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

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

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

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

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

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

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

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

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

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

Řešení. Protože 383 je prvočíslo a $(2, \varphi(383)) = 2$, z Věty 27 plyne, že daná kongruence je řešitelná (a má 2 řešení), právě tehdy, když $219^{\frac{383}{2}} = 219^{191} \equiv 1 \pmod{383}$. Ověření platnosti není bez použití výpočetní techniky snadné (i když je to pořád ještě „na papíře“ vyčíslitelné). Závěrem této části tuto podmínku ověříme s pomocí Legendreova symbolu daleko snadněji.

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

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

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

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

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

Důkaz. ad 1. Pro $p \mid a$ je tvrzení zřejmé; pokud je a kvadratický zbytek modulo p, pak tvrzení plyne z Věty 27. Z téže věty plyne, že v případě kvadratického nezbytku je $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Pak ale, protože $p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$ nutně $p \mid a^{\frac{p-1}{2}} + 1$, tj. $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

ad 2. Podle 1. dostáváme

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

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

ad 3. Zřejmé z definice. □

$\left(\frac{a}{p}\right) = -1$ nezbytek
$\left(\frac{b}{p}\right) = 1$ zbytek
$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = -1 \cdot 1 = -1$ nezbytek

Důsledek. *1. V libovolné redukované soustavě zbytků modulo p je stejný počet kvadratických zbytků a nezbytků.* $p \neq 2$

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

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

$p = 7$

a	± 1	± 2	± 3
$a^2 (7)$	1	4	2

kvadratické zbytky mod 7: 1, 2, 4
nezbytky: 3, 5, 6

Důkaz. ad 1. Kvadratické zbytky získáme tak, že všechny prvky redukované soustavy zbytků umocníme na druhou. Těchto prvků je $p - 1$, přitom druhé mocniny 2 prvků jsou spolu kongruentní právě tehdy, když je součet těchto prvků násobkem p. Máme tedy právě $\frac{p-1}{2}$ kvadratických zbytků, a tedy rovněž $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ kvadratických nezbytků modulo p. Předpoklad, že p je prvočíslo, je podstatný – pro složená čísla je kvadratických nezbytků více než zbytků (viz dále část o Jacobiho symbolu).

$a^2 \equiv b^2 \pmod p$
$\Updownarrow$
$p \mid a^2 - b^2 = (a+b)(a-b)$
$\iff a \equiv \pm b \pmod p$

ad 2. Tvrzení je zřejmé z předchozího lemmatu.

ad 3. Zřejmé. □

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

Tvrzení 4.6. *Prvočísel tvaru $4k + 1$ je nekonečně mnoho.*

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

$p = 7$:
$a = 3$
$1, 2, \frac{p-1}{2} = 3$
$1 \cdot a, 2 \cdot a, 3 \cdot a$
$3 \quad 6 \quad 9$
$3 \quad -1 \quad 2$
S

Nyní odvodíme další pravidla pro výpočet Legendreova symbolu.

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

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

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

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

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

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

$\mu_p(a)$
$\left(\frac{a}{p}\right) = (-1)$

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

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

Př: $\left(\frac{3}{7}\right) = -1$
$\left(\frac{3}{11}\right) = +1$
$x^2 \equiv 3 (11)$ má řeš. $x \equiv \pm 5 (11)$

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

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

$$1 \cdot a \equiv \pm m_1 \pmod p$$
$$2 \cdot a \equiv \pm m_2 \pmod p$$
$$\dots\dots$$
$$\frac{p-1}{2} \cdot a \equiv \pm m_{\frac{p-1}{2}} \pmod p$$

$\{m_1, m_2, \dots, m_{\frac{p-1}{2}}\} = \{1, 2, \dots, \frac{p-1}{2}\}$

dostáváme

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

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

Př: z Gaussova lze přímo dokázat: (i) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$; (ii) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

ad i) $a=-1$: $-1,-2,\dots,-\frac{p-1}{2}\in S \Rightarrow \mu_p(-1)=\frac{p-1}{2} \Rightarrow \left(\frac{-1}{p}\right)=(-1)^{\mu_p(-1)}=(-1)^{\frac{p-1}{2}}$

všechna záporná

$S=\{1,2,\dots,2k\}$

ad ii) $p\equiv 1\ (4)$ $a=2$: $2\cdot 1, 2\cdot 2,\dots,2\cdot 2k$, přičemž: $2\cdot 1, 2\cdot 2,\dots,2\cdot k, 2\cdot(k+1),\dots,2\cdot 2k$ $\equiv 2, 4, \dots, 2k, -(2k-1), \dots, -1$ $\Rightarrow \mu_p(2)=k=\frac{p-1}{4}$

