DĚLITELNOST

JAN MALÝ
UK v Praze a UJEP v Ústí n. L.

1. Značení

$\mathbb{N}$..... přirozená čísla $1, 2, \ldots$
$\mathbb{Z}$..... celá čísla
$\mathbb{Z}_n$..... zbytková třída modulo n, tedy $\{0, 1, 2, \ldots, n-1\}$
$a \div b$.....celočíselný podíl (např. $17 \div 5 = 3$)
$a \bmod b$.....zbytek při celočíselném dělení (např. $17 \bmod 5 = 2$)
$k|n$ .....k je dělitelem čísla n, tedy $n \bmod k = 0$.

2. Kongruence

Relace *kongruence*, $a \equiv b \pmod q$,
čteme a je kongruentní s b modulo q, znamená to $q|\, a-b$.

Vzorečky:

$$\left.\begin{array}{l} a \equiv A, \\ b \equiv B \end{array}\right\} \implies \begin{array}{c} a + b \equiv A + B, \\ ab \equiv AB \end{array}$$

3. Rozklad na prvočinitele

Každé přirozené číslo má tzv. *rozklad na prvočinitele*: dá se zapsat ve tvaru součinu, kde každý činitel je prvočíslo. Některá prvočísla se v seznamu prvočinitelů mohou vyskytnout víckrát, pak zápis zjednodušujeme pomocí mocnin.

$$\begin{array}{ll} 1 = \text{prázdný součin} & 6 = 2 \cdot 3 \\ 2 = 2 & 7 = 7 \\ 3 = 3 & \ldots \\ 4 = 2^2 & 180 = 2^2 \cdot 3^2 \cdot 5 \\ 5 = 5 & \ldots \end{array}$$

Jiný způsob zápisu: do "děr" dáme nulté mocniny, aby posloupnost po sobě jdoucích prvočísel byla úplná.

Např. $63 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1$.

Na množině všech přirozených čísel máme *přirozené uspořádání* a uspořádání pomocí relace $a|b$. To druhé je *nelineární* uspořádání, totiž, existují při něm neporovnatelné prvky (podobně jako při uspořádání množin inkluzí).

4. Největší společný dělitel

Každá dvě přirozená čísla a, b mají *nejmenší společný násobek* $\mathrm{nsn}(a,b)$ a *největšího společného dělitele* $\mathrm{nsd}(a,b)$.

Je jasné co to znamená? Největší společný dělitel čísel a,b je prvek množiny všech společných dělitelů čísel a,b největší:

a) v přirozeném uspořádání
b) v uspořádání relací $k|n$.

Naštěstí obě definice vyjdou nastejno.

Říkáme, že a a b jsou *nesoudělná*, jestliže $\mathrm{nsd}(a,b)=1$.
Jak najít největšího společného dělitele čísel a,b ?

Intuitivní přístup: Pokud najdeme vůbec nějakého společného dělitele k čísel a, b, pak obě čísla vydělíme k a tím zredukujeme úlohu na jednodušší.

Příklad 1. $a=120$ a $b=100$. Obě čísla jsou dělitelná 10, označme
$k_1=10,\quad a_1=120/10=12,\ b_1=100/10=10.$
Čísla a_1, b_1 jsou dělitelná dvěma, označme
$k_2=2,\quad a_2=12/2=6,\ b_2=10/2=5.$
Ověříme, že čísla a_2 a b_2 jsou nesoudělná, tedy $\mathrm{nsd}(a,b)=k_1k_2=20$.

Čísla $\mathrm{nsn}(a,b)$ a $\mathrm{nsd}(a,b)$ se dají charakterizovat pomocí rozkladů na prvočinitele: $\mathrm{nsd}(a,b)$ najdeme tak, že každé prvočíslo umocníme na menší z exponentů, pro $\mathrm{nsn}(a,b)$ bychom naopak použili větší z exponentů.

Příklad 2.

$$\begin{aligned} a := 20 &= 2^2\cdot 3^0\cdot 5^1\\ b := 24 &= 2^3\cdot 3^1\cdot 5^0\\ \mathrm{nsd}(a,b)=4 &= 2^2\cdot 3^0\cdot 5^0\\ \mathrm{nsn}(a,b)=120 &= 2^3\cdot 3^1\cdot 5^1 \end{aligned}$$

Výše uvedené metody jsou prakticky výhodné jen pro malá data!!!
Hledání dělitelů velkých čísel je úloha natolik obtížná, že se dá využít k šifrování.

