Kongruence

7. kapitola. Kongruence vyšších stupňů o jedné neznámé. Kvadratické kongruence o jedné neznámé s prvočíselným modulem

In: Alois Apfelbeck (author): Kongruence. (Czech). Praha: Mladá fronta, 1968. pp. 85–124.

7. kapitola

KONGRUENCE VYŠŠÍCH STUPŇŮ O JEDNÉ NEZNÁMÉ. KVADRATICKÉ KONGRUENCE O JEDNÉ NEZNÁMÉ S PRVOČÍSELNÝM MODULEM

Ve čtvrté kapitole jsme se seznámili s pojmy algebraická rovnice n-tého stupně o jedné neznámé a kongruence n-tého stupně o jedné neznámé. V této kapitole budeme nejprve zkoumat počet reálných řešení algebraické rovnice n-tého stupně s reálnými koeficienty a počet řešení kongruence n-tého stupně o jedné neznámé ve zvolené úplné soustavě zbytků podle daného modulu.

Víme, že každá lineární rovnice s reálnými koeficienty má právě jedno reálné řešení. Avšak už u kvadratických rovnic nastává situace složitější. Každá kvadratická rovnice s reálnými koeficienty má, jak známo, dva kořeny, které jsou však obecně komplexní. Mohou nastat z našeho hlediska celkem tři kvalitativně různé případy.

1. Rovnice má dva reálné kořeny vzájemně různé. Tak je tomu např. u rovnice $x^2 - 5x + 6 = 0$, kde $x_1 = 2$, $x_2 = 3$.
2. Rovnice má jeden dvojnásobný reálný kořen, jako je tomu např. u rovnice $x^2 - 4x + 4 = 0$, kde $x_1 = x_2 = 2$.
3. Rovnice má dva komplexní kořeny, které jsou vzájemně různé. Tak je tomu např. u rovnice $x^2 + 1 = 0$, kde $x_1 = \mathrm{i}$, $x_2 = -\mathrm{i}$.

Shrneme-li tyto tři případy, můžeme říci, že každá kvadratická rovnice s reálnými koeficienty má nejvýše dvě vzájemně různá reálná řešení.

V algebře se dokazuje obecně věta, že každá rovnice n-tého stupně s reálnými koeficienty má nejvýše n navzájem různých reálných řešení.

Podrobnějším studiem těchto otázek se zabývá např. učebnice [6].

Věta, kterou jsme právě vyslovili, nemá u kongruencí o jedné neznámé obecně platné obdoby. To jsme konečně už poznali u lineárních kongruencí (viz příklad 20) a ještě se s tím setkáme u kongruencí vyšších stupňů (příklad 37). Přesto však pro některé speciální případy modulů budeme moci pro kongruence vyslovit větu analogickou (viz větu 36).

V dalším textu budeme stále předpokládat, že

$$P_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

je polynom n-tého stupně s celočíselnými koeficienty.

Nechť $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, kde $p_1, p_2, \ldots, p_r$ jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_r$ přirozená čísla. V páté kapitole jsme zobecněním věty 33 poznali, že kongruence n-tého stupně o jedné neznámé.

$$P_n(x) \equiv 0 \bmod m \tag{61}$$

je ekvivalentní se soustavou kongruencí n-tého stupně o jedné neznámé

$$P_n(x) \equiv 0 \bmod p_i^{\alpha_i} \ (i = 1, 2, \ldots, r). \tag{62}$$

Z tvrzení a) věty 33 plyne, že nemá-li některá z kongruencí (62) řešení, nemá řešení ani kongruence (61). Z tvrzení c) této věty pak plyne, že označíme-li písmenem ν počet řešení kongruence (61) vzájemně inkongruentních podle modulu m a písmenem ν_i počet řešení kongruence $P_n(x) \equiv 0 \bmod p_i^{\alpha_i}$ vzájemně inkongruent-

ních podle modulu $p_i^{\alpha_i}$ ($i = 1, 2, \ldots, r$), bude platit

$$\nu = \nu_1 \nu_2 \ldots \nu_r. \tag{63}$$

Vět 33 a 32 lze tedy principiálně vždy užít jak ke stanovení počtu řešení kongruence (61), tak i k nalezení těchto řešení. Znamená to ovšem, že dovedeme určit počet řešení každé z r kongruencí soustavy (62), resp. že dovedeme tato řešení najít. Jak to lze někdy provést prakticky, ukážeme na jednoduchém příkladě.

