Kapitola 4

Kongruence, kvadratické zbytky, Legendreův symbol

4.1 Opakování z přednášky

Definice. Číslo a nazveme *kvadratickým zbytkem modulo* n, pokud kongruence

$$x^2 \equiv a \pmod{n}$$

má řešení.

Věta (27 z přednášky)**.** *Buď p liché prvočíslo a a číslo s ním nesoudělné. Pak kongruence $x^2 \equiv a \pmod{p}$ má řešení právě tehdy, když $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Definice. Pro prvočíslo p a číslo a definujeme *Legendreův symbol* předpisem

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ je kvadratický zbytek modulo } p, \\ -1 & a \text{ není kvadratický zbytek modulo } p, \\ 0 & a \text{ je soudělné s } p. \end{cases}$$

Čteme „a vzhledem k p“.

Jednoduchým důsledkem Věty je, že pro liché prvočíslo p a a s ním nesoudělné máme $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$. Nyní uvedeme další vlastnosti Legendreova symbolu.

i) Pokud $a \equiv b \pmod{p}$, pak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

ii) $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

iv) pro liché prvočíslo q platí $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$.

Pomocí těchto vlastností je možné Legendreův symbol dopočítat.

Zastavme se na chvíli u vlastnosti iii). U nich počítáme znaménko, jehož výpočet si můžeme zjednodušit. Vzpomeňme si na Příklad 1.1. Tam jsme dokázali, že pro libovolné n je zbytek n^2 po dělení osmi 0, 1, nebo 4. To jsme dokazovali tak, že jsme uvažovali n zbytkové třídy po dělení 4. Vzhledem k tomu, že p je liché prvočíslo, máme $p = 4k \pm 1$ pro nějaké $k \in \mathbb{N}$. Pak

$$p^2 - 1 = (4k \pm 1)^2 - 1 = 16k^2 \pm 8k + 1 - 1 = 8(2k^2 + k).$$

Tudíž $\frac{p^2-1}{8}$ bude tvaru $2k^2 \pm k$. Pak

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{2k^2 \pm k} = (-1)^{\pm k} = (-1)^k$$

a vidíme, že stačí najít k p nejbližší násobek 4 a podívat se na paritu podílu. Ten bude sudý, pouze pokud bude tento nejbližší násobek 4 dělitelný osmi, jinými slovy $p \pm 1 = 8l$, neboli $p \equiv \pm 1 \pmod 8$. Pokud bude podíl lichý, bude pak $p \pm 1 \equiv 4 \pmod 8$, neboli $p \equiv 3$ nebo $5 \pmod 8$. Tudíž máme pro p liché

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1 \text{ nebo } 7 \pmod 8, \\ -1 & p \equiv 3 \text{ nebo } 5 \pmod 8. \end{cases}$$

Podobně můžeme řešit i vlastnost iv). Zde bude exponent lichý pouze tehdy, pokud bude $\frac{p-1}{2}\frac{q-1}{2}$ liché, neboli pokud nebudou ani $p-1$ ani $q-1$ dělitelné 4, neboli pokud p i q budou kongruentní 3 modulo 4. Tedy můžeme napsat opět

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & p \equiv q \equiv 3 \pmod 4, \\ \left(\frac{p}{q}\right) & \text{jinak.} \end{cases}$$

4.2 Příklady řešené na cvičení

Příklad 4.1. Určete poslední cifru čísla $3^{7^{11^5}}$ a poslední dvě cifry čísla 13^{2024}.

