Literatura

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

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

[3] 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 [1] a [3], pro zájemce o bližší seznámení s nkterými tématy doporučujeme knihu [2], 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

Literatura 1
1. Základní pojmy 6
1.1. Dělitelnost 6
1.2. Největší společný dělitel a nejmenší společný násobek 9
1.3. Dělitelé a násobky mnoha čísel 14
1.4. Nesoudělnost 15
2. Prvočísla 18
3. Kongruence 31
3.1. Základní vlastnosti kongruencí 32
3.2. Aritmetické funkce 38
3.3. Eulerova funkce φ 41
3.4. Malá Fermatova věta, Eulerova věta 44

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 [1, §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:

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

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

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

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

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. $\square$

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 $q\in\mathbb{Z}$, $r\in\{0,1,\dots,m-1\}$ 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 $a'\in\{0,1,2,\dots,a-1\}$. Speciálně pro $a'=a-m$ tedy existují q',r' tak, že $a'=q'm+r'$ a přitom $r'\in\{0,1,\dots,m-1\}$. 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 $q'\in\mathbb{Z}$, $r'\in\{0,1,\dots,m-1\}$ 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 $a=q_1m+r_1=q_2m+r_2$. 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. $\square$

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). $\square$

Použití v Pari-GP. Výpočet největšího společného dělitele pomocí Eukli-dova 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\
00000000223
? bezout(A,B)
time = 0 ms.
%20 = [284455128205128205128205128205128205128205\
1282051282051282051282051282051282051282051282051\
282051358, -1422275641025641025641025641025641025\
6410256410256410256410256410256410256410256410256\
```

```
410256410256435, 300000000000000000000000000000000\
00000000000000000000000000000000000000000000000000\
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, ..., 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 $1 \leq i < j \leq n$, 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). $\square$

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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$. 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. $\square$

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/rsalabs/node.asp?id=2093`). 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* $m_1 \le n_1$, $m_2 \le n_2$, $\dots$, $m_k \le n_k$.
Číslo a má tedy právě

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

kladných dělitelů, jejichž součet je

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

(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 $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, $\ldots$, 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. 8 by bylo i N tvaru $3k+1$, což neplatí. Prvočíslo p ovšem nemůže být žádné z prvočísel $p_1, p_2, \ldots, p_n$, jak plyne z tvaru čísla N, a to je spor. □

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.pdf □

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. [2, kap. ???] □

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

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

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

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

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

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. $\square$

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. $a_1 \cdot d = b_1 \cdot d + m_1 dt$, odkud $a_1 = b_1 + m_1 t$, což podle lemmatu znamená, že $a_1 \equiv b_1 \pmod{m_1}$. □

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

Důkaz. Jestliže $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, podle lemmatu je rozdíl $a - b$ společný násobek čísel $m_1, m_2, \ldots, m_k$ 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 8 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

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

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

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

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

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

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

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*

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

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 $0 \leq \beta_i \leq \alpha_i$ pro všechna $i \in \{1, \dots, k\}$. Proto

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

□

S Möbiovou funkcí úzce souvisí pojem *Dirichletův součin*:

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

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

Lemma. *Dirichletův součin je asociativní.*

DŮKAZ.

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

$\square$

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 $0, 1, \ldots, m-1$).
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* $x_1, x_2, \ldots, x_{\varphi(m)}$ *tvoří redukovanou soustavu zbytků modulo* m*. Je-li* $a \in \mathbb{Z}$, $(a, m) = 1$ *pak i čísla* $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ *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 $x_1, x_2, \ldots, x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo m. Podle předchozího lemmatu je i $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo m. Platí tedy, že pro každé i existuje j (oba indexy jsou z množiny $\{1, 2, \ldots, \varphi(m)\}$) 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. $\square$

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

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

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.

$$2^1 = 2 \not\equiv 1 \pmod{7}$$
$$2^2 = 4 \not\equiv 1 \pmod{7}$$
$$2^3 = 8 \equiv 1 \pmod{7}$$

Řád čísla 2 modulo 7 je tedy roven 3. $\square$

Uveďme nyní několik zásadních tvrzení udávajících možné hodnoty 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 $r \mid t - s$. $\square$

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. □