5. Euklidův algoritmus

Jak najít "profesionálně" $\mathrm{nsd}(a,b)$?

Můžeme předpokládat $a>b$. Nechť c je zbytek při dělení $a\div b$, tedy $c<b$ a existuje $k\in\mathbb{N}$ tak, že $a=kb+c$. Pak každý dělitel a je i dělitel c a naopak. Úlohu najít $\mathrm{nsd}(a,b)$ jsme převedli na jednodušší úlohu najít $\mathrm{nsd}(b,c)$.

Označme $a_0=a$, $a_1=b$.
$a_0=k_1a_1+a_2$, kde $a_2=a_0 \bmod a_1$, máme $0\le a_2<a_1$.
$a_1=k_2a_2+a_3$, kde $a3=a_1 \bmod a_2$, máme $0\le a_3<a_2$.
$a_2=k_3a_3+a_4,\ldots$
Máme $a_0>a_1>a_2>\ldots$, po konečném počtu kroků musíme dojít do situace, kdy dělení vyjde beze zbytku, tj. $a_{m-1}=k_ma_m$, pak $\mathrm{nsd}(a,b)=a_m$.

Příklad 3. Položme $a = a_0 = 31416$, $b = a_1 = 10000$. Máme

$$\begin{aligned} 31416 &= 3 \cdot 10000 + 1416, & k_1 &= 3, & a_2 &= 1416, \\ 10000 &= 7 \cdot 1416 + 88, & k_2 &= 7, & a_3 &= 88, \\ 1416 &= 16 \cdot 88 + 8, & k_3 &= 16, & a_4 &= 8, \\ 88 &= 11 \cdot 8, & k_4 &= 11, & a_5 &= 0, \end{aligned}$$

$$\operatorname{nsd}(31416, 10000) = 8$$

Příklad 4. Položme $a = a_0 = 314159$, $b = a_1 = 100000$. Máme

$$\begin{aligned} 314159 &= 3 \cdot 100000 + 14159, & k_1 &= 3, & a_2 &= 14159, \\ 100000 &= 7 \cdot 14159 + 887, & k_2 &= 7, & a_3 &= 887, \\ 14159 &= 15 \cdot 887 + 854, & k_3 &= 15, & a_4 &= 854, \\ 887 &= 1 \cdot 854 + 33, & k_4 &= 1, & a_5 &= 33, \\ 854 &= 25 \cdot 33 + 29, & k_5 &= 25, & a_6 &= 29, \\ 33 &= 1 \cdot 29 + 4, & k_6 &= 1, & a_7 &= 4, \\ 29 &= 7 \cdot 4 + 1, & k_7 &= 7, & a_8 &= 1, \\ 4 &= 4 \cdot 1, & k_8 &= 4, & a_9 &= 0, \end{aligned}$$

$$\operatorname{nsd}(314159, 100000) = 1$$

6. Řetězové zlomky

Příklad 5. Máme

$$\begin{aligned} \frac{31416}{10000} &= 3 + \frac{1416}{10000} = 3 + \frac{1}{\frac{10000}{1416}} = 3 + \frac{1}{7 + \frac{88}{1416}} \\ &= 3 + \frac{1}{7 + \frac{1}{16 + \frac{8}{88}}} = 3 + \frac{1}{7 + \frac{1}{16 + \frac{1}{11}}} \end{aligned}$$

Hle:

$$\frac{a}{b} = k_1 + \frac{1}{k_2 + \frac{1}{k_3 + \ldots}}$$

$$x = k_1 + \frac{1}{k_2 + \frac{1}{k_3 + \ldots}}, \qquad k_j \in \mathbb{N}. \tag{1}$$

Věta 1. Každý zlomek se dá jednoznačně zapsat ve tvaru konečného řetězového zlomku (1),

Každé iracionální číslo se dá jednoznačně napsat ve tvaru nekonečného řetězového zlomku (1).

Hodnoty k_j lze najít pomocí "Euklidova algoritmu".

