Řetězové zlomky

III. část. Použití řetězových zlomků

In: Pavel Vít (author): Řetězové zlomky. (Czech). Praha: Mladá fronta, 1982. pp. 119–152.

Persistent URL: http://dml.cz/dmlcz/404021

III. ČÁST

POUŽITÍ ŘETĚZOVÝCH ZLOMKŮ

16. ŘEŠENÍ KONGRUENCE $ax \equiv b (\mathrm{mod}\ m)$

Dříve než se pustíme do naší úlohy, řekneme si pár slov o kongruencích. Nebudeme vytvářet žádnou teorii; jde nám jen o to, aby čtenář mohl s větším pochopením sledovat výklad o řešení lineární kongruence $ax \equiv b \pmod{m}$. Nebudeme dokazovat všechny možné věty o kongruencích, nýbrž jen ty, které budeme v dalším výkladu potřebovat. (Ostatně důkaz několika jednoduchých vět přenecháme čtenáři za cvičení. Všechny se dokazují bezprostředně z definice kongruence.)

Buďte $a, b \in \mathbf{Z}$, $m \in \mathbf{N}$, $m \geqq 2$; jestliže platí

$$m \mid a - b,$$

tj. jestliže existuje $t \in \mathbf{Z}$ takové, že

$$a - b = mt,$$

píšeme

$$a \equiv b \pmod{m} \tag{1}$$

a čteme *a je kongruentní s b podle modulu m.*

Tedy např. $25 \equiv 11 (\mathrm{mod}\ 7)$,

$$38 \equiv 3 \pmod 5,$$

$$12 \equiv 4 \pmod 8.$$

Věta 1. *Kongruence mezi dvěma čísly* $a, b \in \mathbf{Z}$ *je ekvivalence v* $\mathbf{Z}$, *tj. pro každá tři* $a, b, c \in \mathbf{Z}$ *platí*

(a) $a \equiv a \pmod m$,
(b) *jestliže* $a \equiv b \pmod m$, *pak* $b \equiv a \pmod m$,
(c) *jestliže* $a \equiv b \pmod m$ *a zároveň* $b \equiv c \pmod m$, *pak* $a \equiv c \pmod m$.

Vlastnosti (a) se říká *reflexívnost*, (b) *symetričnost*, (c) *tranzitivnost* kongruence.

To, že binární relace $\equiv$ je ekvivalence, se ovšem projevuje tak, že v $\mathbf{Z}$ existuje k relaci $\equiv$ příslušný *rozklad* na třídy ekvivalence, kterým v tomto případě říkáme *zbytkové třídy*, úplněji zbytkové třídy (mod m); jsou totiž určeny modulem m. Zbytkových tříd (mod m) je právě m. Označíme-li je $\mathbf{Z}_0, \mathbf{Z}_1, \ldots, \mathbf{Z}_{m-1}$, jsou to tyto množiny čísel vzájemně kongruentních (mod m):

$$\mathbf{Z}_0 = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\},$$

$$\mathbf{Z}_1 = \{\ldots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \ldots\},$$

$$\ldots\ldots$$

$$\mathbf{Z}_{m-1} = \{\ldots, -2m-1, -m-1, -1, m-1, 2m-1, \ldots\}.$$

Protože $\mathbf{Z}_0, \mathbf{Z}_1, \ldots, \mathbf{Z}_{m-1}$ jsou třídy ekvivalence množiny $\mathbf{Z}$, platí:

(a) $Z_0 \cup Z_1 \cup \ldots \cup Z_{m-1} = Z$,
(b) $Z_m \cap Z_n = \emptyset$ pro každá dvě $m, n \in N_0$, $m \neq n$.

Odtud: Každé číslo $a \in Z$ patří právě do jedné zbytkové třídy (mod m).

Příklad 1. Budiž $m = 3$. Zbytkové třídy označíme Z_0, Z_1, Z_2.
Jsou to tyto množiny:

$$Z_0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$

$$Z_1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$

$$Z_2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Indexy u označení zbytkových tříd, totiž čísla $0, 1, \ldots, m-1$, volíme tak, že je jednak $0 \in Z_0$, $1 \in Z_1, \ldots, i \in Z_i, \ldots$ $m-1 \in Z_{m-1}$ a jednak tak, že jsou to v příslušných zbytkových třídách nejmenší nezáporná čísla. Množina čísel $\{0, 1, \ldots, m-1\}$ se nazývá *úplná soustava nejmenších nezáporných zbytků* (mod m) a každé číslo $a \in Z$ je kongruentní (mod m) právě s jedním číslem této soustavy, zatímco žádná dvě čísla této soustavy nejsou kongruentní (mod m).

Proč vlastně mluvíme o zbytcích a zbytkových třídách? Připomeňme si algoritmus dělení v Z pro čísla $a \in Z$, $m \in N$, $m \geqq 2$:

$$a = mq_1 + r_1, \quad 0 \leqq r_1 < m.$$

Může tedy zbytek $r_1 \in N_0$ nabýt právě jedné z hodnot $0, 1, \ldots, m-1$.

Věta 2. *Jestliže*

$$a \equiv b \pmod{m}$$

a

$$c \equiv d \pmod{m},$$

pak také

$$a + c \equiv b + d \pmod{m},$$

$$ac \equiv bd \pmod{m}.$$

Důsledek. Platí

$$c \equiv c \pmod{m}$$

(reflexívnost kongruence) pro každé $c \in \mathbf{Z}$, a tedy, platí-li

$$a \equiv b \pmod{m},$$

pak platí také

$$a + c \equiv b + c \pmod{m},$$

$$ac \equiv bc \pmod{m}$$

pro každé $c \in \mathbf{Z}$.

