3, 4)$. A hle! Pro $(n_1, n_2) = (2, 2)$ je $u = v = 1$, $w = 4$. Pro $(n_1, n_2) = (2, 3)$ je $u = v = 2$, $w = 6$. Pro $(n_1, n_2) = (3, 4)$ je $u = v = 6$, $w = 12$.

(viii) Nechť $s = 2$ a $v \mid w - 1$.

Z (vi) plyne, že $n_2 - 1 \mid n_1 - 1$, čili $n_1 = n_2$, $v = n_1 - 1$, $w - 1 = n_1^2 - 1 = (n_1 - 1)(n_1 + 1)$. Zjistili jsme, že $n_1 = n_2$.

(ix) Nechť $s = 2$ a $v \mid w + 1$.

Z (vi) plyne, že $n_2 - 1 \mid n_1 + 1$ a, jelikož $n_1 \leq n_2$, tak $n_2 \in \{n_1, n_1 + 1, n_1 + 2\}$.

Je-li $n_1 = n_2$, pak $n_1 - 1 = v \mid w + 1 = n_1^2 + 1 = (n_1 - 1)^2 + 2n_1$, $n_1 - 1 \mid 2n_1$. Tedy $\underline{P}(n_1 - 1) \subseteq \underline{P}(2n_1) = \{2\} \cup \underline{P}(n_1)$. Jelikož $P(n_1 - 1) \cap \underline{P}(n_1) = \emptyset$, tak $\underline{P}(n_1 - 1) = 2$, $n_1 = 2^k + 1$, $k \geq 0$, $2^k \mid 2^{k+1} + 2 = 2(2^k + 1)$, $k = 0, 1$, $n_1 = 2, 3$.

Je-li $n_1 + 1 = n_2$, pak $v = \mathrm{nsn}(n_1 - 1, n_1) = n_1(n_1 - 1) = n_1^2 - n_1$, $v \mid w = n_1(n_1 + 1) + 1 = n_1^2 + n_1 + 1$, $\underline{P}(n_1) \subseteq \underline{P}(v) \subseteq \underline{P}(w) = \underline{P}(n_1^2 + n_1 + 1)$, $n_1 = 1$, spor.

Je-li $n_1 + 2 = n_2$, pak $v = \mathrm{nsn}(n_1 - 1, n_1 + 1)$, $w = n_1(n_1 + 2) = n_1^2 + 2n_1$. Je-li n_1 sudé, tak $v = (n_1 - 1)(n_1 + 1)$, $v \mid w + 1 = (n_1 + 1)^2$, $n_1 - 1 \mid n_1 + 1$, $n_1 = 2$, $n_2 = 4$. Je-li n_1 liché, tak $v = (n_1 - 1)(n_1 + 1)/2$, $v \mid w + 1 = (n_1 + 1)^2$, $(n_1 - 1)(n_1 + 1) \mid 2(n_1 + 1)^2$, $n_1 - 1 \mid 2(n_1 + 1)$, $n_1 - 1 = 2^k$, $k \geq 1$, $2^k \mid 2^{k+1} + 4$, $k = 1, 2$, $n_1 = 3, 5$.

Zjistili jsme, že $(n_1, n_2) = (2, 2), (3, 3), (2, 4), (3, 5), (5, 7)$. A hle! Pro $(n_1, n_2) = (2, 2)$ je $u = v = 1$, $w = 4$. Pro $(n_1, n_2) = (3, 3)$ je $u = 4$, $v = 2$,

$w = 9$. Pro $(n_1, n_2) = (2, 4)$ je $u = v = 3$, $w = 8$. Pro $(n_1, n_2) = (3, 5)$ je $u = 8$, $v = 4$, $w = 15$. Pro $(n_1, n_2) = (5, 7)$ je $u = v = 12$, $w = 35$.

III.5 Největší společný dělitel a nejmenší společný násobek společně

III.5.1 Věta. Nechť $a, b \in \mathbb{Z}$. Potom $\mathrm{nsn}(a,b) \cdot \mathrm{nsd}(a,b) = |ab|$ ($= ab$ pro $a, b \in \mathbb{N}_0$.

Důkaz. Buď $r = \mathrm{nsd}(a,b)$ a $s = \mathrm{nsn}(a,b)$. Je-li $a = 0$ či $b = 0$, pak $ab = 0 = s = rs$ a tvrzení je dokázáno. Můžeme předpokládat, že obě čísla jsou kladná. Tedy $|ab| = ab$.

Nechť $p \in \mathbb{P}$. Potom $\mathrm{cont}_p(r) = \min\{\mathrm{cont}_p(a), \mathrm{cont}_p(b)\}$ dle III.1.8, $\mathrm{cont}_p(s) = \max\{\mathrm{cont}_p(a), \mathrm{cont}_p(b)\}$ dle III.4.9 a, samozřejmě, $\mathrm{cont}_p(ab) = \mathrm{cont}_p(a) + \mathrm{cont}_p(b)$. Odtud, $\mathrm{cont}_p(rs) = \mathrm{cont}_p(ab)$ a to pro každé $p \in \mathbb{P}$. Tedy $rs = ab$. □

III.5.2 Poznámka. Umíme-li spočítat největší společný dělitel čísel a, b, pak pomocí III.5.1 nalezneme i nejmenší společný násobek těchto čísel. Pro tři (a více) čísel použijeme III.4.11 (a III.4.10).

III.5.3 Poznámka. (i) Nechť $a_1, \ldots, a_k$, $k \geq 1$, jsou celá čísla. Z důkazu III.5.1 je snadno vidět, že číslo $w = \mathrm{nsd}(a_1, \ldots, a_k)\ \mathrm{nsn}(a_1, \ldots, a_k)$ dělí číslo $|a_1 \cdots a_k|$. Ovšem rovnost těchto čísel obecně neplatí. Například, pro čísla $2, 4, 6$ je $\mathrm{nsd}(2,4,6) = 2$ a $\mathrm{nsn}(2,4,6) = 12$, $w = 24 \neq 48 = 2 \cdot 4 \cdot 6$,

(ii) Nechť a, b, c jsou kladná celá čísla, $r = \mathrm{nsd}(a,b,c)$, $s = \mathrm{nsn}(a,b,c)$. Jestliže čísla a, b, c jsou po dvou nesoudělná, pak $r = 1$, $s = abc$ a rovnost $r \cdot s = abc$ platí triviálně.

Nyní si dokážeme opak. Nechť $rs = abc$. Buď $p \in \mathbb{P}$ takové prvočíslo, že $p \mid a$, $p \mid b$ a $\mathrm{cont}_p(a) \leq \mathrm{cont}_p(b)$. Je-li $\mathrm{cont}_p(c) \leq \mathrm{cont}_p(a)$, pak $\mathrm{cont}_p(c) + \mathrm{cont}_p(b) = \mathrm{cont}_p(rs) = \mathrm{cont}_p(abc) = \mathrm{cont}_p(a) + \mathrm{cont}_p(b) + \mathrm{cont}_p(c)$, takže $\mathrm{cont}_p(a) = 0$, spor. Tedy $\mathrm{cont}_p(a) < \mathrm{cont}_p(c)$. Je-li $\mathrm{cont}_p(a) \leq \mathrm{cont}_p(c) \leq \mathrm{cont}_p(b)$, pak $\mathrm{cont}_p(a) + \mathrm{cont}_p(b) = \mathrm{cont}_p(rs) = \mathrm{cont}_p(a) + \mathrm{cont}_p(b) + \mathrm{cont}_p(c)$, $\mathrm{cont}_p(c) = 0$, což implikuje $\mathrm{cont}_p(a) = 0$, spor. Tedy $\mathrm{cont}_p(a) \leq \mathrm{cont}_p(b) < \mathrm{cont}_p(c)$. Pak $\mathrm{cont}_p(a) + \mathrm{cont}_p(c) = \mathrm{cont}_p(rs) = \mathrm{cont}_p(a) + \mathrm{cont}_p(b) + \mathrm{cont}_p(c)$, $\mathrm{cont}_p(b) = 0$, spor.