Řešení. Hledáme vlastně (kladný) zbytek po dělení čísla $3^{7^{11^5}}$ desíti. Víme, že $3^2 = 9 \equiv -1 \pmod{10}$. Tudíž $3^4 \equiv 1 \pmod{10}$. Můžeme si napsat exponent $7^{11^5} = 4k + l$. Pak

$$3^{7^{11^5}} = 3^{4k+l} = (3^4)^k \cdot 3^l \equiv 1^k \cdot 3^l = 3^l \pmod{10}. \tag{4.1}$$

Musíme tedy určit l. Hledáme zbytek 7^{11^5} po dělení 4. Víme, že $7^2 = 49 \equiv 1 \pmod 4$. Napíšeme-li si exponent $11^5 = 2m + n$, uvidíme, že

$$7^{11^5} = 7^{2m+n} = (7^2)^m \cdot 7^n \equiv 1^m \cdot 7^n = 7^n \pmod 4. \tag{4.2}$$

Stačí tedy určit zbytek 11^5 po dělení 2. Ovšem 11 je liché číslo, 11^5 tedy také a $m = 1$. Pak, díky (4.2), máme

$$7^{11^5} \equiv 7^1 = 7 \equiv 3 \pmod 4,$$

tedy $l = 3$. Dosazením do (4.1) dostáváme

$$3^{7^{11^5}} \equiv 3^3 = 9 \cdot 3 \equiv -1 \cdot 3 = -3 \equiv 7 \pmod{10}$$

a poslední cifra čísla $3^{7^{11^5}}$ je 7.

Hledáme zbytek 13^{2024} po dělení 100. Víme, že $\varphi(100) = 40$, tedy $13^{40} \equiv 1 \pmod{100}$. Poté

$$13^{2024} = 13^{40 \cdot 50 + 24} = (13^{40})^{50} \cdot 13^{24} \equiv 13^{24} \pmod{100},$$

tedy stačí počítat mocniny 13 modulo 100. Máme

$$\begin{aligned} 13^2 &\equiv 69 \pmod{100} \\ 13^4 \equiv 69^2 &\equiv 61 \pmod{100} \\ 13^8 \equiv 61^2 &\equiv 21 \pmod{100} \\ 16^{16} \equiv 21^2 &\equiv 41 \pmod{100} \end{aligned}$$

a odtud $13^{24} = 13^{16} \cdot 13^8 \equiv 41 \cdot 21 \equiv 61 \pmod{100}$. Také bychom mohli zjistit, že $13^{20} = = 13^{16} \cdot 13^4 \equiv 41 \cdot 61 \equiv 1 \pmod{100}$, takže bychom viděli, že řád 13 modulo 100 je nejvýše 20 (ve skutečnosti je to 20, ověřte sami), takže pak bychom měli rovnou $13^{2024} = = 13^{101 \cdot 20 + 4} \equiv 13^4 \equiv 61 \pmod{100}$. Poslední dvě cifry čísla 13^{2024} jsou tedy 61.

Jiná, lepší, metoda je počítat zvlášť modulo 4 a modulo 25. Protože $13 \equiv 1 \pmod{4}$, máme rovnou, že $13^{2024} \equiv 1 \pmod{4}$. Jelikož $\varphi(25) = 5 \cdot 4 = 20$, máme $13^{20} \equiv 1 \pmod{25}$. (Odtud bychom viděli, že řád 13 modulo 100 je 20.) Pak $13^{2024} \equiv 13^4 \pmod{25}$, takže počítáme

$$\begin{aligned} 13^2 = 169 &\equiv -6 \pmod{25}, \\ 13^4 \equiv (-6)^2 = 36 &\equiv 11 \pmod{25}, \end{aligned}$$

tudíž 13^{2024} je kongruentní 1 modulo 4 a 11 modulo 25. Řešením soustavy lineárních kongruencí pak dostaneme, že $13^{2024} \equiv 61 \pmod{100}$. △

Příklad 4.2. Určete všechna $n \in \mathbb{N}$ taková, že

a) $5^{3n+4} \equiv 8 \pmod{13}$;

b) $5^{2^{3n+1}} \equiv -7 \pmod{22}$.