Ze vztahu (1), tj.

$$a - b = mt \text{ pro } t \in \mathbf{Z},$$

okamžitě plyne

$$a = b + mt. \tag{2}$$

Zřejmě je

$$mt \equiv 0 \pmod{m}$$

pro každé $t \in \mathbf{Z}$, tedy také

$$0 \equiv mt \pmod{m}$$

(symetričnost kongruence), a jestliže tuto kongruenci přičteme podle věty 2 ke kongruenci

$$a \equiv b \pmod{m},$$

dostáváme kongruenci

$$a \equiv b + mt \pmod{m}. \tag{3}$$

Kongruence (3) a rovnost (2) mají stejný význam při zapisování řešení lineární kongruence.

Druhé tvrzení důsledku věty 2 mluví o tom, že obě strany kongruence

$$a \equiv b \pmod{m},$$

tj. obě čísla a, $b \in \mathbf{Z}$, lze vynásobit libovolným celým číslem, aniž se tím poruší platnost kongruence.

Z platné kongruence

$$25 \equiv 11 \pmod{7}$$

dostáváme tedy např. tyto platné kongruence:

$$50 \equiv 22 \pmod{7},$$

$$100 \equiv 44 \pmod{7},$$

$$-25 \equiv -11 \pmod{7}.$$

S dělením kongruencí jsou však potíže. Vezměme platnou kongruenci

$$12 \equiv 4 \pmod 8$$

a dělme obě strany kongruence tak, jako jsme je doposud násobili. Můžeme je dělit čtyřmi:

$$3 \equiv 1 \pmod 8;$$

tato kongruence však neplatí.

Pro dělení kongruencí platí složitější věta.

Věta 3. *Nechť platí*

$$a \equiv b \pmod m.$$

Nechť dále

(a) *existuje* $d \in \mathbb{N}$, *pro které* $d|a$, $d|b$, $d|m$. *Pak platí*

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right);$$

(b) *existuje* $d \in \mathbb{Z}$, *pro které* $d|a$, $d|b$, *ale neplatí* $d|m$. *Pak platí*

$$\frac{a}{d} \equiv \frac{b}{d} \pmod m.$$

Příklad, ve kterém jsme obě strany kongruence

$$12 \equiv 4 \pmod 8$$

dělili čtyřmi, se tedy měl počítat podle věty 3(a), tj. měli

jsme dělit čtyřmi i modul. Skutečně tak dostáváme platnou kongruenci

$$3 \equiv 1 \pmod 2.$$

Vztah (3) má při řešení kongruencí důležitý praktický význam. Dovoluje nám totiž zmenšit čísla v dané kongruenci. Ukážeme si to na příkladu:

$$38 \equiv 3 \pmod 5.$$

Na levé straně kongruence můžeme přičíst (-6)-násobek modulu:

$$38 - 6.5 \equiv 3 \pmod 5$$

a dostáváme kongruenci s menšími čísly

$$8 \equiv 3 \pmod 5.$$

Kongruenci

$$ax \equiv b \pmod m \tag{4}$$

nazýváme *lineární kongruencí* s neznámou x; a, $b \in \mathbf{Z}$, $m \in \mathbf{N}$, $m \geqq 2$. Celá čísla x, která vyhovují (4), jsou řešení kongruence (4). Jestliže takové x existuje, pak jich existuje nekonečně mnoho a dostaneme je podle (2) nebo podle (3). Budeme však vždy vybírat takové řešení x_0, které je prvkem úplné soustavy nejmenších nezáporných zbytků (mod m). Takových x_0 není ovšem nekonečně mnoho. Uvidíme, že to nikterak neznamená, že by kongruence (4) měla jediné takové řešení, ale že je jich konečný počet

(jestliže konečným počtem řešení nazveme také 0 řešení, tj. žádné řešení).

Než toto všechno dokážeme, zabývejme se nejprve jednodušší kongruencí

$$x \equiv b \pmod{m}, \tag{5}$$

kterou dostaneme z (4) pro $a = 1$. Ale $x \equiv b \pmod{m}$ je už svým vlastním řešením. Podle (3) můžeme psát

$$x \equiv b + mt \pmod{m},$$

kde t je libovolné celé číslo; to má podle (2) ten význam, že je

$$x = b + mt.$$

Kongruence (5) má tedy vždy nekonečný počet řešení. Vhodnou volbou $t \in \mathbf{Z}$ dostaneme řešení x_0, které je prvkem množiny $\{0, 1, \ldots, m-1\}$. Obecné řešení se z tohoto x_0 získá přičtením mt, $t \in \mathbf{Z}$.

Příklad 2. Řešme kongruence

(a) $x \equiv 5 \pmod{11}$,
(b) $x \equiv 22 \pmod{3}$,
(c) $x \equiv -4 \pmod{20}$,
(d) $x \equiv -10 \pmod{10}$.

Řešení jsou po řadě: (a) $x_0 = 5$, (b) $x_0 = 1$, (c) $x_0 = 16$, (d) $x_0 = 0$.

Nyní se obrátíme k řešení kongruence (4). Může nastat několik případů.

Věta 4. *Nechť v kongruenci* (4) *platí:*

(1) *Největší společný dělitel čísel* a, m *je* $d = 1$. *Pak má* (4) *právě jedno řešení* x_0 *ze soustavy* $\{0, 1, \ldots, m-1\}$. (*Toto byl ovšem případ kongruence* (5).)

(2) *Největší společný dělitel čísel* a, m *je* $d > 1$. *Pak mohou nastat dva případy:*

(a) *Neplatí* $d|b$: *pak* (4) *nemá řešení.*

(b) *Platí* $d|b$: *pak* (4) *má právě* d *řešení, z nichž každé je prvkem soustavy* $\{0, 1, \ldots, m-1\}$.

Důkaz. Budeme potřebovat znát ještě pojem *úplná soustava zbytků* (mod m) (tedy nikoli nejmenších nezáporných). Úplná soustava zbytků (mod m) vznikne z úplné soustavy nejmenších nezáporných zbytků (mod m) $\{0, 1, \ldots, m-1\}$, jestliže v ní každé číslo nahradíme libovolným číslem s ním kongruentním (mod m). Vezměme například $m = 3$: úplná soustava nejmenších nezáporných zbytků je $\{0, 1, 2\}$, úplná soustava zbytků (mod 3) je např. $\{6, -2, 11\}$ nebo $\{3, 10, -1\}$. Zejména je ovšem úplná soustava nejmenších nezáporných zbytků (mod m) také úplnou soustavou zbytků (mod m).

