Literatura

[1] M. Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, March 1973. `http://links.jstor.org/sici?sici=0002-9890%28197303%2980%3A3%3C233%3AHTPIU%3E2.0.CO%3B2-E`.

[2] J. Herman, R. Kučera a J. Šimša. *Metody řešení matematických úloh I.* MU Brno, druhé vydání, 2001.

[3] K. Ireland a M. Rosen. *A Classical Introduction to Modern Number Theory.* Číslo 84 v Graduate Texts in Mathematics. Springer, druhé vydání, 1998.

[4] I. M. Vinogradov. *Základy theorie čísel.* Nakladatelství ČSAV, 1953.

Algebra 2 — Teorie čísel

Michal Bulant

katedra matematiky, Přírodovědecká fakulta, Masarykova univerzita, Janáčkovo nám. 2a, 662 95 Brno

E-mail address: bulant@math.muni.cz

Abstrakt. Na této přednášce se budeme zabývat úlohami o celých číslech. Převážně v nich půjde o dělitelnost celých čísel, popřípadě o řešení rovnic v oboru celých nebo přirozených čísel. Ačkoli jsou přirozená a konec konců i celá čísla v jistém smyslu nejjednodušší matematickou strukturou, zkoumání jejich vlastností postavilo před generace matematiků celou řadu velice obtížných problémů. Často jsou to problémy, které je možno snadno formulovat, přesto však dodnes neznáme jejich řešení. Uveďme některé z nejznámějších: *problém prvočíselných dvojčat* (rozhodnout, zda existuje nekonečně mnoho prvočísel p takových, že i $p+2$ je prvočíslo), *Goldbachovu hypotézu* (rozhodnout, zda každé sudé číslo větší než 2 je možno psát jako součet dvou prvočísel), nebo klenot mezi problémy teorie čísel - *velkou Fermatovu větu* (rozhodnout, zda existují přirozená čísla n, x, y, z tak, že $n > 2$ a platí $x^n + y^n = z^n$).

Tento text výrazně čerpá z knih [**2**] a [**4**], pro zájemce o bližší seznámení s nkterými tématy doporučujeme knihu [**3**], dostupnou v knihovně PřF MU.

V mnoha problémech je výhodné vyzkoušet chování algoritmů na reálných příkladech. K tomu lze využít SW nainstalovaný na počítačích sekce matematika. Doporučujeme zejména:

- PARI-GP : specializovaný SW na teorii čísel, při výpočtech s většími čísly obvykle výrazně efektivnější než obecně orientované balíky. Spouští se příkazem `gp`. Nejdůležitější příkazy: `\q` – ukončení, `?` – help, `??` – kompletní uživatelský manuál, `?? tutorial` – tutoriál pro úvodní seznámení. Viz také `pari.math.u-bordeaux.fr`.
- Maple: vhodný zejména kvůli existenci mnoha výukových pracovních listů (worksheets, i pro teorii čísel), např. na `www.mapleapps.com`.

Obsah

1. Základní pojmy

1.1. Dělitelnost.

Definice. Řekneme, že celé číslo a *dělí* celé číslo b (neboli číslo b je *dělitelné* číslem a, též b je *násobek* a), právě když existuje celé číslo c tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$.

Přímo z definice plyne několik jednoduchých tvrzení, jejichž důkaz přenecháváme čtenáři jako cvičení s návodem v [**2**, §12]: Číslo nula je dělitelné každým celým číslem; jediné celé číslo, které je dělitelné nulou, je nula; pro libovolné číslo a platí $a \mid a$; pro libovolná čísla a, b, c platí tyto čtyři implikace:

$$a \mid b \ \wedge\ b \mid c \implies a \mid c \tag{1}$$

$$a \mid b \ \wedge\ a \mid c \implies a \mid b + c \ \wedge\ a \mid b - c \tag{2}$$

$$c \neq 0 \implies (a \mid b \iff ac \mid bc) \tag{3}$$

$$a \mid b \ \wedge\ b > 0 \implies a \leq b \tag{4}$$

Příklad. Zjistěte, pro která přirozená čísla n je číslo $n^2 + 1$ dělitelné číslem $n + 1$.

Řešení. Platí $n^2 - 1 = (n + 1)(n - 1)$, a tedy číslo $n + 1$ dělí číslo $n^2 - 1$. Předpokládejme, že $n + 1$ dělí i číslo $n^2 + 1$. Pak ovšem musí dělit i rozdíl $(n^2 + 1) - (n^2 - 1) = 2$. Protože $n \in \mathbb{N}$, platí $n + 1 \geq 2$, a tedy z $n + 1 \mid 2$ plyne $n + 1 = 2$, proto $n = 1$. Uvedenou vlastnost má tedy jediné přirozené číslo 1. □

Věta 1. *(Věta o dělení celých čísel se zbytkem) Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m - 1\}$ tak, že $a = qm + r$.*

Důkaz. Dokažme nejprve existenci čísel q, r. Předpokládejme, že přirozené číslo m je dáno pevně a dokažme úlohu pro libovolné $a \in \mathbb{Z}$. Nejprve budeme předpokládat, že $a \in \mathbb{N}_0$ a existenci čísel q, r dokážeme indukcí:

Je-li $0 \leq a < m$, stačí volit $q = 0$, $r = a$ a rovnost $a = qm + r$ platí.

Předpokládejme nyní, že $a \geq m$ a že jsme existenci čísel q, r dokázali pro všechna $a' \in \{0, 1, 2, \ldots, a - 1\}$. Speciálně pro $a' = a - m$ tedy existují q', r' tak, že $a' = q'm + r'$ a přitom $r' \in \{0, 1, \ldots, m - 1\}$. Zvolíme-li $q = q' + 1$, $r = r'$, platí $a = a' + m = (q' + 1)m + r' = qm + r$, což jsme chtěli dokázat.

Existenci čísel q, r jsme tedy dokázali pro libovolné $a \geq 0$. Je-li naopak $a < 0$, pak ke kladnému číslu $-a$ podle výše dokázaného existují $q' \in \mathbb{Z}$, $r' \in \{0, 1, \ldots, m - 1\}$ tak, že $-a = q'm + r'$, tedy $a = -q'm - r'$. Je-li $r' = 0$, položíme $r = 0$, $q = -q'$; je-li $r > 0$, položíme $r = m - r'$, $q = -q' - 1$. V obou případech $a = q \cdot m + r$, a tedy čísla q, r s požadovanými vlastnostmi existují pro každé $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

Nyní dokážeme jednoznačnost. Předpokládejme, že pro některá čísla $q_1, q_2 \in \mathbb{Z}$; $r_1, r_2 \in \{0, 1, \dots, m-1\}$ platí $a = q_1 m + r_1 = q_2 m + r_2$. Úpravou dostaneme $r_1 - r_2 = (q_2 - q_1)m$, a tedy $m \mid r_1 - r_2$. Ovšem z $0 \leq r_1 < m$, $0 \leq r_2 < m$ plyne $-m < r_1 - r_2 < m$, odkud podle (4) platí $r_1 - r_2 = 0$. Pak ale i $(q_2 - q_1)m = 0$, a proto $q_1 = q_2$, $r_1 = r_2$. Čísla q, r jsou tedy určena jednoznačně. Tím je důkaz ukončen. $\square$

Číslo q, resp. r z věty se nazývá *(neúplný) podíl*, resp. *zbytek* při dělení čísla a číslem m se zbytkem. Vhodnost obou názvů je zřejmá, přepíšeme-li rovnost $a = mq + r$ do tvaru

$$\frac{a}{m} = q + \frac{r}{m}, \quad \text{přitom} \quad 0 \leq \frac{r}{m} < 1.$$

Je vhodné též si uvědomit, že z věty 1 plyne, že číslo m dělí číslo a, právě když zbytek r je roven nule.

Příklad. Dokažte, že jsou-li zbytky po dělení čísel $a, b \in \mathbb{Z}$ číslem $m \in \mathbb{N}$ jedna, je jedna i zbytek po dělení čísla ab číslem m.

Řešení. Podle věty 1 existují $s, t \in \mathbb{Z}$ tak, že $a = sm+1$, $b = tm+1$. Vynásobením dostaneme vyjádření

$$ab = (sm + 1)(tm + 1) = (stm + s + t)m + 1 = qm + r,$$

kde $q = stm + s + t$, $r = 1$, které je podle věty 1 jednoznačné, a tedy zbytek po dělení čísla ab číslem m je jedna. $\square$

Použití v Pari-GP. Vydělením čísla 1234567890 číslem 321 se zbytkem dostáváme 3846005, zbytek 285 - jak vidíme v PARI:

```
? divrem(1234567890,321)
%2 = [3846005, 285]~
```

nebo i jinak:

```
? 1234567890\321
%3 = 3846005
? 1234567890%321
%4 = 285
```

1.2. Největší společný dělitel a nejmenší společný násobek.

Definice. Mějme celá čísla a_1, a_2. Libovolné celé číslo m takové, že $m \mid a_1$, $m \mid a_2$ (resp. $a_1 \mid m$, $a_2 \mid m$) se nazývá *společný dělitel* (resp. *společný násobek*) čísel a_1, a_2. Společný dělitel (resp. násobek) $m \geq 0$ čísel a_1, a_2, který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) čísel a_1, a_2, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel a_1, a_2 a značí se (a_1, a_2) (resp. $[a_1, a_2]$).

Poznámka. Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{Z}$ platí $(a, b) = (b, a)$, $[a, b] = [b, a]$, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, $[a, 0] = 0$. Ještě však není jasné, zda pro každou dvojici $a, b \in \mathbb{Z}$ čísla (a, b) a

$[a, b]$ vůbec existují. Pokud však existují, jsou určena jednoznačně: Pro každá dvě čísla $m_1, m_2 \in \mathbb{N}_0$ totiž podle (4) platí, že pokud $m_1 \mid m_2$ a zároveň $m_2 \mid m_1$, je nutně $m_1 = m_2$. Důkaz existence čísla (a, b) podáme (spolu s algoritmem jeho nalezení) ve větě 2, důkaz existence čísla $[a, b]$ a způsob jeho určení pak popíšeme ve větě 4.

VĚTA 2. *(Euklidův algoritmus) Nechť a_1, a_2 jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.*

DŮKAZ. Podle věty 1 platí $a_2 > a_3 > a_4 > \dots$. Protože jde o nezáporná celá čísla, je každé následující alespoň o 1 menší než předchozí, a proto po určitém konečném počtu kroků dostáváme $a_k = 0$, přičemž $a_{k-1} \neq 0$. Z definice čísel a_n plyne, že existují celá čísla $q_1, q_2, \dots, q_{k-2}$ tak, že

$$\begin{aligned} a_1 &= q_1 \cdot a_2 + a_3, \\ a_2 &= q_2 \cdot a_3 + a_4, \\ &\vdots \\ a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1} \\ a_{k-2} &= q_{k-2} \cdot a_{k-1}. \end{aligned} \tag{5}$$

Z poslední rovnosti plyne, že $a_{k-1} \mid a_{k-2}$, z předposlední, že $a_{k-1} \mid a_{k-3}$, atd., až nakonec ze druhé $a_{k-1} \mid a_2$ a z první dostaneme $a_{k-1} \mid a_1$. Je tedy a_{k-1} společný dělitel čísel a_1, a_2. Naopak jejich libovolný společný dělitel dělí i číslo $a_3 = a_1 - q_1 a_2$, proto i $a_4 = a_2 - q_2 a_3, \dots,$ a proto i $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$. Dokázali jsme, že a_{k-1} je největší dělitel čísel a_1, a_2. □

POZNÁMKA. Z poznámky za definicí, z věty 2 a z toho, že pro libovolná $a, b \in \mathbb{Z}$ platí $(a, b) = (a, -b) = (-a, b) = (-a, -b)$ plyne, že existuje největší společný dělitel libovolných dvou celých čísel.

VĚTA 3. *(Bezoutova) Pro libovolná celá čísla a_1, a_2 existuje jejich největší společný dělitel (a_1, a_2), přitom existují celá čísla k_1, k_2 tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$.*

DŮKAZ. Jistě stačí větu dokázat pro $a_1, a_2 \in \mathbb{N}$. Všimněme si, že jestliže je možné nějaká čísla $r, s \in \mathbb{Z}$ vyjádřit ve tvaru $r = r_1 a_1 + r_2 a_2$, $s = s_1 a_1 + s_2 a_2$, kde $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, můžeme tak vyjádřit i

$$r + s = (r_1 + s_1) a_1 + (r_2 + s_2) a_2$$

a také

$$c \cdot r = (c \cdot r_1) a_1 + (c \cdot r_2) a_2$$

pro libovolné $c \in \mathbb{Z}$. Protože $a_1 = 1 \cdot a_1 + 0 \cdot a_2$, $a_2 = 0 \cdot a_1 + 1 \cdot a_2$, plyne z (5), že takto můžeme vyjádřit i $a_3 = a_1 - q_1 a_2$, $a_4 = a_2 - q_2 a_3$, $\dots$, $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$, což je ovšem (a_1, a_2). □

Použití v Pari-GP. Výpočet největšího společného dělitele pomocí Euklidova algoritmu je s využitím výpočetní techniky i pro relativně velká čísla poměrně rychlý. V našem příkladu to vyzkoušíme na 2 číslech A,B, z nichž každé je součinem dvou 101-ciferných prvočísel. Všimněme si, že výpočet největšího společného dělitele i takto velkých čísel trval zandbatelný čas.

```
? p=nextprime(5*10^100);
? q=nextprime(3*10^100);
? r=nextprime(10^100);
? A=p*q;
? B=q*r;
? #
   timer = 1 (on)
? gcd(A,B)
time = 0 ms.
%19 = 300000000000000000000000000000000000000000\
000000000000000000000000000000000000000000000000\
0000000223
? bezout(A,B)
time = 0 ms.
%20 = [284455128205128205128205128205128205128205\
1282051282051282051282051282051282051282051282051\
282051358, -1422275641025641025641025641025641025\
6410256410256410256410256410256410256410256410256\
410256410256435, 30000000000000000000000000000000\
0000000000000000000000000000000000000000000000000\
00000000000000000223]
```

Poznámka. Euklidův algoritmus a Bezoutova věta jsou jedny z nejdůležitějších výsledků elementární teorie čísel a tvoří jeden ze základních pilířů algoritmů algebry a teorie čísel.

To, že znalost těchto základů je občas důležitá i v praktickém životě, dokazuje B. Willis a Samuel Jackson ve filmu Smrtonosná past 3, kde mají za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů. Zde stačí s využitím Euklidova algoritmu najít celá čísla k, l tak, že bude platit $3k + 5l = 4$.
Netroufám si tvrdit, že zmínění herci ovládají uvedené základy teorie čísel (tuto konkrétní úlohu jistě snadno vyřešíte experimentálně), nicméně předchozí věty dávají návod, jak vyřešit úlohu tohoto typu s libovolnými zadanými parametry, což podrobně rozebereme v části o diofantických rovnicích.

Věta 4. *Pro libovolná celá čísla a_1, a_2 existuje jejich nejmenší společný násobek $[a_1, a_2]$ a platí $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.*

Důkaz. Věta jistě platí, je-li některé z čísel a_1, a_2 rovno nule. Můžeme navíc předpokládat, že obě nenulová čísla a_1, a_2 jsou kladná, neboť jejich znaménka se v dokazovaném vzorci neprojeví. Budeme hotovi, ukážeme-li, že $q = a_1 \cdot a_2/(a_1, a_2)$ je nejmenší společný násobek čísel a_1, a_2. Protože (a_1, a_2) je společný dělitel čísel a_1, a_2, jsou $a_1/(a_1, a_2)$ i $a_2/(a_1, a_2)$ celá čísla, a proto

$$q = \frac{a_1 a_2}{(a_1, a_2)} = \frac{a_1}{(a_1, a_2)} \cdot a_2 = \frac{a_2}{(a_1, a_2)} \cdot a_1$$

je společný násobek čísel a_1, a_2. Podle věty 3 existují $k_1, k_2 \in \mathbb{Z}$ tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$. Předpokládejme, že $n \in \mathbb{Z}$ je libovolný společný násobek čísel a_1, a_2 a ukážeme, že je dělitelný číslem q. Je tedy $n/a_1, n/a_2 \in \mathbb{Z}$, a proto je i celé číslo

$$\frac{n}{a_2} \cdot k_1 + \frac{n}{a_1} \cdot k_2 = \frac{n(k_1 a_1 + k_2 a_2)}{a_1 a_2} = \frac{n(a_1, a_2)}{a_1 a_2} = \frac{n}{q}.$$

To ovšem znamená, že $q \mid n$, což jsme chtěli dokázat. $\square$

1.3. Dělitelé a násobky mnoha čísel.

Definice. Největší společný dělitel a nejmenší společný násobek n čísel $a_1, a_2, \dots, a_n \in \mathbb{Z}$ definujeme analogicky jako v 1.2. Libovolné $m \in \mathbb{Z}$ takové, že $m \mid a_1, m \mid a_2, \dots, m \mid a_n$ (resp. $a_1 \mid m, a_2 \mid m, \dots, a_n \mid m$) se nazývá *společný dělitel* (resp. *společný násobek*) čísel $a_1, a_2, \dots, a_n$. Společný dělitel (resp. násobek) $m \geq 0$ čísel $a_1, a_2, \dots, a_n$, který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) těchto čísel, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel $a_1, a_2, \dots, a_n$ a značí se $(a_1, a_2, \dots, a_n)$ (resp. $[a_1, a_2, \dots, a_n]$).

Snadno se přesvědčíme, že platí

$$(a_1, \dots, a_{n-1}, a_n) = ((a_1, \dots, a_{n-1}), a_n), \tag{6}$$

$$[a_1, \dots, a_{n-1}, a_n] = [[a_1, \dots, a_{n-1}], a_n]. \tag{7}$$

Největší společný dělitel $(a_1, \dots, a_n)$ totiž dělí všechna čísla $a_1, \dots, a_n$, a tedy je společným dělitelem čísel $a_1, \dots, a_{n-1}$, a proto dělí i největšího společného dělitele $(a_1, \dots, a_{n-1})$, tj. $(a_1, \dots, a_n) \mid ((a_1, \dots, a_{n-1}), a_n)$. Naopak největší společný dělitel čísel $(a_1, \dots, a_{n-1}), a_n$ musí kromě čísla a_n dělit i všechna čísla $a_1, \dots, a_{n-1}$, protože dělí jejich největšího společného dělitele, a proto $((a_1, \dots, a_{n-1}), a_n) \mid (a_1, \dots, a_n)$. Dohromady dostáváme rovnost (6) a zcela analogicky se dokáže (7).

Pomocí (6) a (7) snadno dokážeme existenci největšího společného dělitele i nejmenšího společného násobku libovolných n čísel indukcí vzhledem k n: pro $n = 2$ je jejich existence dána větami 2 a 4, jestliže pro některé $n > 2$ víme, že existuje největší společný dělitel i nejměnší společný násobek libovolných $n - 1$ čísel, podle (6) a (7) existuje i pro libovolných n čísel.

1.4. Nesoudělnost.

Definice. Čísla $a_1, a_2, \dots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a_1, a_2, \dots, a_n) = 1$. Čísla $a_1, a_2, \dots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé i, j takové, že $1 \le i < j \le n$, platí $(a_i, a_j) = 1$.

Poznámka. V případě $n = 2$ oba pojmy splývají, pro $n > 2$ plyne z nesoudělnosti po dvou nesoudělnost, ne však naopak: například čísla $6, 10, 15$ jsou nesoudělná, ale nejsou nesoudělná po dvou, neboť dokonce žádná dvojice z nich vybraná nesoudělná není: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

Příklad. Nalezněte největší společný dělitel čísel $2^{63} - 1$ a $2^{91} - 1$.

Řešení. Užijeme Euklidův algoritmus. Platí

$$\begin{aligned} 2^{91} - 1 &= 2^{28}(2^{63} - 1) + 2^{28} - 1, \\ 2^{63} - 1 &= (2^{35} + 2^7)(2^{28} - 1) + 2^7 - 1, \\ 2^{28} - 1 &= (2^{21} + 2^{14} + 2^7 + 1)(2^7 - 1). \end{aligned}$$

Hledaný největší společný dělitel je tedy $2^7 - 1 = 127$. □

Věta 5. *Pro libovolná přirozená čísla a, b, c platí*

(1) $(ac, bc) = (a, b) \cdot c$,
(2) *jestliže* $(a, b) = 1$ *a* $a \mid bc$, *pak* $a \mid c$,
(3) $d = (a, b)$ *právě tehdy, když existují* $q_1, q_2 \in \mathbb{N}$ *tak, že* $a = dq_1$, $b = dq_2$ *a* $(q_1, q_2) = 1$.

Důkaz. ad 1. Protože (a, b) je společný dělitel čísel a, b, je $(a, b) \cdot c$ společný dělitel čísel ac, bc, proto $(a, b) \cdot c \mid (ac, bc)$. Podle věty 3 existují $k, l \in \mathbb{Z}$ tak, že $(a, b) = ka + lb$. Protože (ac, bc) je společný dělitel čísel ac, bc, dělí i číslo $kac + lbc = (a, b) \cdot c$. Dokázali jsme, že $(a, b) \cdot c$ a (ac, bc) jsou dvě přirozená čísla, která dělí jedno druhé, proto se podle (4) rovnají.

ad 2. Předpokládejme, že $(a, b) = 1$ a $a \mid bc$. Podle Bezoutovy věty (věta 3) existují $k, l \in \mathbb{Z}$ tak, že $ka + lb = 1$, odkud plyne, že $c = c(ka + lb) = kca + lbc$. Protože $a \mid bc$, plyne odsud, že i $a \mid c$.

ad 3. Nechť $d = (a, b)$, pak existují $q_1, q_2 \in \mathbb{N}$ tak, že $a = dq_1$, $b = dq_2$. Pak podle části (1) platí $d = (a, b) = (dq_1, dq_2) = d \cdot (q_1, q_2)$, a tedy $(q_1, q_2) = 1$. Naopak, je-li $a = dq_1$, $b = dq_2$ a $(q_1, q_2) = 1$, pak $(a, b) = (dq_1, dq_2) = d(q_1, q_2) = d \cdot 1 = d$ (opět užitím 1. části tohoto tvrzení). □

2. Prvočísla

Prvočíslo je jeden z nejdůležitějších pojmů elementární teorie čísel. Jeho důležitost je dána především větou o jednoznačném rozkladu libovolného přirozeného čísla na součin prvočísel, která je silným a účinným nástrojem při řešení celé řady úloh z teorie čísel.

Definice. Každé přirozené číslo $n \geq 2$ má aspoň dva kladné dělitele: 1 a n. Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se *prvočíslo*. V opačném případě hovoříme o *složeném čísle*.

V dalším textu budeme zpravidla prvočíslo značit písmenem p. Nejmenší prvočísla jsou 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem (největší známé prvočíslo $2^{30\,402\,457} - 1$ má pouze 9 152 052 cifer).

Věta 6. *Přirozené číslo $p \geq 2$ je prvočíslo, právě když platí: pro každá celá čísla a, b z $p \mid ab$ plyne $p \mid a$ nebo $p \mid b$.*

Důkaz. „$\Rightarrow$“ Předpokládejme, že p je prvočíslo a $p \mid ab$, kde $a, b \in \mathbb{Z}$. Protože (p, a) je kladný dělitel p, platí $(p, a) = p$ nebo $(p, a) = 1$. V prvním případě $p \mid a$, ve druhém $p \mid b$ podle věty 5.

„$\Leftarrow$“ Jestliže p není prvočíslo, musí existovat jeho kladný dělitel různý od 1 a p. Označíme jej a; pak ovšem $b = \frac{p}{a} \in \mathbb{N}$ a platí $p = ab$, odkud $1 < a < p$, $1 < b < p$. Našli jsme tedy celá čísla a, b tak, že $p \mid ab$ a přitom p nedělí ani a, ani b. $\square$

Příklad. Nalezněte všechna čísla $k \in \mathbb{N}_0$, pro která je mezi deseti po sobě jdoucími čísly $k+1, k+2, \dots, k+10$ nejvíce prvočísel.

Řešení. Pro $k = 1$ je mezi našimi čísly pět prvočísel: 2, 3, 5, 7, 11. Pro $k = 0$ a $k = 2$ pouze čtyři prvočísla. Jestliže $k \geq 3$, není mezi zkoumanými čísly číslo 3. Mezi deseti po sobě jdoucími celými čísly pět sudých a pět lichých čísel, mezi kterými je zase aspoň jedno dělitelné třemi. Našli jsme tedy mezi čísly $k+1$, $k+2$, ..., $k+10$ aspoň šest složených, jsou tedy mezi nimi nejvýše čtyři prvočísla. Zadání proto vyhovuje jediné číslo $k = 1$. $\square$

Příklad. Dokažte, že pro libovolné přirozené číslo n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

Řešení. Zkoumejme čísla $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$. Mezi těmito n po sobě jdoucími čísly není žádné prvočíslo, protože pro libovolné $k \in \{2, 3, \dots, n+1\}$ platí $k \mid (n+1)!$, a tedy $k \mid (n+1)! + k$, a proto $(n+1)! + k$ nemůže být prvočíslo. $\square$

Příklad. Dokažte, že pro libovolné prvočíslo p a libovolné $k \in \mathbb{N}$, $k < p$, je kombinační číslo $\binom{p}{k}$ dělitelné p.