Zjistili jsme, že a, b jsou nesoudělná čísla. Zcela obdobně nám vyjde, že i čísla a, c jsou nesoudělná a čísla b, c jsou také nesoudělná.

III.5.4 Lemma. Pro všechna $a, b \in \mathbb{Z}$ je $\mathrm{nsd}(\mathrm{nsn}(a,b), a) = a = \mathrm{nsn}(\mathrm{nsd}(a,b), a)$.

Důkaz. Tvrzení je zřejmé, neboť $a \mid \mathrm{nsn}(a,b)$ a $\mathrm{nsd}(a,b) \mid a$. □

III.5.5 Lemma. Nechť $a_1, \ldots, a_{k+1}$, $k \geq 1$ jsou celá čísla. Potom $\mathrm{nsd}(\mathrm{nsd}(a_1, \ldots, a_k), a_{k+1}) = \mathrm{nsn}(\mathrm{nsd}(a_1, a_{k+1}), \ldots, \mathrm{nsd}(a_k, a_{k+1}))$.

Důkaz. Pro $k = 1$ je rovnost zřejmá. Buď $k \geq 2$, $r = \mathrm{nsd}(t, a_{k+1})$, $t = \mathrm{nsn}(a_1, \ldots, a_k)$ a $s = \mathrm{nsn}(\ \mathrm{nsd}(a_1, a_{k+1}), \ldots, \ \mathrm{nsd}(a_k, a_{k+1}))$. Chceme nalézt rovnost $r = s$. Je-li $a_j = 0$ pro nějaké j, $1 \leq j \leq k$, pak $t = 0$, $r = |a_{k+1}| = s$ (neboť $\mathrm{nsd}(a_j, a_{k+1}) = \mathrm{nsd}(0, a_{k+1} = |a_{k+1}|)$. Je-li $a_{k+1} = 0$, pak $r = t = s$. Předpokládejme tedy, že všechna čísla $a_1, \ldots, a_{k+1}$ jsou nenulová. Potom r, t a s jsou kladná čísla a je potřeba ověřit, že $\mathrm{cont}_p(r) = \mathrm{cont}_p(s)$ pro každé $p \in \mathbb{P}$.

Buď $v \geq 1$ takové číslo, že $p^v \mid r$. Potom $p^v \mid a_{k+1}$, $p^v \mid t$, čili $p^v \mid a_j$ pro aspoň jedno j, $1 \leq j \leq k$. Odtud, $p^v \mid \mathrm{nsd}(a_j, a_{k+1})$ a $p^v \mid s$.

Nyní naopak. Nechť $p^v \mid s$. Potom $p^v \mid \mathrm{nsd}(a_j, a_{k+1})$ pro nějaké j, $1 \leq j \leq k$, čili $p^v \mid a_{k+1}$, $p^v \mid a_j$, $p^v \mid t$ a, na konec, $p^v \mid r$. Jsme hotovi. □

III.5.6 Lemma. Nechť $a_1, \ldots, a_{k+1}$, $k \geq 1$, jsou celá čísla. Potom
$\mathrm{nsn}(\ \mathrm{nsd}(a_1, \ldots, a_k), a_{k+1}) = \mathrm{nsd}(\ \mathrm{nsn}(a_1, a_{k+1}), \ldots, \ \mathrm{nsn}(a_k, a_{k+1}))$.

Důkaz. Můžeme předpokládat, že $k \geq 2$ a $a_{k+1} \neq 0$. Označme $r = \mathrm{nsn}(t, a_{k+1})$, $t = \mathrm{nsd}(a_1, \ldots, a_k)$ a $s = \mathrm{nsd}(\ \mathrm{nsn}(a_1, a_{k+1}), \ldots, \mathrm{nsn}(a_k, a_{k+1}))$. Podobně jako v důkazu III.5.5 ověříme snadno, že $\mathrm{cont}_p(r) = \mathrm{cont}_p(s)$ pro každé $p \in \mathbb{P}$. Tedy $r = s$. □

III.5.7 Poznámka. Uvažme znovu množinu $\mathbb{N}_0$ nezáporných celých čísel uspořádaných dělitelností (viz II.1.10). Tedy, v tomto uspořádání je a "menší či rovno" b právě když a dělí b ($a \mid b$). "Nejmenším" číslem je číslo 1 a "největším" je číslo 0. Atomy jsou právě prvočísla a duální atomy neexistují.

Pro $a, b \in \mathbb{N}_0$ jen $\mathrm{nsd}(a, b) = \inf(a, b) = a \wedge b$ právě infimum (průsek) těchto čísel. Podobně $\mathrm{nsn}(a, b) = \sup(a, b) = a \vee b$ je supremum (spojení). Z III.5.4 pak plyne, že dělitelností uspořádáná množina $\mathbb{N}_0$ všech nezáporných čísel je svaz.

Odpovídající algebraický svaz je $\mathbb{N}_0(\wedge, \vee)$. Navíc, platí rovnosti $a(b \wedge c) = (ab) \wedge (ac)$, $a(b \vee c) = (ab) \vee (ac)$, $(a \wedge b)(a \vee b) = ab$ pro všechna $a, b, c \in \mathbb{N}_0$ (III.1.11, III.4.12, III.5.1). Dále platí $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$, $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ (III.5.5, III.5.6). Náš svaz je distributivní.

Svaz je také úplný. Pro každou množinu N nezáporných čísel je $\inf(N) = \mathrm{nsd}(N)$ a $\sup(N) = \mathrm{nsn}(N)$.

Svaz můžeme reprezentovat pomocí nekonečných posloupností nezáporných celých čísel s konečně mnoha nenulovými členy (a přidaným největším prvkem) – viz II.3.16(ii).

III.6 Euklidův algoritmus

III.6.1 Lemma. Buďtež $a, b, c, d \in \mathbb{Z}$, přičemž $a = bc+d$. Potom $\mathrm{nsd}(a, b) = \mathrm{nsd}(b, d)$ a $\mathrm{nsd}(a, c) = \mathrm{nsd}(c, d)$.

Důkaz. Je-li $n \in \mathbb{Z}$ takové číslo, že $n \mid a$ a $n \mid b$, pak $n \mid a - bc = d$. Naopak, jestliže $n \mid b$ a $n \mid d$, pak $n \mid bc + d = a$. Tedy $\mathrm{sd}(a, b) = \mathrm{sd}(b, d)$ a $\mathrm{nsd}(a, b) = \mathrm{nsd}(b, d)$. Symetricky $\mathrm{sd}(a, c) = \mathrm{sd}(c, d)$ a $\mathrm{nsd}(a, c) = \mathrm{nsd}(c, d)$. □

III.6.2 Lemma. Nechť a, b jsou nenulová celá čísla. Potom $\mathrm{nsd}(a, b) = \mathrm{nsd}(b, [a]_b) = \mathrm{nsd}(|b|, [a]_{|b|})$.

Důkaz. Je $a = rb + [a]_b$, kde $r \in \mathbb{Z}$, $0 \leq [a]_b < |b|$ (I.9.4). Podle III.6.1 je $\mathrm{nsd}(a, b) = \mathrm{nsd}(b, [a]_b)$. Ovšem $[a]_b = [a]_{|b|}$ podle I.9.5(iii) a $\mathrm{nsd}(b, [a]_b) = \mathrm{nsd}(-b, [a]_b)$. □

III.6.3 Euklidův algoritmus Předchozí lemma nás vede k následujícímu postupu při výpočtu největšího společného dělitele dvou čísel.