(1) Budiž $d = 1$. Je-li $x_i \in \mathbf{Z}$ některý prvek úplné soustavy zbytků (mod m), je také $ax_i \in \mathbf{Z}$ prvek úplné soustavy zbytků (mod m), neboť z kongruence $ax_i \equiv ax_j \pmod{m}$ plyne podle věty 3(b) $x_i \equiv x_j \pmod{m}$. Pro právě jedno x_0 kongruentní s některým z čísel $0, 1, \ldots, m-1$ patří ax_0 do téže zbytkové třídy jako b, tedy pro právě jedno x_0 je

$$ax_0 \equiv b \pmod{m}.$$

(2) Budiž $d>1$. Pak existují $a_1, m_1 \in \mathbf{Z}$ tak, že je $a = a_1 d$, $m = m_1 d$. (4) pak znamená

$$m = m_1 d \mid a_1 dx - b,$$

tj. existuje $t \in \mathbf{Z}$ tak, že je

$$a_1 dx - b = m_1 dt.$$

Ale tato rovnost může platit jen tehdy, existuje-li $b_1 \in \mathbf{Z}$ tak, že je $b = b_1 d$, tj. $d \mid b$; jestliže není $d \mid b$, uvažovaná rovnost neplatí pro žádné $t \in \mathbf{Z}$ a (4) nemá řešení.

Pro $d \mid b$, tedy $b = b_1 d$, však (4) přechází v kongruenci

$$a_1 x \equiv b_1 \pmod{m_1},$$

kde největší společný dělitel čísel a_1, m_1 je 1. Tato kongruence má tedy řešení x_0, ale také $x_0 + m_1$, $x_0 + 2m_1$, ..., $x_0 + (d-1)m_1$. Žádná dvě z těchto řešení nejsou kongruentní (mod m) a všechna jsou prvky soustavy $\{0, 1, \ldots, m-1\}$. Těchto řešení je celkem d a jsou to všechna řešení původní („nezkrácené") kongruence (4). Pro $d \mid b$ má tedy (4) d řešení, jež jsou vesměs prvky úplné soustavy nejmenších nezáporných zbytků (mod m).

Při řešení kongruencí lze tedy případ (2)b snadno (krácením) převést na případ (1), kterým se budeme zabývat podrobněji. Případ (2)a je nezajímavý; jde o takové kongruence jako

$$3x \equiv 2 \pmod{6},$$

které na první pohled nemají řešení, protože pro žádné celé x nemůže být $6 \mid 3x - 2$.

Budeme tedy řešit kongruenci

$$ax \equiv b \pmod{m}$$

za předpokladu, že největší společný dělitel čísel a, m je 1. Použijeme řetězového zlomku racionálního čísla $\frac{m}{a}$; všimněme si, že vhodnou úpravou vždy můžeme dostat kladné racionální číslo. Nechť je tedy $a, m \in \mathbb{N}$. Sblížené zlomky kladného racionálního čísla $\frac{m}{a}$ nechť jsou

$$\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots, \frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{m}{a}.$$

Použijeme vztahu (2) z kapitoly 4:

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$$

čili

$$mQ_{n-1} - aP_{n-1} = (-1)^n.$$

Odtud

$$aP_{n-1} = -(-1)^n + mQ_{n-1}.$$

První člen na pravé straně můžeme psát jako $(-1)^{n-1}$, a protože $Q_{n-1} \in \mathbb{Z}$, platí

$$aP_{n-1} \equiv (-1)^{n-1} \pmod{m}.$$

Násobme obě strany této kongruence číslem $(-1)^{n-1}b$:

$$a(-1)^{n-1} P_{n-1} b \equiv b \pmod{m}.$$

To však znamená, že je

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m}. \qquad (6)$$

Jestliže takto vypočítané x není prvkem soustavy $\{0, 1, \ldots, m-1\}$, dostaneme x_0 přičtením mt, kde t je vhodné celé číslo.

Příklad 3. Řešme kongruenci

$$42x \equiv 11 \pmod{95}.$$

Řešení. Je $42, 95 \in \mathbf{N}$ a čísla 42, 95 jsou nesoudělná. Vypočítáme nejprve prvky řetězového zlomku čísla $\frac{95}{42}$:

$$\begin{aligned} 95 &: 42 = 2 \\ 42 &: 11 = 3 \\ 11 &: 9 = 1 \\ 9 &: 2 = 4 \\ 2 &: 1 = 2 \end{aligned}$$

Tedy $\frac{95}{42} = (2, 3, 1, 4, 2)$. Sestavíme tabulku:

q_k	2	3	1	4	2
P_k	2	7	9	43	95
Q_k	1	3	4	19	42

Nápadně jsme označili číslo $P_{n-1} = P_4 = 43$, které vystupuje ve vzorci (6). Je ovšem $n = 5$ a máme

$$x \equiv 43 . 11 \pmod{95},$$

$$x \equiv 473 \pmod{95},$$

$$x_0 = 473 - 4.95 = 93.$$

Příklad 4. Řešme kongruenci

$$285x \equiv 177 \pmod{924}.$$

Řešení. Největší společný dělitel čísel 285, 177 a 924 je 3; dostaneme tedy tři řešení. Podle vzorce (6) řešíme „vykrácenou" kongruenci

$$95x \equiv 59 \pmod{308},$$

v níž je největší společný dělitel čísel 95 a 308 roven 1. Dostaneme (výpočty nechť si provede čtenář sám) $\frac{308}{95} =$ $= (3, 4, 7, 1, 2)$. Odtud $n = 5$, $\frac{P_4}{Q_4} = \frac{107}{33}$. Je tedy $P_4 = 107$ a

$$x \equiv 107.59 \pmod{308},$$

$$x \equiv 6313 \pmod{308},$$

$$x_0 = 6313 - 20.308 = 153.$$

Řešení původní kongruence jsou čísla

$$153, 153 + 308, 153 + 2.308,$$

tj. čísla

$$153, 461, 769.$$

Ihned vidíme, že jsou to čísla nekongruentní (mod 924) a že všechna tři jsou prvky soustavy $\{0, 1, \ldots, 923\}$.