Řešení. Podle definice kombinačního čísla

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{1 \cdot 2 \cdot \dots \cdot k} \in \mathbb{N},$$

a tedy $k! \mid p \cdot a$, kde jsme označili $a = (p-1) \cdot \dots \cdot (p-k+1)$. Protože $k < p$, není žádné z čísel $1, 2, \dots, k$ dělitelné prvočíslem p, a tedy podle věty 6 není ani $k!$ dělitelné prvočíslem p, odkud $(k!, p) = 1$. Podle věty 5 platí $k! \mid a$, a tedy $b = \frac{a}{k!}$ je celé číslo. Protože $\binom{p}{k} = \frac{pa}{k!} = pb$, je číslo $\binom{p}{k}$ dělitelné číslem p. □

Věta 7. *Libovolné přirozené číslo $n \geq 2$ je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li n prvočíslo, pak jde o „součin“ jednoho prvočísla.)*

Poznámka. Dělitelnost je možné obdobným způsobem jako v 1.1 definovat v libovolném oboru integrity (zkuste si rozmyslet, proč se omezujeme na obory integrity). V některých oborech integrity přitom žádné prvky s vlastností prvočísla (říkáme jim *ireducibilní*) neexistují (např. $\mathbb{Q}$), v jiných sice ireducibilní prvky existují, ale zase tam neplatí věta o jednoznačném rozkladu (např. v $\mathbb{Z}(\sqrt{-5})$ máme následující rozklady: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$; zkuste si rozmyslet, že všichni uvedení činitelé jsou skutečně v $\mathbb{Z}(\sqrt{-5})$ ireducibilní).

Důkaz. Nejprve dokážeme indukcí, že každé $n \geq 2$ je možné vyjádřit jako součin prvočísel.

Je-li $n = 2$, je n součin jediného prvočísla 2.

Předpokládejme nyní, že $n > 2$ a že jsme již dokázali, že libovolné n', $2 \leq n' < n$, je možné rozložit na součin prvočísel. Jestliže n je prvočíslo, je součinem jediného prvočísla. Jestliže n prvočíslo není, pak existuje jeho dělitel d, $1 < d < n$. Označíme-li $c = \frac{n}{d}$, platí také $1 < c < n$. Z indukčního předpokladu plyne, že c i d je možné vyjádřit jako součin prvočísel, a proto je takto možné vyjádřit i jejich součin $c \cdot d = n$.

Nyní dokážeme jednoznačnost. Předpokládejme, že platí rovnost součinů $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$, kde $p_1, \dots, p_m$, $q_1, \dots, q_s$ jsou prvočísla a navíc platí $p_1 \leq p_2 \leq \dots \leq p_m$, $q_1 \leq q_2 \leq \dots \leq q_s$ a $1 \leq m \leq s$. Indukcí vzhledem k m dokážeme, že $m = s$, $p_1 = q_1, \dots, p_m = q_m$.

Je-li $m = 1$, je $p_1 = q_1 \cdot \dots \cdot q_s$ prvočíslo. Kdyby $s > 1$, mělo by číslo p_1 dělitele q_1 takového, že $1 < q_1 < p_1$ (neboť $q_2 q_3 \dots q_s > 1$), což není možné. Je tedy $s = 1$ a platí $p_1 = q_1$.

Předpokládejme, že $m \geq 2$ a že tvrzení platí pro $m - 1$. Protože $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$, dělí p_m součin $q_1 \cdot \dots \cdot q_s$, což je podle věty 6 možné jen tehdy, jestliže p_m dělí nějaké q_i pro vhodné $i \in \{1, 2, \dots, s\}$. Protože q_i je prvočíslo, plyne odtud $p_m = q_i$ (neboť $p_m > 1$). Zcela analogicky se dokáže, že $q_s = p_j$ pro vhodné $j \in \{1, 2, \dots, m\}$. Odtud plyne

$$q_s = p_j \leq p_m = q_i \leq q_s,$$

takže $p_m = q_s$. Vydělením dostaneme $p_1 \cdot p_2 \cdot \dots \cdot p_{m-1} = q_1 \cdot q_2 \cdot \dots \cdot q_{s-1}$, a tedy z indukčního předpokladu $m - 1 = s - 1$, $p_1 = q_1, \dots, p_{m-1} = q_{m-1}$. Celkem tedy $m = s$ a $p_1 = q_1, \dots, p_{m-1} = q_{m-1}$, $p_m = q_m$. Jednoznačnost, a proto i celá věta 7 je dokázána. □

Poznámka. Již jsme se zmínili, že je složité o velkých číslech s jistotou rozhodnout, jde-li o prvočíslo (na druhou stranu je o naprosté většině složených čísel snadné prokázat, že jsou skutečně složená). Přesto se v roce 2002 podařilo indickým matematikům (Agrawal, Saxena, Kayal: `http://www.cse.iitk.ac.in/users/manindra/primality_v6.pdf`) dokázat, že problém prvočíselnosti je možné rozhodnout algoritmem s časovou složitostí polynomiálně závislou na počtu cifer vstupního čísla. Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán).

Že je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i výzva učiněná firmou RSA Security (viz `http://www.rsasecurity.com/rsalab`
Pokud se vám podaří rozložit čísla označená podle počtu cifer jako RSA-704, RSA-768, ..., RSA-2048, obdržíte 30 000, 50 000, ..., resp. 200 000 dolarů (čísla RSA-576 a RSA-640 již byla rozložena v roce 2003, resp. 2005; byla-li vyplacena slíbená odměna, mi není známo).

Důsledek. (1) *Jsou-li* $p_1, \dots, p_k$ *navzájem různá prvočísla a* $n_1, \dots, n_k \in \mathbb{N}_0$, *je každý kladný dělitel čísla* $a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ *tvaru* $p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$, *kde* $m_1, \dots, m_k \in \mathbb{N}_0$ *a* $m_1 \leq n_1$, $m_2 \leq n_2$, $\dots$, $m_k \leq n_k$.
Číslo a má tedy právě

$$\tau(a) = (n_1 + 1)(n_2 + 1) \cdot \dots \cdot (n_k + 1)$$

kladných dělitelů, jejichž součet je

$$\sigma(a) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

(2) *Jsou-li* $p_1, \dots, p_k$ *navzájem různá prvočísla a* $n_1, \dots, n_k, m_1, \dots, m_k \in \mathbb{N}_0$ *a označíme-li* $r_i = \min\{n_i, m_i\}$, $t_i = \max\{n_i, m_i\}$ *pro každé* $i = 1, 2, \dots, k$, *platí*

$$(p_1^{n_1} \cdot \dots \cdot p_k^{n_k}, p_1^{m_1} \cdot \dots \cdot p_k^{m_k}) = p_1^{r_1} \cdot \dots \cdot p_k^{r_k},$$

$$[p_1^{n_1} \cdot \dots \cdot p_k^{n_k}, p_1^{m_1} \cdot \dots \cdot p_k^{m_k}] = p_1^{t_1} \cdot \dots \cdot p_k^{t_k}.$$

Poznámka. S pojmem *součet všech kladných dělitelů čísla* a souvisí pojem tzv. *dokonalého čísla* a, které splňuje podmínku $\sigma(a) = 2a$, resp. slovně: „součet všech kladných dělitelů čísla a menších než a samotné je roven číslu a“.

Takovými čísly jsou např. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$ a 8128 (jde o všechna dokonalá čísla menší než 10 000).

Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž: *a je sudé dokonalé číslo, právě když je tvaru* $a = 2^{q-1} \cdot (2^q - 1)$, *kde* $2^q - 1$ *je prvočíslo*. Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Bez zajímavosti není ani to, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět“ – obecně je pro velká čísla, u kterých se nedaří nalézt netriviálního dělitele, obtížné prokázat, že jsou prvočísla. Pro Mersenneho prvočísla existuje poměrně jednoduchý a rychlý postup. Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$ (viz např. `http://www.utm.edu/research/primes/largest.html`).

Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje**

Příklad. Dokažte, že pro každé celé $n > 2$ existuje mezi čísly n a $n!$ alespoň jedno prvočíslo.

Řešení. Označme p libovolné prvočíslo dělící číslo $n! - 1$ (takové existuje podle věty 7, protože $n! - 1 > 1$). Kdyby $p \leq n$, muselo by p dělit číslo $n!$ a nedělilo by $n! - 1$. Je tedy $n < p$. Protože $p \mid (n! - 1)$, platí $p \leq n! - 1$, tedy $p < n!$. Prvočíslo p splňuje podmínky úlohy. □

Nyní uvedeme několik důkazů toho, že existuje nekonečně mnoho prvočísel (i když tvrzení v podstatě vyplývá už z předchozího příkladu).

Věta 8. *Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

Důkaz. (Eukleides) Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1, p_2, \dots, p_n$. Položme $N = p_1 \cdot p_2 \dots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \dots, p_n$ (čísla $p_1, \dots, p_n$ totiž dělí číslo $N - 1$), což je spor.

(Kummer, 1878): Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1 < p_2 < \cdots < p_n$. Položme $N = p_1 \cdot p_2 \cdots p_n > 2$. Číslo $N - 1$ je podle věty 7 dělitelné některým prvočíslem p_i, které dělí zároveň číslo N a tedy i $N - (N - 1) = 1$. Spor.

(Fürstenberg, 1955):

> *V této poznámce uvedeme elementární „topologický“ důkaz existence nekonečně mnoha prvočísel. Zavedeme topologii prostoru celých čísel pomocí báze tvořené aritmetickými posloupnostmi (od $-\infty$ do $+\infty$). Lze snadno ověřit, že jde skutečně o topologický prostor, navíc lze ukázat, že je normální a tedy metrizovatelný. Každá aritmetická posloupnost je uzavřená i otevřená množina (její*

komplement je sjednocení ostatních aritmetických posloupností se stejnou diferencí). Dostáváme, že sjednocení konečného počtu aritmetických posloupností je uzavřená množina. Uvažme množinu $A = \cup A_p$, kde A_p je tvořena všemi násobky p a p probíhá všechna prvočísla. Jediná celá čísla nepatřící do A jsou -1 a 1 a protože množina $\{-1, 1\}$ zřejmě není otevřená, množina A nemůže být uzavřená. A tedy není konečným sjednocením uzavřených množin, což znamená, že musí existovat nekonečně mnoho prvočísel.

□

Příklad. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$, kde $k \in \mathbb{N}_0$.

Řešení. Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, …, p_n. Položme $N = 3p_2 \cdot p_3 \cdot \dots \cdot p_n + 2$. Rozložíme-li N na součin prvočísel podle věty 7, musí v tomto rozkladu vystupovat aspoň jedno prvočíslo p tvaru $3k+2$, neboť v opačném případě by bylo N součinem prvočísel tvaru $3k+1$ (uvažte, že N není dělitelné třemi), a tedy podle příkladu na str. 7 by bylo i N tvaru $3k+1$, což neplatí. Prvočíslo p ovšem nemůže být žádné z prvočísel $p_1, p_2, \dots, p_n$, jak plyne z tvaru čísla N, a to je spor. □

Poznámka. Analogicky se dokáže i tvrzení o prvočíslech tvaru $4k+3$, bohužel na obecný případ nám naše omezené prostředky nestačí. V kapitole o kvadratických kongruencích budeme alespoň schopni dokázat obdobné tvrzení pro prvočísla tvaru $4k + 1$.

Předchozí příklady je možné značně zobecnit. Platí totiž tvrzení, které bývá nazýváno Bertrandovým postulátem nebo Čebyševovou větou:

Věta 9. *(Čebyševova)*

(1) *libovolné přirozené číslo $n > 5$ existují mezi čísly n a $2n$ alespoň dvě prvočísla.*

(2) *Pro každé číslo $n > 3$ existuje mezi čísly n a $2n - 2$ alespoň jedno prvočíslo.*

Důkaz. Důkaz lze provést elementárními prostředky, je však poměrně dlouhý, proto zde není uveden. Viz např. `http://matholymp.com/TUTORIALS/Bertrand.pd`

□

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak „hustě“ se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když „pouze“ asymptoticky) to popisuje tzv. „prime number theorem“:

Věta 10. *(o hustotě prvočísel) Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x \in \mathbb{R}$. Pak*

$$\pi(x) \sim \frac{x}{\ln x},$$

tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x \to \infty$ limitně blíží k nule.

Poznámka. To, jak jsou prvočísla hustě rozmístěna v množině přirozených čísel, rovněž udává Eulerův výsledek

$$\sum_{p \text{ prvočíslo}} \frac{1}{p} = \infty.$$

Přitom např.

$$\sum_{n \in \mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6},$$

což znamená, že prvočísla jsou v $\mathbb{N}$ rozmístěna „hustěji“ než druhé mozniny.

Použití v Pari-GP. O tom, jak odpovídá asymptotický odhad $\pi(x) \sim x/\ln(x)$, v některých konkrétních příkladech vypovídá následující tabulka (získáná s využitím funkce `primepi(x)` v Pari-GP.

```
? v=[100,1000,10000,100000,500000];
? for(k=1,5,print(v[k],„&",primepi(v[k]),„&",\
  v[k]/log(v[k]),„&",\
  (primepi(v[k])-v[k]/log(v[k]))/primepi(v[k])))
```

x	$\pi(x)$	$x/\ln(x)$	relativní chyba
100	25	21.71	0.13
1000	168	144.76	0.13
10000	1229	1085.73	0.11
100000	9592	8685.88	0.09
500000	41538	38102.89	0.08

Poslední příklad (o nekonečnosti počtu prvočísel tvaru $3k + 2$) zobecňuje *Dirichletova věta o aritmetické posloupnosti*:

Věta 11. *(Dirichletova) Jsou-li a, m nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel k tak, že $mk + a$ je prvočíslo. Jinými slovy, mezi čísly $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \ldots$ existuje nekonečně mnoho prvočísel.*

Důkaz. Jde o hlubokou větu teorie čísel, k jejímuž důkazu je zapotřebí aparát značně přesahující její elementární část. Viz např. [**3**, kap. ???] $\square$

Označení. Pro libovolné prvočíslo p a libovolné přirozené číslo n je podle věty 7 jednoznačně určen exponent, se kterým vystupuje p v rozkladu čísla n na prvočinitele (pokud p nedělí číslo n, považujeme tento exponent za nulový). Budeme jej označovat symbolem $v_p(n)$. Pro záporné celé číslo n klademe $v_p(n) = v_p(-n)$.

Podle důsledku 2 můžeme právě zavedené označení $v_p(n)$ charakterizovat tím, že $p^{v_p(n)}$ je nejvyšší mocninou prvočísla p, která dělí číslo n, nebo tím, že $n = p^{v_p(n)} \cdot m$, kde m je celé číslo, které není dělitelné číslem p. Odtud snadno plyne, že pro libovolná nenulová celá čísla a, b platí

$$v_p(ab) = v_p(a) + v_p(b) \tag{8}$$

$$v_p(a) \le v_p(b) \;\wedge\; a + b \ne 0 \implies v_p(a+b) \ge v_p(a) \tag{9}$$

$$v_p(a) < v_p(b) \implies v_p(a+b) = v_p(a) \tag{10}$$

$$v_p(a) \le v_p(b) \implies v_p((a,b)) = v_p(a) \;\wedge\; v_p([a,b]) = v_p(b) \tag{11}$$

Na následujícím příkladu demonstrujme užitečnost zavedeného označení.

Příklad. Dokažte, že pro libovolná přirozená čísla a, b, c platí

$$([a,b],[a,c],[b,c]) = [(a,b),(a,c),(b,c)]$$

Řešení. Podle věty 7 budeme hotovi, ukážeme-li, že $v_p(L) = v_p(P)$ pro libovolné prvočíslo p, kde L, resp. P značí výraz na levé, resp. pravé straně. Nechť je tedy p libovolné prvočíslo. Vzhledem k symetrii obou výrazů můžeme bez újmy na obecnosti předpokládat, že $v_p(a) \le v_p(b) \le v_p(c)$. Podle (11) platí $v_p([a,b]) = v_p(b)$, $v_p([a,c]) = v_p([b,c]) = v_p(c)$; $v_p((a,b)) = v_p((a,c)) = v_p(a)$, $v_p((b,c)) = v_p(b)$, odkud $v_p(L) = v_p(b) = v_p(P)$, což jsme měli dokázat. □

3. Kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice. Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \le r < m$, nazývají se a, b *kongruentní modulo* m (též *kongruentní podle modulu* m), což zapisujeme takto:

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

V opačném případě řekneme, že a, b nejsou kongruentní modulo m, a píšeme

$$a \not\equiv b \pmod{m}.$$

Lemma. *Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ jsou následující podmínky ekvivalentní:*

(1) $a \equiv b \pmod{m}$,
(2) $a = b + mt$ *pro vhodné* $t \in \mathbb{Z}$,
(3) $m \mid a - b$.

Důkaz. „(1)⇒(3)“ Jestliže $a = q_1 m + r$, $b = q_2 m + r$, pak $a - b = (q_1 - q_2)m$.

„(3)⇒(2)“ Jestliže $m \mid a - b$, pak existuje $t \in \mathbb{Z}$ tak, že $m \cdot t = a - b$, tj. $a = b + mt$.

„(2)⇒(1)“ Jestliže $a = b + mt$, pak z vyjádření $b = mq + r$ plyne $a = m(q + t) + r$, tedy a i b mají při dělení číslem m týž zbytek r, tj. $a \equiv b \pmod{m}$. □

3.1. Základní vlastnosti kongruencí. Přímo z definice plyne, že kongruence podle modulu m je reflexivní (tj. $a \equiv a \pmod{m}$ platí pro každé $a \in \mathbb{Z}$), symetrická (tj. pro každé $a, b \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$) a tranzitivní (tj. pro každé $a, b, c \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$) relace, jde tedy o *ekvivalenci*. Dokážeme nyní další vlastnosti:

Věta 12. *(Základní vlastnosti kongruencí)*

(1) ***Kongruence*** *podle téhož modulu* ***můžeme sčítat****. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou.* ***Na libovolnou stranu*** *kongruence* ***můžeme přičíst*** *jakýkoliv* ***násobek modulu.***

Důkaz. Je-li $a_1 \equiv b_1 \pmod{m}$ a $a_2 \equiv b_2 \pmod{m}$, existují podle lemmatu $t_1, t_2 \in \mathbb{Z}$ tak, že $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. Pak ovšem $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$ a opět podle lemmatu $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$. Sečteme-li kongruenci $a + b \equiv c \pmod{m}$ s kongruencí $-b \equiv -b \pmod{m}$, která zřejmě platí, dostaneme $a \equiv c - b \pmod{m}$. Sečteme-li kongruenci $a \equiv b \pmod{m}$ s kongruencí $mk \equiv 0 \pmod{m}$, jejíž platnost je zřejmá, dostaneme $a + mk \equiv b \pmod{m}$. □

(2) ***Kongruence*** *podle téhož modulu* ***můžeme násobit****. Obě strany kongruence je možné* ***umocnit na totéž přirozené číslo****. Obě strany kongruence je možné* ***vynásobit stejným celým číslem****.*

DŮKAZ. Je-li $a_1 \equiv b_1 \pmod{m}$ a $a_2 \equiv b_2 \pmod{m}$, existují podle $t_1, t_2 \in \mathbb{Z}$ tak, že $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. Pak ovšem

$$a_1a_2 = (b_1 + mt_1)(b_2 + mt_2) = b_1b_2 + m(t_1b_2 + b_1t_2 + mt_1t_2),$$

odkud podle dostáváme $a_1a_2 \equiv b_1b_2 \pmod{m}$.

Je-li $a \equiv b \pmod{m}$, dokážeme indukcí vzhledem k přirozenému číslu n, že platí $a^n \equiv b^n \pmod{m}$. Pro $n = 1$ není co dokazovat. Platí-li $a^n \equiv b^n \pmod{m}$ pro nějaké pevně zvolené n, vynásobením této kongruence a kongruence $a \equiv b \pmod{m}$ dostáváme $a^n \cdot a \equiv b^n \cdot b \pmod{m}$, tedy $a^{n+1} \equiv b^{n+1} \pmod{m}$, což je tvrzení pro $n + 1$. Důkaz indukcí je hotov.

Jestliže vynásobíme kongruenci $a \equiv b \pmod{m}$ a kongruenci $c \equiv c \pmod{m}$, dostaneme $ac \equiv bc \pmod{m}$. □

(3) ***Obě strany*** *kongruence* ***můžeme vydělit jejich společným dělitelem****, jestliže je tento dělitel* ***nesoudělný s modulem.***

DŮKAZ. Předpokládejme, že $a \equiv b \pmod{m}$, $a = a_1 \cdot d$, $b = b_1 \cdot d$ a $(m, d) = 1$. Podle lemmatu je rozdíl $a - b = (a_1 - b_1) \cdot d$ dělitelný číslem m. Protože $(m, d) = 1$, je podle věty 5 číslo $a_1 - b_1$ také dělitelné číslem m, odtud podle lemmatu plyne $a_1 \equiv b_1 \pmod{m}$. □

(4) *Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.*

DŮKAZ. Je-li $a \equiv b \pmod{m}$, existuje podle lemmatu celé číslo t tak, že $a = b + mt$, odkud pro $c \in \mathbb{N}$ platí $ac = bc + mc \cdot t$, odkud opět podle lemmatu plyne $ac \equiv bc \pmod{mc}$. □

(5) *Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.*

DŮKAZ. Předpokládejme, že $a \equiv b \pmod{m}$, $a = a_1 \cdot d$, $b = b_1 \cdot d$, $m = m_1 \cdot d$, kde $d \in \mathbb{N}$. Podle lemmatu existuje $t \in \mathbb{Z}$ tak, že $a = b + mt$, tj. $a_1 \cdot d = b_1 \cdot d + m_1dt$, odkud $a_1 = b_1 + m_1t$, což podle lemmatu znamená, že $a_1 \equiv b_1 \pmod{m_1}$. □

(6) ***Jestliže kongruence*** $a \equiv b$ ***platí podle různých modulů*** $m_1, \dots, m_k$, ***platí i podle modulu, kterým je nejmenší společný násobek*** $[\mathbf{m_1}, \dots, \mathbf{m_k}]$ ***těchto čísel.***

Důkaz. Jestliže $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$, podle lemmatu je rozdíl $a - b$ společný násobek čísel $m_1, m_2, \dots, m_k$ a tedy je dělitelný jejich nejmenším společným násobkem $[m_1, m_2, \dots, m_k]$, odkud plyne $a \equiv b \pmod{[m_1, \dots, m_k]}$. □

(7) *Jestliže kongruence platí podle modulu m, platí podle libovolného modulu d, který je dělitelem čísla m.*

Důkaz. Jestliže $a \equiv b \pmod{m}$, je $a - b$ dělitelné m, a proto také dělitelem d čísla m, odkud $a \equiv b \pmod{d}$. □

(8) *Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana kongruence.*

Důkaz. Předpokládejme, že $a \equiv b \pmod{m}$, $b = b_1 d$, $m = m_1 d$. Pak podle lemmatu existuje $t \in \mathbb{Z}$ tak, že $a = b + mt = b_1 d + m_1 dt = (b_1 + m_1 t)d$, a tedy $d \mid a$. □

Poznámka. Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad ze strany 7 lze přeformulovat do tvaru „jestliže $a \equiv 1 \pmod{m}$, $b \equiv 1 \pmod{m}$, pak také $ab \equiv 1 \pmod{m}$“, což je speciální případ tvrzení věty 12 (2). Nejde o náhodu. Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

Příklad. Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Řešení. Protože $5^2 = 25 \equiv -1 \pmod{26}$, platí podle věty 12 (2)

$$5^{20} \equiv (-1)^{10} = 1 \pmod{26},$$

a tedy zbytek po dělení čísla 5^{20} číslem 26 je jedna. □

Příklad. Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Řešení. Platí $37 \equiv 16 \equiv 23 \equiv 2 \pmod{7}$, a tedy podle 12 (2) a (1) platí

$$37^{n+2}+16^{n+1}+23^n \equiv 2^{n+2}+2^{n+1}+2^n = 2^n(4+2+1) = 2^n \cdot 7 \equiv 0 \pmod{7},$$

což jsme chtěli dokázat. □

Příklad. Dokažte, že číslo $n = (835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

Řešení. Rozložíme $112 = 7 \cdot 16$. Protože $(7, 16) = 1$, stačí ukázat, že $7 \mid n$ a $16 \mid n$. Platí $835 \equiv 2 \pmod 7$, a tedy podle 12

$$n \equiv (2^5+6)^{18}-1 = 38^{18}-1 \equiv 3^{18}-1 = 27^6-1 \equiv (-1)^6-1 = 0 \pmod 7,$$

proto $7 \mid n$. Podobně $835 \equiv 3 \pmod{16}$, a tedy

$$\begin{aligned} n \equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \equiv (3 \cdot 1 + 6)^{18} - 1 = \\ = 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16}, \end{aligned}$$

proto $16 \mid n$. Celkem tedy $112 \mid n$, což jsme měli dokázat. □

Příklad. Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a + b)^p \pmod p.$$

Řešení. Podle binomické věty platí

$$(a + b)^p = a^p + \tbinom{p}{1}a^{p-1}b + \tbinom{p}{2}a^{p-2}b^2 + \cdots + \tbinom{p}{p-1}ab^{p-1} + b^p.$$

Podle příkladu za větou 6 pro libovolné $k \in \{1, \dots, p-1\}$ platí $\binom{p}{k} \equiv 0 \pmod p$, odkud plyne tvrzení. □

Následující tvrzení je další užitečnou vlastností kongruencí:

Lemma. *Dokažte, že pro libovolné přirozené číslo m a libovolná $a, b \in \mathbb{Z}$ taková, že $a \equiv b \pmod{m^n}$, kde $n \in \mathbb{N}$, platí, že $a^m = b^m \pmod{m^{n+1}}$.*

Důkaz. Platí

$$a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1}) \qquad (12)$$

a protože $m \mid m^n$, tak podle 12 (7) platí i $a \equiv b \pmod m$. Jsou tedy všechny sčítance ve druhé závorce v (12) kongruentní s a^{m-1} modulo m, a tedy

$$a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1} \equiv m \cdot a^{m-1} \equiv 0 \pmod m,$$

proto je $a^{m-1}+a^{m-2}+\cdots+ab^{m-2}+b^{m-1}$ dělitelné m. Z $a \equiv b \pmod{m^n}$ plyne, že m^n dělí $a - b$, a tedy m^{n+1} dělí jejich součin, což vzhledem k (12) vede k závěru, že $a^m \equiv b^m \pmod{m^{n+1}}$. □

3.2. Aritmetické funkce. Aritmetickou funkcí zde rozumíme funkci, jejímž definičním oborem je množina přirozených čísel.

Definice. Rozložme přirozené číslo n na prvočísla: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hodnotu *Möbiovy funkce* $\mu(n)$ definujeme rovnu 0, pokud pro některé i platí $\alpha_i > 1$ a rovnu $(-1)^k$ v opačném případě. Dále definujeme $\mu(1) = 1$.