Nechť $a, b \in \mathbb{Z}$ a $r = \mathrm{nsd}(a, b)$. Předně, je-li $a = 0$, pak $r = |b|$. Je-li $b = 0$, pak $r = |a|$. Můžeme tedy předpokládat, že obě čísla a, b jsou kladná. Je-li $a = 1$ či $b = 1$, pak $r = 1$. Můžeme se tedy omezit na čísla $a \geq 2$ a $b \geq 2$. Je-li $a = b$, pak $r = a$. Takže, celkově se můžeme omezit na $2 \leq b < a$.

Je $a = r_1 b + s_1$, $s_1 = [a]_b$, $0 \leq s_1 < b$ (z důkazů vět I.9.1, I.9.3 a z poznámky I.9.2 je jasné, jak postupovat při hledání čísel r_1 a s_1). Podle III.6.2 je $r = \mathrm{nsd}(b, s_1)$. Je-li $s_1 = 0$, pak $r = b$. Je-li $s_1 \geq 1$, pak $b = r_2 s_1 + s_2$, $s_2 = [b]_{s_1}$ a $r = \mathrm{nsd}(s_1, s_2)$.

Opět, je-li $s_2 = 0$, pak $r = s_1$. Je-li $s_1 \geq 1$, pak dostáváme následující schema:

$$\begin{gathered} a = s_{-1} = r_1 s_0 + s_1,\ s_0 = b,\ 0 < s_1 < s_2 \\ b = s_0 = r_2 s_1 + s_2,\ 0 < s_1 < s_2 \end{gathered}$$

$$\vdots$$

$$\begin{gathered} s_{n-1} = r_{n+1} s_n + s_{n+1},\ 0 < s_{n+1} < s_2 \\ s_n = r_{n+2} s_{n+1},\ s_{n+2} = 0, \end{gathered}$$

kde $n \geq 1$ (to proto že posloupnost nezáporných celých čísel $b = s_0 > s_1 > s_2 > \ldots$ musí skončit na nule). Nyní je $\mathrm{nsd}(a, b) = r = s_{n+1}$. Všimněme si, že $s_{n+1} \leq b - n - 1$ a $n \leq b - 2$ (to je ovšem velmi hrubý odhad).

III.6.4 Příklad. Buď $a = 561$ a $b = 330$. Je $a = 1 \cdot b + 231$, $b = 1 \cdot 231 + 99$, $231 = 2 \cdot 99 + 33$, $99 = 3 \cdot 33 + 0$. Tedy $\mathrm{nsd}(a, b) = \mathrm{nsd}(561, 330) = 33$. Z III.5.1 nyní plyne $33 \cdot \mathrm{nsn}(561, 330) == 561 \cdot 330 = 561 \cdot 10 \cdot 33$, čili $\mathrm{nsn}(561, 330) = 5610$.

III.6.5 Příklad. Buď $a = 2147483648$ a $b = 196608$. Je $a = 10922b + 131072$, $b = 1 \cdot 131072 + 65536$, $131072 = 2 \cdot 65536$. Takže $\mathrm{nsd}(a, b) = 65536$ $(= 2^{16})$ a $\mathrm{nsn}(a, b) = 6442450944$.

III.6.6 Příklad. Buď $a = 55$ a $b = 34$. Je $a = 1 \cdot b + 21$, $b = 1 \cdot 21 + 13$, $21 = 1 \cdot 13 + 8$, $13 = 1 \cdot 8 + 5$, $8 = 1 \cdot 5 + 3$, $5 = 1 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$ a, nakonec, $2 = 2 \cdot 1$. Tedy $\mathrm{nsd}(55, 34) = 1$.

Zde máme $s_{-1} = 55$, $s_0 = 34$, $s_1 = 21$, $s_2 = 13$, $s_3 = 8$, $s_4 = 5$, $s_5 = 2$, $s_6 = 1$ a $s_7 = 0$, $r_1 = r_2 = r_3 = r_4 = r_5 = r_6 = r_7 = 1$. V tom je také důvod, proč zde algoritmus běžel "pomalu".

III.6.7 Pokud se zamyslíme nad rychlostí algoritmu, tak na základě příkladu III.6.6 vidíme, že nejvíce kroků dostaneme vždy, když $r_i = 1$ pro každé i. Dochází tak vždy k nejmenšímu možnému snížení hodnoty součtu $a + b$.

Rekonstruujme tedy "nejpomalejší" posloupnost postupně odzadu. $s_{n+1} = 1$, $s_n = 2$, $s_{n-1} = 3$, $s_{n-2} = 5$, ... Vidíme, že pro člen s_k musí platit $s_k = s_{k+1} + s_{k+2}$.

Nejhorší možný případ tak dostáváme tehdy, když a, b jsou dva po sobě jdoucí členové posloupnosti $f_0 = f_1 = 1$ a $f_n = f_{n-1} + f_{n-2}$ pro $n \geq 2$. Tato posloupnost je známa pod názvem Fibonacciho posloupnost.

Naopak, nechť $a \geq b$ a n je takové přirozené číslo, že $f_{n-1} < a \leq f_n$. Pak Euklidův algoritmus na nalezení $\mathrm{nsd}(a, b)$ končí nejpozději v n krocích.

III.6.8 Euklidův algoritmus je pojmenován po řeckém matematikovi Euklidovi (± 325 př. n. l. – ± 260 př. n. l). Euklid (též Eukleidés či Euklides) tento algoritmus pravděpodobně sám nevymyslel, ale publikoval jej ve svém díle Základy, kde se nám zachoval pro další generace.

Euklidův algoritmus je možná nejstarším dochovaným netriviálním algoritmem.

III.7 Rozšířený Euklidův algoritmus

III.7.1 Rozšířený Euklidův algoritmus. Nechť $a, b \in \mathbb{Z}$ a $r = \mathrm{nsd}(a, b)$. Chceme nalézt čísla $c, d \in \mathbb{Z}$ taková, že $r = ca + db$ (viz III.1.5(i)).

Předně, je-li $a = 0$, pak $r = |b|$ a volíme c libovolně, $d = 1$ pro $b \geq 0$ a $d = -1$ pro $b < 0$. Podobně, je-li $b = 0$. Nechť tedy $a \neq 0$, $b \neq 0$.

Dále, je $r = \mathrm{nsd}(|a|, |b|)$ a $r = ca + bd$ znamená, že $r = (-c)(-a) + db = ca + (-d)(-b) = (-c)(-a) + (-d)(-b)$. Můžeme se tedy omezit na případ kladných čísel a, b.

Je-li $a = 1$, pak $r = 1 = 1a + 0b$. Podobně, je-li $b = 1$. Je-li $a = b$, pak $r = a = 1a + 0b$. Jestliže $b \mid a$, pak $r = b = 0a + 1b$. Podobně, jestliže $a \mid b$. Můžeme se tedy omezit na případ $2 \leq b < a$, $b \nmid a$.