Příklad 5. V předešlých dvou příkladech bylo n liché, takže x nám vyšlo podle vzorce (6) kladné. To ovšem nemusí vždycky tak být. Řešme proto ještě kongruenci

$$102x \equiv 49 \pmod{121}.$$

Řešení. Největší společný dělitel čísel 102, 121 je 1; dále je (vypočítejte to) $\frac{121}{102} = (1, 5, 2, 1, 2, 2)$, tedy $n = 6$. Je $P_5 = 51$ a vzorec (6) dává

$$x \equiv -51.49 \pmod{121},$$

$$x \equiv -2499 \pmod{121},$$

$$x_0 = -2499 + 21.121 = 42.$$

Nedostali jsme ovšem nic nového; t v činiteli mt je zde kladné a dostaneme opět nezáporné x_0.

Cvičení

1. Dokažte věty 1, 2, 3 z definice kongruence.
2. V textu jsme se zmínili, že bývá prakticky výhodné při řešení kongruence (4) na jedné nebo druhé straně nebo na obou přičíst vhodné násobky modulu. Někdy takto dojdeme až ke kongruenci (5), tj. k řešení. Na ukázku příklad takových úprav kongruence:

$$11x \equiv 25 \pmod{9}$$

upravíme na

$$2x \equiv 16 \pmod{9};$$

protože největší společný dělitel obou stran kongruence, totiž 2, nedělí modul, máme podle věty 3(b)

$$x \equiv 8 \pmod 9,$$

$$x_0 = 8.$$

Řešte tímto způsobem kongruence:
(a) $39x \equiv 11 \pmod{53}$; (b) $196x \equiv 77 \pmod{13}$.

3. Užitím vzorce (6) řešte kongruence:

(a) $5x \equiv 7 \pmod 8$; (b) $15x \equiv 35 \pmod{55}$; (c) $17x \equiv 25 \pmod{28}$; (d) $7x \equiv 10 \pmod{18}$; (e) $25x \equiv 1 \pmod{17}$; (f) $13x \equiv 32 \pmod{28}$; (g) $28x \equiv 21 \pmod{35}$; (h) $111x \equiv 75 \pmod{321}$; (i) $256x \equiv 179 \pmod{337}$; (j) $1215x \equiv 560 \pmod{2755}$.

17. ŘEŠENÍ NEURČITÉ ROVNICE $ax + by = c$

Buďte $a, b, c \in \mathbf{Z}$. Úlohu najít čísla $x, y \in \mathbf{Z}$, která splňují vztah $ax + by = c$, nazýváme *lineární neurčitou (diofantickou) rovnicí* o dvou neznámých x, y. Známe-li jedno řešení (x_0, y_0), dovedeme okamžitě napsat nekonečně mnoho řešení (x, y): buďte $x_0, y_0 \in \mathbf{Z}$ a nechť platí

$$ax_0 + by_0 = c. \tag{1}$$

Hledejme nyní nějaká dvě jiná čísla $x, y \in \mathbf{Z}$, pro která také platí

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

Odečteme-li (1) od (2), dostáváme

$$a(x-x_0)+b(y-y_0)=0,$$

$$a(x-x_0)=-b(y-y_0). \qquad (3)$$

Levá strana této rovnosti je dělitelná číslem $a \in \mathbf{Z}$, tedy jím musí být dělitelná i pravá strana:

$$a \mid b(y-y_0).$$

Předpokládejme nejprve, že neplatí $a \mid b$; pak je

$$a \mid y-y_0$$

$$y-y_0=at,$$

kde $t \in \mathbf{Z}$. Dosadíme-li odtud do (3), dostáváme

$$x-x_0=-bt.$$

Celkem tedy máme řešení (x, y), kde

$$x=x_0-bt,$$

$$y=y_0+at,$$

kde t je libovolné celé číslo a platí

$$ax_0+by_0=c,$$

tj. (x_0, y_0) je řešení rovnice (2).
Je-li $a \mid b$, musí, aby rovnice byla řešitelná, být také $a \mid c$; pak celou rovnici vydělíme číslem a a dostáváme předešlý případ.

Otázka existence řešení je spjata s jednou větou z algebry, která je důsledkem Euklidova algoritmu. Platí:

Buďte $a, b \in \mathbb{Z}$, d největší společný dělitel čísel a, b. Potom existují čísla $x, y \in \mathbb{Z}$ taková, že platí

$$ax + by = d. \tag{4}$$

Tato čísla lze najít Euklidovým algoritmem, jak ukazuje následující příklad.

Příklad 1. Největší společný dělitel čísel 326, 72 je 2. Existují tedy čísla $x, y \in \mathbb{Z}$ taková, že platí

$$326x + 72y = 2.$$

Najděme tato čísla x, y.

Řešení. Napíšeme rovnosti Euklidova algoritmu pro čísla 326, 72:

$$326 = 72.4 + 38,$$

$$72 = 38.1 + 34,$$

$$38 = 34.1 + 4,$$

$$34 = 4.8 + 2,$$

$$4 = 2.2.$$

(Poslední nenulový zbytek 2 mimochodem znovu dokazuje, že 2 je skutečně největší společný dělitel čísel 326, 72.)