$p=4k+1 \Rightarrow \frac{p-1}{2}=2k$

$S=\{1,2,\dots,2k+1\}$

$p\equiv 3\ (4)$, $p=4k+3 \Rightarrow \frac{p-1}{2}=2k+1$: $2\cdot 1,\dots,2\cdot k, 2\cdot(k+1),\dots,2(2k+1)$ $\equiv 2,\dots,2k,-(2k+1),\dots,-1$ $\Rightarrow \mu_p(2)=k+1=\frac{p+1}{4}$

(mezi pravými stranami je jich právě μ záporných). Po vydělení obou stran číslem $((p-1)/2)!$ dostáváme díky vztahu $(a/p)\equiv a^{\frac{p-1}{2}} \pmod p$ požadované tvrzení. □

Souhrnně: $\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{4}\cdot\frac{p+1}{2}}=(-1)^{\frac{p+1}{4}\cdot\frac{p-1}{2}}=(-1)^{\frac{p^2-1}{8}}$

Carl Friedrich Gauß – 8 důkazů (1801)

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

Věta 32. *Nechť p,q jsou lichá prvočísla. Pak*

1. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ kvadratická reciprocita $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

ad 1. Máme již dokázáno, nebo plyne z Gaussova L.

Důkaz. Věta se v tomto tvaru uvádí zejména proto, že pomocí těchto tří vztahů a základních pravidel pro úpravy Legendreova symbolu jsme schopni vypočítat hodnotu (a/p) pro libovolné celé číslo a. První část tvrzení již máme dokázánu, v dalším nejprve odvodíme mezivýsledek, který využijeme k důkazu zbylých částí. Poznamenejme rovněž, že v literatuře existuje mnoho různých důkazů této věty (v roce 2010 uváděl F. Lemmermeyer 233 důkazů), obvykle ovšem využívajících (zejména u těch stručnějších z nich) hlubších znalostí z algebraické teorie čísel.

$x=[x]+\langle x\rangle$, $[x]\in\mathbb{Z}$, $0\le\langle x\rangle<1$, $[\pi]=3$, $[-4{,}5]=-5$, $z\in\mathbb{Z}: [z+x]=z+[x]$

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

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

$$\left[\frac{2ak}{p}\right]=\left[2\underbrace{\left[\frac{ak}{p}\right]}_{\in\mathbb{Z}}+2\left\langle\frac{ak}{p}\right\rangle\right]=2\left[\frac{ak}{p}\right]+\left[2\overbrace{\left\langle\frac{ak}{p}\right\rangle}^{\langle 0,1)}\right].$$

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

$p=11$, $a=3$, $k=3$: $\left\langle\frac{3\cdot 3}{11}\right\rangle=\frac{9}{11}>\frac{1}{2}$, $3\cdot 3\equiv -2\ (11)$

Proto je

$$\left(\frac{a}{p}\right)\overset{\text{G.L.}}{=}(-1)^{\mu}\overset{\text{vyšetřeno výše}}{=}(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{2ak}{p}\right]}.$$

$\frac{a+p}{2}\to a$

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

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

$\left[\frac{(a+p)k}{p}\right]=\left[\frac{ak}{p}\right]+k$

$1+2+\dots+\frac{p-1}{2}$
$\frac{p-1}{2}+\dots+1$
$\frac{p+1}{2}+\dots+\frac{p+1}{2}$
$\Sigma=\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot\frac{1}{2}=\frac{p^2-1}{8}$

Celkem tak dostáváme (pro liché a)

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

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

$\Rightarrow \left(\frac{2}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\underbrace{\left[\frac{k}{p}\right]}_{=0}}\cdot(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^2-1}{8}}$

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

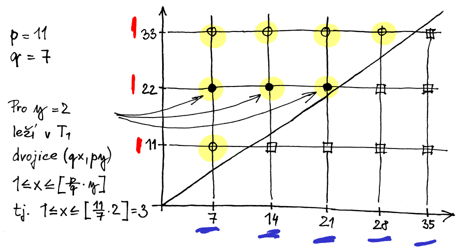
$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}.$$

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

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

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

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



$[qx, py]$ $qx \neq py$

T_1 „nad“

T_2 „pod“

čímž budeme vzhledem k předchozímu hotovi.

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

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

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

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

$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

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

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

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

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

Je řešitelná $x^2 \equiv 79 \pmod{101}$?