Buď $s_{-1} = a = r_1 s_0 + s_1$, $s_0 = b, 0 \leq s_1 < s_0$, $s_0 = b = r_2 s_1 + s_2$, $0 \leq s_2 < s_1$, Je-li $s_2 = 0$, pak $r = s_1 = a - r_1 b, c = 1, d = -r_1$. Je-li však $s_2 \geq 1$, pak máme toto schema (viz III.6.3):

$$\begin{gathered} a = s_{-1} = r_1 s_0 + s_1,\ s_0 = b,\ 0 < s_1 < s_2, \\ b = s_0 = r_2 s_1 + s_2,\ 0 < s_2 < s_1, \end{gathered}$$

$$\vdots$$

$$\begin{gathered} s_{n-1} = r_{n+1} s_n + s_{n+1},\ 0 < s_{n+1} < s_n, \\ s_n = r_{n+2} s_{n+1},\ s_{n+2} = 0, \\ r = s_{n+1}, n \geq 1. \end{gathered}$$

Nyní si všimněme, že pro každé $-1 \leq i \leq n+1$ existují celá čísla u_i, v_i taková, že $s_i = u_i a + v_i b$. Je-li totiž $i = -1$, pak volíme $u_{-1} = 1, v_{-1} = 0$. Je-li $i = 0$, pak volíme $u_0 = 0, v_0 = 1$. Dále indukcí podle i. Je-li $0 \leq i \leq n$, pak $s_{i+1} = s_{i-1} - r_{i+1} s_i = u_{i-1} a + v_{i-1} b - r_{i+1} u_i a - r_{i+1} v_i b =$
$(u_{i-1} - r_{i+1} u_i) a + (v_{i-1} - r_{i+1} v_i) b$. Tedy $u_{i+1} = u_{i-1} - r_{i+1} u_i$ a
$v_{i+1} = v_{i-1} - r_{i+1} v_i$.
Tím je indukční krok završen a dostáváme $r = r_{n+1} = u_{n+1} a + v_{n+1} b$,
$c = u_{n+1}, d = v_{n+1}$ (samozřejmě, $s_{n+2} = 0 = 0a + 0b$).

III.7.2 Příklad. Buď $a = 110313$ a $b = 34709$. Máme:
$s_{-1} = a = 110313 = 104127 + 6186 = 3b + 6186 = r_1 s_0 + s_1$,
$r_1 = 3, s_1 = 6186 = a - 3b$;
$s_0 = b = 34709 = 30930 + 3779 = r_2 s_1 + s_2$,
$r_2 = 5, s_2 = 3779 = s_0 - r_2 s_1 = b - 5(a - 3b) = -5a + 16b$;
$s_1 = 6186 = 3779 + 2407 = r_3 s_2 + s_3$,
$r_3 = 1, s_3 = 2407 = s_1 - r_3 s_2 = (a - 3b) - (-5a + 16b) = 6a - 19b$;
$s_2 = 3779 = 2407 + 1372 = r_4 s_3 + s_4$,

$r_4 = 1, s_4 = 1372 = s_2 - r_4 s_3 = (-5a + 16b) - (6a - 19b) = -11a + 35b;$
$s_3 = 2407 = 1372 + 1035 = r_5 s_4 + s_5,$
$r_5 = 1, s_5 = 1035 = s_3 - r_5 s_4 = (6a - 19b) - (-11a + 35b) = 17a - 54b;$
$s_4 = 1372 = 1035 + 337 = r_6 s_5 + s_6,$
$r_6 = 1, s_6 = 337 = s_4 - r_6 s_5 = (-11a + 35b) - (17a - 54b) = -28a + 89b;$
$s_5 = 1035 = 1011 + 24 = r_7 s_6 + s_7,$
$r_7 = 3, s_7 = 24 = s_5 - r_7 s_6 = (17a - 54b) - 3(-28a + 89b) = 101a - 321b;$
$s_6 = 337 = 336 + 1 = r_8 s_7 + s_8,$
$r_8 = 14, s_8 = 1 = s_6 - r_8 s_7 = -(-28b + 89b) - 14(101a - 321b) = 1442a + 4583b.$

Zpětnou kontrolou dostaneme, že $1442a = 159071346$ a $4583b = 159071347$. Takže to vyšlo dobře.

Všimněme si též, že $u_{-1} = 1, u_0 = 0, u_1 = 1, u_2 = -5, u_3 = 6, u_4 = -11, u_5 = 17, u_6 = -28, u_7 = 101, u_8 = -1442$, $v_{-1} = 0, v_0 = 1, v_1 = -3, v_2 = 16, v_3 = -19, v_4 = 35, v_5 = -54, v_6 = 89, v_7 = -321, v_8 = 4583$.

III.7.3 Zábavka. Pro chvíle oddechu si zábavně počítejme.

Vezměme si číslo $n \geq 2$ a položme $z_1 = n$. Nalezněme nejmenší číslo z_2 takové, že $z_2 \geq z_1$ a $n-1 \mid z_2$. Nalezněme nejmenší číslo z_3 takové, že $z_3 \geq z_2$ a $n - 2 \mid z_3$. A tak dále. Celý postup končí na čísle z_n; je ovšem $z_n = z_{n-1}$.

Pro $2 \leq n \leq 16$ dostáváme tyto posloupnosti:
$2, 2;$
$3, 4, 4;$
$4, 6, 6, 6;$
$5, 8, 9, 10, 10;$
$6, 10, 12, 12, 12, 12;$
$7, 12, 15, 16, 18, 18, 18;$
$8, 14, 18, 20, 20, 21, 22, 22;$
$9, 16, 21, 24, 25, 28, 30, 30, 30;$
$10, 18, 24, 35, 36, 40, 40, 42, 42, 42;$
$11, 20, 27, 32, 35, 36, 40, 40, 42, 42, 42;$
$12, 22, 30, 36, 40, 42, 42, 45, 48, 48, 48, 48;$
$13, 24, 33, 40, 45, 48, 49, 54, 55, 56, 57, 58, 58;$
$14, 26, 36, 44, 50, 54, 56, 56, 60, 60, 60, 60, 60, 60;$
$15, 28, 39, 48, 55, 60, 63, 64, 70, 72, 75, 76, 78, 78, 78;$
$16, 30, 42, 52, 60, 66, 70, 72, 72, 77, 78, 80, 80, 81, 82, 82.$

Pro $n \geq 2$ si označme $z(n)$ poslední číslo z_n příslušné posloupnosti.

Dostaneme tuto tabulku:

n	2	3	4	5	6	7	8	9
n^2	4	9	16	25	36	49	64	81
$z(n)$	2	4	6	10	12	18	22	30
$3z(n)$	6	12	18	30	36	54	66	90
$4z(n)$	8	16	24	40	48	72	88	120

n	10	11	12	13	14	15	16	
n^2	100	121	144	169	196	225	256	
$z(n)$	42	42	48	58	60	78	82	
$3z(n)$	126	126	144	174	180	234	246	
$4z(n)$	168	168	192	232	240	312	328	

Vidíme, že $4z(n) > n^2$ pro všechna $2 \leq n \leq 16$, $n^2 = 3z(n)$ pro $n = 6, 12$ a $n^2 > 3z(n)$ pro $n = 14, 16$. A jestlipak od určitého n výše není vždy $315z(n) > 100n^2 > 314z(n)$?

III.8 $n^k = m^l$

III.8.1 Věta. Nechť $n \geq 2, m \geq 2, k \geq 1, l \geq 1$. Následující tři podmínky jsou ekvivalentní:

(i) $n^k = m^l$.

(ii) Existuje (jednoznačně určené) číslo $w \geq 2$ takové, že $n = w^u$ a $m = w^v$ kde $vq = k$ a $uq = l$, $q = \text{nsd}(k, l)$ (potom $\text{nsd}(u, v) = 1$ a $ku = lv = \text{nsn}(k, l)$).

(iii) Existují kladná čísla a, b, c taková, že $n = a^b, m = a^c$ a $kb = lc$ (potom $b = du, c = dv, w = a^d, a \geq 2, d = \text{nsd}(b, c)$).