Řešení. Začneme a). Nejprve zjistíme řád 5 modulo 13. Víme, že $5^2 = 25 \equiv -1 \pmod{13}$, tedy $5^4 \equiv 1 \pmod{13}$ a řád 5 je 4. Tudíž si můžeme výraz upravit

$$5^{3n+4} \equiv 5^{3n} = (5^3)^n = (5^2 \cdot 5)^n \equiv (-1 \cdot 5)^n = (-5)^n \pmod{13}.$$

Následně zjistíme, že $-5 \equiv 8 \pmod{13}$, tudíž kongruence platí pro $n = 1$. Jelikož řád 5 modulo 13 je 4, budou se kongruence opakovat s periodou 4. Dostáváme tedy, že tak bude pro $n = 4k + 1$, neboli $n \equiv 1 \pmod{4}$.

Řešíme b). Upravujeme si výraz

$$5^{2^{3n+1}} = 5^{2\cdot 2^{3n}} = (5^2)^{2^{3n}} \equiv 3^{(2^3)^n} = 3^{8^n} \pmod{22}$$

neboť $25 \equiv 3 \pmod{22}$. Následně můžeme počítat rekurentně $3^{8^{n+1}} = \left(3^{8^n}\right)^8$ modulární mocniny. Pak

- $n = 1$:
$$3^8 = (3^4)^2 = 81^2 \equiv (-7)^2 = 49 \equiv 5 \pmod{22}$$
- $n = 2$:
$$3^{8^2} = 3^{8\cdot 8} = \left(3^8\right)^8 \equiv 5^8 = 25^4 \equiv 3^4 = 81 \equiv -7 \pmod{22}$$
(Zde vidíme, že pro $n = 2$ kongruence platí.)
- $n = 3$:
$$3^{8^3} = \left(3^{8^2}\right)^8 \equiv (-7)^8 = 7^8 = 49^4 \equiv 5^4 = 25^2 \equiv 3^2 = 9 \pmod{22}$$
- $n = 4$:
$$3^{8^4} = \left(3^{8^3}\right)^8 \equiv 9^8 = 3^{16} = \left(3^8\right)^2 \equiv 5^2 \equiv 3 \pmod{22}$$

takže pro $n \geq 5$ můžeme využít rekurentního vztahu, posloupnost bude periodická (jelikož $3^{8^5} = \left(3^{8^4}\right)^8 \equiv 3^8$ atd.). Celkem tedy máme

$$5^{2^{3n+1}} \equiv 3^{8^n} \equiv \begin{cases} 3 & n \equiv 0 \pmod 4 \\ 5 & n \equiv 1 \pmod 4 \\ -7 & n \equiv 2 \pmod 4 \\ 9 & n \equiv 3 \pmod 4 \end{cases} \pmod{22},$$

takže řešením jsou všechna n kongruentní 2 modulo 4. △

Příklad 4.3. Určete, zda je 7 kvadratickým zbytkem modulo 13.

Řešení. Jinými slovy řešíme, jestli má kongruence $x^2 \equiv 7 \pmod{13}$ řešení. Použijeme Větu 27 z přednášky. Kongruence má řešení právě tehdy, když $7^{\frac{13-1}{2}} \equiv 1 \pmod{13}$. Počítáme tedy 7^6 modulo 13. $7^2 = 49 \equiv -3 \pmod{13}$, takže

$$7^6 = \left(7^2\right)^3 \equiv (-3)^3 = -27 \equiv -1 \not\equiv 1 \pmod{13}$$

a 7 není kvadratickým zbytkem modulo 13. Skutečně, můžeme si do tabulky s využitím toho, že $x \equiv 13 - x \pmod{13}$, napsat do tabulky hodnoty druhých mocnin modulo 13

x	± 1	± 2	± 3	± 4	± 5	± 6
x^2 modulo 13	1	4	-4	3	-1	-3

odkud vidíme, že jedinými kvadratickými zbytky modulo 13 jsou ±1, ±3 a ±4. $\triangle$

Příklad 4.4. Řešte kongruenci $3\,x^2 + x - 5 \equiv 0 \pmod{13}$.