Příklad. $\mu(4) = \mu(2^2) = 0, \mu(6) = \mu(2 \cdot 3) = (-1)^2, \mu(2) = \mu(3) = -1$.

Dokážeme nyní několik důležitých vlastností Möbiovy funkce, zejména tzv. *Möbiovu inverzní formuli.*

Lemma. *Pro $n \in \mathbb{N} \setminus \{1\}$ platí*

$$\sum_{d|n} \mu(d) = 0.$$

Důkaz. Zapíšeme-li n ve tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak všechny dělitele d čísla n jsou tvaru $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, kde $0 \le \beta_i \le \alpha_i$ pro všechna $i \in \{1, \dots, k\}$. Proto

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{\substack{(\beta_1,\dots,\beta_k) \in (\mathbb{N} \cup \{0\})^k \\ 0 \le \beta_i \le \alpha_i}} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) = \\
&= \sum_{(\beta_1,\dots,\beta_k) \in \{0,1\}^k} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) \\
&= \tbinom{k}{0} + \tbinom{k}{1} \cdot (-1) + \tbinom{k}{2} \cdot (-1)^2 + \dots + \tbinom{k}{k} \cdot (-1)^k \\
&= \big(1 + (-1)\big)^k = 0.
\end{aligned}$$

□

S Möbiovou funkcí úzce souvisí pojem *Dirichletův součin*:

Definice. Buďte f, g aritmetické funkce. Jejich *Dirichletův součin* je definován předpisem

$$(f \circ g)(n) = \sum_{d|n} f(d) \cdot g\left(\tfrac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) \cdot g(d_2).$$

Lemma. *Dirichletův součin je asociativní.*

Důkaz.

$$((f \circ g) \circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3) = (f \circ (g \circ h))(n)$$

□

Příklad. Definujme dvě pomocné funkce $\mathbb{I}$ a I předpisem $\mathbb{I}(1) = 1$, $\mathbb{I}(n) = 0$ pro všechna $n > 1$, resp. $I(n) = 1$ pro všechna $n \in \mathbb{N}$. Pak pro každou aritmetickou funkci f platí:

$$f \circ \mathbb{I} = \mathbb{I} \circ f = f$$

a

$$(I \circ f)(n) = (f \circ I)(n) = \sum_{d|n} f(d).$$

Dále platí $I \circ \mu = \mu \circ I = \mathbb{I}$, neboť

$$(I \circ \mu)(n) = \sum_{d|n} I(d)\mu(\tfrac{n}{d}) = \sum_{d|n} I(\tfrac{n}{d})\mu(d) =$$
$$= \sum_{d|n} \mu(d) = 0 \quad \text{pro všechna } n > 1$$

podle lemmatu za definicí Möbiovy funkce (pro $n = 1$ je tvrzení zřejmé).

Věta 13. *(Möbiova inverzní formule) Nechť je aritmetická funkce F definovaná pomocí aritmetické funkce f předpisem $F(n) = \sum_{d|n} f(d)$. Pak lze funkci f vyjádřit ve tvaru*

$$f(n) = \sum_{d|n} \mu(\tfrac{n}{d}) \cdot F(d).$$

Důkaz. Vztah $F(n) = \sum_{d|n} f(d)$ lze jiným způsobem zapsat jako $F = f \circ I$. Proto $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$, což je tvrzení věty. □

Definice. Multiplikativní funkcí přirozených čísel rozumíme takovou aritmetickou funkci, která splňuje, že pro všechny dvojice nesoudělných čísel $a, b \in \mathbb{N}$ platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

Příklad. Multiplikativními funkcemi jsou např. funkce $f(n) = \sigma(n)$, $f(n) = \tau(n)$, či $f(n) = \mu(n)$ nebo, jak brzy dokážeme i tzv. Eulerova funkce $f(n) = \varphi(n)$.

3.3. Eulerova funkce φ.

Definice. Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

$$\varphi(n) = |\{a \in \mathbb{N} \mid 0 < a \leq n,\ (a, n) = 1\}|$$

Příklad. $\varphi(1) = 1, \varphi(5) = 4, \varphi(6) = 2$, je-li p prvočíslo, je zřejmě $\varphi(p) = p - 1$.

Nyní dokážeme několik důležitých tvrzení o funkci φ:

Lemma. *Nechť $n \in \mathbb{N}$. Pak $\sum_{d|n} \varphi(d) = n$.*

Důkaz. Uvažme n zlomků

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}, \frac{n}{n}.$$

Zkrátíme-li zlomky na základní tvar a seskupíme podle jmenovatelů, snadno dostaneme právě uvedené tvrzení. □

Věta 14. *Nechť $n \in \mathbb{N}$, jehož rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Důkaz. S využitím předchozího lemmatu a Möbiovy inverzní formule dostáváme

$$\begin{aligned}\varphi(n) &= \sum_{d|n}\mu(d)\frac{n}{d} = n - \frac{n}{p_1} - \cdots - \frac{n}{p_k} + \cdots + (-1)^k\frac{n}{p_1\cdots p_k} = \\ &= n\cdot\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned} \tag{13}$$

□

Poznámka. Předchozí výsledek lze obdržet i bez použití Möbiovy inverzní formule pomocí principu inkluze a exkluze na základě zjištění poučtu čísel soudělných s n.

Důsledek. *Nechť $a, b \in \mathbb{N}$, $(a, b) = 1$. Pak*

$$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b).$$

Důkaz. Zřejmý. □

Poznámka. Rovněž toto tvrzení lze odvodit nezávisle na základě poznatku $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$. Spolu se snadno odvoditelným výsledkem

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)\cdot p^{\alpha-1} \tag{14}$$

pak lze odvodit vztah (13) již třetím způsobem.

Příklad. Vypočtěte $\varphi(72)$.

Řešení. $72 = 2^3\cdot 3^2 \implies \varphi(72) = 72\cdot(1-\frac{1}{2})\cdot(1-\frac{1}{3}) = 24$, alternativně $\varphi(72) = \varphi(8)\cdot\varphi(9) = 4\cdot 6 = 24$. □

Příklad. Dokažte, že $\forall n \in \mathbb{N} : \varphi(4n+2) = \varphi(2n+1)$.

Řešení. $\varphi(4n+2) = \varphi(2\cdot(2n+1)) = \varphi(2)\cdot\varphi(2n+1) = \varphi(2n+1)$. □

3.4. Malá Fermatova věta, Eulerova věta. Tvrzení v tomto odstavci patří mezi nejdůležitější výsledky teorie čísel.

Věta 15 (Fermatova, Malá Fermatova). *Nechť $a \in \mathbb{Z}$, p prvočíslo, $p \nmid a$. Pak*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{15}$$

Důkaz. Tvrzení vyplyne jako snadný důsledek Eulerovy věty 16. □

Důsledek. *Nechť $a \in \mathbb{Z}$, p prvočíslo. Pak*

$$a^p \equiv a \pmod{p}.$$

Důkaz. Pokud $p \mid a$, pak jsou obě strany kongruentní s $0 \mod p$, jinak tvrzení snadno plyne vynásobením obou stran kongruence (15) číslem a. □

Definice. *Úplná soustava zbytků* modulo m je libovolná m-tice čísel po dvou nekongruentních modulo m (nejčastěji $0, 1, \dots, m-1$). *Redukovaná soustava zbytků* modulo m je libovolná $\varphi(m)$-tice čísel nesoudělných s m a po dvou nekongruentních modulo m.

Poznámka. Snadno lze vidět, že jsou-li $a, b \in \mathbb{Z}$, $a \equiv b \pmod{m}$, a $(a, m) = 1$, pak i $(b, m) = 1$.

Lemma. *Nechť $x_1, x_2, \dots, x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m. Je-li $a \in \mathbb{Z}$, $(a, m) = 1$ pak i čísla $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m.*

Důkaz. Protože $(a, m) = 1$ a $(x_i, m) = 1$, platí $(a \cdot x_i, m) = 1$. Kdyby pro nějaká i, j platilo $a \cdot x_i \equiv a \cdot x_j \pmod{m}$, po vydělení obou stran kongruence číslem a nesoudělným s m dostaneme $x_i \equiv x_j \pmod{m}$. □

Věta 16 (Eulerova). *Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. Pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{16}$$

Důkaz. Buď $x_1, x_2, \dots, x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo m. Podle předchozího lemmatu je i $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo m. Platí tedy, že pro každé i existuje j (oba indexy jsou z množiny $\{1, 2, \dots, \varphi(m)\}$) tak, že $a \cdot x_i \equiv x_j \pmod{m}$. Vynásobením čísel obou redukovaných soustav zbytků dostáváme

$$(a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_{\varphi(m)}) \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}.$$

Po úpravě

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$$

a protože $(x_1 \cdot x_2 \cdots x_{\varphi(m)}, m) = 1$, můžeme obě strany kongruence vydělit číslem $x_1 \cdot x_2 \cdots x_{\varphi(m)}$ a dostaneme $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Poznámka. Eulerova věta je rovněž důsledkem Lagrangeovy věty uplatněným na grupu $(\mathbb{Z}_m^\times, \cdot)$.

Příklad. Nalezněte všechna prvočísla p, pro která $5^{p^2} + 1 \equiv 0 \pmod{p^2}$.

Řešení. Snadno se přesvědčíme, že $p = 5$ úloze nevyhovuje. Pro $p \neq 5$ platí $(p, 5) = 1$, a tedy podle Fermatovy věty $5^{p-1} \equiv 1 \pmod{p}$. Umocněním na $p+1$ dostaneme $5^{p^2-1} \equiv 1 \pmod{p}$, odkud $5^{p^2} \equiv 5 \pmod{p}$. Z podmínky $5^{p^2} + 1 \equiv 0 \pmod{p}^2$ plyne $5^{p^2} \equiv -1 \pmod{p}$, celkem tedy $5 \equiv -1 \pmod{p}$, a proto $p \mid 6$. Je tedy buď $p = 2$, nebo $p = 3$. Pro $p = 2$ však $5^4 + 1 \equiv 1^4 + 1 = 2 \not\equiv 0 \pmod{4}$. Pro $p = 3$ dostáváme $5^9 + 1 = 5^6 \cdot 5^3 + 1 \equiv 5^3 + 1 = 126 \equiv 0 \pmod{9}$, kde jsme užili důsledek Eulerovy věty $5^6 \equiv 1 \pmod{9}$. Jediným prvočíslem, vyhovujícím úloze je tedy $p = 3$. □

Příklad. Pro liché číslo $m > 1$ nalezněte zbytek po dělení čísla $2^{\varphi(m)-1}$ číslem m.

Řešení. Z Eulerovy věty plyne $2^{\varphi(m)} \equiv 1 \equiv 1+m = 2r \pmod{m}$), kde $r = \frac{1+m}{2}$ je přirozené číslo, $0 < r < m$. Podle 12 (3) platí $2^{\varphi(m)-1} \equiv r \pmod{m}$, a tedy hledaný zbytek po dělení je $r = \frac{1+m}{2}$. □

Tvrzení 3.1. *Je-li p prvočíslo, $p \equiv 3 \pmod{4}$, pak pro libovolná celá čísla a, b z kongruence $a^2 + b^2 \equiv 0 \pmod{p}$ plyne $a \equiv b \equiv 0 \pmod{p}$.*

Důkaz. Předpokládejme, že pro $a, b \in \mathbb{Z}$ platí $a^2+b^2 \equiv 0 \pmod{p}$. Jestliže $p \mid a$, platí $a \equiv 0 \pmod{p}$, proto $b^2 \equiv 0 \pmod{p}$, tedy $p \mid b^2$, odkud vzhledem k tomu, že p je prvočíslo, dostáváme $p \mid b$, a proto $a \equiv b \equiv 0 \pmod{p}$, což jsme chtěli dokázat.

Zbývá prošetřit případ, kdy a není dělitelné prvočíslem p. Odtud dostáváme, že p nedělí ani b (kdyby $p \mid b$, dostali bychom $p \mid a^2$). Vynásobíme-li obě strany kongruence $a^2 \equiv -b^2 \pmod{p}$ číslem b^{p-3}, dostaneme podle Fermatovy věty

$$a^2 b^{p-3} \equiv -b^{p-1} \equiv -1 \pmod{p}.$$

Protože $p \equiv 3 \pmod{4}$, je $p-3$ sudé číslo, a proto $\frac{p-3}{2} \in \mathbb{N}_0$. Označme

$$c = ab^{\frac{p-3}{2}}.$$

Pak c není dělitelné p a platí $c^2 = a^2 b^{p-3} \equiv -1 \pmod{p}$. Umocníme-li poslední kongruenci na $\frac{p-1}{2} \in \mathbb{N}$, dostaneme

$$c^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Protože $p \equiv 3 \pmod{4}$, existuje celé číslo t tak, že $p = 3+4t$. Pak ovšem $\frac{p-1}{2} = 1 + 2t$, což je číslo liché a proto $(-1)^{(p-1)/2} = -1$. Podle Fermatovy věty naopak platí $c^{p-1} \equiv 1 \pmod{p}$, odkud $1 \equiv -1 \pmod{p}$ a $p \mid 2$, spor. □

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m* – jde přitom pouze o jinak nazvaný řád prvku v grupě invertibilních zbytkových tříd modulo m:

Definice. Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $(a, m) = 1$. *Řádem čísla a modulo m* rozumíme nejmenší přirozené číslo n splňující

$$a^n \equiv 1 \pmod{m}.$$

Poznámka. To, že je řád definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Jak později uvidíme, velmi důležitá jsou právě ta čísla, jejichž řád je roven právě $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo m a hrají důležitou roli mj. při řešení binomických kongruencí (viz 4.5). Tento pojem je přitom jen jiným názvem pro generátor grupy $(\mathbb{Z}_m^\times, \cdot)$.

Příklad. Pro libovolné $m \in \mathbb{N}$ má číslo 1 modulo m řád 1. Číslo -1 má řád

- 1 pro $m = 1$ nebo $m = 2$
- 2 pro $m > 2$

Příklad. Určete řád čísla 2 modulo 7.

Řešení.

$$\begin{aligned} 2^1 &= 2 \not\equiv 1 \pmod 7 \\ 2^2 &= 4 \not\equiv 1 \pmod 7 \\ 2^3 &= 8 \equiv 1 \pmod 7 \end{aligned}$$

Řád čísla 2 modulo 7 je tedy roven 3. □

Uveďme nyní několik zásadních tvrzení udávajících vlastnosti řádu čísla modulo m:

Lemma. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže $a \equiv b \pmod m$, pak obě čísla a, b mají stejný řád modulo m.*

Důkaz. Umocněním kongruence $a \equiv b \pmod m$ na n-tou dostaneme $a^n \equiv b^n \pmod m$, tedy $a^n \equiv 1 \pmod m \iff b^n \equiv 1 \pmod m$. □

Lemma. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \cdot s$, (kde $r, s \in \mathbb{N}$), pak řád čísla a^r modulo m je roven s.*

Důkaz. Protože žádné z čísel $a, a^2, a^3, \dots, a^{rs-1}$ není kongruentní s 1 modulo m, není ani žádné z čísel $a^r, a^{2r}, a^{3r}, \dots, a^{(s-1)r}$ kongruentní s 1. Platí ale $(a^r)^s \equiv 1 \pmod m$, proto je řád a^r modulo m roven s. □

Poznámka. Opak obecně neplatí – z toho, že řád čísla a^r modulo m je roven s ještě neplyne, že řád čísla a modulo m je $r \cdot s$.
Př: $m = 13$
$a = 3$, $a^2 = 9 \pmod{13}$, $a^3 = 27 \equiv 1 \pmod{13} \Rightarrow 3$ má řád 3 mod 13.
$b = -4$, $b^2 = 16 \not\equiv 1 \pmod{13}$, $b^3 = -64 \equiv 1 \pmod{13} \Rightarrow -4$ má řád 3 modulo 13.
Přitom $(-4)^2 = 16 \equiv 3 \pmod{13}$ má stejný řád 3 jako číslo 3, ale číslo -4 nemá řád $2 \cdot 3$.
Přesný popis závislosti řádu na exponentu dávají následující 2 věty:

Věta 17. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m. Pak pro libovolná $t, s \in \mathbb{N} \cup \{0\}$ platí*

$$a^t \equiv a^s \pmod m \iff t \equiv s \pmod r.$$

Důkaz. Bez újmy na obecnosti lze předpokládat, že $t \geq s$. Vydělíme-li číslo $t - s$ číslem r se zbytkem, dostaneme $t - s = q \cdot r + z$, kde $q, z \in \mathbb{N}_0, 0 \leq z < r$.

„$\Leftarrow$“ Protože $t \equiv s \pmod r$, máme $z = 0$, a tedy $a^{t-s} = a^{qr} = (a^r)^q \equiv 1^q \pmod m$. Vynásobením obou stran kongruence číslem a^s dostaneme tvrzení.

„$\Rightarrow$“ Z $a^t \equiv a^s \pmod m$ plyne $a^s \cdot a^{qr+z} \equiv a^s \pmod m$. Protože je $a^r \equiv 1 \pmod m$, je rovněž $a^{qr+z} \equiv a^z \pmod m$. Celkem po vydělení obou stran kongruence číslem a^s (které je nesoudělné s modulem), dostáváme $a^z \equiv 1 \pmod m$. Protože $z < r$, plyne z definice řádu, že $z = 0$, a tedy $r \mid t - s$. □

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení (jehož druhá část je přeformulováním Lagrangeovy věty z Algebry pro naši situaci):

Důsledek. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m.*

(1) *Pro libovolné $n \in \mathbb{N} \cup \{0\}$ platí*

$$a^n \equiv 1 \pmod m \iff r \mid n.$$

(2) $r \mid \varphi(m)$

Důkaz.

(1) stačí v předchozí větě volit $t = n$, $s = r$.
(2) zřejmé z (1) díky Eulerově větě volbou $n = \varphi(m)$.

□

Následující věta je zobecněním předchozího Lemmatu.

Věta 18. *Nechť $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \in \mathbb{N}$, je řád čísla a^n modulo m roven $\frac{r}{(n,r)}$.*

Důkaz. Protože $\frac{r \cdot n}{(r,n)} = [r, n]$, což je zřejmě násobek r, máme

$$(a^n)^{\frac{r}{(r,n)}} = a^{[r,n]} \equiv 1 \pmod m$$

(plyne z předchozího Důsledku neboť $r \mid [r, n]$). Na druhou stranu, je-li $k \in \mathbb{N}$ libovolné takové, že $(a^n)^k = a^{n \cdot k} \equiv 1 \pmod m$, dostáváme ($r$ je řád a), že $r \mid n \cdot k$ a dále z Věty 5 plyne, že $\frac{r}{(n,r)} \mid \frac{n}{(n,r)} \cdot k$ a díky nesoudělnosti čísel $\frac{r}{(n,r)}$ a $\frac{n}{(n,r)}$ dostáváme $\frac{r}{(n,r)} \mid k$. Proto je $\frac{r}{(n,r)}$ řádem čísla a^n modulo m. □

Poslední z této řady tvrzení dává do souvislosti řády dvou čísel a řád jejich součinu:

Lemma. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže a je řádu r a b je řádu s modulo m, kde $(r, s) = 1$, pak číslo $a \cdot b$ je řádu $r \cdot s$ modulo m.*

Důkaz. Označme δ řád čísla $a\cdot b$. Pak $(ab)^\delta \equiv 1 \pmod m$ a umocněním obou stran kongruence dostaneme $a^{r\delta}b^{r\delta} \equiv 1 \pmod m$. Protože je r řádem čísla a, je $a^r \equiv 1 \pmod m$, tj. $b^{r\delta} \equiv 1 \pmod m$, a proto $s \mid r\delta$. Z nesoudělnosti r a s plyne $s \mid \delta$. Analogicky dostaneme i $r \mid \delta$, a tedy (opět s využitím nesoudělnosti r, s) $r \cdot s \mid \delta$. Obráceně zřejmě platí $(ab)^{rs} \equiv 1 \pmod m$, proto $\delta \mid rs$. Celkem tedy $\delta = rs$. □

4. Řešení kongruencí o jedné neznámé

Definice. Nechť $m \in \mathbb{N}$, $f(x), g(x) \in \mathbb{Z}[x]$. Zápis

$$f(x) \equiv g(x) \pmod m \tag{17}$$

nazýváme *kongruencí o jedné neznámé* x a rozumíme jím úkol nalézt *množinu řešení*, tj. množinu všech takových čísel $c \in \mathbb{Z}$, pro která $f(c) \equiv g(c) \pmod m$.

Dvě kongruence o jedné neznámé nazveme *ekvivalentní*, mají-li stejnou množinu řešení.

Kongruence (17) je ekvivalentní s kongruencí $\underbrace{f(x) - g(x)}_{\in \mathbb{Z}[x]} \equiv 0 \pmod m$.

Věta 19. *Nechť $m \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$. Pro libovolná $a, b \in \mathbb{Z}$ platí*

$$a \equiv b \pmod m \implies f(a) \equiv f(b) \pmod m.$$

Důkaz. Nechť je $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, kde $c_0, c_1, \ldots, c_n \in \mathbb{Z}$. Protože $a \equiv b \pmod m$, pro každé $i = 1, 2, \ldots, n$ platí podle Věty 12(2)

$$c_i a^i \equiv c_i b^i \pmod m,$$

a tedy sečtením těchto kongruencí pro $i = 1, 2, \ldots, n$ a kongruence $c_0 \equiv c_0 \pmod m$ dostaneme

$$c_n a^n + a_{n-1}a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 \pmod m,$$

tj. $f(a) \equiv f(b) \pmod m$. □

Důsledek. *Množina řešení libovolné kongruence modulo m je sjednocením některých zbytkových tříd modulo m.*

Definice. *Počtem řešení* kongruence o jedné neznámé modulo m rozumíme počet zbytkových tříd modulo m obsahujících řešení této kongruence.

Příklad. (1) Kongruence $2x \equiv 3 \pmod 3$ má jedno řešení (modulo 3).

(2) Kongruence $10x \equiv 15 \pmod{15}$ má pět řešení (modulo 15).

(3) Kongruence z příkladu (1) a (2) jsou ekvivalentní.

4.1. Lineární kongruence o jedné neznámé.

Věta 20. *Nechť* $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. *Označme* $d = (a, m)$. *Pak kongruence*

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

(o jedné neznámé x*) má řešení právě tehdy, když* $d \mid b$.

V případě, kdy $d \mid b$*, má tato kongruence právě* d *řešení (modulo* m*).*

Důkaz. Dokážeme nejprve, že uvedená podmínka je nutná. Je-li celé číslo c řešením této kongruence, pak nutně $m \mid a \cdot c - b$. Pokud přitom $d = (a, m)$, pak protože $d \mid m$ i $d \mid a \cdot c - b$ a $d \mid a \cdot c - (a \cdot c - b) = b$.

Obráceně dokážeme, že pokud $d \mid b$, pak má daná kongruence právě d řešení modulo m. Označme $a_1, b_1 \in \mathbb{Z}$ a $m_1 \in \mathbb{N}$ tak, že $a = d \cdot a_1$, $b = d \cdot b_1$ a $m = d \cdot m_1$. Řešená kongruence je tedy ekvivalentní s kongruencí

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

kde $(a_1, m_1) = 1$. Tuto kongruenci můžeme vynásobit číslem $a_1^{\varphi(m_1)-1}$ a díky Eulerově větě obdržíme

$$x \equiv b_1 \cdot a_1^{\varphi(m_1)-1} \pmod{m_1}.$$

Tato kongruence má jediné řešení modulo m_1 a tedy $d = m/m_1$ řešení modulo m. □

Následující příklad ukáže, že postup uvedený v důkazu věty obvykle není tím nejefektivnějším – s výhodou lze použít jak Bezoutovu větu, tak ekvivalentní úpravy řešené kongruence.

Příklad. Řešte $39x \equiv 41 \pmod{47}$

Řešení. (1) Nejprve využijeme Eulerovu větu.