Důkaz. (i) implikuje (ii). Je $\underline{P}(n) = \underline{P}(n^k) = \underline{P}(m^l) = \underline{P}(m)$, čili $\underline{P}(n) = \underline{P}(m) = \{p_1, \ldots, p_t\}$ kde $t \geq 1$ a p_i jsou po dvou různá prvočísla (viz II.3.19). Zajisté, $kr_i = ls_i$, kde $r_i = \text{cont}_{p_i}(n)$, $s_i = \text{cont}_{p_i}(m)$, $i = 1, \ldots, t$. Dále, $qvr_i = kr_i, ls_i = qus_i, vr_i = us_i$, $v \mid s_i$, $u \mid r_i$, $s_i = q_i v, r_i = q_i u$. Položme $w = p_1^{q_1} \cdots p_t^{q_t}$. Je pak $w^u = p_1^{uq_1} \cdots p_t^{uq_t} = p_1^{r_1} \cdots p_t^{r_t} = n$ a, podobně, $w^v = m$. Samozřejmě, $\text{nsn}(k, l) = ku = vl$.

(ii) implikuje (iii). Tato implikace je triviální.

(iii) implikuje (i). Máme $n^k = (a^b)^k = a^{kb} = a^{lc} = (a^c)^l = m^l$. Dále $qvb = kb = lc = quc$, $vb = uc, v \mid c$, $u \mid b, b = du, c = dv$ a $w = a^d$. Zbytek je jasný. □

III.8.2 Poznámka. Nechť $n, m \in \mathbb{Z}$ a $k, l \in \mathbb{N}_0$ jsou taková čísla, že $n^k = m^l$.

(i) Je-li $|n| \geq 2$ (popř., $|m| \geq 2$), pak buďto $|m| \geq 2$ (popř., $|n| \geq 2$) a nebo $n^k = 1 = m^l$ a $k = 0$ (popř. $l = 0$).

(ii) Nechť $n \geq 2, m \geq 2$ a $k \geq 1$. Potom $l \geq 1$ a tento případ je popsán v III.8.1.

(iii) Nechť $n \geq 2, m \leq -2$ a $k \geq 1$. Potom $l \geq 2$ je sudé číslo a $n^k = (-m)^l$, $-m \geq 2$. Podle III.8.1 je $n = a^b, m = -a^c, a \geq 2, b \geq 1, c \geq 1, kb = lc$. Zřejmě $m = (-a)^c$ právě když $\text{cont}_2(k) \leq \text{cont}_2(l)$. Podobně, $n = (-a)^b, m = (-a)^c$ právě když $\text{cont}_2(k) \leq \text{cont}_2(l)$.

(iv) Nechť $n \leq -2, m \geq 2$ a $l \geq 1$. Tento případ je symetrický k předchozímu.

(v) Nechť $n \leq -2, m \leq -2$ a $k, l \geq 1$. Pak čísla k, l mají stejnou paritu. Samozřejmě, $(-n)^k = (-m)^l$. Tedy $n = -a^b, m = -a^c$, $a \geq 2, b, c \geq 1$, $kb = lc$. Teď $n = (-a)^b$ a $m = (-a)^c$ právě když b, c jsou lichá čísla (potom $\text{cont}_2(k) = \text{cont}_2(l)$).

Buď $\text{cont}_2(k) = \text{cont}_2(l)$. Je pak $\text{cont}_2(b) = z = \text{cont}_2(c)$, $b = 2^z \cdot b_1$, $c = 2^z \cdot c_1$, b_1, c_1 liché, $kb_1 = lc_1, n = a_1^{b_1}, m = a_1^{c_1}$, $a_1 = -a^{2^z}$.

(vi) Nechť $|n| \geq 2$ (popř. $|m| \geq 2$) a $k \geq 1$ (popř. $l \geq 1$). Potom $|n| \geq 2, |m| \geq 2, k \geq 1, l \geq 1$.

(vii) Nechť $|n| \geq 2, |m| \geq 2$ a $k = 0$ (popř. $l = 0$). Potom $k = l = 0, n^k = 1 = m^l$.

III.8.3 Poznámka. Nechť $n, m \in \mathbb{Z}$ a $k, l \in \mathbb{N}_0$ jsou taková čísla, že $n^k = m^l$. V III.8.2 jsme probrali případ $|n| \geq 2$, $|m| \geq 2$.

Teď buď $n = 0, \pm 1$, případ $m = 0, \pm 1$ je symetrický.

(i) Nechť $n = 0, k \geq 1$. Pak $n^k = 0 = m^l$, čili $m = 0$ a $l \geq 1$. Samozřejmě $n = 0^l, m = 0^k, kl = lk$.

(ii) Nechť $n = 0, k = 0$. Pak $n^k = 1 = m^l$ a tedy buďto $l = 0$, nebo $m = 1$ a nebo $m = -1$ a l je sudé.

(iii) Nechť $n = 1$. Potom $n^k = 1 = m^l$ (viz předchozí bod).

(iv) Nechť $n = -1$ a k je sudé. Opět $n^k = 1 = m^l$.

(v) Nechť $n = -1$ a k je liché. Potom $n^k = -1 = m^l$, $m = -1$, l je liché. Samozřejmě, $n = (-1)^l, m = (-1)k, kl = lk$.

III.8.4 Cvičení. Nechť $n, m \in \mathbb{N}_0$ jsou taková čísla, že $n^m = m^n, n \neq m$. Zjistíme, že potom $(n, m) = (2, 4), (4, 2)$ (je $2^4 = 16 = 4^2$).

Především, velmi lehce nahlédneme, že $n \geq 2, m \geq 2$. Z III.8.1 plyne, že existuje $w \geq 2$ takové, že $n = w^u, m = w^v$, kde $wq = m$ a $uq = n$. Potom je $u < v$ a $2 \leq v$. Dále $uw^v = um = uvq = vn = vw^u$, $v = uw^{v-u}$, $u \mid v$ a $u = 1$, neboť $\mathrm{nsd}(u, v) = 1$. Takže $n = w = q$ a $vn = m = n^v$. Odtud $n = 2 = v$ (I.4.11) a tak $m = 4$.

III.8.5 Poznámka. (i) Číslo tvaru $n^m + m^n$, $n \geq 2, m \geq 2$ je známo jako Leylandovo číslo. Je-li to prvočíslo, pak je to Leylandovo prvočíslo.

Nejmenší Leylandovo číslo je $8 = 2^2 + 2^2$. Prvních 10 Leylandových čísel tvoří posloupnost 8,17,32,54,100,145,177,320,368,512. Čísla $17(= 2^3 + 3^2)$, $593(= 2^9 + 9^2)$, $32993(= 2^{15} + 15^2)$, $2097593(= 2^{21} + 21^2)$ jsou první 4 Leylandova prvočísla. Také číslo $5122^{6753} + 6753^{5122}$ je prý prvočíslo (v dekadickém zápisu má 25050 číslic). Totéž se říká o číslu $8656^{2929} + 2929^{8656}$ (30008 číslic).

(ii) Můžeme také uvažovat čísla tvaru $n^m - m^n$. Např. $1 = 3^2 - 2^3$, $7 = 2^5 - 5^2$, $17 = 3^4 - 4^3$, $79 = 2^7 - 7^2$, $1927 = 2^{11} - 11^2$. Čísla $7, 17, 79$ jsou prvočísla a $1927 = 41 \cdot 47$ prvočíslo není.

(iii) Čísla typu (i) a (ii) jsou proslulá tím, že vzdorují různým testům prvočíselnosti.

III.9 Procvičení

Vrátíme se k látce probírané v III.2.11, III.2.12, III.2.13, III.2.14 a III.2.15. Látku si doplníme o nové poznatky. Výklad bude vhodný i pro ty, co chyběli.