Řešení. Polynom $3\,x^2 + x - 5$ nemá v $\mathbb{Z}$ kořeny, dále postupujeme podobně jako bychom řešili kvadratickou rovnici v $\mathbb{C}$, totiž úpravou na čtverec, kde ovšem počítáme modulo 13, tedy místo dělení násobíme modulární inverzí.[1]

Nejprve si polynom vynásobíme modulární inverzí k 3. Jelikož $3{\cdot}4 = 12 \equiv -1 \pmod{13}$, máme

$$3\,x^2 + 4 - 5 \equiv x^2 - 4\,x + 20 \equiv x^2 - 4\,x + 7.$$

Nyní již přímo upravujeme na čtverec, protože 4 se dá vydělit dvěma. Neboť $(x-2)^2 = x^2 - 4\,x + 4$, $x^2 - 4\,x = (x-2)^2 - 4$, a tudíž je původní polynom kongruentní $(x-2)^2 + 3$, tedy původní kongruence je ekvivalentní kongruenci

$$(x-2)^2 \equiv -3 \pmod{13}.$$

Tato má řešení, neboť -3 je kvadratický zbytek modulo 13 (viz konec řešení Příkladu 4.3, odkud také vidíme, že $x - 2 \equiv \pm6 \pmod{13}$), neboli $x \equiv 8$ nebo $9 \pmod{13}$. $\triangle$

Příklad 4.5. Řešte kongruence $x^2 - 3\,x - 10 \equiv 0$ a $x^2 - 3\,x - 14 \equiv 0 \pmod{49}$.

Řešení. Nejprve řešíme kongruenci $x^2 - 3\,x - 10 \equiv 0 \pmod{49}$. V $\mathbb{Z}[x]$ máme rozklad $x^2 - 3\,x - 10 = (x+2)\,(x-5)$, tedy automaticky $x \equiv -2$ nebo $5 \pmod{49}$ je řešením kongruence. Zjistíme, zda existují i jiná řešení metodou úpravy na čtverec.[2]

Zjistíme modulární inverzi k 2. Máme $2 \cdot 25 = 50 \equiv 1 \pmod{49}$. Pak naše verze „$\frac{3}{2}$“ je $3 \cdot 25 = 75 \equiv 26 \pmod{49}$. Pak máme $2 \cdot 26 \equiv 3 \pmod{49}$, tedy můžeme doplnit na čtverec, pouze dopočítáme 26^2 modulo 49. Máme

$$26^2 = 2^2 \cdot 13^2 = (4 \cdot 13) \cdot 13 = 52 \cdot 13 \equiv 3 \cdot 13 = 39 \equiv -10 \pmod{49},$$

tedy

$$(x - 26)^2 \equiv x^2 - 3\,x - 10 \pmod{49}.$$

Vidíme, že 26 také řeší naši kongruenci. Máme tedy $x^2 - 3\,x - 10 \equiv 0$ pro $x \equiv -2$, 5 nebo $26 \pmod{49}$.[3]

Polynom $x^2 - 3\,x - 14$ nad $\mathbb{Z}$ nerozložíme (ověřte sami), ale můžeme si jej díky předchozímu vyjádřit jako

$$x^2 - 3\,x - 14 = x^2 - 3\,x - 10 - 4 \equiv (x - 26)^2 - 4 \pmod{49}$$

[1] Ve skutečnosti fakt, že 13 je prvočíslo, dává, že zbytkové třídy modulo 13 spolu se sčítáním a násobením tvoří těleso, takže polynomiální kongruence může mít nejvýše tolik řešení, kolik je stupeň polynomu.

[2] 49 není prvočíslo, tudíž zbytkové třídy modulo 49 netvoří těleso a může se stát, že polynomy mohou mít více „kořenů“ (tj. čísel, kde hodnota je dělitelná 49), než je stupeň polynomu. Kupříkladu kongruence $x^2 - 1 \equiv 0 \pmod{8}$ má čtyři kořeny, ±1 a ±3, i když je stupeň polynomu pouze 2.