Příklad 6. $3 < \pi < 4$

$3,1 < \pi < 3,2$ neboli $3 + \frac{1}{10} < \pi < 3 + \frac{1}{5}$ ..... $k_1 = 3$

$3,14 < \pi < 3,15$ neboli $3 + \dfrac{1}{7 + \frac{1}{7}} \leq \pi \leq 3 + \dfrac{1}{6 + \frac{1}{1 + \frac{1}{2}}}$ .... nic nového

$3,1415 < \pi < 3,1416$ neboli $3 + \dfrac{1}{7 + \frac{1}{14 + \frac{1}{1 + \frac{1}{8 + \frac{1}{2}}}}} < \pi < 3 + \dfrac{1}{7 + \frac{1}{16 + \frac{1}{11}}}$ ... $k_2 = 7$

Pro $x = \pi$ jsou členy řetězového rozvoje $3, 7, 15, 1, 292, 1, 1, \ldots$.

V teorii aproximace se často používají částečné řetězové rozvoje, tedy řetězový zlomek daný konečnou či nekonečnou posloupností $\{k_j\}$ nahradíme "uříznutým zlomkem" počítaným jen z $\{k_j\}_{j=1}^m$

Označme $\frac{p_j}{q_j}$ j-tý *sblížený zlomek*, který dostaneme úpravou částečného řetězového zlomku:

$$\begin{aligned}\frac{p_1}{q_1} &= k_1,\\ \frac{p_2}{q_2} &= k_1 + \frac{1}{k_2},\\ \frac{p_3}{q_3} &= k_1 + \frac{1}{k_2 + \frac{1}{k_3}}\\ &\ldots\end{aligned}$$

Tyto *sblížené zlomky* řetězového rozvoje čísla x velmi dobře aproximují x.
Je-li $\frac{p}{q}$ sblížený zlomek z řetězového rozvoje čísla x a $\frac{P}{Q}$ je jiný zlomek, pak buď je $\frac{P}{Q}$ dál od čísla x než $\frac{p}{q}$, nebo $q > Q$.

Zdálo by se, že zlomky $\frac{p_j}{q_j}$ se musí počítat odzadu, např.

$$3 + \frac{1}{7 + \frac{1}{15}} = 3 + \frac{1}{\frac{106}{15}} = 3 + \frac{15}{106} = \frac{333}{106}.$$

Ale co když napočítáme sblížený zlomek odzadu, zjistím, že ještě není dost přesný a je třeba přidat člen, pak je třeba počítat odzadu úplně znovu!

$$3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} = 3 + \frac{1}{7 + \frac{1}{16}} = 3 + \frac{16}{113} = \frac{355}{113}.$$

Zázrak: Existuje rekurentní formule pro p_j a q_j: Klademe $p_0 = 1$, $q_0 = 0$, ačkoli $\frac{p_0}{q_0}$ nemá smysl.

$$\begin{aligned}p_0 &= 1, \qquad & p_1 &= k_1\\ q_0 &= 0, \qquad & q_1 &= 1\\ p_j &= k_j p_{j-1} + p_{j-2}, \qquad & j &\geq 2,\\ q_j &= k_j q_{j-1} + q_{j-2}, \qquad & j &\geq 2.\end{aligned}$$

Příklad 7. Pro $x = \pi$ jsou členy řetězového rozvoje $3, 7, 15, 1, 292, 1, 1, \ldots$.

j	k_j	p_j	q_j	p_j/q_j
0	-	1	0	-
1	3	3	1	3,000000...
2	7	22	7	3,142857...
3	15	333	106	3,141509...
4	1	355	113	3,141592...

Nechť x má rozvoj do řetězového zlomku o členech $k_1, k_2, \ldots$ a p_j/q_j jsou sblížené zlomky. Pak

- zlomky $\frac{p_1}{q_1}$, $\frac{p_3}{q_3}$, $\frac{p_5}{q_5}$, ... se blíží k aproximované hodnotě x zleva.
- zlomky $\frac{p_2}{q_2}$, $\frac{p_4}{q_4}$, $\frac{p_6}{q_6}$, ... se blíží k aproximované hodnotě x zprava.

- chybu lze tedy odhadnout
$$\left|x - \frac{p_j}{q_j}\right| \leq \left|\frac{p_{j+1}}{q_{j+1}} - \frac{p_j}{q_j}\right|$$
- A hle! po úpravě vyjde vpravo $\frac{1}{q_j q_{j+1}}$. Totiž $p_j q_{j+1} - p_{j+1} q_j = (-1)^j$.