Rovnosti Euklidova algoritmu přepíšeme ve tvaru:

$$38 = 326 - 72.4,$$

$$34 = 72 - 38.1,$$

$$4 = 38 - 34.1,$$

$$2 = 34 - 4.8.$$

Odtud postupně dostáváme:

$$34 = 72 - (326 - 72.4).1 =$$

$$= -326 + 72.5,$$

$$4 = 326 - 72.4 - (72.5 - 326).1 =$$
$$= 326.2 - 72.9,$$

$$2 = -326 + 72.5 - (326.2 - 72.9).8 =$$

$$= -17.326 + 77.72.$$

Srovnáme-li tento výsledek s rovnicí

$$2 = 326x + 72y,$$

vidíme, že jsme dostali

$$x = -17, \quad y = 77.$$

Vyřešili jsme tedy svou první neurčitou rovnici, kterou bychom ovšem raději psali ve zkráceném tvaru

$$163x + 36y = 1.$$

Prozatím jsme se omezili na dosti úzkou třídu rovnic. Jestliže totiž rovnici

$$ax + by = d,$$

kde d je největším společným dělitelem čísel a, b, vydělí-

me číslem d, dostaneme rovnici

$$a_1 x + b_1 y = 1 .$$

Není ovšem nutné omezovat se na pravou stranu rovnou jedné. Z citované algebraické věty snadno plyne: *Budiž d největší společný dělitel celých čísel a, b. Pak rovnice*

$$ax + by = d \tag{5}$$

má řešení (x_0, y_0), *tj. platí*

$$ax_0 + by_0 = d .$$

Budiž nyní t libovolné celé číslo. Položme

$$x = x_0 t ,$$

$$y = y_0 t .$$

Čísla x, y sice zřejmě nebudou řešením (5), ale zato pro ně bude platit

$$ax + by = dt .$$

Dostáváme podmínku řešitelnosti rovnice

$$ax + by = c ,$$

a, b, $c \in \mathbf{Z}$: Tato rovnice má řešení x, $y \in \mathbf{Z}$ právě tehdy, jestliže největší společný dělitel d čísel a, b je také dělitelem čísla c, tj. jestliže platí $d \mid c$.

Věta 1. *Buďte a, b, $c \in \mathbf{Z}$; neurčitá rovnice*

$$ax + by = c \tag{6}$$

má řešení x_0, y_0 v oboru celých čísel, jestliže největší společný dělitel d čísel a, b dělí také číslo c. Řešení je pak nekonečně mnoho a jsou určena vzorci

$$x = x_0 - bt,$$

$$y = y_0 + at, \tag{7}$$

kde t je libovolné celé číslo.

Abychom nalezli jednu dvojici kořenů $x_0, y_0 \in \mathbf{Z}$, která určuje všechna řešení x, y podle (7), použijeme opět řetězových zlomků.

Vyjdeme jako při řešení kongruencí ze vzorce

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n \tag{8}$$

a vypočítáme řetězový zlomek čísla $\frac{b}{a}$, což je zlomek v základním tvaru, jestliže rovnici

$$ax + by = c$$

dělíme společným činitelem, největším společným dělitelem čísel a, b.

Na rozdíl od kongruencí se zde můžeme setkat se záporným zlomkem. Na postupu řešení se tím nic nemění, jen si musíme být vědomi (viz kapitola 8), že pro záporná racionální čísla jsou všechna čísla P_k záporná. Určíme sblížené zlomky $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{b}{a}$. Dosadíme do (8) a vynásobíme na obou stranách číslem $(-1)^n c$:

$$bc(-1)^n Q_{n-1} - ac(-1)^n P_{n-1} = c,$$

tj.

$$ac(-1)^{n-1} P_{n-1} + bc(-1)^n Q_{n-1} = c,$$

$$a[(-1)^{n-1} P_{n-1} c] + b[(-1)^n Q_{n-1} c] = c,$$

odkud srovnáním s rovnicí

$$ax_0 + by_0 = c$$

dostáváme

$$x_0 = (-1)^{n-1} P_{n-1} c, \qquad (9)$$

$$y_0 = (-1)^n Q_{n-1} c.$$

Příklad 2. Budeme teď rovnici z příkladu 1 řešit pomocí vzorců (9). Rovnici ovšem vykrátíme:

$$163x + 36y = 1.$$

Najdeme prvky řetězového zlomku $\frac{b}{a} = \frac{36}{163}$:

$$\begin{aligned} 36 &: 163 = 0 \\ 163 &: 36 = 4 \\ 36 &: 19 = 1 \\ 19 &: 17 = 1 \\ 17 &: 2 = 8 \\ 2 &: 1 = 2 \end{aligned}$$

Je tedy $\frac{36}{163} = (0, 4, 1, 1, 8, 2)$, $n = 6$. Vypočítáme sblížené zlomky, přičemž silnou čarou ohraničíme P_5 a Q_5:

q_k	0	4	1	1	8	2
P_k	0	1	1	2	17	36
Q_k	1	4	5	9	77	163

Je $P_5 = 17$, $Q_5 = 77$ a podle vzorců (9)

$$x_0 = -17 . 1 = -17,$$

$$y_0 = 77 . 1 = 77$$

jako v příkladu 1.

Obecné řešení je

$$x = -17 - 36t,$$

$$y = 77 + 163t,$$

$t \in \mathbf{Z}$. Odtud např. pro $t = -1$ dostáváme řešení $(19, -86)$; pro $t = 1$ řešení $(-53, 240)$.

Příklad 3. Řešme rovnici

$$5x - 3y = 1.$$

Řešení. Zde je $\frac{b}{a} = -\frac{3}{5} = -1 + \frac{2}{5} = (-1, 2, 2)$; $n = 3$ a tabulka vypadá takto:

q_k	-1	2	2
P_k	-1	-1	-3
Q_k	1	2	5

$P_2 = -1$, $Q_2 = 2$ a vzorce (9) dávají

$$x_0 = -1,$$

$$y_0 = -2.$$

Obecné řešení je

$$x = -1 + 3t,$$

$$y = -2 + 5t.$$

Pro $t = 1$ dostáváme odtud kladné hodnoty x, y:

$$x = 2, \quad y = 3.$$

Cvičení

1. Často bývá dána úloha řešit neurčitou rovnici $ax + by = c$ v oboru přirozených čísel, tj. pro $x, y \in \mathbb{N}$. (Ale koeficienty a, b, c jsou stále čísla celá, ne jenom přirozená.)
   Dokažte těchto několik vět o řešení rovnice $ax + by = c$ v oboru přirozených čísel. Ve všech případech předpokládáme $a > 0$, $b > 0$.
   (1) Rovnice $ax - by = c$ (kde největší společný dělitel čísel a, b dělí číslo c) má nekonečně mnoho řešení v oboru N.
   (2) Rovnice $ax + by = c$ buď nemá žádné řešení v oboru N, nebo jich má konečný počet.
   (3) Některé případy, kdy rovnice $ax + by = c$ nemá žádné řešení v oboru N: (a) $c \leqq 0$; (b) $c > 0$, ale buď $c < a$ nebo $c < b$; (c) $c = ab$.
2. Řešte v oboru přirozených čísel ($x, y \in \mathbb{N}$) rovnice: (a) $x + 15y = 25$; (b) $x - 13y = 100$; (c) $7x + 2y = 35$; (d) $25x - 21y = 60$; (e) $15x + 2y = 30$.
3. Řešte v oboru celých čísel ($x, y \in \mathbb{Z}$) rovnice: (a) $11x - 9y = 25$; (b)

$10x+7y=97$; (c) $19x-23y=3$; (d) $47x-25y=279$; (e) $17x+21y=1001$; (f) $23x+41y=1299$; (g) $65x-37y=-212$; (h) $31x+41y=1837$; (i) $103x-15y=-882$; (j) $96x+65y=1000$.

18. PELLOVA ROVNICE

Je to neurčitá rovnice *druhého* stupně v x, y tvaru

$$x^2-Ny^2=1, \tag{1}$$

kde N má známý význam. Jako u každé neurčité rovnice hledáme řešení v oboru celých čísel a zapisujeme je jako uspořádanou dvojici (x, y).

Připusťme pro okamžik, že N se rovná druhé mocnině nějakého celého čísla: $N=a^2$, kde $a\in\mathbf{Z}$. Pak z (1) dostáváme

$$x^2-(ay)^2=1.$$

Rozdíl dvou druhých mocnin celých čísel se však může rovnat 1 jen tehdy, jde-li o čísla 1, 0 nebo -1, 0 (v tomto pořadí). Má tedy Pellova rovnice s $N=a^2$ řešení $(1, 0)$ a $(-1, 0)$. Ale tyto dvojice jsou dokonce řešeními Pellovy rovnice pro jakékoli N. Nazveme je triviálními řešeními a v dalším se jimi nebudeme zabývat.

Zajímají nás tedy řešení (x, y), pro něž je $x\neq 0$, $y\neq 0$. Buďte x, y přirozená čísla, pro která platí (1). Zřejmě jsou pak další řešení rovnice (1) uspořádané dvojice $(x, -y)$, $(-x, y)$, $(-x, -y)$. Abychom našli všechna řešení Pellovy rovnice, pokud existují, stačí tedy najít její řešení

v přirozených číslech. Omezíme se tedy nadále na ta řešení (x, y), kde $x, y \in \mathbb{N}$. Pro některá dosti malá N není obtížné řešení rovnice (1) prostě uhodnout. Pro $N=2$ má zřejmě rovnice $x^2-2y^2=1$ řešení $(3, 2)$; pro $N=3$ je řešení Pellovy rovnice $(2, 1)$, pro $N=5$ je to $(9, 4)$, pro $N=6$ pak $(5, 2)$. Jistě bychom takto uhodli řešení Pellovy rovnice i pro některá $N>6$. Sotva bychom však uhodli, že nejmenším řešením rovnice $x^2-13y^2=1$ je uspořádaná dvojice $(649, 180)$ (vzhledem k tomu, že hledáme řešení v přirozených číslech, je snad jasné, co míníme „nejmenším" řešením: má-li rovnice $x^2-13y^2=1$ ještě nějaké jiné řešení v přirozených číslech (x', y'), musí být $x'>649$, $y'>180$). A rovnice $x^2-29y^2=1$ má dokonce nejmenší řešení $(9801, 1820)$, ač N není nijak příliš velké. Nechť se čtenář nedomnívá, že s rostoucím N rostou také hodnoty nejmenšího řešení Pellovy rovnice: nejmenší řešení Pellovy rovnice $x^2-30y^2=1$ je $(11, 2)$.

Platí toto tvrzení: Má-li rovnice (1) alespoň jedno řešení v přirozených číslech, má jich nekonečně mnoho. Budiž (x_0, y_0) nejmenší řešení rovnice (1). Pak všechna řešení (x, y) v přirozených číslech dostaneme ze vzorce

$$x+y\sqrt{N}=(x_0+y_0\sqrt{N})^n \qquad (2)$$

pro $n=1, 2, 3, \ldots$ (Pro $n=1$ zřejmě dostaneme řešení (x_0, y_0).) Tento vzorec dokazuje Perron ve své knize [4]. Ukážeme si, jak se s ním počítá.

Pro $N=2$ jsme našli $x_0=3$, $y_0=2$. Všechna ostatní

přirozená řešení rovnice $x^2-2y^2=1$ jsou tedy dána vztahem

$$x+y\sqrt{2}=(3+2\sqrt{2})^n$$

pro $n=2, 3, \ldots$

Pro $n=2$ dostáváme

$$x+y\sqrt{2}=9+12\sqrt{2}+8,$$

$$x+y\sqrt{2}=17+12\sqrt{2},$$

$$x=17, \quad y=12.$$

Pro $n=3$ je

$$x+y\sqrt{2}=27+54\sqrt{2}+72+16\sqrt{2},$$

$$x+y\sqrt{2}=99+70\sqrt{2},$$

$$x=99, \quad y=70.$$

Pro větší n bychom musili použít binomické věty a výpočet by byl komplikovanější, i když ovšem uskutečnitelný. Pro nás je důležité, že vzorec (2) zaručuje existenci nekonečně mnoha řešení rovnice (1), pokud známe nejmenší řešení (x_0, y_0).

Později si ukážeme jednodušší vzorce, umožňující výpočet všech řešení ze znalosti řešení (x_0, y_0).

Přesvědčte se zkouškou, že uspořádané dvojice (17, 12) a (99, 70) jsou řešeními rovnice $x^2-2y^2=1$.