Protože $(39, 47) = 1$, platí

$$39^{\varphi(47)} = 39^{46} \equiv 1 \pmod{47},$$

tj.

$$\underbrace{39^{45} \cdot 39}_{39^{46} \equiv 1} x \equiv 39^{45} \cdot 41 \pmod{47},$$

z čehož už dostáváme

$$x \equiv 39^{45} \cdot 41 \pmod{47}.$$

Úplné řešení vyžaduje ještě vypočtení zbytku po dělení čísla $39^{45} \cdot 41$ číslem 47, ale to již jistě laskavý čtenář zvládne sám a zjistí výsledek $x \equiv 36 \pmod{47}$

(2) Další možností je využít Bezoutovu větu.
Euklidovým algoritmem pro vypočtení $(39, 47)$ dostáváme

$$\begin{aligned} 47 &= 1 \cdot 39 + 8 \\ 39 &= 4 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \end{aligned}$$

Z čehož zpětným odvozením dostáváme

$$\begin{aligned} 1 &= 8 - 7 = 8 - (39 - 4 \cdot 8) = 5 \cdot 8 - 39 = \\ &= 5 \cdot (47 - 39) - 39 = 5 \cdot 47 - 6 \cdot 39. \end{aligned}$$

Uvážíme-li tuto rovnost modulo 47, dostaneme

$$\begin{aligned} 1 &\equiv -6 \cdot 39 \pmod{47} \quad / \cdot 41 \\ 41 &\equiv \underbrace{41 \cdot (-6)} \cdot 39 \pmod{47} \quad / \cdot 41 \\ x &\equiv 41 \cdot (-6) \pmod{47} \\ x &\equiv -246 \pmod{47} \\ x &\equiv 36 \pmod{47} \end{aligned}$$

(3) Obvykle nejrychlejším, ale nejhůře algoritmizovatelným způsobem řešení je metoda takových úprav kongruence, které zachovávají množinu řešení.

$$\begin{aligned} 39x &\equiv 41 \pmod{47} \\ -8x &\equiv -6 \pmod{47} \\ 4x &\equiv 3 \pmod{47} \\ 4x &\equiv -44 \pmod{47} \\ x &\equiv -11 \pmod{47} \\ x &\equiv 36 \pmod{47} \end{aligned}$$

□

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. významnou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

Věta 21 (Wilsonova). *Přirozené číslo $n > 1$ je prvočíslo, právě když*

$$(n-1)! \equiv -1 \pmod{n} \tag{18}$$

Důkaz. Dokážeme nejprve, že pro libovolné složené číslo $n > 4$ platí $n \mid (n-1)!$, tj. $(n-1)! \equiv 0 \pmod{n}$. Nechť $1 < d < n$ je netriviální dělitel n. Je-li $d \neq n/d$, pak protože $1 < d, n/d \leq n-1$, je $n = d \cdot n/d \mid (n-1)!$. Pokud $d = n/d$, tj. $n = d^2$, pak protože je $n > 4$, je i $d > 2$ a $n \mid (d \cdot 2d) \mid (n-1)!$. Pro $n = 4$ snadno dostáváme $(4-1)! \equiv 2 \not\equiv -1 \pmod{4}$.

Nechť je nyní p prvočíslo. Čísla z množiny $\{2, 3, \dots, p-2\}$ seskupíme do dvojic vzájemně inverzních čísel modulo p, resp. dvojic čísel, jejichž součin dává zbytek 1 po dělení p. Pro dané číslo a z této množiny existuje podle předchozí věty jediné řešení kongruence $a \cdot x \equiv 1 \pmod{p}$. Protože $a \neq 0, 1, p-1$, je zřejmé, že rovněž pro řešení c této kongruence platí $c \not\equiv 0, 1, -1 \pmod{p}$. Číslo a nemůže být ve dvojici samo se sebou; kdyby totiž $a \cdot a \equiv 1 \pmod{p}$, pak nutně $a \equiv \pm 1 \pmod{p}$. Součin všech čísel uvedené množiny je tedy tvořen součinem $(p-3)/2$ dvojic (jejichž součin je vždy kongruentní s 1 modulo p). Proto je

$$(p-1)! \equiv 1^{(p-3)/2} \cdot (p-1) \equiv -1 \pmod{p}.$$

$\square$

4.2. Soustavy lineárních kongruencí o jedné neznámé. Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle Věty 20 rozhodnout o řešitelnosti každé z nich. V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{19}$$

Zkoumejme nejprve případ $k = 2$, který – jak uvidíme později – má stěžejní význam pro řešení soustavy (19) s $k > 2$.

Věta 22. *Nechť c_1, c_2 jsou celá čísla, m_1, m_2 přirozená. Označme $d = (m_1, m_2)$. Soustava dvou kongruencí*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{20}$$

v případě $c_1 \not\equiv c_2 \pmod{d}$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod{d}$, pak existuje celé číslo c tak, že $x \in \mathbb{Z}$ splňuje soustavu (19), právě když vyhovuje kongruenci

$$x \equiv c \pmod{[m_1, m_2]}.$$

Důkaz. Má-li soustava (20) nějaké řešení $x \in \mathbb{Z}$, platí nutně $x \equiv c_1 \pmod{d}$, $x \equiv c_2 \pmod{d}$, a tedy i $c_1 \equiv c_2 \pmod{d}$. Odtud plyne, že v případě $c_1 \not\equiv c_2 \pmod{d}$ soustava (20) nemůže mít řešení.

Předpokládejme dále $c_1 \equiv c_2 \pmod{d}$. První kongruenci soustavy (20) vyhovují všechna celá čísla x tvaru $x = c_1 + tm_1$, kde $t \in \mathbb{Z}$ je libovolné. Toto x bude vyhovovat i druhé kongruenci soustavy (20), právě když bude platit $c_1 + tm_1 \equiv c_2 \pmod{m_2}$, tj.

$$tm_1 \equiv c_2 - c_1 \pmod{m_2}.$$

Podle Věty 20 má tato kongruence (vzhledem k t) řešení, neboť $d = (m_1, m_2)$ dělí $c_2 - c_1$, a $t \in \mathbb{Z}$ splňuje tuto kongruenci právě když

$$t \equiv \frac{c_2 - c_1}{d} \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})-1} \left(\mathrm{mod}\ \frac{m_2}{d}\right),$$

tj. právě když

$$t = \frac{c_2 - c_1}{d} \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})-1} + r \cdot \frac{m_2}{d},$$

kde $r \in \mathbb{Z}$ je libovolné. Dosazením

$$x = c_1 + tm_1 = c_1 + (c_2 - c_1) \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})} + r\frac{m_1 m_2}{d} = c + r \cdot [m_1, m_2],$$

kde $c = c_1 + (c_2 - c_1) \cdot (m_1/d)^{\varphi(m_2/d)}$, neboť $m_1 m_2 = d \cdot [m_1, m_2]$. Našli jsme tedy takové $c \in \mathbb{Z}$, že libovolné $x \in \mathbb{Z}$ splňuje soustavu (20), právě když

$$x \equiv c \pmod{[m_1, m_2]},$$

což jsme chtěli dokázat. $\square$

Všimněme si, že důkaz této věty je konstruktivní, tj. udává vzorec, jak číslo c najít. Věta 22 nám tedy dává metodu, jak pomocí jediné kongruence zachytit podmínku, že x vyhovuje soustavě (20). Podstatné je, že tato nová kongruence je téhož tvaru jako obě původní. Můžeme proto tuto metodu aplikovat i na soustavu (19) – nejprve z první a druhé kongruence vytvoříme kongruenci jedinou, které vyhovují právě ta x, která vyhovovala původním dvěma kongruencím, pak z nově vzniklé a z třetí kongruence vytvoříme další atd. Při každém kroku se nám počet kongruencí soustavy sníží o 1, po $k-1$ krocích tedy dostaneme kongruenci jedinou, která nám bude popisovat všechna řešení soustavy (19). Poznamenejme ještě, že číslo c z Věty 22 není nutné určovat pomocí uvedeného vzorce. Můžeme vzít libovolné $t \in \mathbb{Z}$ vyhovující kongruenci

$$t \cdot \frac{m_1}{d} \equiv \frac{c_2 - c_1}{d} \left(\mathrm{mod}\ \frac{m_2}{d}\right)$$

a položit $c = c_1 + tm_1$.

Důsledek (Čínská zbytková věta). *Nechť $m_1, , \dots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná, $a_1, \dots, a_k \in \mathbb{Z}$. Pak platí: soustava*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{21}$$

má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.

Příklad. Řešte systém kongruencí

$$\begin{aligned} x &\equiv -3 \pmod{49} \\ x &\equiv 2 \pmod{11}. \end{aligned}$$

Řešení. První kongruenci splňují právě všechna celá čísla x tvaru $x = -3 + 49t$, kde $t \in \mathbb{Z}$. Dosazením do druhé kongruence dostáváme

$$-3 + 49t \equiv 2 \pmod{11},$$

odkud

$$5t \equiv 5 \pmod{11},$$

tedy, vzhledem k $(5, 11) = 1$, po vydělení pěti

$$t \equiv 1 \pmod{11},$$

neboli $t = 1+11s$ pro libovolné $s \in \mathbb{Z}$. Proto $x = -3+49(1+11s) = 46+539s$, kde $s \in \mathbb{Z}$, což můžeme také zapsat jako $x \equiv 46 \pmod{539}$. $\square$

Příklad. Řešte systém kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

Řešení. Z první kongruence dostáváme $x = 1 + 10t$ pro $t \in \mathbb{Z}$. Dosazením do druhé kongruence získáme

$$1 + 10t \equiv 5 \pmod{18},$$

tedy $10t \equiv 4 \pmod{18}$. Protože $(10, 18) = 2$ dělí číslo 4, má tato kongruence podle věty 4.2 řešení $t \equiv 2 \cdot 5^5 \pmod 9$, přičemž $2 \cdot 5^5 = 10 \cdot 25^2 \equiv 1 \cdot (-2)^2 = 4 \pmod 9$, a tedy $t = 4+9s$, kde $s \in \mathbb{Z}$. Dosazením $x = 1 + 10(4 + 9s) = 41 + 90s$. Z třetí kongruence pak vychází

$$41 + 90s \equiv -4 \pmod{25},$$

tedy $90s \equiv -45 \pmod{25}$. Vydělením pěti (včetně modulu, neboť $5 \mid 25$)

$$18s \equiv -9 \pmod 5,$$

odkud $-2s \equiv 1 \pmod 5$, tedy $2s \equiv 4 \pmod 5$, $s \equiv 2 \pmod 5$, a proto $s = 2 + 5r$, kde $r \in \mathbb{Z}$. Dosazením $x = 41 + 90(2 + 5r) = 221 + 450r$, tedy $x \equiv 221 \pmod{450}$. $\square$

Příklad. Řešte systém kongruencí

$$\begin{aligned} x &\equiv 18 \pmod{25} \\ x &\equiv 21 \pmod{45} \\ x &\equiv 25 \pmod{73}. \end{aligned}$$

Řešení. Z první kongruence $x = 18 + 25t$, kde $t \in \mathbb{Z}$. Dosazením do druhé kongruence

$$18 + 25t \equiv 21 \pmod{45},$$

tedy

$$25t \equiv 3 \pmod{45}.$$

Tato kongruence však podle Věty 20 nemá řešení, neboť $(25, 45) = 5$ nedělí číslo 3. Proto nemá řešení ani celý systém. Tento výsledek bychom také dostali přímo z Věty 22, neboť $18 \not\equiv 21 \pmod{(25, 45)}$.

□

Příklad. Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení. Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a tedy podle Věty 22 má kongruence řešení. Protože $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak. Podle Věty 12 (6) je $x \in \mathbb{Z}$ řešením dané kongruence právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11} \end{aligned} \tag{22}$$

Vyřešíme nyní každou z kongruencí soustavy (22) zvlášť. První z nich je splněna, právě když

$$x \equiv 3 \pmod{4},$$

druhá, právě když

$$46x \equiv 24 \pmod{81},$$

odkud vynásobením dvěma $92x \equiv 48 \pmod{81}$, tj. $11x \equiv -33 \pmod{81}$ a po vydělení jedenácti

$$x \equiv -3 \pmod{81}.$$

Třetí kongruence je splněna, právě když

$$5x \equiv 2 \pmod{11},$$

odkud vynásobením číslem -2 dostaneme $-10x \equiv -4 \pmod{11}$, tedy

$$x \equiv -4 \pmod{11}.$$

Libovolné $x \in \mathbb{Z}$ je tedy řešením soustavy (22), právě když je řešením soustavy

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11} \end{aligned} \tag{23}$$

Z druhé kongruence dostáváme, že $x = -3 + 81t$, kde $t \in \mathbb{Z}$. Dosazením do třetí kongruence soustavy (23) dostaneme

$$-3 + 81t \equiv -4 \pmod{11},$$

tedy $81t \equiv -1 \pmod{11}$, tj. $4t \equiv 32 \pmod{11}$, odkud $t \equiv 8 \pmod{11}$, a proto $t = -3 + 11s$, kde $s \in \mathbb{Z}$. Dosazením $x = -3 + 81(-3 + 11s) = -3 - 3 \cdot 81 + 11 \cdot 81s$ do první kongruence soustavy (23) dostaneme

$$-3 - 3 \cdot 81 + 11 \cdot 81s \equiv 3 \pmod{4},$$

tedy

$$1 + 1 \cdot 1 + (-1) \cdot 1s \equiv 3 \pmod{4},$$

tj. $-s \equiv 1 \pmod{4}$ a proto $s = -1 + 4r$, kde $r \in \mathbb{Z}$. Je tedy

$$x = -3 - 3 \cdot 81 + 11 \cdot 81(-1 + 4r) = -3 - 14 \cdot 81 + 4 \cdot 11 \cdot 81r = -1137 + 3564r,$$

neboli $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence. $\square$

4.3. Kongruence vyšších stupňů. Vraťme se k obecnějšímu případu, kdy na obou stranách kongruence stojí mnohočleny téže proměnné x s celočíselnými koeficienty. Snadno můžeme tuto kongruenci odečtením upravit na tvar

$$F(x) \equiv 0 \pmod{m}, \tag{24}$$

kde $F(x)$ je mnohočlen s celočíselnými koeficienty a $m \in \mathbb{N}$. Popíšeme si jednu sice pracnou, ale univerzální metodu řešení této kongruence, která je založena na následující větě.

Tvrzení 4.1. *Pro libovolný mnohočlen $F(x)$ s celočíselnými koeficienty, přirozené číslo m a celá čísla a, b taková, že $a \equiv b \pmod{m}$, platí $F(a) \equiv F(b) \pmod{m}$.*

Důkaz. Nechť je $F(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, kde $c_0, c_1, \ldots, c_n \in \mathbb{Z}$. Protože $a \equiv b \pmod{m}$, pro každé $i = 1, 2, \ldots, n$ platí podle Věty 12(2)

$$c_i a^i \equiv c_i b^i \pmod{m},$$

a tedy sečtením těchto kongruencí pro $i = 1, 2, \ldots, n$ a kongruence $c_0 \equiv c_0 \pmod{m}$ dostaneme

$$c_n a^n + a_{n-1}a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 \pmod{m},$$

tj. $F(a) \equiv F(b) \pmod{m}$. $\square$

Při řešení kongruence (24) tedy stačí zjistit, pro která celá čísla a, $0 \le a < m$, platí $F(a) \equiv 0 \pmod{m}$. Nevýhodou této metody je její pracnost, která se zvyšuje se zvětšující se hodnotou m. Je-li m složené,

$m = p_1^{n_1} \dots p_k^{n_k}$, kde $p_1, \dots, p_k$ jsou různá prvočísla, a je-li navíc $k > 1$, můžeme nahradit kongruenci (24) soustavou kongruencí

$$\begin{aligned} F(x) &\equiv 0 \pmod{p_1^{n_1}} \\ &\vdots \\ F(x) &\equiv 0 \pmod{p_k^{n_k}}, \end{aligned} \tag{25}$$

která má stejnou množinu řešení, a řešit každou kongruenci této soustavy zvlášť. Tím získáme obecně několik soustav kongruencí (19), které už umíme řešit. Výhoda této metody spočívá v tom, že moduly kongruencí soustavy (25) jsou menší než modul původní kongruence (24).

Příklad. Řešte kongruenci $x^5 + 1 \equiv 0 \pmod{11}$.

Řešení. Označme $F(x) = x^5 + 1$. Pak platí $F(0) = 1$, $F(1) = 2$ a dále platí

$$\begin{aligned} &F(2) = 33 \equiv 0 \pmod{11}, \\ &F(3) = 3^5 + 1 = 9 \cdot 9 \cdot 3 + 1 \equiv (-2)^2 \cdot 3 + 1 = 12 + 1 \equiv 2 \pmod{11}, \\ &F(4) = 4^5 + 1 = 2^{10} + 1 \equiv 1 + 1 = 2 \pmod{11}, \end{aligned}$$

kde jsme využili Fermatovu větu 15, podle které $2^{10} \equiv 1 \pmod{11}$. Podobně dále

$$\begin{aligned} &F(5) = 5^5 + 1 \equiv 16^5 + 1 = 4^{10} + 1 \equiv 1 + 1 = 2 \pmod{11}, \\ &F(6) = 6^5 + 1 \equiv (-5)^5 + 1 \equiv -16^5 + 1 \equiv -4^{10} + 1 \equiv 0 \pmod{11}, \\ &F(7) = 7^5 + 1 \equiv (-4)^5 + 1 = -2^{10} + 1 \equiv -1 + 1 = 0 \pmod{11}, \\ &F(8) = 8^5 + 1 \equiv 2^5 \cdot 2^{10} + 1 \equiv 32 + 1 \equiv 0 \pmod{11}, \\ &F(9) = 9^5 + 1 = 3^{10} + 1 \equiv 1 + 1 = 2 \pmod{11}, \\ &F(10) = 10^5 + 1 \equiv (-1)^5 + 1 = 0 \pmod{11}, \end{aligned}$$

a tedy řešením kongruence $x^5 + 1 \equiv 0 \pmod{11}$ jsou právě všechna x, vyhovující některé z kongruencí $x \equiv 2 \pmod{11}$, $x \equiv 6 \pmod{11}$, $x \equiv 7 \pmod{11}$, $x \equiv 8 \pmod{11}$, $x \equiv 10 \pmod{11}$. □

Příklad. Řešte kongruenci $x^3 - 3x + 5 \equiv 0 \pmod{105}$.

Řešení. Kdybychom postupovali obdobně jako dříve pro $m = 105$, museli bychom spočítat pro $F(x) = x^3 - 3x + 5$ sto pět hodnot $F(0)$, $F(1), \dots, F(104)$. Proto raději rozložíme $105 = 3 \cdot 5 \cdot 7$ a budeme řešit kongruence $F(x) \equiv 0$ postupně pro moduly 3, 5, 7. Platí $F(0) = 5$, $F(1) = 3$, $F(2) = 7$, $F(3) = 23$, $F(-1) = 7$, $F(-2) = 3$, $F(-3) = -13$ (pro snadnější výpočty jsme počítali například $F(-1)$ místo $F(6)$ – využijeme toho, že $F(6) \equiv F(-1) \pmod{7}$ podle předchozího Tvrzení a podobně). Kongruence $F(x) \equiv 0 \pmod{3}$ má tedy řešení $x \equiv 1 \pmod{3}$; kongruence $F(x) \equiv 0 \pmod{5}$ má řešení $x \equiv 0 \pmod{5}$; řešením kongruence $F(x) \equiv 0 \pmod{7}$ jsou $x \in \mathbb{Z}$ splňující $x \equiv 2 \pmod{7}$

nebo $x \equiv -1 \pmod 7$. Zbývá tedy vyřešit dvě soustavy kongruencí:

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 0 \pmod 5, \\ x &\equiv 2 \pmod 7 \end{aligned} \qquad \text{a} \qquad \begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 0 \pmod 5, \\ x &\equiv -1 \pmod 7. \end{aligned}$$

Protože první dvě kongruence jsou u obou soustav stejné, budeme se nejprve zabývat jimi. Ze druhé kongruence dostáváme $x = 5t$ pro $t \in \mathbb{Z}$, dosazením do první

$$5t \equiv 1 \pmod 3,$$

tedy $-t \equiv 1 \pmod 3$, odkud $t = -1 + 3s$ pro $s \in \mathbb{Z}$, odkud $x = -5 + 15s$. Dosaďme nejprve do třetí kongruence první soustavy:

$$-5 + 15s \equiv 2 \pmod 7,$$

odkud $s \equiv 0 \pmod 7$, tj. $s = 7r$ pro $r \in \mathbb{Z}$ a proto $x = -5 + 105r$. Dosadíme-li $x = -5 + 15s$ do třetí kongruence druhé soustavy, dostaneme

$$-5 + 15s \equiv -1 \pmod 7,$$

odkud $s \equiv 4 \pmod 7$, tj. $s = 4 + 7r$ pro $r \in \mathbb{Z}$, a proto $x = -5 + 15(4 + 7r) = 55 + 105r$. Celkem jsou tedy řešením dané kongruence $F(x) \equiv 0 \pmod{105}$ všechna celá čísla x, splňující $x \equiv -5 \pmod{105}$ nebo $x \equiv 55 \pmod{105}$. □

Postup pro řešení kongruencí modulo mocnina prvočísla udává důkaz následující věty.

VĚTA 23 (Henselovo lemmma). *Nechť p je prvočíslo, $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ je takové, že $p \mid f(a), p \nmid f'(a)$. Pak platí: pro každé $n \in \mathbb{N}$ má soustava*

$$\begin{aligned} x &\equiv a \pmod p \\ f(x) &\equiv 0 \pmod{p^n} \end{aligned} \tag{26}$$

právě jedno řešení modulo p^n.

DŮKAZ. Indukcí vzhledem k n. Případ $n = 1$ je zřejmý. Nechť dále $n > 1$ a věta platí pro $n - 1$. Je-li x řešením (26) pro n, je řešením (26) i pro $n - 1$. Libovolné řešení (26) pro n je tedy tvaru

$$x = c_{n-1} + k \cdot p^{n-1}, \quad \text{kde } k \in \mathbb{Z}.$$

Je třeba zjistit, zda $f(c_{n-1} + k \cdot p^{n-1}) \equiv 0 \pmod{p^n}$. Víme, že $p^{n-1} \mid f(c_{n-1} + k \cdot p^{n-1})$ a užijme binomickou větu pro $f(x) = a_m x^m + \cdots + a_1 x + a_0$, kde $a_0, \ldots, a_m \in \mathbb{Z}$. Pak

$$(c_{n-1} + k \cdot p^{n-1})^i \equiv c_{n-1}^i + i \cdot c_{n-1}^{i-1} \cdot kp^{n-1} \pmod{p^n}.$$

Platí tedy

$$f(c_{n-1} + k \cdot p^{n-1}) \equiv f(c_{n-1}) + k \cdot p^{n-1} f'(c_{n-1}),$$

tj.

$$f(c_{n-1}+k\cdot p^{n-1})\equiv 0 \pmod{p^n} \iff$$
$$\iff 0\equiv \frac{f(c_{n-1})}{p^{n-1}}+k\cdot f'(c_{n-1}) \pmod{p}.$$

Protože $c_{n-1}\equiv a \pmod{p}$, dostaneme $f'(c_{n-1})\equiv f'(a)\not\equiv 0 \pmod{p}$, tedy $(f'(c_{n-1}),p)=1$. Užitím Věty 20 o řešitelnosti lineárních kongruencí dostáváme, že existuje právě jedno řešení k (modulo p) této kongruence a protože c_{n-1} bylo podle indukčního předpokladu jediné řešení modulo p^{n-1}, je číslo $c_{n-1}+k\cdot p^{n-1}$ jediným řešením (26) modulo p^n. □

Příklad. Řešte kongruenci $x^4+7x+4\equiv 0 \pmod{27}$.

Řešení. Řešme nejprve tuto kongruenci modulo 3 (např. dosazením) – snadno zjistíme, že řešení je $x\equiv 1 \pmod{3}$. Zapišme řešení ve tvaru $x=1+3t$, kde $t\in\mathbb{Z}$ a řešme kongruenci modulo 9.

$$\begin{aligned}
x^4+7x+4&\equiv 0 \pmod{9}\\
(1+3t)^4+7(1+3t)+4&\equiv 0 \pmod{9}\\
(1+3t)^4+7(1+3t)+4&\equiv 0 \pmod{9}\\
1+4\cdot 3t+7+7\cdot 3t+4&\equiv 0 \pmod{9}\\
33t&\equiv -12 \pmod{9}\\
11t&\equiv -4 \pmod{3}\\
t&\equiv 1 \pmod{3}
\end{aligned}$$

Zapsáním $t=1+3s$, kde $s\in\mathbb{Z}$ dostaneme $x=4+9s$ a po dosazení

$$\begin{aligned}
(4+9s)^4+7(4+9s)+4&\equiv 0 \pmod{27}\\
4^4+4\cdot 4^3\cdot 9s+28+63s+4&\equiv 0 \pmod{27}\\
256\cdot 9s+63s&\equiv -288 \pmod{27}\\
256s+7s&\equiv -32 \pmod{3}\\
2s&\equiv 1 \pmod{3}\\
s&\equiv 2 \pmod{3}
\end{aligned}$$

Celkem dostáváme řešení $x=4+9s=4+9(2+3r)=22+27r$, kde $r\in\mathbb{Z}$, neboli $x\equiv 22 \pmod{27}$. □

Řešení obecných kongruencí vyššího stupně jsme tedy převedli na řešení kongruencí modulo prvočíslo. Ukazuje se, že zde je největší „kámen úrazu“, protože pro tyto kongruence žádný obecný postup (s výjimkou postupu podle Věty 4.1, tj. vyzkoušení všech možností) není znám. Uvedeme alespoň několik obecných tvrzení ohledně řešitelnosti a počtu řešení takových kongruencí a v dalších částech skript podrobnější výsledky v některých speciálních případech.