Tedy dostáváme odhad zlomkem o přesnosti $\left|x - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

Pro srovnání, desetinný zlomek zaručuje jen přesnost $\left|x - \frac{p}{q}\right| \leq \frac{1}{q}$

Chceme-li najít aproximaci s chybou $< 1/n$, použijeme sblížený zlomek $\frac{p_k}{q_k}$ takový, že $q_k q_{k+1} > n \geq q_k q_{k-1}$. Pak $q_{k-1} \leq \sqrt{n}$.

Máme-li štěstí, může být q_k malé jako $\sqrt{n}$, ale když mezi q_{k-1} a q_k je velký skok, také můžeme mít smůlu.

Pro některá iracionální čísla se dá nekonečný řetězový rozvoj popsat vzorečkem, třeba
$x = \frac{1+\sqrt{5}}{2}$, odtud $x = 1 + \frac{1}{x}$, odtud $x = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\cdot}}}$.

7. Rovnice v $\mathbb{Z}_n$

Věta 2. Nechť čísla a, n jsou nesoudělná a $c \in \mathbb{Z}_n$. Potom existuje řešení $x \in \mathbb{Z}_n$ "rovnice" $ax \equiv c (\mathrm{mod}\, n)$.

Důkaz. Uvažujme zobrazení
$$f : x \mapsto ax \bmod n : \ \mathbb{Z}_n \to \mathbb{Z}_n.$$
Ověříme, že $f : \mathbb{Z}_n \to \mathbb{Z}_n$ je prosté. Kdyby bylo $f(x) = f(x')$, bylo by $f(x - x') = 0$, tedy $n | x - x'$. Protože ale $x, x' \in \mathbb{Z}_n$, toto je možné jen tak, že $x = x'$.

Obecný fakt: když definiční obor X a cílový prostor Y mají stejný konečný počet prvků, pak každé prosté zobrazení $g : X \to Y$ je na! Tedy i zobrazení f je na $\mathbb{Z}_n$ a existuje řešení dané rovnice.

□

Příklad 8. Řešme v $\mathbb{Z}_{10}$ rovnici $2x \equiv 2 (\mathrm{mod}\, 10)$. Úloha svádí k vykrácení $x \equiv 1$. Ale krátit se smí jen tak, že se krátí i s modulem!! Tedy
$x \equiv 1 (\mathrm{mod}\, 5)$,
$x = 1, 6$.

Příklad 9. Řešme v $\mathbb{Z}_{10}$ rovnici $7x \equiv 1 (\mathrm{mod}\, 10)$. Po úpravách
$$\begin{aligned} 7x &\equiv 1 \qquad | \cdot 2 \\ 4x &\equiv 2 \end{aligned}$$
Teď jsme ztratili informaci, neboť původní rovnice má jen jedno řešení a odvozená rovnice má dvě řešení, $x = 3, 8$! Lépe:
$$\begin{aligned} 7x &\equiv 1 \qquad | \cdot 3 \\ 1x &\equiv 3 \end{aligned}$$

Postupně se vždy nějak dostaneme k cíli, takový postup je však spíš magie, než algoritmus.

8. Diofantické rovnice

Hledáme celočíselná řešení rovnice o dvou neznámých

$$ax + by = c \tag{2}$$

Má-li rovnice (2) řešení (x, y), pak má nekonečně mnoho řešení: $(x+kb,\ y-ka)$, $k \in \mathbb{Z}$.

Stačí tedy najít jedno řešení úlohy, a to najdeme převedením na rovnici v $\mathbb{Z}_b$:

$$ax \equiv c (\bmod b). \tag{3}$$

Je-li x řešení rovnice (3) a

$$y = (c - ax)/b,$$

pak (x, y) řeší (2) (a naopak).

Věta 3. Rovnice $ax + by = c$ je řešitelná v celých číslech, právě když $\mathrm{nsd}(a, b) \mid c$.

Důkaz. Označme $d = \mathrm{nsd}(a, b)$. Nechť rovnice má řešení (x, y). Potom $d \mid ax+by$, tedy $d|c$.