Budeme tedy nyní hledat řešení (x, y) Pellovy rovnice. Budeme přitom pracovat s iracionálním číslem $\sqrt{N}$.

Vyjádříme číslo $\sqrt{N}$ nekonečným řetězovým zlomkem

$$\sqrt{N}=(q_1, \overline{q_2, \ldots, q_n, 2q_1}).$$

Počet prvků v symetrické části periody je $n-1$, což může být číslo liché nebo sudé. Číslo n udává počet prvků v předperiodě, za nimiž jsou vypsány všechny prvky v symetrické části periody. Těchto n prvků je

$$q_1, q_2, \ldots, q_n$$

a s nimi také budeme při řešení Pellovy rovnice pracovat. Číslo n je opět buď sudé, nebo liché. Při sudém n povedou naše další úvahy k řešení Pellovy rovnice, při lichém n však k řešení rovnice

$$x^2 - Ny^2 = -1,$$

ale uvidíme, že i toto řešení lze převést na řešení rovnice (1).

Buďte $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n}$ sousední sblížené zlomky řetězového zlomku čísla $\sqrt{N}$. Je ovšem

$$\frac{P_{n-1}}{Q_{n-1}}=(q_1, q_2, \ldots, q_{n-1}),$$

$$\frac{P_n}{Q_n}=(q_1, q_2, \ldots, q_n)$$

a platí

$$\sqrt{N} = \alpha = \frac{\alpha_n P_n + P_{n-1}}{\alpha_n Q_n + Q_{n-1}}.$$

Pro α_n platí

$$\alpha_n = (2q_1, q_2, \ldots) = \sqrt{N} + q_1.$$

Po dosazení tedy je

$$\sqrt{N} = \frac{(\sqrt{N} + q_1) P_n + P_{n-1}}{(\sqrt{N} + q_1) Q_n + Q_{n-1}}$$

a odtud

$$\sqrt{N}(\sqrt{N} + q_1) Q_n + \sqrt{N} Q_{n-1} = (\sqrt{N} + q_1) P_n + P_{n-1}.$$

Tuto rovnost lze převést na rovnost tvaru

$$a + b\sqrt{N} = c + d\sqrt{N},$$

$a, b, c, d \in \mathbb{Q}$, $\sqrt{N} \in \mathbb{I}$. Z toho, že množiny $\mathbb{Q}$, $\mathbb{I}$ nemají společné prvky, plyne $a = c$, $b = d$. (Ostatně jsme už této úvahy použili v jednom numerickém případě, při počítání podle vzorce (2). Ale protože zde jde o počítání s obecnými výrazy, raději jsme si to rozepsali.)

V našem případě tedy

$$NQ_n = q_1 P_n + P_{n-1},$$

$$q_1 Q_n + Q_{n-1} = P_n.$$

Odtud

$$P_{n-1} = NQ_n - q_1 P_n,$$

$$Q_{n-1} = P_n - q_1 Q_n.$$

Tyto výrazy dosadíme do vzorce

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n;$$

dostaneme

$$P_n(P_n - q_1 Q_n) - (NQ_n - q_1 P_n) Q_n = (-1)^n,$$

což ihned dává

$$P_n^2 - NQ_n^2 = (-1)^n,$$

tedy pro sudé n řešení Pellovy rovnice

$$x = P_n, \quad y = Q_n.$$

Takto dostaneme řešení rovnice (1) pro $N=3$ (zde je $n=2$), $N=6$ $(n=2)$, $N=7$ $(n=4)$, $N=8$ $(n=2)$, $N=11$ $(n=2)$, ..., $N=47$ $(n=4)$, $N=48$ $(n=2)$ (viz tabulku druhých odmocnin v kapitole 9).

Pro liché n přidáme ještě jednu periodu a místo hodnoty $\frac{P_n}{Q_n}$ vypočítáme hodnotu $\frac{P_{2n}}{Q_{2n}}$ (bereme ovšem $2q_1 \to q_{n+1}$, $q_2 \to q_{n+2}$, $q_3 \to q_{n+3}$, ..., $q_n \to q_{2n}$ podle tohoto schematu:

$$\begin{array}{l} q_1, q_2, \ldots, q_n, 2q_1, \quad q_2, \quad \ldots, q_n \\ \qquad\qquad\qquad\quad \downarrow \quad\quad \downarrow \quad\quad\quad \downarrow \\ \qquad\qquad\qquad\quad q_{n+1}, \quad q_{n+2}, \quad \ldots, q_{2n}). \end{array}$$

Číslo $2n$ je sudé; opakování předešlých úvah dává

$$P_{2n}^2 - NQ_{2n}^2 = 1,$$

tedy pro liché n jsou kořeny Pellovy rovnice

$$x = P_{2n}, \quad y = Q_{2n}.$$

Z naší úvahy a z vlastností sblížených zlomků vyplývá, že čísla x, y jsou přirozená a že jsou to nejmenší čísla, která jsou řešením Pellovy rovnice. Dostali jsme tedy v obou případech nejmenší řešení (x_0, y_0).

Vzhledem k platnosti vzorce (2) platí: Pellova rovnice (1) má pro $\sqrt{N} \notin \mathbb{I}$ nekonečně mnoho řešení v přirozených číslech.

Příklad 1. Řešme rovnici

$$x^2 - 21y^2 = 1.$$

Řešení. Je $\sqrt{21} = (4, \overline{1, 1, 2, 1, 1, 8})$. Tabulku sestavíme z prvků 4, 1, 1, 2, 1, 1. Je tedy $n = 6$ a čísla $x = P_6$, $y = Q_6$ jsou nejmenší přirozená čísla, která vyhovují dané rovnici.

q_k	4	1	1	2	1	1
P_k	4	5	9	23	32	55
Q_k	1	1	2	5	7	12

Je tedy $x = 55$, $y = 12$. Zkouška: $55^2 - 21 \cdot 12^2 = 3025 - 21 \cdot 144 = 3025 - 3024 = 1$.