ANO

Řešení.

$$\left(\frac{79}{101}\right) \overset{+}{=} \left(\frac{101}{79}\right) \qquad \textit{neboť 101 dává po dělení 4 zbytek 1}$$

79 je prvočíslo

$$= \left(\frac{22}{79}\right) \qquad 101 \equiv 22\ (79)$$

$$= \left(\frac{2}{79}\right) \cdot \left(\frac{11}{79}\right) \qquad 79 \equiv -1\ (8) \Rightarrow \left(\frac{2}{79}\right) = 1$$

$$= \left(\frac{11}{79}\right) \qquad \textit{neboť 79 dává po dělení 8 zbytek -1}$$

$$= (-1)\left(\frac{79}{11}\right) \qquad \textit{neboť 11 i 79 dávají po dělení 4 zbytek 3}$$

$$= (-1)\underbrace{\left(\frac{2}{11}\right)}_{= -1} = 1 \qquad \textit{neboť 11 dává pod dělení 8 zbytek 3}$$

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

b nemusí být prvočíslo

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

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

se nazývá *Jacobiho symbol*.

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

$$\left(\frac{a}{b}\right) = -1 \;\Downarrow\; x^2 \equiv a\ (b)\ \text{N.R.}$$

Příklad.

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

a přitom kongruence

$$x^2 \equiv 2 \pmod{15} \qquad \left(\frac{2}{3}\right) = -1$$

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

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

Tvrzení 4.7. *Nechť $b, b' \in \mathbb{N}$ jsou lichá, $a, a_1, a_2 \in \mathbb{Z}$ libovolná. Pak platí:*

1. $a_1 \equiv a_2 \pmod{b} \implies \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$,
2. $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$,
3. $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$.

Lemma. *Buďte $a, b \in \mathbb{N}$ lichá. Pak platí*

1. $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$,
2. $\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod{2}$.

Důsledek. *Pro $a_1, \dots, a_m \in \mathbb{N}$ lichá platí*

1. $\sum_{k=1}^{m} \frac{a_k-1}{2} \equiv \frac{\prod_{k=1}^{m} a_k - 1}{2} \pmod{2}$,
2. $\sum_{k=1}^{m} \frac{a_k^2-1}{8} \equiv \frac{\prod_{k=1}^{m} a_k^2 - 1}{8} \pmod{2}$.

Věta 33. *Nechť $a, b \in \mathbb{N}$ jsou lichá. Pak*
$(a,b)=1$

1. $\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$,
2. $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$,
3. $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$. (příp. $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)\cdot(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$)

Důkaz. Snadný. □

4.8. Aplikace Legendreova a Jacobiho symbolu. Primární motivací k zavedení Jacobiho symbolu byla potřeba vyčíslení Legendreova symbolu (a tedy rozhodnutí o řešitelnosti kvadratických kongruencí) bez nutnosti rozkladu čísel na prvočísla. Ukažme si proto příklad takového výpočtu.

Příklad. Rozhodněte o řešitelnosti kongruence $x^2 \equiv 219 \pmod{383}$.

Řešení. 383 je prvočíslo, proto bude kongruence řešitelná, bude-li Legendreův symbol $(219/383) = 1$.

Jacobiho symbol

$$\begin{aligned}
\left(\frac{219}{383}\right) &= -\left(\frac{383}{219}\right) && \text{(Jacobi) 383 i 219 dávají po dělení 4 zbytek 3}\\
&= -\left(\frac{164}{219}\right) = -\left(\frac{4}{219}\right)\cdot\left(\frac{41}{219}\right)\\
&= -\left(\frac{41}{219}\right) && 164 = 2^2 \cdot 41\\
&= -\left(\frac{219}{41}\right) && \text{(Jacobi) neboť 41 dává po dělení 4 zbytek 1}\\
&= -\left(\frac{14}{41}\right)\\
&= -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)\\
&= -\left(\frac{7}{41}\right) && \text{neboť 41 dává pod dělení 8 zbytek 1}\\
&= -\left(\frac{41}{7}\right) && \text{neboť 41 dává pod dělení 4 zbytek 1}\\
&= -\left(\frac{-1}{7}\right) = 1 && \text{neboť 7 dává po dělení 4 zbytek 3.}
\end{aligned}$$

Výpočet podstatně efektivnější, než výpočet $219^{191} \stackrel{?}{\equiv} 1 \pmod{383}$

① je a kvadr. zbytek mod p? $\left(\frac{a}{p}\right) = ?$

Další aplikací je v jistém smyslu opačná otázka: *Pro která prvočísla je dané číslo a kvadratickým zbytkem?* (tuto otázku již umíme odpovědět např. pro $a = 2$). Prvním krokem je zodpovězení této otázky pro prvočísla.

