$n = \sigma(m)$. Mezi dělitele čísla m přitom patří čísla m i n (a protože $\frac{m}{n} = 2^{k+1} - 1 > 1$, jsou tato čísla nutně různá), proto

$$2^{k+1} \cdot n = \sigma(m) \geq m + n = 2^{k+1} \cdot n,$$

a tedy $\sigma(m) = m+n$. To znamená, že m je prvočíslo s jedinými děliteli m a $n = 1$, odkud $a = 2^k \cdot (2^{k+1} - 1)$, kde $2^{k+1} - 1 = m$ je prvočíslo. □

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

Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Není bez zajímavosti, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět“ – pro Mersenneho čísla existuje poměrně jednoduchý a rychlý postup, jak ověřit, že jde o prvočísla. Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$.

Jakkoliv může být hledání největšího známého prvočísla chápáno jako pochybná zábava bez valného praktického užitku[2], jednak posunuje hranice matematického poznání a zdokonaluje použité metody (a často i hardware), navíc může přinést benefit i samotným objevitelům (Electronic Frontier Foundation vypsala odměny EFF Cooperative Computing Awards za nalezení prvočísla majícího alespoň $10^6, 10^7, 10^8$ a 10^9 číslic – odměny 50, resp. 100 tisíc dolarů za první dvě kategorie byly vyplaceny v letech 2000, resp. 2009 – v obou případech projektu GIMPS – na další odměny si ještě zřejmě nějaký čas počkáme).

2.2. Rozložení prvočísel.

> *There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision.*
>
> Don Zagier

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

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

[2]Viz např. titulek iDnes z 6.února 2013: *Největší známé prvočíslo na světě má 17 milionů číslic a je k ničemu*

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 $p_1, p_2, \ldots, p_n$. Položme $N = p_1 \cdot p_2 \ldots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \ldots, p_n$ (čísla $p_1, \ldots, p_n$ 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 $N = 3p_2 \cdot p_3 \cdot \cdots \cdot p_n + 2$. 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. 5 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. □

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 $4k+1$.

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

Věta 9. *(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. 16, s. 249-257] □

Poznámka. Dirichletovo tvrzení je ve skutečnosti daleko hlubší, říká totiž, že zvolíme-li libovolnou zbytkovou třídu modulo m, pak v ní buď není (až na jednu možnou výjimku) žádné prvočíslo, nebo je ve všech takových třídách prvočísel „zhruba stejně“ (tj. pravděpodobnost, že náhodně zvolené prvočíslo bude patřit do konkrétní třídy, je pro všechny třídy stejná a je rovna $\frac{1}{\varphi(m)}$).

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

Věta 10. *(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. □

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“, dokázaná nezávisle J. Hadamardem a Ch. J. de la Vallée-Poussinem v roce 1896.

Věta 11. *(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 1.

Hustotu rozmístění prvočísel v množině přirozených čísel, rovněž částečně popisuje následující Eulerův výsledek.

Věta 12. *(Euler) Je-li P množina všech prvočísel, pak*

$$\sum_{p \in P} \tfrac{1}{p} = \infty.$$

Poznámka. 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 mocniny.

Důkaz. Buď n libovolné přirozené číslo a $p_1, \ldots, p_{\pi(n)}$ všechna prvočísla nepřevyšující n. Položme

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Jednotlivé činitele lze chápat jako součet geometrické řady, proto

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(\sum_{\alpha_i=0}^{\infty} \frac{1}{p_i^{\alpha_i}}\right) = \sum \frac{1}{p_1^{\alpha_1} \cdots p_{\pi(n)}^{\alpha_{\pi(n)}}},$$

kde sčítáme přes všechny $\pi(n)$-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_{\pi(n)})$. Protože každé číslo nepřevyšující n se rozkládá pouze na prvočísla z množiny $\{p_1, \ldots, p_{\pi(n)}\}$, je určitě každé takové číslo v tomto součtu zahrnuto. Tedy $\lambda(n) > 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, a protože harmonická řada diverguje, je i $\lim_{n\to\infty} \lambda(n) = \infty$.

S využitím rozvoje funkce $\ln(1+x)$ do mocninné řady dále dostáváme

$$\ln \lambda(n) = -\sum_{i=1}^{\pi(n)} \ln\left(1 - \tfrac{1}{p_i}\right) = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} (m p_i^m)^{-1} =$$

$$= p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} (m p_i^m)^{-1}.$$

Protože vnitřní součet lze shora odhadnout jako

$$\sum_{m=2}^{\infty} (m p_i^m)^{-1} < \sum_{m=2}^{\infty} p_i^{-m} =$$

$$= p_i^{-2} \left(1 - p_i^{-1}\right)^{-1} \le 2 p_i^{-2},$$

umíme shora odhadnout i divergující posloupnost $\ln \lambda(n) < \sum_{i=1}^{\pi(n)} p_i^{-1} + 2 \sum_{i=1}^{\pi(n)} p_i^{-2}$. Druhý součet přitom zřejmě konverguje (viz konvergence

řady $\sum_{n=1}^{\infty} n^{-2}$), proto musí nutně divergovat první součet $\sum_{i=1}^{\pi(n)} p_i^{-1}$, což jsme chtěli dokázat. □

SW ukázka. 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

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. □

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 $0 \leq r < m$, 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 13. *(Základní vlastnosti kongruencí)*

(1) ***Kongruence*** *podle téhož modulu* ***můžeme sčítat****. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou.* ***K libovolné straně*** *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

$$a_1a_2 = (b_1 + mt_1)(b_2 + mt_2) = b_1b_2 + m(t_1b_2b_1t_2 + mt_1t_2),$$

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 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 $[m_1, m_2, \ldots, m_k]$, odkud plyne $a \equiv b \pmod{[m_1, \ldots, m_k]}$. □

(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 5 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 13 (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 13 (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 13 (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 13

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

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

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

Podle příkladu za větou 6 pro libovolné $k \in \{1, \ldots, p-1\}$ 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 13 (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. $\mu(4) = \mu(2^2) = 0, \mu(6) = \mu(2 \cdot 3) = (-1)^2, \mu(2) = \mu(3) = -1$.