Příklad 2. Řešme rovnici

$$x^2 - 29y^2 = 1.$$

Řešení. Zde je $\sqrt{29} = (5, \overline{2, 1, 1, 2, 10})$, $n = 5$, budeme proto počítat čísla P_{10}, Q_{10}:

q_k	5	2	1	1	2	10	2	1	1	2
P_k	5	11	16	27	70	727	1524	2251	3775	9801
Q_k	1	2	3	5	13	135	283	418	701	1820

Vychází $x = 9801$, $y = 1820$ (jak se čtenář dověděl už v úvodu této kapitoly). Zkouška: $9801^2 - 29 \cdot 1820^2 = 96\,059\,601 - 29 \cdot 3\,312400 = 96\,059\,601 - 96\,059\,600 = 1$.

Zbývá nalézt nějaké numericky výhodnější vzorce místo vzorce (2). Sierpiński ve své populární knížce [6] uvádí bez důkazu tvrzení, že všechna řešení rovnice (1) dostaneme ze vzorců

$$x_{k+1} = x_0 x_k + N y_0 y_k, \qquad (3)$$

$$y_{k+1} = y_0 x_k + x_0 y_k,$$

$$k \in \mathbb{N}_0,$$

kde (x_0, y_0) je nejmenší řešení.

Dokažme, že vzorce (3) dávají řešení Pellovy rovnice. Důkaz provedeme matematickou indukcí. Platí

$$x_0^2 - N y_0^2 = 1;$$

předpokládejme, že platí

$$x_k^2 - Ny_k^2 = 1.$$

Dokážeme, že pak platí také

$$x_{k+1}^2 - Ny_{k+1}^2 = 1,$$

kde x_{k+1}, y_{k+1} jsou dána vzorci (3).

$$x_{k+1}^2 - Ny_{k+1}^2 = (x_0x_k + Ny_0y_k)^2 - N(y_0x_k + x_0y_k)^2 =$$

$$= x_0^2x_k^2 + 2Nx_0y_0x_ky_k + N^2y_0^2y_k^2 - Ny_0^2x_k^2 - 2Nx_0y_0x_ky_k -$$

$$- Nx_0^2y_k^2 = x_k^2(x_0^2 - Ny_0^2) - Ny_k^2(x_0^2 - Ny_0^2) =$$

$$= x_k^2 - Ny_k^2 = 1.$$

Budiž dáno N. Výrazy (3) dávají pěkné rekurentní vzorce pro řešení rovnice $x^2 - Ny^2 = 1$. Např. pro $N = 2$ je $x_0 = 3$, $y_0 = 2$ a vzorce (3) dávají pro řešení rovnice $x^2 - 2y^2 = 1$ rekurentní vzorce

$$x_{k+1} = 3x_k + 4y_k,$$

$$y_{k+1} = 2x_k + 3y_k$$

pro všechna $k \in \mathbb{N}_0$. Tedy

$$x_1 = 17, \quad y_1 = 12,$$

$$x_2 = 99, \quad y_2 = 70,$$

$$x_3 = 577, \quad y_3 = 408,$$

.....

Porovnejme s řešením téže rovnice podle vzorce (2).

Vraťme se nyní k tabulce řetězových zlomků čísel $\sqrt{N}$ v kapitole 9. Její poslední tři sloupce se vztahují k Pellově rovnici. Sloupce nadepsané „x" a „y" udávají nejmenší řešení buď Pellovy rovnice (jestliže totiž v řetězovém zlomku čísla $\sqrt{N}=(q_1, \overline{q_2, \ldots, q_n, 2q_1})$ je n sudé číslo) nebo rovnice $x^2 - Ny^2 = -1$ (je-li n liché). O kterou z obou rovnic jde, je vyznačeno v posledním sloupci buď číslem $+1$ nebo číslem -1. (V tabulce jsou tedy pro sudé i liché n zapsána čísla $x = P_n$, $y = Q_n$.)

Poznámka. V této kapitole jsme se setkali nejen s Pellovou rovnicí, ale také s rovnicí

$$x^2 - Ny^2 = -1. \tag{4}$$

Mezi oběma rovnicemi je zásadní rozdíl. Zatímco Pellova rovnice má řešení pro každé N, rovnice (4) nemusí být pro některá N vůbec řešitelná v celých číslech. Příkladem toho je např. rovnice

$$x^2 - 3y^2 = -1,$$

která nemá celočíselné řešení. Čtenář si to dokáže ve cvičení 5.

Cvičení

1. Řešte ty Pellovy rovnice s $N \leqq 50$, jejichž řešení nejsou uvedena v tabulce v kapitole 9 (tj. v řádku N je v posledním sloupci číslo -1).
2. S použitím cvičení 2 kapitoly 12 dokažte, že Pellova rovnice má pro $N = n^2 + 1$, $n \in \mathbb{N}$, řešení $x = 2n^2 + 1$, $y = 2n$.

3. Ze vztahů (3) odvoďte rekurentní vzorce pro řešení Pellovy rovnice pro (a) $N=3$; (b) $N=8$; v obou případech z (x_0, y_0) vypočítejte (x_1, y_1), (x_2, y_2), (x_3, y_3).

4. V textu kapitoly 12 jsou uvedeny řetězové zlomky čísel $\sqrt{53}$, $\sqrt{54}$. Řešte s jejich pomocí Pellovy rovnice: (a) $x^2-53y^2=1$; (b) $x^2-54y^2=1$.

5. Dokažte, že rovnice

$$x^2-3y^2=-1$$

nemá řešení v celých číslech.
Návod. Rovnici pište ve tvaru

$$x^2+1=3y^2;$$

má-li být $x, y \in \mathbb{Z}$, musí být $3|x^2+1$. Vyšetřujte zvlášť případy $x=3k$, $x=3k+1$, $x=3k+2$; vyjde vám, že ve všech případech vychází při dělení čísla x^2+1 třemi zbytek, a to buď 1 nebo 2. Dovedete tímto způsobem dokázat neřešitelnost rovnice (4) pro nějaké jiné N?