[3] Zde si všimněte $26 \equiv -2 \equiv 5 \pmod{7}$. $49 = 7^2$ je mocnina prvočísla. Pokud bychom uvažovali projekci řešení úlohy modulo 7 (což je prvočíslo, takže máme maximálně dvě řešení), budou všechna kongruentní (modulo 7 bychom dostali polynom $(x+2)^2$). Podobně, u polynomu $x^2 - 1$ modulo 8 jsou všechna řešení kongruentní modulo 2.

kde na pravé straně máme rozdíl druhých mocnin, takže si jej můžeme napsat jako

$$(x-26)^2 - 2^2 = (x-26-2)\,(x-26+2) = (x-28)\,(x-24),$$

tudíž řešeními kongruence $x^2 - 3\,x - 14 \equiv 0$ jsou pouze $x \equiv 24$ nebo $28 \pmod{49}$. △

Příklad 4.6. Řešte kongruenci $x^2 \equiv 58 \pmod{163}$.

Řešení. Nejprve zjistíme, jestli je 58 kvadratickým zbytkem modulo 163 (sami ověřte, že je to prvočíslo). Využijeme k tomu Legendreův symbol. Máme rozklad $58 = 2 \cdot 29$ Počítáme

$$\left(\frac{58}{163}\right) = \left(\frac{2}{163}\right) \cdot \left(\frac{29}{163}\right)$$

díky vlastnosti ii),

$$= (-1)^{\frac{163^2-1}{8}} \cdot \left(\frac{163}{29}\right) \cdot (-1)^{\frac{163-1}{2}\,\frac{29-1}{2}}$$

díky vzorcům z vlastností iii) a iv), kde $(-1)^{\frac{163^2-1}{8}} = -1$, neboť $163 \equiv 3 \pmod 8$, a $(-1)^{\frac{163-1}{2}\,\frac{29-1}{2}} = 1$, jelikož $29 \equiv 1 \pmod 4$,

$$= -\left(\frac{18}{29}\right) = -\left(\frac{2}{29}\right) \cdot \left(\frac{3}{29}\right)^2 = -(-1)^{\frac{29^2-1}{8}} = 1$$

díky vlastnostem i) a ii), přičemž trojku máme ve druhé mocnině, takže druhá mocnina Legendreova symbolu bude jistě 1 ($(3, 29) = 1$), a pro dvojku použijeme stejný vzoreček a $(-1)^{\frac{29^2-1}{8}} = -1$, jelikož $29 \equiv 5 \pmod 8$. 58 tedy je kvadratický zbytek modulo 163 a můžeme přejít k řešení kongruence. Máme

$$58^{\frac{163-1}{2}} = 58^{81} \equiv \left(\frac{58}{163}\right) = 1 \pmod{163}$$

tedy si celou rovnici můžeme vynásobit jedničkou, zleva psanou jako 1 a zprava jako 58^{81}. Dostaneme

$$x^2 \equiv 58^{82} \pmod{163}$$

tedy odmocněním získáme $x \equiv \pm 58^{41} \pmod{163}$. Zbývá spočítat modulární mocniny 58. Máme

$$\begin{aligned} 58^2 &= 3\,364 \equiv 104 \equiv -59 && \pmod{163} \\ 58^3 &\equiv -59 \cdot 58 = -3\,422 \equiv 1 && \pmod{163} \end{aligned}$$

tudíž vidíme, že $58^{41} \equiv 58^2 \equiv -59$, tedy vidíme, že řešeními jsou $x \equiv 59$ nebo $104 \pmod{163}$. △

Příklad 4.7. Řešte kongruenci $x^2 \equiv 58 \pmod{157}$.