4.4. Kongruence s prvočíselným modulem.

Věta 24. *Buď p prvočíslo, $f(x) \in \mathbb{Z}[x]$. Libovolná kongruence $f(x) \equiv 0 \pmod{p}$ je ekvivalentní s kongruencí stupně nejvýše $p-1$.*

Věta 25. *Buď p prvočíslo, $f(x) \in \mathbb{Z}[x]$. Má-li kongruence $f(x) \equiv 0 \pmod{p}$ více než $\mathrm{st}(f)$ řešení, pak jsou všechny koeficienty polynomu f násobkem p.*

Důsledek. *(Jiný důkaz Wilsonovy věty) Pro každé prvočíslo p platí*

$$(p-1)! \equiv -1 \pmod{p}.$$

Důkaz. Pro $p = 2$ je tvrzení zřejmé, dále uvažujme jen lichá prvočísla p. Řešením kongruence

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{(p-1)} - 1) \equiv 0 \pmod{p}$$

je podle Malé Fermatovy věty libovolné $a \in \mathbb{Z}$, které není násobkem p, tj. kongruence má $p-1$ řešení. Přitom je ale její stupeň menší než $p-1$, proto jsou podle předchozí věty všechny koeficienty polynomu na levé straně kongruence násobkem p, speciálně absolutní člen, kterým je $(p-1)! + 1$. Tím je Wilsonova věta dokázána. $\square$

4.5. Binomické kongruence a primitivní kořeny. V této části se zaměříme na řešení speciálních typů polynomiálních kongruencí vyššího stupně, tzv. *binomických kongruencí*. Jde o analogii binomických rovnic, kdy polynomem $f(x)$ je dvojčlen $x^n - a$. Snadno se ukáže, že se můžeme omezit na případ, kdy je a nesoudělné s modulem kongruence – v opačném případě totiž vždy můžeme pomocí ekvivalentních úprav kongruenci na tento případ převést nebo rozhodnout, že kongruence není řešitelná.

Příklad. Řešte kongruenci

$$x^2 \equiv 18 \pmod{63}.$$

Řešení. Protože je $(18, 63) = 9$, musí platit $9 \mid x^2$, tj. $3 \mid x$. Položíme-li $x = 3x_1$, $x_1 \in \mathbb{Z}$, dostáváme ekvivalentní kongruenci $x_1^2 \equiv 2 \pmod{7}$, která již splňuje omezení na nesoudělnost modulu a pravé strany kongruence. Podle Věty 25 víme, že má nejvýše 2 řešení a snadno se vidí, že jimi jsou $x_1 \equiv \pm 3 \pmod{7}$, tj. $x_1 \equiv \pm 3, \pm 10, \pm 17, \pm 24, \pm 31, \pm 38, \pm 45, \pm 52, \pm 59 \pmod{63}$. Řešeními původní kongruence jsou tedy $x \equiv 3 \cdot x_1 \pmod{63}$, tj. $x \equiv \pm 9, \pm 12, \pm 30 \pmod{63}$.

Příklad. Řešte kongruenci

$$x^3 \equiv 3 \pmod{18}.$$

Řešení. Protože je $(3, 18) = 3$, nutně $3 \mid x$. Užijeme-li, podobně jako výše, substituci $x = 3 \cdot x_1$, dostáváme kongruenci

$$27x_1^3 \equiv 3 \pmod{18},$$

která zřejmě nemá řešení, protože $(27, 18) \nmid 3$.

Definice. Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Číslo a nazveme *n-tým mocninným zbytkem modulo m*, pokud je kongruence

$$x^n \equiv a \pmod{m}$$

řešitelná. V opačném případě nazveme a *n-tým mocninným nezbytkem modulo m.*

Pro $n = 2, 3, 4$ používáme termíny kvadratický, kubický a bikvadratický zbytek, resp. nezbytek modulo m.

V tomto odstavci ukážeme, jakým způsobem řešit binomické kongruence modulo m, pokud modulo m existují tzv. primitivní kořeny.

Definice. Nechť $m \in \mathbb{N}$. Celé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ nazveme *primitivním kořenem* modulo m, pokud je jeho řád modulo m roven $\varphi(m)$.

Lemma. *Je-li g primitivní kořen modulo m, pak pro každé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ existuje jediné $x_a \in \mathbb{Z}$, $0 \le x_a < \varphi(m)$ s vlastností $g^{x_a} \equiv a \pmod{m}$.*

Funkce $x \to x_a$ se nazývá diskrétní logaritmus, příp. index čísla x (vzhledem k danému m a zafixovanému primitivnímu kořeni g) a je bijekcí mezi množinami
$\{a \in \mathbb{Z};\, (a, m) = 1, 0 < a < m\}$ *a* $\{x \in \mathbb{Z};\, 0 \le x < \varphi(m)\}$.

Důkaz. Stačí ukázat tvrzení o bijekci a protože obě množiny mají stejný počet prvků, stačí dokázat injektivitu uvedeného zobrazení. Předpokládejme, že pro $x, y \in \mathbb{Z}$, $0 \le x, y < \varphi(m)$ je $g^x \equiv g^y \pmod{m}$. Podle Věty 17 pak $x \equiv y \pmod{\varphi(m)}$, tj. $x = y$. $\square$

Později ukážeme, že primitivní kořeny existují „dostatečně často“ na to, aby následující věta řešila všechny potřebné případy.

Věta 26. *Buď $m \in \mathbb{N}$ takové, že modulo m existují primitivní kořeny. Dále nechť $a \in \mathbb{Z}$, $(a, m) = 1$. Pak kongruence*

$$x^n \equiv a \pmod{m}$$

je řešitelná (tj. a je n-tý mocninný zbytek modulo m), právě když

$$a^{\varphi(m)/d} \equiv 1 \pmod{m},$$

kde $d = (n, \varphi(m))$.
Přitom, je-li tato kongruence řešitelná, má právě d řešení.

Důkaz. Nechť g je primitivní kořen modulo m. Pak podle předchozího Lemmatu existuje pro libovolné x nesoudělné s m jediné $y \in \mathbb{Z}$; $0 \le y < \varphi(m)$ tak, že $x \equiv g^y \pmod{m}$, podobně pro dané a existuje jediné $b \in \mathbb{Z}$; $0 \le b < \varphi(m)$ tak, že $a \equiv g^b \pmod{m}$. Řešená binomická kongruence je tedy po této substituci ekvivalentní s kongruencí

$$(g^y)^n \equiv g^b \pmod{m}$$

a s využitím Věty 17 i s lineární kongruencí

$$n \cdot y \equiv b \pmod{\varphi(m)}.$$

Tato kongruence je řešitelná, právě když $d = (n, \varphi(m)) \mid b$ (a je-li řešitelná, pak má d řešení). Zbývá dokázat, že $d \mid b$, právě když $a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

Kongruence $1 \equiv a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d}$ platí, právě když $\varphi(m) \mid \frac{b\varphi(m)}{d}$, a to platí právě když $d \mid b$. □

Důsledek. *Za předpokladů předchozí věty, je-li navíc $(n, \varphi(m)) = 1$, má kongruence $x^n \equiv a \pmod{m}$ vždy řešení, a to jediné. Jinými slovy, umocňování na n-tou (kde n je nesoudělné s $\varphi(m)$) je bijekce na množině $\mathbb{Z}_m^\times$ invertibilních zbytkových tříd modulo m.*

Důkaz. Zřejmý. □

Následující věty nám dávají obecnou informaci o počtu řešení kongruencí podle modulu, kterým je mocnina prvočísla. Jde o speciální případy Henselova lemmatu pro případ binomických kongruencí.

Věta 27. *Buď p prvočíslo, $a \in \mathbb{Z}$, $n \in \mathbb{N}, p \nmid a$, $p \nmid n$. Je-li kongruence $x^n \equiv a \pmod{p}$ řešitelná, je řešitelná i kongruence $x^n \equiv a \pmod{p^\alpha}$ pro libovolné přirozené číslo α a má stejný počet řešení jako kongruence modulo p.*

Důkaz. Plyne z Henselova lemmatu pro kongruenci $f(x) \equiv 0 \pmod{p}$, kde $f(x) = x^n - a$. Pak totiž $f'(x) = n \cdot x^{n-1}$ a pokud $b \in \mathbb{Z}$ splňuje $f(b) \equiv 0 \pmod{p}$, pak jistě $p \nmid b$, a proto $p \nmid f'(b)$.

□

Věta 28. *Buď $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $2 \nmid a$. Označme dále $l \in \mathbb{N}_0$ největší takové, že $2^l \mid n$. Je-li kongruence $x^n \equiv a \pmod{2^{2l+1}}$ řešitelná, je řešitelná i kongruence $x^n \equiv a \pmod{2^\alpha}$ pro libovolné $\alpha \in \mathbb{N}$, $\alpha \geq 2l+1$ a má stejný počet řešení jako kongruence modulo $2l + 1$.*

Důkaz. Prozatím neuveden. □

Poznámka. Uvážíme-li v předchozí větě přirozené číslo $n \equiv 2 \pmod{4}$, pak je $l = 1$. Pro liché a je kongruence $x^n \equiv a \pmod{8}$ řešitelná právě když je $a \equiv 1 \pmod{8}$ (a má 4 řešení). Díky přechozí větě víme, že pro $a \equiv 1 \pmod{8}$ má řešení libovolná kongruence tvaru $x^n \equiv a \pmod{2^\alpha}$ pro $\alpha \geq 3$ a má 4 řešení.

V předchozích odstavcích jsme se zabývali řešitelností binomických kongruencí podle modulů, pro které existuje přirozený kořen. Ve zbytku této části se budeme zabývat tím, pro která čísla primitivní kořeny existují. Postupně dokážeme následující větu:

Věta 29. *Buď $m \in \mathbb{N}$, $m > 1$. Primitivní kořeny modulo m existují právě tehdy, když m splňuje některou z následujících podmínek:*

- *$m = 2$ nebo $m = 4$,*
- *m je mocnina lichého prvočísla*
- *m je dvojnásobek mocniny lichého prvočísla.*

Poznámka. Pokud pro přirozené číslo existují primitivní kořeny, tak jich mezi čísly $1, 2, \dots, m$ existuje právě $\varphi(\varphi(m))$. Je-li totiž g primitivní kořen a $a \in \{1, 2, \dots, \varphi(m)\}$ libovolné, pak g^a je podle Věty 18 řádu $\frac{\varphi(m)}{(a,\varphi(m))}$, což je rovno $\varphi(m)$ právě tehdy, je-li $(a, \varphi(m)) = 1$. Takových a je v množině $\{1, 2, \dots, \varphi(m)\}$ právě $\varphi(\varphi(m))$.

Důkaz Věty provedeme v několika krocích. Snadno je vidět, že primitivní kořen modulo 2 je 1 a modulo 4 je 3. Dále ukážeme, že primitivní kořeny existují modulo libovolné liché prvočíslo (pro ty, kdo si pamatují základy algebry, tak vlastně jiným způsobem dokážeme, že grupa $(\mathbb{Z}_m^\times, \cdot)$ invertibilních zbytkových tříd modulo m je cyklická.

Tvrzení 4.2. *Nechť p je liché prvočíslo. Pak existují primitivní kořeny modulo p.*

Důkaz. Označme $r_1, r_2, \dots, r_{p-1}$ řády čísel $1, 2, \dots, p-1$ modulo p. Buď $\delta = [r_1, r_2, \dots, r_{p-1}]$ nejmenší společný dělitel těchto řádů. Ukážeme, že mezi čisly $1, 2, \dots, p-1$ existuje číslo řádu δ a že $\delta = p - 1$.

Nechť $\delta = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ je rozklad δ na prvočísla. Pro libovolné $s \in \{1, \dots k\}$ existuje $c \in \{1, \dots, p-1\}$ tak, že $q_s^{\alpha_s} \mid r_c$ (jinak by existoval menší společný dělitel čísel $r_1, r_2, \dots, r_{p-1}$ než je δ), tj. ex. $b \in \mathbb{Z}$ tak, že $r_c = b \cdot q_s^{\alpha_s}$. Protože c má řád r_c, má číslo $g_s := c^b$ podle Věty 18 řád $q_s^{\alpha_s}$.

Provedením předchozí úvahy pro libovolné $s \in \{1, \dots k\}$ dostaneme $g_1, \dots, g_k$ a můžeme položit $g := g_1 \cdots g_k$. Podle Lemmatu za Větou 18 dostáváme, že řád g je roven součinu řádů čísel $g_1, \dots, g_k$, tj. číslu $q_1^{\alpha_1} \cdots q_k^{\alpha_k} = \delta$.

Nyní dokážeme, že $\delta = p - 1$. Protože řády čísel $1, 2, \dots, p-1$ dělí δ, dostáváme pro libovolné $x \in \{1, 2, \dots, p-1\}$ vztah $x^\delta \equiv 1 \pmod{p}$. Kongruence stupně δ modulo p má podle Věty 25 nejvýše δ řešení (a podle předchozího má $p-1$ řešení), proto nutně $\delta \geq p - 1$. Přitom $\delta \mid p - 1$ (jakožto řád čísla g), proto zejména $\delta \leq p - 1$, a celkem $\delta = p - 1$. □

Nyní ukážeme, že primitivní kořeny existují dokonce modulo mocniny lichých prvočísel. K tomuto budeme potřebovat dvě pomocná tvrzení.

Lemma. *Buď p liché prvočíslo, $l \geq 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$ platí*

$$(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}.$$

Důkaz. Plyne snadno z binomické věty.

□

LEMMA. *Buď p liché prvočíslo, $l \geq 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$, splňující $p \nmid a$ platí, že řád čísla $1 + ap$ modulo p^l je roven p^{l-1}.*

DŮKAZ. Podle předchozího Lemmatu je

$$(1 + ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}},$$

a uvážíme-li tuto kongruenci modulo p^l, dostaneme $(1 + ap)^{p^{l-1}} \equiv 1 \pmod{p^l}$. Přitom přímo z předchozího Lemmatu a faktu $p \nmid a$ plyne $(1 + ap)^{p^{l-2}} \not\equiv 1 \pmod{p^l}$, což dává požadované. □

TVRZENÍ 4.3. *Buď p liché prvočíslo. Pak pro každé $l \in \mathbb{N}$ existuje primitivní kořen modulo p^l.*

DŮKAZ. Nechť g je primitivní kořen modulo p. Ukážeme, že pokud $g^{p-1} \not\equiv 1 \pmod{p^2}$, je g dokonce primitivním kořenem modulo p^l pro libovolné $l \in \mathbb{N}$. (Pokud by platilo $g^{p-1} \equiv 1 \pmod{p^2}$, pak $(g+p)^{p-1} \equiv 1+(p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}$, a tedy místo g můžeme volit za původní primitivní kořen číslo $g + p$.)

Nechť tedy g splňuje $g^{p-1} \not\equiv 1 \pmod{p^2}$. Pak existuje $a \in \mathbb{Z}$, $p \nmid a$ tak, že $g^{p-1} = 1 + p \cdot a$. Ukážeme, že g je modulo p^l řádu $\varphi(p^l) = (p-1)p^{l-1}$. Buď $n \in \mathbb{N}$ nejmenší číslo, splňující $g^n \equiv 1 \pmod{p^l}$. Podle předchozího Lemmatu je $g^{p-1} = 1 + p \cdot a$ řádu p^{l-1} modulo p^l. Pak ale

$$(g^{p-1})^n = (g^n)^{p-1} \equiv 1 \pmod{p^l} \implies p^{l-1} \mid n.$$

Zároveň z $g^n \equiv 1 \pmod{p}$ plyne $p - 1 \mid n$. Protože jsou čísla $p - 1$ a p^{l-1} nesoudělná, dostáváme $(p-1)p^{l-1} \mid n$. Proto $n = \varphi(p^l)$ a g je tedy primitivní kořen modulo p^l. □

TVRZENÍ 4.4. *Buď p liché prvočíslo a g primitivní kořen modulo p^l pro $l \in \mathbb{N}$. Pak liché z čísel $g, g + p^l$ je primitivním kořenem modulo $2p^l$.*

DŮKAZ. Nechť c je liché přirozené číslo. Pak pro libovolné $n \in \mathbb{N}$ platí $c^n \equiv 1 \pmod{p^l}$, právě když $c^n \equiv 1 \pmod{2p^l}$. Protože $\varphi(2p^l) = \varphi(p^l)$, je každý lichý primitivní kořen modulo p^l rovněž primitivním kořenem modulo $2p^l$. □

Další tvrzení popisuje případ mocnin sudého prvočísla. K tomtu využijeme obdobných pomocných tvrzení jako v případě lichých prvočísel.

LEMMA. *Buď $l \in \mathbb{N}$, $l \geq 3$. Pak $5^{2^{l-3}} \equiv 1 + 2^{l-1} \pmod{2^l}$.*

DŮKAZ. Obdobně jako výše pro $2 \nmid p$. □

LEMMA. *Buď $l \in \mathbb{N}$, $l \geq 3$. Pak řád čísla 5 modulo 2^l je 2^{l-2}.*

DŮKAZ. Snadný z předchozího Lemmatu. □

TVRZENÍ 4.5. *Nechť $l \in \mathbb{N}$. Primitivní kořeny existují modulo 2^l právě tehdy, když $l \leq 2$.*

Důkaz. Buď $l \geq 3$. Pak množina

$$S = \{(-1)^a \cdot 5^b; a \in \{0,1\}, 0 \leq b < 2^{l-2}; b \in \mathbb{Z}\}$$

tvoří redukovanou soustavu zbytků modulo 2^l (má totiž $\varphi(2^l)$ prvků o kterých se snadno ukáže, že jsou po dvou nekongruentní modulo 2^l).

Přitom zřejmě (s využitím předchozího Lemmatu) řád každého prvku S dělí 2^{l-2}, proto v této (a tedy ani v žádné jiné) redukované soustavě nemůže existovat prvek řádu $\varphi(2^l) = 2^{l-1}$. □

Posledním kamínkem do mozaiky tvrzení, která společně dokazují Větu 29 je tvrzení popisující neexistenci primitivních kořenů pro složená čísla, která nejsou mocninou prvočísla (ani jejím dvojnásobkem).

Tvrzení 4.6. *Nechť $m \in \mathbb{N}$ je dělitelné alespoň 2 prvočísly a není dvojnásobkem mocniny lichého prvočísla. Pak modulo m neexistují primitivní kořeny.*

Důkaz. Buď rozklad m na prvočísla tvaru $2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde $\alpha \in \mathbb{N}_0, \alpha_i \in \mathbb{N}, 2 \nmid p_i$ a buď platí $k \geq 2$ nebo $k \geq 1$ a $\alpha \geq 2$. Označíme-li $\delta = [\varphi(2^\alpha), \varphi(p_1^{\alpha_1}), \ldots, \varphi(p_1^{\alpha_1})]$, pak se snadno vidí, že $\delta < \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_1^{\alpha_1}) = \varphi(m)$ a že pro libovolné $a \in \mathbb{Z}$, $(a,m) = 1$ platí $a^\delta \equiv 1 \pmod m$. Proto modulo m neexistují primitivní kořeny. □

Nyní máme dokázáno tvrzení přesně charakterizující ty moduly, pro které existují primitivní kořeny. Obecně je ale pro daný modul nalezení primitivního kořene velmi výpočetně náročná operace. Následující věta nám udává ekvivalentní podmínku pro to, aby zkoumané číslo bylo primitivním kořenem, jejíž ověření je o něco snažší než přímý výpočet řádu tohoto čísla.

Věta 30. *Buď m takové, že modulo m existují primitivní kořeny. Zapišme $\varphi(m) = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$. Pak pro libovolné $g \in \mathbb{Z}$, $(g,m) = 1$ platí, že g je primitivní kořen modulo m, právě když*

$$g^{\frac{\varphi(m)}{q_1}} \not\equiv 1 \pmod m, \ldots, g^{\frac{\varphi(m)}{q_k}} \not\equiv 1 \pmod m.$$

Důkaz. Pokud by platila některá z uvedených kongruencí, znamenalo by to, že řád g je menší než $\varphi(m)$.

Obráceně, pokud g není primitivní kořen, pak existuje $d \in \mathbb{N}$, $d \mid \varphi(m)$, kde $d < \varphi(m)$ a $g^d \equiv 1 \pmod m$. Je-li $u = \frac{\varphi(m)}{d} > 1$, nutně existuje $i \in \{1, \ldots, k\}$ tak, že $q_i \mid u$. Pak ale

$$g^{\frac{\varphi(m)}{q_i}} = g^{d \cdot \frac{u}{q_i}} \equiv 1 \pmod m.$$

□

Příklad. Postupně určíme primitivní kořeny modulo $41, 41^2$ a $2 \cdot 41^2$.

Řešení. Protože $\varphi(41) = 40 = 2^3 \cdot 5$, je libovolné celé číslo g, které je s 41 nesoudělné, primitivním kořenem modulo 41 právě tehdy, když

$$g^{20} \not\equiv 1 \pmod{41} \wedge g^8 \not\equiv 1 \pmod{41}.$$

$$\begin{aligned}
g = 2: \quad & 2^8 = 2^5 \cdot 2^3 \equiv -9 \cdot 8 \equiv 10 \pmod{41} \\
& 2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41} \\
g = 3: \quad & 3^8 = (3^4)^2 \equiv (-1)^2 = 1 \pmod{41} \\
g = 4: \quad & \text{řád } 4 = 2^2 \text{ vždy dělí řád } 2 \\
g = 5: \quad & 5^8 = (5^2)^4 \equiv (-2^4)^4 = 2^{16} = (2^8)^2 \equiv 10^2 \equiv 18 \pmod{41} \\
& 5^{20} = (5^2)^{10} \equiv (-2^4)^{10} = 2^{40} = (2^{20})^2 \equiv 1 \pmod{41} \\
g = 6: \quad & 6^8 = 2^8 \cdot 3^8 \equiv 10 \cdot 1 = 10 \pmod{41} \\
& 6^{20} = 2^{20} \cdot 3^{20} \equiv 2^{20} \cdot (3^8)^2 \cdot 3^4 \equiv 1 \cdot 1 \cdot (-1) = -1 \pmod{41}
\end{aligned}$$

Dokázali jsme tak, že 6 je (nejmenší kladný) primitivní kořen modulo 41 (pokud by nás zajímaly i ostatní primitivní kořeny modulo 41, tak bychom je dostali umocněním 6 na všechna čísla od 1 do 40, která jsou se 40 nesoudělná – je jich právě $\varphi(40) = \varphi(2^3 \cdot 5) = 16$ a jsou jimi mezi tyto zbytky modulo 41: $\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$.

Dokážeme-li nyní, že $6^{40} \not\equiv 1 \pmod{41^2}$, budeme vědět, že 6 je i primitivním kořenem modulo libovolná mocnina 41 (pokud bychom „měli smůlu“ a $6^{40} \equiv 1 \pmod{41^2}$, pak by primitivním kořenem modulo 41^2 bylo číslo $47 = 6 + 41$). Při ověření podmínky si vypomůžeme několika triky (tzv. modulární reprezentace čísel), abychom se obešli bez manipulace s velkými čísly.

Nejprve vypočtěme zbytek po dělení 6^8 číslem 41^2; k tomu se nám bude hodit vypočítat zbytek po dělení čísel 2^8 a 3^8:

$$\begin{aligned}
2^8 &= 256 = 6 \cdot 41 + 10 \\
3^8 &= (3^4)^2 = (2 \cdot 41 - 1)^2 \equiv -4 \cdot 41 + 1 \pmod{41^2} \\
\text{Pak } 6^8 &= 2^8 \cdot 3^8 \equiv (6 \cdot 41 + 10)(-4 \cdot 41 + 1) \equiv \\
&\equiv -34 \cdot 41 + 10 \equiv 7 \cdot 41 + 10 \pmod{41^2} \\
\text{a } 6^{40} &= (6^8)^5 \equiv (7 \cdot 41 + 10)^5 \equiv (10^5 + 5 \cdot 7 \cdot 41 \cdot 10^4) = \\
&= 10^4(10 + 35 \cdot 41) \equiv (-2 \cdot 41 - 4)(-6 \cdot 41 + 10) \equiv \\
&\equiv (4 \cdot 41 - 40) = 124 \not\equiv 1 \pmod{41^2}.
\end{aligned}$$

Přitom jsme využili toho, že $10^4 = 6 \cdot 41^2 - 86$, tj. $10^4 \equiv -2 \cdot 41 - 4 \pmod{41^2}$.

Je tedy 6 primitivním kořenem modulo 41^2 a protože je to sudé číslo, je primitivním kořenem modulo $2\cdot 41^2$ číslo $1687 = 6+41^2$ (nejmenším kladným primitivním kořenem modulo $2\cdot 41^2$ je přitom číslo 7).

4.6. Kvadratické kongruence a Legendreův symbol. Naším úkolem bude najít jednodušší podmínku, jak zjistit, jestli je řešitelná (a případně, kolik má řešení) kvadratická kongruence

$$ax^2 + bx + c \equiv 0 \pmod{m}.$$

Z obecné teorie, uvedené v předchozích odstavcích, je snadné vidět, že k rozhodnutí, je-li tato kongruence řešitelná, stačí určit, je-li řešitelná (binomická) kongruence

$$x^2 \equiv a \pmod{p}, \tag{27}$$

kde p je liché prvočíslo a a číslo s ním nesoudělné.

Pro určení řešitelnosti kongruence (27) můžeme samozřejmě využít Větu 26, její využití ale často naráží na výpočetní složitost, proto se v kvadratickém případě snažíme najít kritérium jednodušší na výpočet.

Příklad. Určete počet řešení kongruence $x^2 \equiv 219 \pmod{383}$.

Řešení. Protože 383 je prvočíslo a $(2, \varphi(383)) = 2$, z Věty 26 plyne, že daná kongruence je řešitelná (a má 2 řešení), právě tehdy, když $219^{\frac{383}{2}} = 219^{191} \equiv 1 \pmod{383}$. Ověření platnosti není bez použití výpočetní techniky snadné (i když je to pořád ještě „na papíře“ vyčíslitelné). Závěrem této části tuto podmínku ověříme s pomocí Legendreova symbolu daleko snadněji.