Obráceně, nechť $d|c$. Potom celou rovnici můžeme vydělit d a dostaneme rovnici stejného typu, ale tentokrát budou a, b nesoudělná. To je tedy případ, na který se můžeme v dalším omezit. Podle věty o rovnici v kongruencích má rovnice

$$ax \equiv c (\bmod b)$$

řešení a odtud dostaneme existenci řešení diofantické rovnice. □

Věta 4. Nechť čísla a, b, c jsou navzájem nesoudělná. Potom soustava diofantických rovnic

$$ax + by = p$$
$$ax + cz = q$$

má řešení.

Důkaz. Nechť (X, Y) je jedno řešení první rovnice. Pak množina všech řešení je dána vzorci $x = X + bk$, $y = Y - ak$, $k \in \mathbb{Z}$. Potřebujeme

$$q = ax + cz = aX + abk + cz, \qquad \text{neboli } abk + cz = q - aX.$$

To je jedna diofantická rovnice o neznámých k, z, tu už řešit umíme. □

Jak řešit konkrétní diofantickou rovnici?

Budeme-li kopírovat existenční důkaz, musíme probírat $x \in \mathbb{Z}_q$ jedno po druhém a čekat, kdy nastane případ $f(x) = c$.

Lepší myšlenka: Rychlejší a elegantnější metoda je v podstatě opět Euklidův algoritmus! Ukážeme si ji na příkladu.

Úloha 1. Řešte v celých číslech rovnici $314159x - 100000y = 5$.

Řešení.

$314159x - 100000y = 5$	$314159 = 3 \cdot 100000 + 14159$
$14159x - 100000y' = 5$	$100000 = 7 \cdot 14159 + 887$
$14159x' - 887y' = 5$	$14159 = 15 \cdot 887 + 854,$
$854x' - 887y'' = 5$	$887 = 1 \cdot 854 + 33,$
$854x'' - 33y'' = 5$	$854 = 25 \cdot 33 + 29,$
$29x'' - 33y''' = 5$	$33 = 1 \cdot 29 + 4,$
$29x''' - 4y''' = 5$	$29 = 7 \cdot 4 + 1, \quad 5 = 1 \cdot 4 + 1$
$x''' - 4y'''' = 1$	Položme $y'''' = 0 \implies x''' = 1$
$29 \cdot 1 - 4y''' = 5$	$y''' = 6$
$29x'' - 33 \cdot 6 = 5$	$x'' = 7$
$854 \cdot 7 - 33y'' = 5$	$y'' = 181$
$854x' - 887 \cdot 181 = 5$	$x' = 188$
$14159 \cdot 188 - 887y' = 5$	$y' = 3001$
$14159x - 100000 \cdot 3001 = 5$	$x = 21195$
$314159 \cdot 21195 - 100000y = 5$	$y = 66586$

□

Úloha 2. Pro která přirozená n platí
a) $8 \mid n^2-1$,
b) $4 \mid n^2+1$?

Řešení. a) Aby bylo $8 \mid n^2-1$, musí být n^2 liché, tedy n liché. Pak je $n^2 - 1 = (n-1)(n+1)$, jeden z činitelů je dělitelný čtyřmi, druhý dvěma, součin osmi. Závěr: n řeší úlohu, právě když je liché.

b) Aby bylo $4 \mid n^2+1$, musí být n liché, pak $n^2 - 1$ je dělitelné 8 a tudíž $n^2 + 1$ nemůže být dělitelné čtyřmi. Závěr: úloha nemá řešení.

□

Úloha 3. Pro která přirozená n, $1033 \leq n \leq 1132$, je $n^4 - 1$ dělitelné stem.

Řešení. Aby bylo $n^4 - 1$ dělitelné čtyřmi, potřebujeme n liché a tato podmínka je pro dělitelnost 4 také postačující.

Aby bylo číslo $n^4 - 1 = (n^2 + 1)(n^2 - 1)$ dělitelné 25, je třeba, aby aspoň jedno z čísel $n^2 + 1$, $n^2 - 1$ bylo dělitelné pěti.

Je-li jedno z nich dělitelné pěti, druhé už nemůže.