Řešení. Opět nejprve s pomocí Legendreova symbolu ověříme, že má kongruence řešení (sami ověřte, že je 157 prvočíslo). Máme

$$\left(\frac{58}{157}\right) = \left(\frac{2}{157}\right) \cdot \left(\frac{29}{157}\right) = (-1)^{\frac{157^2-1}{8}} \cdot \left(\frac{157}{29}\right) \cdot (-1)^{\frac{157-1}{2}\,\frac{29-1}{2}}$$

díky vlastnostem ii), iii) a iv), přičemž $(-1)^{\frac{157^2-1}{8}} = -1$, jelikož $157 \equiv 5 \pmod{8}$, a $(-1)^{\frac{157-1}{2}\,\frac{29-1}{2}} = 1$, protože $29 \equiv 1 \pmod{4}$,

$$= -\left(\frac{12}{29}\right) = -\left(\frac{3}{12}\right) \cdot \left(\frac{2}{29}\right)^2 = -\left(\frac{3}{29}\right) = -\left(\frac{29}{3}\right) \cdot (-1)^{\frac{29-1}{2}\,\frac{3-1}{2}}$$

díky vlastnostem i), ii) a iv), dále se 2 vyskytuje v druhé mocnině a $(-1)^{\frac{29-1}{2}\,\frac{3-1}{2}} = 1$, protože $29 \equiv 1 \pmod{4}$,

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

díky vlastnosti i) a tomu, že 2 není kvadratický zbytek modulo 3 (všechny druhé mocniny dávají zbytek 0 nebo 1). Kongruence tedy má řešení. Můžeme přistoupit k samotnému řešení. Již nemůžeme použít trik s násobením $58^{78} \equiv 1 \pmod{157}$, protože bychom na pravé straně dostali lichou mocninu. Odmocněním $58^{78} \equiv 1$ dostaneme $58^{39} \equiv \pm 1 \pmod{157}$, zbývá určit znaménko. (Pokud by to byla jednička, mohli bychom rovnici vynásobit 58^{39}, pokud -1, musíme vymyslet něco jiného.) Například modulárním umocňováním získáme

$$\begin{aligned} 58^1 &= 58 & 58^8 &\equiv 14 \\ 58^2 &\equiv 67 & 58^{16} &\equiv 39 \\ 58^4 &\equiv 93 & 58^{32} &\equiv 108 \end{aligned}$$

tedy $58^{39} = 58^{32+4+2+1} \equiv (108 \cdot 93) \cdot (67 \cdot 58) \equiv -4 \cdot 118 \equiv -1 \pmod{157}$. Dále víme, že 2 není kvadratický zbytek modulo 157 (spočítali jsme výše), tedy $2^{78} \equiv \left(\frac{2}{157}\right) = -1$, tím pádem $4^{39} = 2^{78} \equiv -1 \pmod{157}$. Pak $4^{39} \cdot 58^{39} \equiv (-1) \cdot (-1) = 1 \pmod{157}$. Vynásobíme-li si kongruenci $x^2 \equiv 58 \pmod{157}$ čtyřmi, ovšem psáno vlevo jako 4 a vpravo jako $4^{40} \cdot 58^{39}$, dostaneme

$$4\,x^2 \equiv 4^{40} \cdot 58^{40} \pmod{157}$$

odkud odmocněním získáme $2\,x \equiv \pm 2^{40} \cdot 58^{20}$. Vynásobením modulární inverzí k dvojce, tedy $\frac{158}{2} = 79$ dostaneme

$$x \equiv \pm (4 \cdot 58)^{20} \cdot 79 \pmod{157}.$$

Zbývá určit modulární třídu výrazu napravo. $4 \cdot 58 = 232 \equiv 75 \pmod{157}$, dále

$$\begin{aligned}
75^2 &\equiv -27 && \pmod{157} \\
75^4 &\equiv (-27)^2 \equiv -56 && \pmod{157} \\
75^8 &\equiv (-56)^2 \equiv -4 && \pmod{157} \\
75^{16} &\equiv (-4)^2 = 16 && \pmod{157} \\
75^{20} &= 75^{16} \cdot 75^4 \equiv -56 \cdot 16 \equiv 46 && \pmod{157}
\end{aligned}$$

a vynásobením modulární inverzí ke dvojce, 79, dostaneme, že $(4 \cdot 58)^{20} \cdot 79 \equiv 23 \pmod{157}$. Tudíž máme řešení $x \equiv 23$ nebo $134 \pmod{157}$. △