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 13 (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.

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

Řád čísla 2 modulo 7 je tedy roven 3. □

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 $a, a^2, a^3, \ldots, a^{rs-1}$ není kongruentní s 1 modulo m, není ani žádné z čísel $a^r, a^{2r}, a^{3r}, \ldots, a^{(s-1)r}$ 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 $r \cdot s$.
Např pro $m = 13$ máme:
$a = 3$, $a^2 = 9 \pmod{13}$, $a^3 = 27 \equiv 1 \pmod{13} \Rightarrow 3$ 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 mod 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 18. *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 $q, z \in \mathbb{N}_0, 0 \leq z < r$.

„⇐“ 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.

„⇒“ 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 19. *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 20. *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 13(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 21. *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 22 (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 $\{2, 3, \ldots, p-2\}$ 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

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

□

4.2. Soustavy lineárních kongruencí o jedné neznámé. Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle Věty 21 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 23. *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