Definice. Nechť je p liché prvočíslo. *Legendreův symbol* definujeme předpisem

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a,\ a \text{ je kvadratický zbytek modulo } p, \\ 0 & p \mid a, \\ -1 & p \nmid a,\ a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Příklad. Protože je kongruence $x^2 \equiv 1 \pmod{p}$ řešitelná pro libovolné liché prvočíslo p, je $(1/p) = 1$.

$(-1/5) = 1$, protože kongruence $x^2 \equiv -1 \pmod{5}$ je ekvivalentní s kongruencí $x^2 \equiv 4 \pmod{5}$, jejímiž řešeními jsou $x \equiv \pm 2 \pmod{5}$.

Lemma. *Nechť p je liché prvočíslo, $a, b \in \mathbb{Z}$ libovolná. Pak platí:*
1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Důkaz. ad 1. Pro $p \mid a$ zřejmé, pokud je a kvadratický zbytek modulo p, pak tvrzení plyne z Věty 26. Z téže věty plyne, že v případě kvadratického nezbytku je $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Pak ale, protože $p \mid$

$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$ nutně $p \mid a^{\frac{p-1}{2}} + 1$, tj. $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

ad 2. Podle 1. dostáváme

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Protože jsou hodnoty Legendreova symbolu z množiny $\{-1, 0, 1\}$, plyne z kongruence $(ab/p) \equiv (a/p)(b/p) \pmod{p}$ přímo rovnost.

ad 3. Zřejmé z definice. □

Důsledek. *1. V libovolné redukované soustavě zbytků modulo p je stejný počet kvadratických zbytků a nezbytků.*

2. Součin dvou kvadratických zbytků je zbytek, součin dvou nezbytků je zbytek, součin zbytku a nezbytku je nezbytek.

3. $(-1/p) = (-1)^{\frac{p-1}{2}}$, tj. kongruence $x^2 \equiv -1 \pmod{p}$ je řešitelná právě tehdy, když $p \equiv 1 \pmod{4}$.

Důkaz. ad 1. Kvadratické zbytky získáme tak, že všechny prvky redukované soustavy zbytků umocníme na druhou. Těchto prvků je $p-1$, přitom druhé mocniny 2 prvků jsou spolu kongruentní právě tehdy, když je součet těchto prvků násobkem p. Máme tedy právě $\frac{p-1}{2}$ kvadratických zbytků, a tedy rovněž $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ kvadratických nezbytků modulo p.

ad 2. Tvrzení je zřejmé z předchozího lemmatu. Předpoklad, že p je prvočíslo je podstatný – pro složená čísla je kvadratických nezbytků více než zbytků (viz dále část o Jacobiho symbolu).

ad 3. Zřejmé. □

Již s využitím těchto základních tvrzení o hodnotách Legendreova symbolu jsme schopni dokázat větu o nekonečnosti počtu prvočísel tvaru $4k + 1$.

Tvrzení 4.7. *Prvočísel tvaru $4k + 1$ je nekonečně mnoho.*

Důkaz. Sporem. Předpokládejme, že $p_1, p_2, \dots, p_l$ jsou všechna prvočísla tvaru $4k+1$ a uvažme číslo $N = (2p_1 \cdots p_l)^2 + 1$. Toto číslo je opět tvaru $4k + 1$. Pokud je N prvočíslo, jsme hotovi (protože je jistě větší než kterékoli z $p_1, p_2, \dots, p_l$), pokud je složené, musí existovat prvočíslo p, dělící N. Zřejmě přitom žádné z $p_1, p_2, \dots, p_l$ není dělitelem N, proto stačí dokázat, že p je rovněž tvaru $4k + 1$. Protože ale $(2p_1 \cdots p_l)^2 \equiv -1 \pmod{p}$, dostáváme, že $(-1/p) = 1$, a to platí právě tehdy, je-li $p \equiv 1 \pmod{4}$. □

Nyní odvodíme další pravidla pro výpočet Legendreova symbolu.

Uvažujme množinu S nejmenších zbytků (v absolutní hodnotě) modulo p. Je-li p prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$, pak označíme $\mu_p(a)$ počet záporných nejmenších zbytků (v absolutní hodnotě) čísel

$$1 \cdot a, 2 \cdot a, \dots, \frac{p-1}{2} \cdot a,$$

tj. pro každé z těchto čísel určíme, se kterým číslem z množiny S je kongruentní a spočítáme počet záporných z nich.

Poznámka. Obvykle budou p a a zafixované, potom budeme místo $\mu_p(a)$ psát jen μ.

Příklad. Vypočtěte hodnotu μ pro $p = 11$, $a = 3$.

Řešení. $S = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}$. Protože $1 \cdot 3 \equiv 3, 2 \cdot 3 \equiv -5, 3 \cdot 3 \equiv -2, 4 \cdot 3 \equiv 1, 5 \cdot 3 \equiv 4 \pmod{11}$, dostáváme $\mu = 2$.

Lemma (Gaussovo). *Je-li p prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$, pak*

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

Důkaz. Pro každé $i \in \{1, 2, \dots, \frac{p-1}{2}\}$ určíme $m_i \in \{1, 2, \dots, \frac{p-1}{2}\}$ tak, že $i \cdot a \equiv \pm m_i \pmod{p}$. Snadno se vidí, že pokud $k, l \in \{1, 2, \dots, \frac{p-1}{2}\}$ jsou různá, jsou různé i hodnoty m_k, m_l ($m_k = m_l \implies k \cdot a \equiv \pm l \cdot a \pmod{p} \implies k \equiv \pm l \pmod{p}$, což nelze jinak, než že $k = l$).

Proto splývají množiny $\{1, 2, \dots, \frac{p-1}{2}\}$ a $\{m_1, m_2, \dots, m_{\frac{p-1}{2}}\}$. Vynásobením kongruencí

$$\begin{aligned} 1 \cdot a &\equiv \pm m_1 \pmod{p} \\ 2 \cdot a &\equiv \pm m_2 \pmod{p} \\ &\cdots\cdots \\ \frac{p-1}{2} \cdot a &\equiv \pm m_{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

dostáváme

$$\frac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \equiv (-1)^\mu \cdot \frac{p-1}{2}! \pmod{p}$$

(mezi pravými stranami je jich právě μ záporných). Po vydělení obou stran číslem $(p-1/2)!$ dostáváme vzhledem k tomu, že

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

tvrzení. $\square$

S využitím Gaussova lemmatu dokážeme hlavní větu této části, tzv. *zákon kvadratické reciprocity.*

Věta 31. *Nechť p, q jsou lichá prvočísla. Pak*
1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Důkaz. Věta se v tomto tvaru uvádí zejména proto, že pomocí těchto tří vztahů a základních pravidel pro úpravy Legendreova symbolu jsme schopni vypočítat hodnotu (a/p) pro libovolné celé číslo a. Tvrzení 1. máme přitom již dokázáno, v dalším nejprve odvodíme mezivýsledek, který využijeme k důkazu částí 2. a 3. Poznamenejme rovněž, že v literatuře existuje mnoho různých důkazů této věty, obvykle ovšem využívajících (zejména u těch stručnějších z nich) hlubších znalostí z algebraické teorie čísel.

Nechť je dále $a \in \mathbb{Z}$, $p \nmid a$, $k \in \mathbb{N}$ a nechť $[x]$ (resp. $\langle x \rangle$) značí celou (resp. necelou) část reálného čísla x. Pak

$$\left[\frac{2ak}{p}\right] = \left[2\left[\frac{ak}{p}\right] + 2\left\langle\frac{ak}{p}\right\rangle\right] = 2\left[\frac{ak}{p}\right] + \left[2\left\langle\frac{ak}{p}\right\rangle\right].$$

Tento výraz je lichý právě tehdy, když je $\langle \frac{ak}{p} \rangle > \frac{1}{2}$, tj. právě tehdy, je-li nejmenší zbytek (v absolutní hodnotě) čísla ak modulo p záporný (zde by měl pozorný čtenář zaznamenat návrat od výpočtů zdánlivě nesouvisejících výrazů k podmínkám souvisejícím s Legendreovým symbolem).

Proto je

$$\left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{2ak}{p}]}.$$

Je-li navíc a **liché**, je $a + p$ číslo sudé a dostáváme

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{2}{p}\right)^2 \cdot \left(\frac{\frac{a+p}{2}}{p}\right) =$$
$$= (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{(a+p)k}{p}]} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{ak}{p}]} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} k}.$$

Celkem tak dostáváme (pro liché a)

$$\left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{ak}{p}]} \cdot (-1)^{\frac{p^2-1}{8}}, \tag{28}$$

což pro $a = 1$ dává požadované tvrzení z bodu 2.

Podle již dokázané části 2 a ze vztahu (28) dostáváme pro lichá čísla a

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{ak}{p}]}.$$

Uvažme nyní pro daná prvočísla $p \neq q$ množinu

$$T = \{q \cdot x;\ x \in \mathbb{Z},\ 1 \le x \le (p-1)/2\} \times \{p \cdot y;\ y \in \mathbb{Z},\ 1 \le y \le (q-1)/2\}.$$

Zřejmě je $|T| = \frac{p-1}{2} \cdot \frac{q-1}{2}$ a ukážeme, že rovněž

$$(-1)^{|T|} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{pk}{q}]} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{qk}{p}]}, \tag{29}$$

čímž budeme vzhledem k předchozímu hotovi.

Protože pro žádná x, y z přípustného rozsahu nemůže nastat rovnost $qx = py$, můžeme množinu T rozložit na dvě disjunktní podmnožiny T_1 a T_2 tak, že $T_1 = T \cap \{[u, v]; u, v \in \mathbb{Z}, u < v\}$, $T_2 = T \setminus T_1$. Zřejmě je T_1 počet dvojic $[qx, py]$, kde $x < \frac{p}{q}y$. Protože $\frac{p}{q}y \leq \frac{p}{q} \cdot \frac{q-1}{2} < \frac{p}{2}$, je $[\frac{p}{q}y] \leq \frac{p-1}{2}$. Pro pevné y tedy v T_1 leží právě ty dvojice $[qx, py]$, pro které $1 \leq x \leq [\frac{p}{q}y]$, a tedy $|T_1| = \sum_{y=1}^{(q-1)/2} [\frac{p}{q}y]$. Analogicky $|T_2| = \sum_{x=1}^{(p-1)/2} [\frac{q}{p}x]$.

Proto $\left(\frac{p}{q}\right) = (-1)^{|T_1|}$ a $\left(\frac{q}{p}\right) = (-1)^{|T_2|}$ a zákon kvadratické reciprocity je dokázán. □

Důsledek. *1. -1 je kvadratický zbytek pro prvočísla p splňující $p \equiv 1 \pmod 4$ a nezbytek pro prvočísla splňující $p \equiv 3 \pmod 4$.*

2. 2 je kvadratický zbytek pro prvočísla p splňující $p \equiv \pm 1 \pmod 8$ a nezbytek pro prvočísla splňující $p \equiv \pm 3 \pmod 8$.

3. Je-li $p \equiv 1 \pmod 4$ nebo $q \equiv 1 \pmod 4$, je $(p/q) = (q/p)$, jinak (tj. $p \equiv q \equiv 3 \pmod 4$) je $(p/q) = -(q/p)$.

Příklad. Určete $\left(\frac{79}{101}\right)$.

Řešení.

$$\begin{aligned}
\left(\frac{79}{101}\right) &= \left(\frac{101}{79}\right) && \textit{neboť 101 dává po dělení 4 zbytek 1}\\
&= \left(\frac{22}{79}\right)\\
&= \left(\frac{2}{79}\right) \cdot \left(\frac{11}{79}\right)\\
&= \left(\frac{11}{79}\right) && \textit{neboť 79 dává pod dělení 8 zbytek -1}\\
&= (-1)\left(\frac{79}{11}\right) && \textit{neboť 11 i 79 dávají pod dělení 4 zbytek 3}\\
&= (-1)\left(\frac{2}{11}\right) = 1 && \textit{neboť 11 dává pod dělení 8 zbytek 3}
\end{aligned}$$

4.7. Jacobiho symbol. Vyčíslení Legendreova symbolu (jak jsme viděli i v předchozím příkladu) umožňuje používat zákon kvadratické reciprocity jen na prvočísla a nutí nás tak provádět faktorizaci čísel na prvočísla, což je výpočetně velmi náročná operace. Toto lze obejít rozšířením definice Legendreova symbolu na tzv. *Jacobiho symbol* s podobnými vlastnostmi.

Definice. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$. Nechť $b = p_1 p_2 \cdots p_k$ je rozklad b na (lichá) prvočísla (výjimečně neseskupujeme stejná prvočísla do mocniny, ale vypisujeme každé zvlášť, např. $135 = 3\cdot 3\cdot 3\cdot 5$). Symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

se nazývá *Jacobiho symbol*.

Dále ukážeme, že Jacobiho symbol má podobné vlastnosti jako Legendreův symbol (s jednou podstatnou odchylkou). Neplatí totiž obecně, že z $(a/b) = 1$ plyne řešitelnost kongruence $x^2 \equiv a \pmod{b}$.

Příklad.

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$$

a přitom kongruence

$$x^2 \equiv 2 \pmod{15}$$

není řešitelná (není totiž řešitelná kongruence $x^2 \equiv 2 \pmod 3$ a není ani řešitelná kongruence $x^2 \equiv 2 \pmod 5$).

Doplnit tvrzení o Jacobiho symbolu a aplikace

5. Diofantické rovnice

Už ve třetím století našeho letopočtu se řecký matematik Diofantos zabýval řešením rovnic, ve kterých za řešení připouštěl jen celá čísla. Není se čemu divit, vždyť v mnoha praktických úlohách, vedoucích k rovnicím, nemusí mít neceločíselná řešení rozumnou interpretaci. (Jde například o úlohu, jak pomocí pětilitrové a sedmilitrové nádoby odměřit do třetí nádoby osm litrů vody, která vede na rovnici $5x + 7y = 8$.) Na Diofantovu počest se rovnice, ve kterých hledáme jen celočíselná řešení, nazývají diofantické.

Pro řešení těchto rovnic bohužel neexistuje žádná univerzální metoda. Dokonce neexistuje ani metoda (jinými slovy algoritmus), která by určila, jestli má obecná polynomiální diofantická rovnice řešení. Tato otázka je známá pod názvem *10. Hilbertův problém* a důkaz neexistence algoritmu podal Юрий Матиясевич (Yuri Matiasevič) v roce 1970 (viz elementárně psaný text [**1**]).

Přesto však uvedeme několik nejobvyklejších metod, které v řadě konkrétních případů povedou k výsledku.

5.1. Lineární diofantické rovnice.

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{30}$$

kde $x_1, \ldots, x_n$ jsou neznámé, $a_1, \ldots, a_n, b$ daná celá čísla. Budeme předpokládat, že $a_i \neq 0$ pro každé $i = 1, \ldots, n$ (je-li $a_i = 0$, pak neznámá x_i z rovnice „zmizí“). K řešení těchto rovnic je možné užít kongruencí. Nejprve si všimněme, kdy má rovnice (30) řešení. Jestliže číslo b není dělitelné číslem $d = (a_1, \ldots, a_n)$, nemůže mít (30) žádné řešení, protože pro libovolná celá čísla $x_1, \ldots, x_n$ je levá strana (30) dělitelná číslem d. Jestliže naopak $d \mid b$, můžeme celou rovnici (30) vydělit číslem d. Dostaneme tak ekvivalentní rovnici

$$a'_1x_1 + a'_2x_2 + \cdots + a'_nx_n = b',$$

kde $a'_i = a_i/d$ pro $i = 1, \ldots, n$ a $b' = b/n$. Přitom platí

$$d \cdot (a'_1, \ldots, a'_n) = (da'_1, \ldots, da'_n) = (a_1, \ldots, a_n) = d,$$

a tedy $(a'_1, \ldots, a'_n) = 1$. V následující větě ukážeme, že taková rovnice má vždy řešení, a proto naše úvahy můžeme shrnout takto: rovnice (30) má celočíselné řešení, právě když číslo b je dělitelné největším společným dělitelem čísel $a_1, a_2, \ldots, a_n$.

Věta 32. *Nechť $n \geq 2$. Rovnice*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{31}$$

kde $a_1, a_2, \ldots, a_n, b$ jsou celá čísla taková, že $(a_1, \ldots, a_n) = 1$, má vždy celočíselné řešení. Všechna celočíselná řešení této rovnice je možné popsat pomocí $n - 1$ celočíselných parametrů.

Důkaz. Provedeme indukcí vzhledem k počtu n neznámých x_i v rovnici (31).

Je výhodné formálně začít s případem $n = 1$, kdy podmínka $(a_1) = 1$ znamená, že $a_1 = \pm 1$. Tehdy rovnice (31) má tvar buď $x_1 = b$, nebo $-x_1 = b$, a tedy jediné řešení, které zřejmě nezávisí na žádném parametru, což odpovídá tomu, že $n - 1 = 0$.

Předpokládejme, že $n \geq 2$ a že věta platí pro rovnice o $n - 1$ neznámých; dokážeme ji pro rovnici (31) o n neznámých. Označme $d = (a_1, \dots, a_{n-1})$. Pak libovolné řešení $x_1, \dots, x_n$ rovnice (31) triviálně splňuje kongruenci

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{d}.$$

Vzhledem k tomu, že d je společný dělitel čísel $a_1, \dots, a_{n-1}$, je tato kongruence tvaru

$$a_nx_n \equiv b \pmod{d}.$$

Protože platí, že $(d, a_n) = (a_1, \dots, a_{n-1}, a_n) = 1$, má podle věty 20 tato kongruence řešení

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

kde c je vhodné celé číslo, neboli $x_n = c + d \cdot t$, kde $t \in \mathbb{Z}$ je libovolné. Dosazením do (31) a úpravou dostaneme

$$a_1x_1 + \cdots + a_{n-1}x_{n-1} = b - a_nc - a_ndt.$$

Protože $a_nc \equiv b \pmod{d}$, je číslo $(b - a_nc)/d$ celé a poslední rovnici můžeme vydělit číslem d. Dostaneme pak rovnici

$$a'_1x_1 + \cdots + a'_{n-1}x_{n-1} = b',$$

kde $a'_i = a_i/d$ pro $i = 1, \dots, n-1$ a $b' = ((b - a_nc)/d) - a_nt$. Protože

$$(a'_1, \dots, a'_{n-1}) = (da'_1, \dots, da'_{n-1}) \cdot \tfrac{1}{d} = (a_1, \dots, a_{n-1}) \cdot \tfrac{1}{d} = 1,$$

podle indukčního předpokladu má tato rovnice pro libovolné $t \in \mathbb{Z}$ řešení popsatelné pomocí $n - 2$ celočíselných parametrů. Přidáme-li k tomuto řešení podmínku $x_n = c + dt$, dostaneme řešení rovnice (31) popsané pomocí $n - 2$ původních parametrů a nového parametru t. Důkaz indukcí je hotov. $\square$

Metodu z důkazu věty 32 použijeme na řešení následujících diofantických rovnic, v nichž z důvodů přehlednosti zápisu budeme neznámé značit $x, y, z, \dots$ místo $x_1, x_2, x_3, \dots$.

Příklad. $5x + 7y = 8$.

Řešení. Libovolné řešení této rovnice musí splňovat kongruenci

$$5x + 7y \equiv 8 \pmod{5},$$

tedy $2y \equiv -2 \pmod{5})$, odkud $y \equiv -1 \pmod{5})$, tj. $y = -1 + 5t$ pro $t \in \mathbb{Z}$. Dosazením do dané rovnice dostaneme

$$5x + 7(-1 + 5t) = 8,$$

odkud vypočítáme $x = 3 - 7t$. Řešením naší rovnice je tedy

$$x = 3 - 7t, \quad y = -1 + 5t,$$

kde t je libovolné celé číslo. □

PŘÍKLAD. $91x - 28y = 35$.

ŘEŠENÍ. Protože $(91, 28) = 7$ a $7 \mid 35$, má rovnice celočíselné řešení. Vydělme ji sedmi:

$$13x - 4y = 5.$$

Libovolné řešení této rovnice musí splňovat kongruenci

$$13x - 4y \equiv 5 \pmod{13},$$

tj. $-4y \equiv -8 \pmod{13}$, odkud $y \equiv 2 \pmod{13}$ a $y = 2 + 13t$ pro $t \in \mathbb{Z}$. Dosazením

$$13x - 4(2 + 13t) = 5,$$

odkud vypočteme $x = 1+4t$. Řešením je tedy $x = 1+4t$, $y = 2+13t$, kde t je libovolné celé číslo. Tentýž výsledek bychom samozřejmě dostali, i kdybychom uvažovali kongruenci podle modulu 4 místo 13. Protože řešit kongruenci podle menšího modulu bývá snadnější, je vhodné na to pamatovat a uspořádat si výpočet tak, aby nebylo nutné pracovat s kongruencemi podle velkých modulů. □

PŘÍKLAD. $18x + 20y + 15z = 1$.

ŘEŠENÍ. Protože $(18, 20, 15) = 1$, má rovnice celočíselné řešení. Libovolné řešení musí splňovat kongruenci (za modul volíme největší společný dělitel čísel 18, 20)

$$18x + 20y + 15z \equiv 1 \pmod{2},$$

tedy $z \equiv 1 \pmod{2}$, odkud $z = 1 + 2s$, kde $s \in \mathbb{Z}$. Dosazením

$$18x + 20y + 15(1 + 2s) = 1$$

odkud po vydělení dvěma a úpravě dostaneme rovnici,

$$9x + 10y = -7 - 15s$$

kterou budeme řešit pro libovolné $s \in \mathbb{Z}$. Je-li tato rovnice splněna, musí platit

$$9x + 10y \equiv -7 - 15s \pmod{9},$$

odkud $y \equiv 2+3s \pmod{9}$, a proto $y = 2+3s+9t$, kde $t \in \mathbb{Z}$. Dosazením

$$9x + 10(2 + 3s + 9t) = -7 - 15s,$$

odkud po úpravě $x = -3 - 5s - 10t$. Řešení dané rovnice jsou tedy trojice

$$\begin{aligned} x &= -3 - 5s - 10t \\ y &= 2 + 3s + 9t \\ z &= 1 + 2s \end{aligned}$$

kde s, t jsou libovolná celá čísla. □

Příklad. $15x - 12y + 48z - 51u = 1$.

Řešení. Protože $(15, 12, 48, 51) = 3$ není dělitel čísla 1, nemá rovnice celočíselné řešení. □

5.2. Diofantické rovnice lineární vzhledem k některé neznámé. Jde o rovnice, které můžeme upravit do tvaru

$$mx_n = F(x_1, \dots, x_{n-1}), \tag{32}$$

kde m je přirozené číslo a $F(x_1, \dots, x_{n-1})$ mnohočlen s celočíselnými koeficienty. Je zřejmé, že má-li být $x_1, x_2, \dots, x_n$ celočíselným řešením rovnice (32), musí platit

$$F(x_1, \dots, x_{n-1}) \equiv 0 \pmod{m}. \tag{33}$$

Naopak, je-li $x_1, \dots, x_{n-1}$ řešení kongruence (33), pak pro $x_n = F(x_1, \dots, x_{n-1})/m$ dostaneme celočíselné řešení $x_1, \dots, x_{n-1}, x_n$ rovnice (32). Proto pro řešení rovnice (32) postačí vyřešit kongruenci (33). V případě $n = 2$, tj. v případě, kdy je mnohočlen $F(x_1)$ mnohočlenem jedné proměnné, jde o úlohu, kterou jsme se zabývali v části 4. Případ $n > 2$ je však možné řešit zcela analogicky pomocí následující věty.

Věta 33. *Pro libovolný mnohočlen $F(x_1, \dots, x_s)$ s celočíselnými koeficienty, přirozené číslo m a celá čísla $a_1, \dots, a_s$, $b_1, \dots, b_s$ taková, že $a_1 \equiv b_1 \pmod{m}$, ..., $a_s \equiv b_s \pmod{m}$, platí $F(a_1, \dots, a_s) \equiv F(b_1, \dots, b_s) \pmod{m}$.*

Důkaz. Snadný. □

Pro nalezení všech řešení kongruence (33) tedy postačí dosazovat do mnohočlenu $F(x_1, \dots, x_{n-1})$ za $x_1, \dots, x_{n-1}$ nezávisle na sobě postupně čísla $0, 1, 2, \dots, m-1$ (tj. celkem m^{n-1}-krát). A právě tehdy, když pro čísla $a_1, \dots, a_{n-1}$ je splněna podmínka $F(a_1, \dots, a_{n-1}) \equiv \pmod{m}$, dostáváme řešení kongruence (33) ve tvaru

$$x_1 = a_1 + mt_1, \ \dots, \ x_{n-1} = a_{n-1} + mt_{n-1},$$

kde $t_1, \dots, t_{n-1}$ mohou nabývat libovolných celočíselných hodnot. Tak dostaneme i řešení rovnice (32):

$$\begin{aligned} x_1 &= a_1 + mt_1, \\ &\vdots \\ x_{n-1} &= a_{n-1} + mt_{n-1}, \\ x_n &= \frac{1}{m} F(a_1 + mt_1, \dots, a_{n-1} + mt_{n-1}). \end{aligned}$$

Příklad. Řešte diofantickou rovnici $7x^2 + 5y + 13 = 0$.