Tedy maximálně jedno z čísel n^2-1, n^2+1 je dělitelné pěti a má-li být n řešením úlohy, je toto číslo dělitelné 25. Úlohu můžeme rozdělit na dva případy, v nichž se budeme zabývat dělitelností číslem 25.

Případ $5 \mid n^2-1$: Pak $n \equiv \pm 1 (\bmod 5)$, tedy existuje $m \in \mathbb{Z}_5$ tak, že $n \equiv 5m \pm 1 (\bmod 25)$. Řešíme modulo 25

$$\begin{aligned} n^2 - 1 &\equiv 0 \\ n^2 &\equiv 1 \\ (5m \pm 1)^2 &\equiv 1 \\ 25m^2 \pm 10m + 1 &\equiv 1 \\ 10m &\equiv 0 \end{aligned}$$

Máme $25 \mid 10m$, tedy $5 \mid 2m$, odtud $m = 0$. Vychází tedy $n \equiv \pm 1$ a nic víc, zkouškou ověříme, že pro $n = \pm 1$ platí $25 \mid n^2 - 1$.

Případ $5 \,|\, n^2+1$: Pak $n \equiv \pm 2 (\bmod 5)$, tedy existuje $m \in \mathbb{Z}_5$ tak, že $n \equiv 5m \pm 2 (\bmod 25)$. Řešíme modulo 25

$$\begin{aligned} n^2 &\equiv -1 \\ (5m \pm 2)^2 &\equiv -1 \\ 25m^2 \pm 20m + 4 &\equiv -1 \\ \pm 20m &\equiv -5 \end{aligned}$$

Máme $25 \,|\, 5 \pm 20m$, tedy $5 \,|\, 1 \pm 4m$, pro znaménko $+$ vyjde $m = 1$, $n \equiv 7$, pro znaménko $-$ vyjde $m = 4$, $n \equiv 18$. Zkouškou ověříme, že pro $n = 7, 18$ platí $25 \,|\, n^2 + 1$.

Vraťme se k původní úloze, aby $n^4 - 1$ bylo dělitelné stem, je nutné a stačí, aby n bylo liché a současně $n \bmod 25 \in \{1, 7, 18, 24\}$. Odtud

$$n \bmod 100 \in \{1,\ 7,\ 25{+}18,\ 25{+}24,\ 50{+}1,\ 50{+}7,\ 75{+}18,\ 75{+}24\}.$$

V intervalu $1033 \le n \le 1132$ to jsou čísla

$$1043, 1049, 1051, 1057, 1093, 1099, 1101, 1107.$$

□

Úloha 4. Řekneme, že číslo $k \in \mathbb{N}$ je *rozhodné*, jestliže pro všechna $n \in \mathbb{N}$ platí:

$$k | n(n+5) \implies k | n \text{ nebo } k | \, n{+}5.$$

Najděte všechna rozhodná čísla.

Řešení. Uvažujme diofantickou rovnici $ax - by = 5$, kde $a, b \ge 2$ jsou nesoudělná.

Pak rovnice má v přirozených číslech řešení (v celých určitě, rozmyslete, proč v přirozených) (x, y) a máme $a | \, ax = by + 5$, tedy

$$ab \mid by \; ax = by(by + 5).$$

Buď $k = ab$ číslo rozhodné. Pak k dělí jedno z čísel by, $by + 5$.

Pokud $ab \mid by$, pak $a | y$. Odtud $a | \, ax - by = 5$, neboli $a = 5$.

Pokud $ab | \, by + 5 = ax$, pak $b | x$, odtud $b | ax - by = 5$, neboli $b = 5$.

Shrnutí: pokud je číslo k nerozhodné, pak se nedá napsat jako netriviální součin nesoudělných čísel, ledaže jedno z nich by bylo 5.

Možnosti jsou: $k = p^m$ nebo $k = 5p^m$, kde $p \neq 5$ je prvočíslo a $m \in \mathbb{N}$, anebo $k = 5^m$, $m \in \mathbb{N}$.

Pokud $k = p^m$ dělí $n(n + 5)$, potom p dělí nejvýš jedno z čísel n, $n{+}5$ (jinak by dělilo i 5), tedy $p^m \mid n(n + 5) \implies p^m \,|\, n$ nebo $p^m \,|\, n + 5$

Pokud $k = 5p^m$ dělí $n(n + 5)$, potom jedno z čísel n, $n + 5$ je dělitelné pěti, ale pak jsou obě dělitelná pěti. Jako v předchozí části řešení ukážeme, že p^m dělí jedno z čísel n, $n{+}5$, pak i $5p^m$ dělí toto číslo.