III.9.1 Cvičení. V III.2.12 jsme spočetli, že pro $a, b \in \mathbb{Z}$ platí $ab \mid a+b$ právě jen pro $a = -b$ a navíc pro dvojice $(1,1),(2,2),(-1,-1),(-2,-2)$. Postup použitý v III.2.12 lze nezanedbatelně zjednodušit takto:

Je-li $a+b = cab$, pak $b = a(cb-1)$, $a \mid b$. Symetricky, $b \in a$, čili $a = \pm b$. Je-li $a+b \neq 0$, pak $a^2 \mid 2a$, $a \mid 2$, $a = \pm 1, \pm 2$. Zbytek je zřejmý.

III.9.2 Cvičení. A teď se zabývejme tím, kdy $a+b \mid ab$, $a, b \in \mathbb{Z}$. Něco jsme zjistili v III.2.14, avšak zkusme jiný postup:

Buď $r = \mathrm{nsd}(a,b)$, $a = rc$, $b = rd$, $c, d \in \mathbb{Z}$, $\mathrm{nsd}(c,d) = 1$.

(i) Dokážeme, že $a+b \mid ab$ právě když $a+b \mid r^2$.

Zřejmě $r^2 \mid r^2cd = ab$, takže $a+b \mid r^2$ ihned implikuje $a+b \mid ab$. Je třeba dokázat obrácenou implikaci. Nechť tedy $a+b \mid ab$. Je-li $a = 0$, pak $r = |b|$ a $a+b = b \mid b^2 = r^2$. Podobně, je-li $b = 0$. Lze tedy předpokládat, že $a \neq 0 \neq b$. Potom $r \geq 1$, $c \neq 0 \neq d$. Máme $a+b = r(c+d)$, $ab = r^2cd$, z čehož plyne $c+d \mid rcd$, $rcd = w(c+d), w \in \mathbb{Z}$, $c(rd-w) = wd$. Jelikož $\mathrm{nsd}(c,d) = 1$, tak $c \mid w, d \mid rd-1$, $d \mid w$ a $cd \mid w$. Tudíž $w = vcd$, $v \in \mathbb{Z}$, $rcd = w(c+d) = vcd(c+d)$, $r = v(c+d)$. Celkově, $r^2 = v(c+d)r = v(a+b)$.

Můžeme postupovat poněkud komlikovaněji. Nechť $a+b \mid ab, a \neq 0 \neq b$. Je pak $ab \neq 0$, čili $a+b \neq 0$, $r \geq 1$. Navíc, obě čísla a, b nemohou být současně lichá (jinak by totiž sudé číslo $a+b$ dělilo liché číslo ab). Víme, že $a+b \mid (a+b)(a-b) = a^2-b^2$ a $a+b \mid (a+b)^2 = a^2+2ab+b^2$. Jelikož $a+b \mid ab$, tak $a+b \mid a^2+b^2$. Odtud $a+b \mid \mathrm{nsd}(a^2-b^2, a^2+b^2) = s$. Je $a^2-b^2 = r^2(c^2-d^2)$, $a^2+b^2 = r^2(c^2+d^2)$, a tak $s = r^2t$, kde $t = \mathrm{nsd}(c^2-d^2, c^2+d^2)$. Tedy $a+b \mid r^2t$, $r^2t = z(a+b), z \in \mathbb{Z}$. Je $z(a+b) = r(c+d)$, čili $z(c+d) = rt$. Jestliže $c+d \mid r$, pak $a+b = r(c+d) \mid r^2$ a jsme hotovi. Postupujíce sporem, předpokládejme, že $p \mid c+d$ a $p \mid t$ pro nějaké $p \in \mathbb{P}$. Potom $p \mid c^2-d^2$, $p \mid c^2+d^2$, $p \mid 2c^2, p \mid 2d^2$. Je však $\mathrm{nsd}(c,d) = 1$ a $p \mid c+d$. Takže $p \nmid c, p \nmid d$ a nutně $p = 2$. Čísla c, d jsou lichá. Víme, že $a+b \mid a^2-b^2$, $a+b \mid a^2+b^2$, takže $a+b \mid 2a^2, a+b \mid 2b^2$ a $a+b \mid \mathrm{nsd}(2a^2, 2b^2) = 2r^2$. Je $2r^2 = (a+b)e = (c+d)er, e \in \mathbb{Z}$, $2r = (c+d)e$. Jelikož $c+d \nmid r$, tak e je liché číslo a $\mathrm{cont}_2(c+d) = 1 + \mathrm{cont}_2(r)$. A teď si to shrňme. Máme $a+b = r(c+d)\mathrm{cont}_2(a+b) = \mathrm{cont}_2(r) + \mathrm{cont}_2(c+d) = 2\mathrm{cont}_2(r)+1$, $ab = r^2cd, c, d$ liché, $\mathrm{cont}_2(ab) = 2\mathrm{cont}_2(r) < 2\mathrm{cont}_2(r)+1 = \mathrm{cont}_2(a+b)$ což je spor s tím, že $a+b \mid ab$.

(ii) Jsou-li čísla a, b nesoudělná, pak z (i) plyne to,že $a+b \mid ab$ pouze v případě, že $a+b = \pm 1$. Jinak napsáno, buďto $b = 1-a$ a nebo $b = -1-a$ ($a = 1-b$ či $a = -1-b$).

Dostáváme dvojice $(a,b) = \ldots, (-4,5),\ (-3,4),\ (-2,3),\ (-1,2),\ (0,1),$ $(1,0),\ (2,-1),\ (3,-2)$ a dvojice $\ldots, (-4,3),\ (-3,2),\ (-2,1),\ (-1,0),\ (0,-1),$ $(1,-2)$.

(iii) A teď si všimněme, že (i) (potažmo (ii)) snadno plyne z III.2.14. Vskutku. Je-li $a = f(g+h)g$, $b = f(g+h)h$, $f,g,h \in \mathbb{Z}$, pak je $f(g+h) \mid r$ a $a+b = f(g+h)^2 \mid r^2$.

III.9.3 Cvičení. Zabývejme se dále uspořádanými dvojicemi (a,b) celých čísel takovými, že $a \geq b$ a $a+b \mid ab$. Za tím účelem (lokálně) označme symbolem A množinu těchto dvojic.

(i) Předně si všimněme, že $(a,a) \in A$ právě když a je sudé číslo. Dále, $(a,-a) \in A$ pouze pro $a = 0$. Dále, $(a,a-1) \in A$ pouze pro $a = 1$. Dále, $(a,a-2) \in A$ právě pro $a = 0{,}2$.

(ii) Nechť $(a,b) \in A$, přičemž $a > b$, $(a,b) \neq (2,0),(1,0),(0,-2)$. Z (i) plyne, že $a-b \geq 3$. Samozřejmě, $(6,3) \in A$ a $6-3 = 3$.

(iii) Pro každé $r \geq 0$ buď $a_r = \{(a,b) \in A \mid \mathrm{nsd}(a,b) = r\}$. Zřejmě je $A = \cup A_r, r \geq 0$, přičemž toto sjednocení je disjunktní. Víme, že $a+b \mid r^2$ (III.9.2).

Ihned vidíme, že $A_0 = \{(0,0)\}$. Z III.9.2 (ii) plyne, že $A_1 = \{(a,1-a) \mid a \geq 1\} \cup \{(a,-1-a) \mid a \geq 0\}$. Tedy v A_1 jsou právě dvojice $(1,0),(2,-1),(3,-2),\ldots$ a $(0,-1),(1,-2),(2,-3),\ldots$.

(vi) Nechť $(a,b) \in A_r, r \geq 1$. Pak $a+b = s \neq 0$, $b = s-a$, $r \mid s \mid r^2$. Navíc, $r = \mathrm{nsd}(a,s) = \mathrm{nsd}(b,s)$.