② která a jsou kv. zbytky mod p? $x \in \{\pm 1, \dots, \pm \frac{p-1}{2}\}$ x^2 dají kv. zbytky mod 11:

x	±1	±2	±3	±4	±5
x^2 (11)	1	4	9	5	3

③ dáno a, pro která p je a kv. zbytek?

Věta 34. *Nechť q je liché prvočíslo.*

- *je-li $q \equiv 1 \pmod 4$, pak je q kvadratický zbytek modulo ta prvočísla p, která splňují $p \equiv r \pmod q$, kde r je kvadratický zbytek modulo q.*
- *je-li $q \equiv 3 \pmod 4$, pak je q kvadratický zbytek modulo ta prvočísla p, která splňují $p \equiv \pm b^2 \pmod{4q}$, kde b je liché a nesoudělné s q.*

Důkaz. První tvrzení plyne triviálně ze zákona kvadratické reciprocity. Nechť tedy $q \equiv 3 \pmod 4$, tj. $(q/p) = (-1)^{\frac{p-1}{2}}(p/q)$. Nechť nejprve $p \equiv +b^2 \pmod{4q}$, kde b je liché. Pak $p \equiv b^2 \equiv 1 \pmod 4$ a $p \equiv b^2 \pmod q$. Tedy $(-1)^{\frac{p-1}{2}} = 1$ a $(p/q) = 1$, odkud $(q/p) = 1$. Je-li nyní $p \equiv -b^2 \pmod{4q}$, pak obdobně $p \equiv -b^2 \equiv 3 \pmod 4$ a $p \equiv -b^2 \pmod q$. Tedy $(-1)^{\frac{p-1}{2}} = -1$ a $(p/q) = -1$, odkud opět $(q/p) = 1$.

Obráceně, mějme $(q/p) = 1$. Máme dvě možnosti – buď $(-1)^{\frac{p-1}{2}} = 1$ a $(p/q) = 1$, nebo $(-1)^{\frac{p-1}{2}} = -1$ a $(p/q) = -1$. V prvním případě je $p \equiv 1 \pmod 4$ a existuje b tak, že $p \equiv b^2 \pmod q$ (lze přitom předpokládat, že b liché). Pak ale $b^2 \equiv 1 \equiv p \pmod 4$ a celkem $p \equiv b^2 \pmod{4q}$. V druhém případě je $p \equiv 3 \pmod 4$ a existuje b liché tak, že $p \equiv -b^2 \pmod q$. Tedy $-b^2 \equiv 3 \equiv p \pmod 4$ a celkem $p \equiv -b^2 \pmod{4q}$. □

Příklad. Určete modulo která prvočísla je

a) 3 $\left(\frac{a}{p}\right) = 1$? $1 = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}}$

$\left(\frac{p}{3}\right) = 1 \wedge (-1)^{\frac{p-1}{2}} = 1$; $p \equiv 1 (3) \wedge p \equiv 1 (4)$; $p \equiv 1 (12)$

b) -3

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

c) 6

$p \equiv 2 (3) \wedge p \equiv 3 (4)$; $p \equiv -1 (12)$

kvadratickým zbytkem.

Odpověď: $p \equiv \pm 1 \pmod{12}$

Následující tvrzení ukazuje, že pokud je modul kvadratické kongruence prvočíslo splňující $p \equiv 3 \pmod 4$, pak umíme nejen rozhodnout o řešitelnosti kongruenci, ale rovněž popsat všechna řešení.

Tvrzení 4.8. *Nechť $p \equiv 3 \pmod 4$, $a \in \mathbb{Z}$ splňují $(a/p) = 1$. Pak má kongruence $x^2 \equiv a \pmod p$ řešení*

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p.$$

Důkaz. Ověříme snadno zkouškou

$$(\pm a^{\frac{p+1}{4}})^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot \left(\frac{a}{p}\right) \equiv a \pmod p.$$

$a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \wedge \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$

□

Pro dokreslení obrazu o kvadratických zbytcích a nezbytcích formulujeme ještě jedno tvrzení (pro nepříliš obtížný důkaz euklidovského typu viz [**3**]).

Věta 35. *Nechť $a \in \mathbb{N}$ není druhou mocninou. Pak existuje nekonečně mnoho prvočísel, pro která je a kvadratickým nezbytkem.*