Číslo $k = 5^m$, kde $m \ge 2$, je však nerozhodné!!
$k | 5^{m-1}(5^{m-1} + 5)$, avšak k nedělí žádné z čísel 5^{m-1}, $5^{m-1} + 5$.

Závěr: k je rozhodné, právě když má jeden z tvarů $k = p^m$ nebo $k = 5p^m$, kde $p \neq 5$ je prvočíslo a $m \in \mathbb{N}$. □

Úloha 5. Kolik je přirozených čísel $n \le 1\,992\,000$ takových, že $1\,992\,000 \,|\, n^3 - n$.

Řešení. Označme $b = 1\,992\,000$. Máme $b = 2^6 \cdot 3 \cdot 5^3 \cdot 83$. Buď M množina všech celých čísel n takových, že $b|\ n^3 - n$.

Číslo $n^3 - n = n(n-1)(n+1)$ je vždy dělitelné třemi, takže nás zajímá pouze dělitelnost číslem $2a$, kde $a = n/6 = 2^5 \cdot 5^3 \cdot 83$.

Čísla 2^5, 5^3 a 83 jsou nesoudělná. Dále pokud $2a|n(n-1)(n+1)$, pak jen jedno z čísel n, $n-1$, $n+1$ může být dělitelné 4, jen jedno z nich pěti a jen jedno z nich číslem 83. To, které je dělitelné 5, musí být dělitelné 125, to, které je dělitelné 4, musí být dělitelné 32, a pokud je n dělitelné 4, musí být dělitelné 64.

Uspořádanou trojici $s = (s_1, s_2, s_3)$ prvků množiny $\{-1, 0, 1\}$ nazveme *strategií*. Strategii s nazveme *sudou*, jeli $s_1 = 0$ a *lichou* v opačném případě. Řekneme, že n je v M podle strategie s, jestliže

$$4|\ n + s_1,\ 5|\ n + s_2 \ \text{ a } 83|\ n + s_3,$$

potom

$$32(64)|\ n + s_1,\ 125|\ n + s_2 \ \text{ a } 83|\ n + s_3.$$

Každé $n \in M$ je v M podle právě jedné strategie.

Čísla která jsou v M podle sudé strategie s tvoří aritmetickou posloupnost o diferenci $2a$. Na každou sudou strategii připadnou 3 čísla z intervalu $1 \le n \le b$. Počet sudých strategií je 3^2. Počet řešení odpovídajících sudé strategii je $3 \cdot 3^2 = 27$.

Čísla která jsou v M podle liché strategie s tvoří aritmetickou posloupnost o diferenci a, neboť nám stačí dělitelnost 32. Na každou lichou strategii připadne 6 čísel z intervalu $1 \le n \le b$. Počet lichých strategií je $2 \cdot 3^2$. Počet řešení odpovídajících sudé strategii je $6 \cdot 2 \cdot 3^2 = 108$. Počet řešení úlohy je 135.

Je lehké ukázat, že prvky M odpovídající jedné strategii tvoří aritmetickou posloupnost a jakou má diferenci, pokud víme, že aspoň jeden takový prvek existuje. Existenční důkaz budeme demonstrovat na dvou vybraných strategiích.

$s = (0, 0, 1)$. Strategie je sudá, hledáme n tak, že $64|n$, $125|n$, $83|\, n+1$. Jinak: $8000 = 125 \cdot 64\ |n$ a $83\,|\, n+1$. Řešme diferenční rovnici $83x - 8000y = 1$. Protože čísla 83 a 4000 jsou nesoudělná, rovnice má řešení (x, y) a $8000y \in M$.

$s = (-1, 0, 1)$. Strategie je lichá, hledáme n tak, že $32|\ n-1$, $125|n$, $83|\, n+1$. Řešme soustavu diofantických rovnic

$$125x - 32y = 1$$
$$83z - 125x = 1$$

Protože čísla 125, 32 a 83 jsou nesoudělná, rovnice má řešení (x, y, z), pak $n \in M$ najdeme jako $n = 125x$. □