(v) Pro každé $r \geq 1$ a $s \in \mathbb{Z}$ takové, že $r \mid s \mid r^2$ buď $A_{r,s} = \{(a,s-a), a \in \mathbb{Z}, \mathrm{nsd}(a,s) = r, 2a \geq s\}$. Je zajisté $a \geq s-a$. Dále, $a+(s-a) = s \mid r^2, r \mid a$, $r \mid s-a$, $r^2 \mid a(s-a)$, $a+(s-a) \mid a(s-a)$ a tak $(a,s-a) \in A$. Navíc, $r \mid t = \mathrm{nsd}(a,s-a)$, $t \mid a, t \mid s$, $t \mid \mathrm{nsd}(a,s) = r$. Tedy $t = r$. Je tudíž $(a,s-a) \in A_r$.

Tím jsme ověřili, že $A_{r,s} \subseteq A_r$.

(vi) Nechť $r \geq 1$. Z (iv) a (v) plyne, že $A_r = \cup_s A_{r,s}, s \in \mathbb{Z}$, $r \mid s \mid r^2$. Toto sjednocení je disjunktní.

(vii) Pro každé $r \geq 2$ je $(r^2-r, r) \in A_{r,r^2}$. Tedy $(2,2) \in A_{2,4}$, $(6,3) \in A_{3,9}$, $(12,4) \in A_{4,15}$, $(20,5) \in A_{5,25}$, $\ldots$.

(viii) Nechť $r \geq 1$, $s \in \mathbb{Z}$, $r \mid s \mid r^2$. Je-li $a \in \mathbb{Z}$ takové číslo, že $\mathrm{nsd}(a,s) = r$, pak $a = ra_1$, $s = rs_1$, $s_1 \mid r$, $s-a = r(s_1-a_1)$, $\mathrm{nsd}(a_1,s_1) = 1$. Je-li $2a \geq s$, pak $2a_1 \geq s_1$.

(xi) Nechť $r \geq 1$. Z (viii) snadno plyne, že $A_r = \cup_{s_1}\{ra_1, r(s_1-a_1) \mid a_1, s_1 \in \mathbb{Z}, 2a_1 \geq s_1, s_1 \mid r, \mathrm{nsd}(a_1,s_1) = 1\}$. Toto sjednocení je disjunktní.

(x) Buď $r \geq 1$. Označme $A_r^+ = \{(a,b) \in A_r \mid a \geq 1, b \geq 1\}$. Z (ix) plyne, že $A_r^+ = \cup_{s_1}\{(ra_1, r(s_1-a_1) \mid a_1, s_1 \in \mathbb{N}, 2a_1 \geq s_1 \geq a_1, s_1 \mid r, \mathrm{nsd}(a_1,s_1) = 1\}$.

(xi) Takže $A_1^+ = \emptyset$, $A_2^+ = \{(2,2)\}$, $A_3^+ = \{(6,3)\}$, $A_4^+ = \{(4,4),(12,4)\}$, $A_5^+ = \{(15,10),(20,5)\}$, $A_6^+ = \{(6,6),(12,6),(30,6)\}$,
$A_7^+ = \{(28,21),(35,14),(42,7)\}$,
$A_8^+ = \{(8,8),(24,8),(40,24),(56,8)\}$,
$A_9^+ = \{(18,9),(45,36),(63,18),(72,9)\}$,
$A_{10}^+ = \{(10,10),(30,20).(40,10),(70,30),(90,10)\}$.

Máme zde 25 dvojic (a,b) kladných celých čísel takových, že $a+b \mid ab$. Podíly $ab \mid (a+b)$ jsou postupně čísla 1, 2, $2,3,6$, $4,3,4,5$, 12, 10, 6, 4, 6 , 15, 7, 6, 20, 14, $8,10$, $12,8,21,9$.

Je $(132,12) \in A_{12}^+$ a $132 \cdot 12 \mid (132+12) = 11$.

III.9.4 Cvičení. Nechť $a,b \in \mathbb{Z}, r = \mathrm{nsd}(a,b)$. Dokážeme, že následující tři podmínky jsou ekvivalentní:
(1) $a+b \mid a^2+b^2$.
(2) $a+b \mid 2r^2$.
(3) $a+b \mid 2ab$.

Jistě $a+b \mid (a+b)(a-b) = a^2-b^2$. Platí-li (1), pak $a+b \mid a^2-b^2+a^2+b^2 = 2a^2$ a $a+b \mid -a^2+b^2+a^2+b^2 = 2b^2$. Takže $a+b \mid \mathrm{nsd}(2a^2,2b^2) = 2r^2$. Vidíme, že (1) implikuje (2). Zajisté $2r^2 \mid 2ab$ a (2) implikuje (3). Nakonec, $a+b \mid (a+b)^2 = a^2+b^2+2ab$, čili (3) implikuje (1).

Jsou-li navíc čísla a,b nesoudělná, pak podmínky (1),(2),(3) jsou ekvivalentní tomu, že $a+b = \pm 1, \pm 2$. Jako důsledek dostaneme, že $a+1 \mid a^2+1$ pouze pro $a = -3,-2,0,1$. Podobně, $a-1 \mid a^2+1$ pouze pro $a = -1,-0,2,3$. Speciálně, $a^2-1 \mid a^2+1$ pouze pro $a=0$. Oproti tomu $a^2+1 \mid a^2-1$ právě pro $a = 0, \pm 1$.

III.9.5 Cvičení. Nechť $a,b \in \mathbb{Z}$ jsou taková čísla, že $a+b \mid 2ab, a+b \nmid ab$.

(i) Z III.9.2(i) plyne, že $a+b \nmid r^2$, kde $r = \mathrm{nsd}(a,b)$. Pak ale $r \geq 1$. Podle III.9.4 je $2r^2 = z(a+b)$, z liché. Čili $a+b$ je sudé číslo a čísla a,b mají stejnou paritu.

(ii) Buď $a = 2^k e, b = 2^l f$, e,f lichá čísla, $k \geq l \geq 1$. Máme $2^l z(2^{k-l}e+f) = z(a+b) = 2r^2$, $2^{l-1}z(2^{k-l}e+f) = r^2$. Jelikož $\mathrm{cont}_2(r^2) = 2l$, tak $\mathrm{cont}_2(2^{k-l}e+f) = k+1 \geq 2$. Pak je nutně $k=l$ a $\mathrm{cont}_2(e+f) = k+1$. Odtud, $a+b = 2^k(e+f)$ a $\mathrm{cont}_2(a+b) = 2k+1 > 2k = \mathrm{cont}_2(r^2)$.

Například, volme $a = 20, b = 12$. Je teď $r = 4, a+b = 32 = 2^5$, $ab = 240 = 2^4 \cdot 3 \cdot 5$, $32 \nmid 240$, $32 \mid 2 \cdot 240 = 2^5 \cdot 3 \cdot 5$. Navíc, $2ab \mid (a+b) = 15$ a $a^2+b^2 = 544 = 2^5 \cdot 17 = 17(a+b) = (a-b+9)(a+b) = 68(a-b)$, $a^2-b^2 = 256 = 2^8 = (a+b)(a-b)$.

(iii) A nyní nechť a,b jsou lichá čísla. Je $a = 2c+1, b = 2d+1$, $2z(c+d+1) = z(a+b) = 2r^2$, $z(c+d+1) = r^2$, z,r jsou lichá čísla, $c+d+1$ je liché a čísla c,d mají stejnou paritu. Dále, $r \mid a-b = 2(c-d)$, $r \mid c-d$, $r \mid a+b = 2(c+d+1)$, $r \mid c+d+1$, $c-d = ur$, $c+d+1 = vr$,

$(u+v)r = 2c+1 = a$, $(v-u)r = 2d+1 = b$, $\mathrm{nsd}(u+v, v-u) = \mathrm{nsd}(u,v) = 1$. Čísla $u+v, v-u$ jsou lichá a tak čísla u, v mají různou paritu. Je $a+b = 2vr$, $a-b = 2ur$, $2vr = a+b \mid 2r^2$, $v \mid r$, v je liché, u je sudé. Čili $4 \mid a-b$ a $4 \nmid a+b$. Je $zvr = z(c+d+1) = r^2$, $zv = r$, $a+b = 2vr = 2zv^2$.