Řešení. Rovnici upravíme na tvar $5y = -7x^2 - 13$ a budeme řešit kongruenci

$$-7x^2 - 13 \equiv 0 \pmod{5},$$

tj. $3x^2 \equiv 3 \pmod 5$, odkud $x^2 \equiv 1 \pmod 5$. Dosadíme-li za x čísla 0, 1, 2, 3, 4, zjistíme, že kongruence je splněna pro čísla 1 a 4. Řešením této kongruence jsou tedy podle 4.11 právě čísla

$$x = 1 + 5t \qquad \text{nebo} \qquad x = 4 + 5t,$$

kde $t \in \mathbb{Z}$. Dosazením dostaneme v prvním případě

$$5y = -7(1 + 5t)^2 - 13 = -7 - 70t - 175t^2 - 13$$

a tedy

$$y = -4 - 14t - 35t^2,$$

ve druhém případě

$$5y = -7(4 + 5t)^2 - 13 = -112 - 280t - 175t^2 - 13,$$

a proto

$$y = -25 - 56t - 35t^2.$$

Řešením dané rovnice jsou tedy právě všechny dvojice čísel x, y tvaru

$$x = 1+5t, y = -4-14t-35t^2 \quad \text{nebo} \quad x = 4+5t, y = -25-56t-35t^2,$$

kde t je libovolné celé číslo. □

Příklad. Řešte diofantickou rovnici $x(x + 3) = 4y - 1$.

Řešení. Rovnici upravíme na tvar $4y = x^2 + 3x + 1$ a budeme řešit kongruenci

$$x^2 + 3x + 1 \equiv 0 \pmod 4.$$

Dosazením čísel 0, 1, 2, 3 zjistíme, že kongruenci nesplňuje žádné z nich, a tedy tato kongruence nemá řešení. Řešení proto nemá ani daná rovnice. □

Příklad. Řešte diofantickou rovnici $x^2 + 4z^2 + 6x + 7y + 8z = 1$.

Řešení. Rovnici upravíme na tvar

$$7y = -x^2 - 6x - 4z^2 - 8z + 1$$

a doplníme na čtverce

$$7y = -(x + 3)^2 - (2z + 2)^2 + 14.$$

Proto budeme řešit kongruenci

$$(x + 3)^2 + (2z + 2)^2 \equiv 0 \pmod 7 \tag{34}$$

Nyní bychom mohli za uspořádanou dvojici $(x; z)$ postupně dosazovat uspořádané dvojice $(0; 0)$, $(0; 1)$, ..., $(0; 6)$, $(1; 0)$, $(1; 1)$, ..., $(6; 5)$, $(6; 6)$ a spočítat pro všech 49 hodnot výraz stojící na levé straně kongruence (34). Výhodnější ale bude využít tvaru kongruence (34) a odvolat se na tvrzení tvr:nonresidue-3mod-4, odkud pro $p = 7$, $a = x + 3$, $b = 2z + 2$ dostaneme, že z kongruence (34) plyne

$$x + 3 \equiv 2z + 2 \equiv 0 \pmod 7,$$

a tedy všechna řešení kongruence (34) jsou tvaru

$$x = -3 + 7t, \qquad z = -1 + 7s,$$

kde t, s jsou celá čísla. Dosazením do rovnice dostaneme

$$7y = -(x + 3)^2 - (2z + 2)^2 + 14 = -49t^2 - 196s^2 + 14,$$

odkud

$$y = -7t^2 - 28s^2 + 2.$$

Řešením dané rovnice jsou tedy právě všechny trojice čísel x, y, z tvaru

$$x = -3 + 7t, \quad y = -7t^2 - 28s^2 + 2, \quad z = -1 + 7s,$$

kde s, t jsou libovolná celá čísla. □

5.3. Rovnice jiného tvaru. Metodu, kterou jsme řešili předchozí příklady, je možno popsat také takto: „vyjádři některou z neznámých pomocí ostatních a zkoumej, kdy je celočíselná“. Skutečně, vyjádříme-li z rovnice (32) neznámou x_n, dostaneme

$$x_n = \frac{F(x_1, \ldots, x_{n-1})}{m},$$

což je celé číslo, právě když $m \mid F(x_1, \ldots, x_{n-1})$, tj. právě když je splněna kongruence (33). Ukážeme si na příkladech, že tento postup je použitelný i na rovnice, které nejsou tvaru (32). V příkladech uvedeme i případ, kdy je vhodné vyjádřit namísto některé neznámé nějaký jiný vhodný výraz a zkoumat, za jakých okolností bude celočíselný.

Příklad. Řešte diofantickou rovnici $3^x = 4y + 5$.

Řešení. Vyjádřeme z této rovnice neznámou y:

$$y = \frac{1}{4}(3^x - 5).$$

Je-li $x < 0$, je $0 < 3^x < 1$, a tedy $\frac{1}{4}(3^x - 5) \notin \mathbb{Z}$. Pro $x \geq 0$ platí

$$3^x - 5 \equiv (-1)^x - 1 \pmod 4;$$

číslo $(-1)^x - 1$ je kongruentní s nulou podle modulu 4 právě tehdy, když x je sudé, tj. $x = 2k$, kde $k \in \mathbb{N}_0$. Řešením této diofantické rovnice jsou tedy právě všechny dvojice

$$x = 2k, \qquad y = \frac{9^k - 5}{4},$$

kde $k \in \mathbb{N}_0$ je libovolné. □

Příklad. Řešte v $\mathbb{Z}$ rovnici $x(y + 1)^2 = 243y$.

Řešení. Vyjádřeme neznámou x:

$$x = \frac{243y}{(y + 1)^2}.$$

Aby $x \in \mathbb{Z}$, musí $(y + 1)^2$ být dělitelem čísla $243y$. Protože y a $y + 1$ jsou nesoudělná čísla pro libovolné $y \in \mathbb{Z}$, musí být $(y + 1)^2$ dělitelem čísla $243 = 3^5$. Toto číslo má však jen tři dělitele, kteří jsou druhou mocninou celého čísla: 1,9 a 81. Proto musí nastat některá z těchto možností: $y+1 = \pm 1$, $y+1 = \pm 3$ nebo $y+1 = \pm 9$. Dostáváme tedy šest řešení dané rovnice:

$$\begin{array}{ll}
y = 0, & x = 0, \\
y = -2, & x = -2 \cdot 243 = -486, \\
y = 2, & x = 2 \cdot 27 = 54, \\
y = -4, & x = -4 \cdot 27 = -108, \\
y = 8, & x = 8 \cdot 3 = 24, \\
y = -10, & x = -10 \cdot 3 = -30.
\end{array}$$

Jiná řešení daná diofantická rovnice nemá. □

Příklad. Řešte v $\mathbb{N}$ rovnici $\sqrt{x} + \sqrt{y} = \sqrt{1988}$.

Řešení. Odečteme-li od obou stran rovnice $\sqrt{y}$ a umocníme-li na druhou, dostaneme

$$x = 1988 - 4\sqrt{7 \cdot 71 \cdot y} + y.$$

Jsou-li x, y celá čísla, je i $4\sqrt{7 \cdot 71y}$ celé číslo, a tedy $\sqrt{7 \cdot 71y}$ je racionální číslo. Pak je $\sqrt{7 \cdot 71y} = k$ nezáporné celé číslo. Platí tedy $7 \cdot 71y = k^2$, odkud plyne, že k^2 a tedy i k je dělitelné prvočísly 7, 71. Je tedy $k = 7 \cdot 71t$ pro vhodné $t \in \mathbb{N}_0$ a tedy

$$y = \frac{k^2}{7 \cdot 71} = 497t^2.$$

Zcela analogicky je možné odvodit, že existuje $s \in \mathbb{N}_0$ tak, že

$$x = 497s^2.$$

Dosazením do původní rovnice dostáváme

$$\sqrt{497}s + \sqrt{497}t = \sqrt{1988},$$

odkud po vydělení plyne $s + t = 2$. Jsou tedy tři možnosti: $s = 0$, $t = 2$ nebo $s = t = 1$ nebo $s = 2$, $t = 0$, takže daná diofantická rovnice má tři řešení:

$$x = 0, \quad y = 1988 \quad \text{nebo} \quad x = y = 497 \quad \text{nebo} \quad x = 1988, \quad y = 0.$$

□

5.4. Řešení diofantických rovnic pomocí nerovností. Tato metoda je založena na tom, že pro libovolná reálná čísla a, b existuje jen konečně mnoho celých čísel x tak, že $a < x < b$. Proto při řešení dané rovnice hledáme taková čísla a, b, aby nerovnosti $a < x < b$ pro některou neznámou x byly důsledkem této rovnice. Konečně mnoho celých čísel ležících mezi čísly a, b pak můžeme jedno po druhém dosadit do rovnice za x a tím ji zjednodušit. Ukažme si to na následujících příkladech.

Příklad. Řešte diofantickou rovnici $6x^2 + 5y^2 = 74$.

Řešení. Protože pro libovolné $y \in \mathbb{Z}$ platí $5y^2 \geq 0$, musí libovolné řešení x, y dané rovnice splňovat

$$74 = 6x^2 + 5y^2 \geq 6x^2,$$

odkud $x^2 < \frac{37}{3}$, tedy $-3 \leq x \leq 3$, proto x^2 je některé z čísel 0, 1, 4, 9. Dosazením do rovnice postupně dostáváme $5y^2 = 74$, $5y^2 = 68$, $5y^2 = 50$, $5y^2 = 20$. První tři případy jsou ve sporu s $y \in \mathbb{Z}$, z posledního dostáváme $y^2 = 4$, tj. $y = \pm 2$. Rovnice má tedy čtyři řešení: $x = 3$, $y = 2$; $x = 3$, $y = -2$; $x = -3$, $y = 2$; $x = -3$, $y = -2$. □

Příklad. Řešte v $\mathbb{Z}$ rovnici $x^2 + xy + y^2 = x^2y^2$.

Řešení. Protože jsou v dané rovnici neznámé x, y zastoupeny symetricky, můžeme předpokládat, že $x^2 \leq y^2$, odkud plyne $xy \leq y^2$, a tedy

$$x^2y^2 = x^2 + xy + y^2 \leq y^2 + y^2 + y^2 = 3y^2.$$

Platí tedy $y = 0$ nebo $x^2 \leq 3$. Dosazením do rovnice dostáváme v prvním případě $x = 0$, ve druhém pro $x = 0$ opět $y = 0$, pro $x = 1$ je $y = -1$ a pro $x = -1$ je $y = 1$. Rovnice má tedy tři řešení:

$$x = 0, \quad y = 0; \qquad x = 1, \quad y = -1; \qquad x = -1, \quad y = 1.$$

□

Příklad. Řešte v $\mathbb{Z}$ $2^x = 1 + 3^y$.

Řešení. Je-li $y < 0$, platí $1 < 1 + 3^y < 2$, odkud $0 < x < 1$, což je spor. Je tedy $y \geq 0$ a proto $2^x = 1 + 3^y \geq 2$, odkud $x \geq 1$. Ukážeme, že také platí $x \leq 2$. Kdyby totiž bylo $x \geq 3$, platilo by

$$1 + 3^y = 2^x \equiv 0 \pmod 8,$$

odkud bychom dostali

$$3^y \equiv -1 \pmod 8,$$

což však není možné, neboť pro sudá čísla y je $3^y \equiv 1 \pmod 8$ a pro lichá čísla y platí $3^y \equiv 3 \pmod 8$. Zbývá tedy vyřešit případ $1 \leq x \leq 2$. Pro $x = 1$ dostáváme

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

a tedy $y = 0$. Z $x = 2$ plyne

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

takže $y = 1$. Rovnice má tedy dvě řešení: $x = 1$, $y = 0$ a $x = 2$, $y = 1$. □

Příklad. Řešte rovnici $x + y + z = xyz$ v oboru přirozených čísel.

Řešení. Protože jsou v dané rovnici neznámé zastoupeny symetricky, můžeme předpokládat $x \le y \le z$. Pak ale

$$xyz = x + y + z \le z + z + z = 3z,$$

odkud $xy \le 3$. Je tedy $xy = 1$, nebo $xy = 2$, nebo $xy = 3$.

Je-li $xy = 1$, platí $x = 1$, $y = 1$, odkud dostaneme dosazením do rovnice $2 + z = z$, což není možné.

Je-li $xy = 2$, platí $x = 1$, $y = 2$ (předpokládáme $x \le y$), odkud $3 + z = 2z$, a tedy $z = 3$.

Je-li $xy = 3$, platí $x = 1$, $y = 3$, odkud $4 + z = 3z$, tedy $z = 2$, což je ve sporu s předpokladem $y \le z$.

Rovnice má tedy jediné řešení $x = 1$, $y = 2$, $z = 3$ splňující $x \le y \le z$. Všechna řešení v oboru přirozených čísel dostaneme všemi záměnami pořadí čísel 1, 2, 3:

$$(x; y; z) \in \{(1; 2; 3), (1; 3; 2), (2; 1; 3), (2; 3; 1), (3; 1; 2), (3; 2; 1)\}.$$

□

Často je možné s výhodou ukázat sporem, že množina hodnot neznámé x je konečná a omezená nerovnostmi $a < x < b$; přitom z předpokladu $x \le a$ (resp. $x \ge b$) odvodíme nepravdivé tvrzení. V následujících příkladech bude takovým nepravdivým tvrzením dvojice nerovností

$$c^n < d^n < (c + 1)^n,$$

kde c, d jsou celá a n přirozené číslo.

Příklad. Řešte diofantickou rovnici $x(x + 1)(x + 7)(x + 8) = y^2$.

Řešení. Úpravou

$$y^2 = (x^2 + 8x)(x^2 + 8x + 7).$$

Označíme-li $x^2 + 8x = z$, je naše rovnice tvaru

$$y^2 = z^2 + 7z.$$

Ukážeme, že $z \le 9$. Předpokládejme naopak $z > 9$. Pak platí

$$(z + 3)^2 = z^2 + 6z + 9 < z^2 + 7z = y^2 < z^2 + 8z + 16 = (z + 4)^2,$$

což je spor, neboť $z + 3$, y, $z + 4$ jsou celá čísla a z těchto nerovností by plynulo

$$|z + 3| < |y| < |z + 4|.$$

Je tedy $z \le 9$, tj. $x^2 + 8x \le 9$, odkud

$$(x + 4)^2 = x^2 + 8x + 16 \le 25,$$

a proto $-5 \le x + 4 \le 5$, neboli $-9 \le x \le 1$. Dosazením těchto hodnot do rovnice dostaneme všechna řešení: $(x; y) \in \{(-9; 12)$, $(-9; -12)$, $(-8; 0)$, $(-7; 0)$, $(-4; 12)$, $(-4; -12)$, $(-1; 0)$, $(0; 0)$, $(1; 12)$, $(1; -12)\}$.

□

Příklad. Řešte diofantickou rovnici $(x + 2)^4 - x^4 = y^3$.

Řešení. Úpravou získáme

$$y^3 = 8x^3 + 24x^2 + 32x + 16 = 8(x^3 + 3x^2 + 4x + 2),$$

odkud plyne, že y je sudé. Položme $y = 2z$, $z \in \mathbb{Z}$. Platí tedy

$$z^3 = x^3 + 3x^2 + 4x + 2.$$

Je-li $x \geq 0$, platí

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 < x^3 + 3x^2 + 4x + 2 = \\ = z^3 < x^3 + 6x^2 + 12x + 8 = (x+2)^3,$$

odkud $x + 1 < z < x + 2$, což není možné. Daná rovnice tedy nemá řešení $x, y \in \mathbb{Z}$ takové, že $x \geq 0$. Předpokládejme, že má nějaké řešení $x_1, y_1 \in \mathbb{Z}$ takové, že $x_1 \leq -2$. Pak platí

$$(x_1 + 2)^4 - x_1^4 = y_1^3$$

a dosadíme-li $x_2 = -x_1 - 2$, $y_2 = -y_1$, dostaneme

$$x_2^4 - (x_2 + 2)^4 = -y_2^3,$$

a proto x_2, y_2 je také řešení dané rovnice. Ovšem $x_2 = -x_1 - 2 \geq 0$ a z předchozích úvah plyne, že tato situace nastat nemůže. Dohromady tedy $-2 < x < 0$, tj. $x = -1$. Pro $x = -1$ vychází z původní rovnice $y = 0$; dvojice $x = -1$, $y = 0$ je jediným řešením úlohy. □

5.4.1. *Některé nerovnosti.* Při řešení diofantických rovnic jsou někdy užitečné i některé složitější postupy a nerovnosti. Uveďme si některé z nejčastěji používaných.

Věta 34 (AG-nerovnost). *Pro libovolná čísla $a_1, a_2, \dots, a_n \in \mathbb{R}_0^+$ platí nerovnost*

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n}\,, \tag{35}$$

přitom rovnost v (35) nastane, jen když $a_1 = a_2 = \cdots = a_n$.

Důkaz. *Prozatím neuveden.* □

Věta 35 (Bernoulliova nerovnost). $\forall x \in \mathbb{R}, x \geq -1, \forall n \in \mathbb{N}$ *platí:*

$$(1 + x)^n \geq 1 + n \cdot x.$$

Důkaz. Pro $n = 1$ nebo $x = 0$ je tvrzení zřejmé. Pro reálná $A > B \geq 0$ a přirozené číslo $n \geq 2$ platí:

$$n(A - B)B^{n-1} < A^n - B^n < n(A - B)A^{n-1} \quad (A > B \geq 0,\ n \geq 2),$$

z čehož po dosazení $A = 1 + x$ a $B = 1$ (pro $x > 0$), resp. $A = 1$, $B = 1 + x$ (pro $-1 \leq x < 0$) dostaneme požadované tvrzení. □

Příklad. V oboru přirozených čísel řešte rovnici

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3.$$

Řešení. Podíl přirozených čísel je číslo kladné, a proto můžeme pro čísla $\frac{x}{y}$, $\frac{y}{z}$ a $\frac{z}{x}$ použít nerovnost mezi aritmetickým a geometrickým průměrem (viz Věta 34). Geometrický průměr těchto tří čísel je 1, a proto pro jejich aritmetický průměr platí

$$\frac{1}{3}\left(\frac{x}{y}+\frac{y}{z}+\frac{z}{x}\right)\geq 1,$$

kde rovnost nastane právě tehdy, když

$$\frac{x}{y}=\frac{y}{z}=\frac{z}{x}=1.$$

Porovnáme-li získanou nerovnost s danou rovnicí, dostáváme, že rovnice má nekonečně mnoho řešení $x=y=z$, kde z je libovolné přirozené číslo, a žádné jiné řešení nemá. □

Příklad. Dokažte, že pro libovolné přirozené číslo $n>2$ rovnice

$$x^n+(x+1)^n=(x+2)^n$$

nemá řešení v oboru přirozených čísel.

Řešení. Předpokládejme naopak, že pro nějaká přirozená čísla x, n, kde $n>2$, je daná rovnice splněna, a označme $y=x+1\geq 2$. Pak platí

$$(y-1)^n+y^n=(y+1)^n, \tag{36}$$

odkud dostáváme

$$0=(y+1)^n-y^n-(y-1)^n\equiv 1-(-1)^n \pmod{y}.$$

Připusťme, že n je liché, pak $0\equiv 2 \pmod{y}$, tedy $y=2$ a

$$0=3^n-2^n-1,$$

což platí pouze pro $n=1$. Je tedy n sudé a podle binomické věty platí

$$\begin{aligned}(y+1)^n&\equiv \tbinom{n}{2}y^2+\tbinom{n}{1}y+1 \pmod{y^3},\\ (y-1)^n&\equiv \tbinom{n}{2}y^2-\tbinom{n}{1}y+1 \pmod{y^3},\end{aligned}$$

odkud plyne

$$0=(y+1)^n-y^n-(y-1)^n\equiv 2ny \pmod{y^3},$$

tedy $0\equiv 2n \pmod{y^2}$, a proto $2n\geq y^2$. Vydělíme-li (36) číslem y^n, dostaneme

$$\left(1+\frac{1}{y}\right)^n=1+\left(1-\frac{1}{y}\right)^n<2.$$

Naopak podle Bernoulliovy nerovnosti (viz Věta 35) platí

$$\left(1+\frac{1}{y}\right)^n>1+\frac{n}{y}=1+\frac{2n}{2y}\geq 1+\frac{y^2}{2y}=1+\frac{y}{2}\geq 2.$$

Shrneme-li předchozí úvahy, vychází, že pro žádné přirozené číslo $n>2$ nemá daná rovnice řešení v oboru přirozených čísel.

5.5. Řešení diofantických rovnic metodou rozkladu. Tato metoda spočívá v úpravě dané rovnice do tvaru

$$A_1 \cdot A_2 \cdot \dots \cdot A_n = B, \tag{37}$$

kde $A_1, \dots, A_n$ jsou výrazy obsahující neznámé, které pro celočíselné hodnoty neznámých nabývají celočíselných hodnot, a B je číslo (případně výraz), jehož rozklad na prvočísla známe. Pak totiž existuje pouze konečně mnoho rozkladů čísla B na n celočíselných činitelů $a_1, \dots, a_n$. Vyšetříme-li pak pro každý z těchto rozkladů soustavu rovnic

$$A_1 = a_1, \quad A_2 = a_2, \quad \dots, \quad A_n = a_n,$$

získáme všechna řešení rovnice (37). Ukažme si to na příkladech.

Příklad. Řešte diofantickou rovnici $y^3 - x^3 = 91$.

Řešení. Rozložme levou stranu rovnice:

$$(y - x)(y^2 + xy + x^2) = 91.$$

Protože

$$y^2 + xy + x^2 = \left(y + \frac{x}{2}\right)^2 + \frac{3}{4}x^2 \geq 0,$$

musí být také $y - x > 0$. Číslo 91 můžeme rozložit na součin dvou přirozených čísel čtyřmi způsoby: $91 = 1 \cdot 91 = 7 \cdot 13 = 13 \cdot 7 = 91 \cdot 1$. Budeme proto odděleně řešit čtyři systémy rovnic:

(1) $y - x = 1$, $y^2 + xy + x^2 = 91$. Dosazením $y = x + 1$ z první do druhé rovnice dostaneme $x^2 + x - 30 = 0$, odkud $x = 5$ nebo $x = -6$. Příslušné hodnoty druhé neznámé jsou pak $y = 6$, $y = -5$.

(2) $y - x = 7$, $y^2 + xy + x^2 = 13$. Pak $x^2 + 7x + 12 = 0$, tedy $x = -3$ a $y = 4$ nebo $x = -4$ a $y = 3$.

(3) $y - x = 13$, $y^2 + xy + x^2 = 7$. Nyní $x^2 + 13x + 54 = 0$. Tato rovnice však nemá řešení v oboru reálných čísel, a proto ani v oboru čísel celých.

(4) $y - x = 91$, $y^2 + xy + x^2 = 1$. V tomto případě $x^2 + 91x + 2760 = 0$. Ani tato rovnice nemá řešení v oboru reálných čísel.

Daná rovnice má tedy čtyři řešení:

$$(x; y) \in \{(5; 6), (-6; -5), (-3; 4), (-4; 3)\}.$$

□

Příklad. Řešte diofantickou rovnici $x^4 + 2x^7y - x^{14} - y^2 = 7$.

Řešení. Upravme nejprve levou stranu rovnice:

$$x^4 + 2x^7y - x^{14} - y^2 = x^4 - (x^7 - y)^2 = (x^2 - x^7 + y)(x^2 + x^7 - y)$$

a uvažme, že číslo 7 můžeme rozložit čtyřmi způsoby na součin dvou celých čísel: $7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)$. Budeme proto řešit čtyři soustavy rovnic.

(1) $x^2 - x^7 + y = 1, \quad x^2 + x^7 - y = 7$. Sečtením obou rovnic dostaneme $x^2 = 4$, odkud $x = 2$ a $y = 125$, nebo $x = -2$ a $y = -131$.
(2) $x^2 - x^7 + y = 7, \quad x^2 + x^7 - y = 1$. Nyní $x^2 = 4$, a tedy $x = 2$, $y = 131$ nebo $x = -2$, $y = -125$.
(3) $x^2 - x^7 + y = -1, \quad x^2 + x^7 - y = -7$. Sečtením $x^2 = -4$, což je spor.
(4) $x^2 - x^7 + y = -7, \quad x^2 + x^7 - y = -1$. Opět spor $x^2 = -4$.

Rovnice má tedy čtyři řešení:

$$(x; y) \in \{(-2; -131), (-2; -125), (2; 125), (2; 131)\}.$$

□

Příklad. Řešte diofantickou rovnici

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p},$$

kde p je libovolné prvočíslo.

Řešení. Vynásobením číslem xyp a další úpravou dostaneme

$$xy - px - py = 0.$$

Úprava do tvaru (37) vyžaduje nyní umělý obrat: přičteme k oběma stranám rovnice p^2, aby bylo možno její levou stranu zapsat jako součin:

$$(x - p)(y - p) = p^2.$$

Protože p je prvočíslo, lze p^2 rozložit na součin dvou celých čísel jen těmito šesti způsoby: $p^2 = 1 \cdot p^2 = p \cdot p = p^2 \cdot 1 = (-1) \cdot (-p^2) = (-p) \cdot (-p) = (-p^2) \cdot (-1)$. Budeme proto řešit šest systémů rovnic:

(1) $x - p = 1$, $y - p = p^2$, a tedy $x = p + 1$, $y = p^2 + p$;
(2) $x - p = p$, $y - p = p$, a tedy $x = 2p$, $y = 2p$;
(3) $x - p = p^2$, $y - p = 1$, a tedy $x = p^2 + p$, $y = p + 1$;
(4) $x - p = -1$, $y - p = -p^2$, a tedy $x = p - 1$, $y = p - p^2$;
(5) $x - p = -p$, $y - p = -p$, a tedy $x = y = 0$, což nevyhovuje;
(6) $x - p = -p^2$, $y - p = -1$, a tedy $x = p - p^2$, $y = p - 1$.

Daná rovnice má tedy pět řešení, popsaných v případech (1)-(4) a (6).

□

5.5.1. *Pythagorova rovnice.* Pythagorova rovnice se zabývá otázkou hledání všech pravoúhlých trojúhelníků s celočíselnými délkami stran.