Například, volme $a = 15, b = 3$. Je teď $a+b = 18 = 2\cdot 3^2$, $ab = 45 = 3^2\cdot 5$, $18 \nmid 45$, $2ab = 90 = 2\cdot 3^2\cdot 5$, $18 \mid 90$. Navíc, $2ab = 5(a+b)$ a $a^2+b^2 = 234 = 2\cdot 3^2\cdot 13 = 13(a+b) = (a-b+1)(a+b)$, $a-b = 12 \nmid 234 = a^2+b^2$, $a^2-b^2 = 216 = (a+b)(a-b)$.

III.9.6 Cvičení. Nechť $a, b \in \mathbb{Z}$, $r = \mathrm{nsd}(a,b)$. Dokážeme, že následující tři podmínky jsou ekvivalentní:
(1) $2(a+b) \mid a^2+b^2$.
(2) Obě číslé a,b jsta sudiju a $a+b \mid r^2$.
(3) Obě čísla a,b jsou sudá a $a+b \mid ab$;

Vskutku, platí-li (1), pak číslo a^2+b^2 je sudé a čísla a, b mají stejnou paritu. Jsou-li obě čísla lichá, pak $a = 2c+1, b = 2d+1$, $2(a+b) = 4(c+d+1)$, $a^2+b^2 = 2(2c^2+2c+2d^2+2d+1)$, $\mathrm{cont}_2(2(a+b)) \geq 2$, $\mathrm{cont}_2(a^2+b^2) = 1$, spor. Vidíme, že čísla a, b jsou obě sudá, $a = 2e, b = 2f$, $4(e+f) = 2(a+b) \mid a^2+b^2 = 4(e^2+f^2)$, čili $e+f \mid e^2+f^2$. Podle III.9.2(i) máme $e+f \mid 2s^2$, $s = \mathrm{nsd}(e,f)$, $r = 2s$, $a+b = 2(e+f) \mid 4s^2 = r^2$. Tím jsme dokázali (2). Ovšem, (2) implikuje (3) okamžitě a (3) implikuje (1) neb $2(a+b) \mid (a+b)^2 = a^2+b^2+2ab$.

Je $6+2 = 8 \mid 40 = 6^2+2^2$, přičemž $2(6+2) = 16 \nmid 40$.

III.9.7 Cvičení. (i) Nechť $k, l \in \mathbb{N}$. Řešme rovnice $a+b = 2^k$, $a-b = 2^l$. Je to snadné, neb $2a = a+b+a-b = 2^k+2^l$, $a = 2^{k-1}+2^{l-1}$, $b = 2^k-a = 2^{k-1}-2^{l-1}$. Řešení je tedy $a = 2^k+2^l$, $b = 2^{k-1}-2^{l-1}$.

(ii) Nechť $k \in \mathbb{N}$. Řešme rovnice $a+b = 2^k$, $a-b = 1 (= 2^0)$. Je to snadné, neb $b = 2^k-a$, $1 = a-b = a-2^k+a = 2a-2^k$, $2a = 2^k+1$, což nelze. Rovnice nemají řešení.

(iii) Nechť $l \in \mathbb{N}$. Řešme rovnice $a+b = 1$, $a-b = 2^l$. Je to snadné, neb $b = 1-a$, $2^l = a-b = a-1+a = 2a+1$, což nelze. Rovnice nemají řešení.

(iv) Řešme rovnice $a+b = 1$, $a-b = 1$. Je to snadné, neb $b = 1-a$, $1 = a-b = a-1+a = 2a-1$, $2 = 2a, a = 1, b = 0$.

(v) Nechť $k, l \in \mathbb{N}_0$. Zjistili jsme, že rovnice $a+b = 2^k$, $a-b = 2^l$ mají aspoň jedno řešení tehdy a jen tehdy, jestliže $k+l \neq k, l$ a nebo $k = 0 = l$. V obou případech má rovnice jediné řešení.

III.9.8 Cvičení. Nechť $t \in \mathbb{N}_0$. Řešme rovnici $a^2-b^2 = 2^t$ a sice pro nezáporná a, b. Není to těžké, neb $(a+b)(a-b) = a^2-b^2 = 2^t \geq 1$, $a+b \geq 0$, takže $a > b \geq 0$. Je-li $t = 0$, pak $a+b = 1 = a-b$, z čehož plyne $a = 1, b = 0$. Je-li $t = 1$, pak $a+b = 2, a-b = 1$, z čehož plyne $2a = 3$ a

žádné řešení neexistuje. Buď $t \geq 2$. Je $a+b=2^k, a-b=2^l$, kde $k \geq l \geq 0$, $k+l=t$. Pro $k=0$ či $l=0$ nedostáváme žádné řešení. Pro $k \geq 1, l \geq 1$ je řešením $a=2^{k-1}+2^{l-1}$, $b=2^{k-1}-2^{l-1}$ (III.9.7). Pro každý rozklad $t=k+l$, $k \geq 1, l \geq 1$ dostáváme právě jedno řešení.

Například, pro $t=2$ je $k=1=l$, $a=2, b=0$. Pro $t=3$ je $k=2, l=1$, $a=3, b=1$. Pro $t=4$ je $k=3, l=1$, $a=5, b=3$. Pro $t=4$ je $k=2, l=2$, $a=4, b=0$. Pro $t=5$ je $k=4, l=1$, $a=9, b=7$. Pro $t=5$ je $k=3, l=2$, $a=6, b=2$.

III.9.9 Cvičení. Nechť $t \in \mathbb{N}_0$. Řešme rovnici $a^2+b^2=2^t$ a sice pro nezáporná a, b. Není to těžké. Je-li $t=0$, pak $a^2+b^2=1$, čili $a=1, b=0$ nebo $a=0, b=1$. Je-li $t=1$, pak $a^2+b^2=2$, čili $a=1, b=1$.

Buď $t \geq 2$. Je-li $b=0$, pak $a^2=2^t$, t je sudé, $a=2^{t/2}$. Je-li $a=0$, pak $b=2^{t/2}$. Předpokládejme tedy, že $a \geq 1, b \geq 1$. Máme $a=2^u c, b=2^v d$, kde $u \geq 0, v \geq 0$, $c \geq 1, d \geq 1$, c, d lichá čísla. Nyní $2^t=a^2+b^2=2^{2u}c^2+2^{2v}d^2$. Je-li $u>v$, pak $2^t=2^v(2^{(u-v)}c^2+d^2)$, kde $2^{(u-v)}c^2+d^2 \geq 5$ je liché číslo, což není možné. Takže $u=v$ a $2^t=2^{2u}(c^2+d^2)$, $c^2+d^2 \geq 2$, $t \geq 2u$. Čísla c, d jsou lichá, $c=2e+1, d=2f+1$, $e \geq 0, f \geq 0$, $2^{t-2u}=c^2+d^2=4e^2+4e+4f^2+4f+2$. Jelikož $4 \nmid 2$, tak $e=0=f$, $c=1=d$, $a=2^u=b$, $t=2u+1$, t liché, $u=(t-1)/2$, $a=2^{(t-1)/2}=b$.

Nalezli jsme, že naše rovnice má řešení pouze pro $t=0$ (pak (a,b) = (1,0),(0,1)), či pro $t \geq 1$ liché (pak $(a,b)=(2^{(t-1)/2}, 2^{(t-1)/2})$).