Příklad. V oboru přirozených čísel řešte rovnici

$$x^2 + y^2 = z^2.$$

Řešení. Označme $t = (x, y, z)$, $x_1 = \frac{x}{t}$, $y_1 = \frac{y}{t}$, $z_1 = \frac{z}{t}$. Pak platí

$$t^2 x_1^2 + t^2 y_1^2 = t^2 z_1^2,$$

odkud po vydělení číslem $t^2 \neq 0$ vychází

$$x_1^2 + y_1^2 = z_1^2 \tag{38}$$

a navíc $(x_1, y_1, z_1) = 1$. Ukážeme nyní, že čísla x_1, y_1, z_1 jsou dokonce po dvou nesoudělná: kdyby nějaké prvočíslo p dělilo dvě z čísel x_1, y_1, z_1, vyšlo by z (38), že dělí i třetí, což vzhledem k $(x_1, y_1, z_1) = 1$ není možné. Z čísel x_1, y_1 je tedy nejvýše jedno sudé. Připusťme, že jsou obě lichá. Pak z kongruence

$$z_1^2 \equiv x_1^2 + y_1^2 \equiv 1 + 1 \pmod 8$$

plyne, že z_1^2 je sudé číslo, které není dělitelné 4, což není možné. Je tedy z čísel x_1, y_1 právě jedno sudé. Protože v rovnici (38) vystupují x_1 a y_1 symetricky, můžeme pro určitost předpokládat, že sudé je $x_1 = 2r$, $r \in \mathbb{N}$. Z (38) pak plyne

$$4r^2 = z_1^2 - y_1^2$$

a tedy

$$r^2 = \frac{z_1 + y_1}{2} \cdot \frac{z_1 - y_1}{2}.$$

Označme $u = \frac{1}{2}(z_1 + y_1)$, $v = \frac{1}{2}(z_1 - y_1)$. Pak $z_1 = u + v$, $y_1 = u - v$. Protože jsou y_1, z_1 nesoudělná čísla, jsou i u, v nesoudělná čísla. Z rovnice

$$r^2 = u \cdot v$$

pak plyne, že existují nesoudělná přirozená čísla a, b tak, že $u = a^2$, $v = b^2$, navíc vzhledem k $u > v$ platí $a > b$. Celkem tedy dostáváme

$$\begin{aligned}
x &= tx_1 = 2tr = 2tab, \\
y &= ty_1 = t(u - v) = t(a^2 - b^2), \\
z &= tz_1 = t(u + v) = t(a^2 + b^2),
\end{aligned}$$

což skutečně pro libovolné $t \in \mathbb{N}$ a libovolná nesoudělná $a, b \in \mathbb{N}$ taková, že $a > b$, vyhovuje dané rovnici. Zbylá řešení bychom dostali záměnou x a y (v průběhu řešení jsme předpokládali, že právě x_1 je sudé):

$$x = t(a^2 - b^2), \quad y = 2tab, \quad z = t(a^2 + b^2),$$

kde opět $t, a, b \in \mathbb{N}$ jsou libovolná taková, že $a > b$, $(a, b) = 1$. □

5.6. Řešitelnost diofantických rovnic. V předchozí čáasti jsme viděli, že řešení většiny diofantických rovnic není snadné, a ačkoli jsme se naučili několik metod, v mnoha konkrétních případech se nám nepodaří diofantickou rovnici vyřešit ani jednou z nich. Přesto se nám v těchto případech může podařit něco o řešení zjistit. Například nalézt nekonečnou množinu řešení a tím dokázat, že množina všech řešení, i když ji celou neumíme popsat, je nekonečná. Nebo naopak ukázat, že množina všech řešení je prázdná (a tím vlastně danou rovnici vyřešit), popřípadě konečná.

5.6.1. *Neexistence řešení.* Při důkazu, že nějaká diofantická rovnice nemá žádné řešení, je často možné s úspěchem využít kongruencí. Má-li totiž řešení diofantická rovnice $L = P$ (kde L, P jsou výrazy obsahující neznámé, nabývající celočíselných hodnot pro libovolné celočíselné hodnoty neznámých), musí mít řešení i kongruence $L \equiv P \pmod{m}$ pro libovolné $m \in \mathbb{N}$, protože řešením této kongruence je například zmíněné řešení rovnice. Odtud plyne, že nalezneme-li nějaké přirozené číslo m tak, že kongruence $L \equiv P \pmod{m}$ nemá řešení, nemůže mít řešení ani původní diofantická rovnice $L = P$. Je nutno si však uvědomit, že obrácení předchozí úvahy obecně neplatí: má-li kongruence $L \equiv P \pmod{m}$ pro každé přirozené číslo m řešení, neznamená to ještě, že má řešení též diofantická rovnice $L = P$ (ukážeme to v Příkladu na str. 70).

Příklad. Řešte diofantickou rovnici

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 = 15999.$$

Řešení. Ukážeme, že kongruence

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv 15999 \pmod{16}$$

nemá řešení, odkud vyplyne, že řešení nemá ani daná diofantická rovnice. Je-li totiž celé číslo n sudé, je $n = 2k$ pro $k \in \mathbb{Z}$ a tedy $n^4 = 16k^4 \equiv 0 \pmod{16}$. Jestliže je celé číslo n liché, platí $n^4 - 1 = (n-1)(n+1)(n^2+1) \equiv 0 \pmod{16}$, neboť čísla $n-1$, $n+1$ a n^2+1 jsou sudá a jedno z čísel $n-1$, $n+1$ musí být dokonce dělitelné čtyřmi. Znamená to tedy, že podle modulu 16 je n^4 kongruentní s 0 pro sudá n a s 1 pro lichá čísla n. Je-li proto mezi čísly $x_1, x_2, \ldots, x_{14}$ právě r lichých, je

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv r \pmod{16}.$$

Platí $15999 = 16000 - 1 \equiv 15 \pmod{16}$ a protože $0 \le r \le 14$, nemůže mít kongruence

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv 15 \pmod{16}$$

řešení, a nemá ho tedy ani daná rovnice. □

Příklad. V oboru celých čísel řešte soustavu rovnic

$$x^2 + 2y^2 = z^2,$$
$$2x^2 + y^2 = u^2.$$

Řešení. Snadno ověříme, že z $x = y = 0$ plyne také $z = u = 0$, což je řešení dané soustavy. Ukážeme, že další řešení soustava nemá. Předpokládejme, že x, y, z, u je řešení a že $x \ne 0$ nebo $y \ne 0$, a označme $d = (x, y) > 0$ největší společný dělitel čísel x, y. Z první rovnice plyne $d \mid z$, ze druhé $d \mid u$. Označíme-li $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$, $z_1 = \frac{z}{d}$, $u_1 =$

$\frac{u}{d}$, dostáváme, že $(x_1, y_1) = 1$, a po zkrácení obou rovnic číslem d^2 dostaneme

$$x_1^2 + 2y_1^2 = z_1^2,$$
$$2x_1^2 + y_1^2 = u_1^2.$$

Odtud plyne sečtením $3x_1^2 + 3y_1^2 = z_1^2 + u_1^2$ a tedy $3 \mid z_1^2 + u_1^2$. Podle Tvrzení 3.1 platí $3 \mid z_1$, $3 \mid u_1$ a tedy $9 \mid z_1^2 + u_1^2$. Pak ale $9 \mid 3(x_1^2 + y_1^2)$, a tedy $3 \mid x_1^2 + y_1^2$. Opět podle Tvrzení 3.1 platí $3 \mid x_1$, $3 \mid y_1$, což je spor s $(x_1, y_1) = 1$. Soustava má tedy jediné řešení $x = y = z = u = 0$. □

Příklad. V oboru přirozených čísel řešte rovnici

$$1! + 2! + 3! + \cdots + x! = y^2.$$

Řešení. Přímým výpočtem se přesvědčíme, že pro $x < 5$ vyhovují rovnici pouze $x = y = 1$ a $x = y = 3$. Ukážeme, že pro $x \geq 5$ rovnice řešení nemá. Protože pro libovolné $n \geq 5$ je $n!$ dělitelné pěti, platí

$$1! + 2! + 3! + \cdots + x! \equiv 1! + 2! + 3! + 4! = 33 \equiv 3 \pmod 5.$$

Ovšem druhá mocnina přirozeného čísla je podle modulu 5 kongruentní s 0 nebo 1 nebo 4. Kongruence $1! + 2! + \cdots + x! \equiv y^2 \pmod 5$ pro $x \geq 5$ tedy nemá řešení, a proto nemá pro $x \geq 5$ řešení ani daná rovnice. □

Příklad. V oboru přirozených čísel řešte rovnici

$$x^2 - y^3 = 7.$$

Řešení. Ukážeme, že daná rovnice nemá řešení. Předpokládejme naopak, že pro vhodná $x, y \in \mathbb{Z}$ platí $x^2 - y^3 = 7$. Kdyby y bylo sudé, platilo by $x^2 \equiv 7 \pmod 8$, což není možné. Je tedy y liché, $y = 2k + 1$ pro $k \in \mathbb{Z}$. Pak platí

$$x^2 + 1 = y^3 + 2^3 = (y + 2)(y^2 - 2y + 4) = \tag{39}$$
$$= (y + 2)((y - 1)^2 + 3) = (2k + 3)(4k^2 + 3). \tag{40}$$

Číslo $4k^2 + 3$ musí být dělitelné nějakým prvočíslem $p \equiv 3 \pmod 4$. V opačném případě vzhledem k tomu, že $4k^2 + 3$ je liché, by totiž v rozkladu čísla $4k^2 + 3$ na prvočísla vystupovala pouze prvočísla kongruentní s 1 podle modulu 4 a tedy by i jejich součin $4k^2 + 3$ musel být kongruentní s 1 podle modulu 4, což jistě není. Je tedy $4k^2 + 3$ dělitelné prvočíslem $p \equiv 3 \pmod 4$, a tedy platí

$$x^2 + 1 \equiv 0 \pmod p.$$

Podle Tvrzení 3.1 odtud plyne $x \equiv 1 \equiv 0 \pmod p$, a to je spor. □

Nyní uvedeme slibovaný příklad toho, že diofantická rovnice nemusí být řešitelná ani v případě, že je kongruence $L \equiv P \pmod m$ řešitelná pro libovolný modul $m \in \mathbb{N}$.

Příklad. Dokažte, že kongruence

$$6x^2 + 5x + 1 \equiv 0 \pmod{m}$$

má řešení pro každé přirozené číslo m, a přitom diofantická rovnice

$$6x^2 + 5x + 1 = 0$$

řešení nemá.

Řešení. Platí $6x^2 + 5x + 1 = (3x + 1)(2x + 1)$, a tedy rovnice $6x^2+5x+1 = 0$ nemá celočíselné řešení. Nechť m je libovolné přirozené číslo a platí $m = 2^n \cdot k$, kde $n \in \mathbb{N}_0$ a k je liché číslo. Protože $(3, 2^n) = (2, k) = 1$, mají obě kongruence soustavy

$$\begin{aligned} 3x &\equiv -1 \pmod{2^n} \\ 2x &\equiv -1 \pmod{k} \end{aligned}$$

podle Věty 20 řešení, a protože $(2^n, k) = 1$, má podle Věty 22 řešení i celá soustava. Pro libovolné x vyhovující této soustavě je pak $3x + 1$ dělitelné číslem 2^n a $2x + 1$ číslem k a proto součin $(3x + 1)(2x + 1)$ je dělitelný číslem $2^n \cdot k = m$. Je tedy x řešením kongruence

$$6x^2 + 5x + 1 \equiv 0 \pmod{m}.$$

□

5.6.2. *Zmenšování ad absurdum.* Je to metoda důkazu neexistence řešení diofantické rovnice. Při důkazu touto metodou libovolné řešení dané diofantické rovnice charakterizujeme nějakým přirozeným číslem (například největším společným dělitelem hodnot některých neznámých nebo druhou mocninou hodnoty některé neznámé a podobně) a ukážeme, že existuje-li řešení charakterizované přirozeným číslem d, musí existovat jiné řešení, charakterizované přirozeným číslem $d' < d$. Pak totiž žádné takové řešení existovat nemůže, o čemž se snadno můžeme přesvědčit sporem: kdyby existovalo, mohli bychom zvolit to řešení, které je ze všech řešení charakterizováno co nejmenším přirozeným číslem d; pak by ovšem muselo existovat i jiné řešení, charakterizované přirozeným číslem $d' < d$, což však by byl spor s volbou d.

Příklad. Řešte diofantickou rovnici $x^3 + 2y^3 + 4z^3 - 6xyz = 0$.

Řešení. Rovnici jistě vyhovuje $x = y = z = 0$. Ukážeme, že jiné řešení rovnice nemá. Označme $d = x^2+y^2+z^2$ a předpokládejme, že pro nějaké řešení x, y, z dané rovnice platí $d > 0$. Z původní rovnice plyne, že x^3 je sudé číslo, a proto je $x = 2x_1$ pro vhodné $x_1 \in \mathbb{Z}$. Dosazením do rovnice dostaneme

$$8x_1^3 + 2y^3 + 4z^3 - 12x_1yz = 0,$$

po vydělení dvěma

$$4x_1^3 + y^3 + 2z^3 - 6x_1yz = 0,$$

a proto i y^3 je sudé číslo, tedy $y = 2y_1$ pro vhodné $y_1 \in \mathbb{Z}$. Dosazením a vydělením dvěma dostaneme

$$2x_1^3 + 4y_1^3 + z^3 - 6x_1y_1z = 0,$$

odkud plyne, že z^3 je také sudé číslo, a proto $z = 2z_1$ pro vhodné $z_1 \in \mathbb{Z}$. Dosazením a vydělením dvěma dostaneme

$$x_1^3 + 2y_1^3 + 4z_1^3 - 6x_1y_1z_1 = 0,$$

a tedy x_1, y_1, z_1 je řešení původní diofantické rovnice, přičemž platí

$$x_1^2 + y_1^2 + z_1^2 = \frac{x^2}{4} + \frac{y^2}{4} + \frac{z^2}{4} = \frac{d}{4} < d.$$

Podle metody popsané v 6.4 daná diofantická rovnice nemá řešení s vlastností $d > 0$, a tedy $x = y = z = 0$ je jejím jediným řešením. □

Příklad. V oboru přirozených čísel řešte rovnici $x^2 + y^2 = 4^z$.

Řešení. Užijeme metodu 5.6.2 pro $d = z$. Předpokládejme nejprve, že x, y, z je řešením dané rovnice. Pak jistě platí $z \neq 1$, protože je-li $x = y = 1$, platí $x^2 + y^2 = 2 < 4$, a je-li alespoň jedno z čísel x, y větší než jedna, je $x^2 + y^2 > 4$. Je tedy $z > 1$ a platí $x^2 + y^2 = 4^z \equiv 0 \pmod 8$. Protože druhá mocnina lichého čísla je kongruentní s 1 podle modulu 8 a druhá mocnina sudého čísla je kongruentní s 0 nebo 4 podle modulu 8, plyne z této kongruence, že x i y jsou sudá, a tedy $x = 2x_1$, $y = 2y_1$ pro vhodná $x_1, y_1 \in \mathbb{N}$. Pak ovšem

$$x_1^2 + y_1^2 = \frac{x^2}{4} + \frac{y^2}{4} = 4^{z-1},$$

a tedy, označíme-li $z_1 = z - 1 \in \mathbb{N}$, čísla x_1, y_1, z_1 splňují danou rovnici, přičemž $z_1 < z$. Proto daná rovnice nemá řešení.

Příklad. Řešte diofantickou rovnici $x^4 + y^4 + z^4 = 9u^4$.

Řešení. Je-li $u = 0$, musí být rovněž $x = y = z = 0$, což je řešení dané rovnice. Ukážeme, že jiné řešení rovnice nemá. Předpokládejme, že celá čísla x, y, z, u vyhovují dané rovnici, přičemž $u \neq 0$, a označme $d = u^4$. Kdyby číslo u nebylo dělitelné pěti, bylo by $u^4 \equiv 1 \pmod 5$ podle Fermatovy věty, a tedy by platilo

$$x^4 + y^4 + z^4 \equiv 4 \pmod 5,$$

což však není možné, neboť podle Fermatovy věty každé z čísel x^4, y^4, z^4 může být podle modulu 5 kongruentní pouze s 0 nebo 1. Je tedy u dělitelné pěti, $u = 5u_1$ pro vhodné $u_1 \in \mathbb{Z}$, a platí

$$x^4 + y^4 + z^4 \equiv 0 \pmod 5,$$

odkud plyne, že čísla x, y, z jsou dělitelné pěti, tj. $x = 5x_1$, $y = 5y_1$, $z = 5z_1$ pro vhodná $x_1, y_1, z_1 \in \mathbb{Z}$. Dosazením do rovnice a vydělením 5^4 dostaneme

$$x_1^4 + y_1^4 + z_1^4 = 9u_1^4,$$

a tedy x_1, y_1, x_1, u_1 vyhovují dané rovnici. Přitom platí

$$u_1^4 = \frac{u^4}{5^4} < u^4 = d.$$

□

PŘÍKLAD. Řešte diofantickou rovnici $x^2 + y^2 + z^2 = 2xyz$.

ŘEŠENÍ. Rovnice jistě splňuje $x = y = z = 0$. Ukážeme, že další řešení tato rovnice nemá. Dokážeme dokonce silnější tvrzení: žádná rovnice

$$x^2 + y^2 + z^2 = 2^u xyz, \tag{41}$$

kde $x, y, z \in \mathbb{Z}$ a $u \in \mathbb{N}$ nemá jiné řešení než $x = y = z = 0$, $u \in \mathbb{N}$ libovolné. Předpokládejme, že $x, y, z \in \mathbb{Z}$, $u \in \mathbb{N}$ vyhovují rovnici (41) a že $d = x^2 + y^2 + z^2 > 0$. Protože $u \geq 1$, je $2^u xyz$ sudé číslo, a proto i $x^2 + y^2 + z^2$ je sudé číslo. To ale znamená, že právě jedno z čísel x, y, z, nebo všechna tři jsou sudá. V prvním případě je však

$$x^2 + y^2 + z^2 \equiv 1 + 1 + 0 = 2 \pmod 4,$$

kdežto

$$2^u xyz \equiv 0 \pmod 4,$$

neboť $u \geq 1$ a jedno z čísel x, y, z je sudé. Nastane tedy druhý případ a čísla $x_1 = \frac{x}{2}$, $y_1 = \frac{y}{2}$, $z_1 = \frac{z}{2}$ jsou celá. Položme $u_1 = u + 1$ a dosaďme do (41):

$$4x_1^2 + 4y_1^2 + 4z_1^2 = 2^{u_1 - 1} \cdot 2x_1 \cdot 2y_1 \cdot 2z_1,$$

po vydělení čtyřmi

$$x_1^2 + y_1^2 + z_1^2 = 2^{u_1} \cdot x_1 y_1 z_1,$$

a tedy x_1, y_1, z_1, u_1 vyhovují rovnici (41). Přitom platí $0 < x_1^2 + y_1^2 + z_1^2 = \frac{d}{4} < d$, neboť $d > 0$. Podle 5.6.2 tedy rovnice (41) může mít jen řešení s vlastností $d = 0$, což jsou výše uvedená řešení $x = y = z = 0$, $u \in \mathbb{N}$ libovolné. Speciálně, zadaná rovnice má jediné řešení $x = y = z = 0$. □

5.6.3. *Početnost množiny řešení.* V mnoha případech, kdy neumíme najít všechna řešení diofantické rovnice, se nám může alespoň podařit rozhodnout, zda řešení je konečně či nekonečně mnoho. Konečnost je například zaručena zjištěním, že hodnoty neznámých jsou v absolutní hodnotě menší než nějaké číslo. Pokud toto číslo nalezneme a je „rozumně“ malé, můžeme pak najít všechna řešení metodou popsanou v 5.4

To, že daná diofantická rovnice má řešení nekonečně mnoho, můžeme dokázat například tak, že nalezneme pro každou neznámou nějaký výraz s parametrem, a to takový, že po dosazení do rovnice dostaneme rovnost, přitom pro nekonečně mnoho hodnot parametru dostaneme navzájem různé hodnoty neznámých (jde tedy o jakousi zkoušku nekonečně mnoha řešení). Nebo můžeme nalézt jedno řešení rovnice a udat předpis, jak z libovolného řešení spočítat jiné. Máme-li zaručeno, že při další a další aplikaci tohoto předpisu dostáváme stále nová řešení (například jsou-li získávaná řešení stále větší a větší), opět tím dokážeme, že množina řešení je nekonečná. Je zřejmé, že při obou postupech mohou existovat ještě další nenalezená řešení.

Příklad. Dokažte, že diofantická rovnice

$$(x-1)^2 + (x+1)^2 = y^2 + 1$$

má nekonečně mnoho řešení.

Řešení. Rovnici snadno upravíme do tvaru[1]

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

Zkusme najít nějaké řešení. Po chvíli pokusů asi každý objeví, že volba $y = 3$, $x = 2$ vyhovuje dané rovnici. Představme si nyní, že máme k dispozici libovolné řešení $x, y \in \mathbb{Z}$ a pokusme se získat další. Platí tedy

$$\bigl(y + \sqrt{2}x\bigr)\bigl(y - \sqrt{2}x\bigr) = 1.$$

Dosazením nalezených hodnot $y = 3$ a $x = 2$ získáme rovnost $\bigl(3 + 2\sqrt{2}\,\bigr)\bigl(3 - 2\sqrt{2}\,\bigr) = 1$, vynásobením dostaneme

$$\bigl[\bigl(y + \sqrt{2}x\bigr)\bigl(3 + 2\sqrt{2}\,\bigr)\bigr] \cdot \bigl[\bigl(y - \sqrt{2}x\bigr)\bigl(3 - 2\sqrt{2}\,\bigr)\bigr] = 1.$$

Výrazy v obou hranatých závorkách upravíme. Platí

$$\bigl(y + \sqrt{2}x\bigr)\bigl(3 + 2\sqrt{2}\,\bigr) = 3y + 3\sqrt{2}x + 2\sqrt{2}y + 4x = (4x + 3y) + (3x + 2y)\sqrt{2},$$
$$\bigl(y - \sqrt{2}x\bigr)\bigl(3 - 2\sqrt{2}\,\bigr) = 3y - 3\sqrt{2}x - 2\sqrt{2}y + 4x = (4x + 3y) - (3x + 2y)\sqrt{2}.$$

Položme $u = 4x + 3y$, $v = 3x + 2y$. Platí tedy

$$\bigl(u + \sqrt{2}v\bigr)\bigl(u - \sqrt{2}v\bigr) = 1,$$

odkud

$$u^2 - 2v^2 = 1,$$

a tedy $u, v \in \mathbb{Z}$ je další řešení dané rovnice. Položíme-li $x_1 = 2$, $y_1 = 3$ a

$$x_{n+1} = 3x_n + 2y_n, \qquad y_{n+1} = 4x_n + 3y_n$$

pro libovolné $n \in \mathbb{N}$, dostáváme pro každé $n \in \mathbb{N}$ řešení x_n, y_n dané rovnice. A protože platí $0 < x_1 < x_2 < \dots$, $0 < y_1 < y_2 < \dots$, dostáváme pro různé indexy n různá řešení x_n, y_n. Daná rovnice má tedy nekonečně mnoho řešení. $\square$

Příklad. Dokažte, že rovnice

$$k + x^2 + y^2 = z^2$$

má pro libovolné celé číslo k nekonečně mnoho řešení v oboru přirozených čísel.

[1] Jde o speciální případ tzv. Pellovy rovnice

Řešení. Úpravou a rozkladem $z^2 - y^2$ dostaneme

$$k + x^2 = (z - y)(z + y).$$

Není nutné hledat všechna řešení, proto můžeme předpokládat, že

$$z - y = 1,$$
$$z + y = k + x^2.$$

Libovolné řešení této soustavy bude také řešení dané rovnice (neplatí to však obráceně, zkuste sami pro nějaké pevně zvolené k nalézt příklad přirozených čísel x, y, z vyhovujících dané rovnici, avšak nevyhovujících uvedené soustavě rovnic). Řešíme-li soustavu vzhledem k neznámým z, y, dostáváme

$$z = \tfrac{1}{2}(x^2 + k + 1),$$
$$y = \tfrac{1}{2}(x^2 + k - 1).$$

Zvolíme-li $x = |k| + 1 + 2t$, kde $t \in \mathbb{N}$, je x přirozené číslo. Platí

$$x^2 + k \equiv k + 1 + 2t + k \equiv 1 \pmod 2$$

a tedy $z = \frac{1}{2}((|k|+1+2t)^2+k+1) > 0$, $y = \frac{1}{2}((|k|+1+2t)^2+k-1) > 0$ jsou také přirozená čísla. Protože pro různá t dostáváme různá x a tedy různá řešení, má rovnice nekonečně mnoho řešení. $\square$

Příklad. Dokažte, že diofantická rovnice

$$5x^2 - 8xy + 5y^2 - 4k^2 = 0$$

má pro libovolné přirozené číslo k pouze konečně mnoho řešení.

Řešení. Danou rovnici upravíme do tvaru $(2x - y)^2 + (2y - x)^2 = 4k^2$, odkud plyne $(2x - y)^2 \leq (2k)^2$ a $(2y - x)^2 \leq (2k)^2$, a tedy $-2k \leq 2x - y \leq 2k$ a $-2k \leq 2y - x \leq 2k$. Sečtením první a dvojnásobku druhé nerovnosti a vydělením třemi dostaneme $-2k \leq y \leq 2k$ a zcela analogicky $-2k \leq x \leq 2k$. Protože x i y mohou pro pevné k nabývat pouze konečně mnoha hodnot, má daná rovnice pouze konečně mnoho řešení. $\square$