Příklad 37. Řešte kongruenci 6. stupně o jedné neznámé

$$x^6 - 1 \equiv 0 \bmod 35.$$

Řešení. Poněvadž $35 = 5.7$ a $(5, 7) = 1$, rozpadne se daná kongruence na soustavu dvou kongruencí o jedné neznámé

$$x^6 - 1 \equiv 0 \bmod 5,$$

$$x^6 - 1 \equiv 0 \bmod 7.$$

Abychom našli řešení kongruence $x^6 - 1 \equiv 0 \bmod 5$, uvážíme, že podle (39) pro všechna celá x platí $x^5 \equiv x \bmod 5$. Bude tedy $x^6 \equiv x^2 \bmod 5$, takže místo kongruence $x^6 - 1 \equiv 0 \bmod 5$ budeme řešit ekvivalentní kongruenci $x^2 - 1 \equiv 0 \bmod 5$. Snadno zjistíme, že tato kongruence má v každé úplné soustavě zbytků podle modulu 5 dvě vzájemně inkongruentní řešení. V úplné soustavě zbytků $\{0, 1, 2, 3, 4\}$ podle modulu 5 budou těmito řešeními čísla 1 a 4.

Podobně podle (38) vidíme, že řešením kongruence $x^6 - 1 \equiv 0 \bmod 7$ v úplné soustavě zbytků $\{0, 1, 2, 3, 4, 5, 6\}$ podle modulu 7 bude kterékoliv z šesti čísel 1, 2, 3, 4, 5, 6.

Podle (63) bude mít tedy kongruence $x^6 - 1 \equiv 0$ mod 35 v každé úplné soustavě zbytků podle modulu 35 celkem dvanáct řešení, která budou podle tohoto modulu vzájemně inkongruentní. Abychom tato řešení našli, určíme podle věty 31 řešení neurčité rovnice $7u - 5v = 1$. Zřejmě bude $u = 3$ a $v = 4$, takže pro řešení x kongruence $x^6 - 1 \equiv 0$ mod 35 dostaneme podle (52)

$$x \equiv 21x_1 - 20x_2 \bmod 35,$$

kde x_1 je některé z čísel 1 a 4 a nezávisle na tom x_2 některé z čísel 1, 2, 3, 4, 5, 6. Postupně tedy bude

$$\begin{aligned}
x &\equiv 21.1 - 20.1 \equiv 1 \bmod 35,\\
x &\equiv 21.1 - 20.2 \equiv 16 \bmod 35,\\
x &\equiv 21.1 - 20.3 \equiv 31 \bmod 35,\\
x &\equiv 21.1 - 20.4 \equiv 11 \bmod 35,\\
x &\equiv 21.1 - 20.5 \equiv 26 \bmod 35,\\
x &\equiv 21.1 - 20.6 \equiv 6 \bmod 35,\\
x &\equiv 21.4 - 20.1 \equiv 29 \bmod 35,\\
x &\equiv 21.4 - 20.2 \equiv 9 \bmod 35,\\
x &\equiv 21.4 - 20.3 \equiv 24 \bmod 35,\\
x &\equiv 21.4 - 20.4 \equiv 4 \bmod 35,\\
x &\equiv 21.4 - 20.5 \equiv 19 \bmod 35,\\
x &\equiv 21.4 - 20.6 \equiv 34 \bmod 35.
\end{aligned}$$

Kongruence $x^6 - 1 \equiv 0$ mod 35 má tedy v každé úplné soustavě zbytků podle modulu 35 dvanáct vzájemně inkongruentních řešení. V úplné soustavě zbytků $\{0, 1, 2, \ldots, 34\}$ podle modulu 35 jsou těmito řešeními čísla 1, 4, 6, 9, 11, 16, 19, 24, 26, 29, 31 a 34.

Ekvivalence kongruence (61) se soustavou kongruencí (62) nám dovoluje zabývat se pouze kongruencemi se speciálním modulem $m = p^\alpha$, kde p je prvočíslo a α přirozené číslo. Budeme proto chvíli věnovat pozornost kongruencím tohoto tvaru.

Předpokládejme, že x_1 je libovolné řešení kongruence n-tého stupně o jedné neznámé

$$P_n(x) \equiv 0 \bmod p^\alpha, \tag{64}$$

tj. že platí $P_n(x_1) \equiv 0 \bmod p^\alpha$. Pro každé přirozené číslo $\alpha > 1$ je však $p | p^\alpha$, takže podle věty 18 bude též $P_n(x_1) \equiv 0 \bmod p$. Odtud vidíme, že každé řešení kongruence (64) bude též řešením kongruence

$$P_n(x) \equiv 0 \bmod p. \tag{65}$$

Řešení kongruence (64) můžeme proto hledat mezi řešeními kongruence (65). Nemá-li kongruence (65) řešení, nemůže mít řešení ani kongruence (64).

Dá se však dokázat, že z každého řešení kongruence (65) lze za určitých předpokladů sestrojit řešení kongruence (64). Známe-li nějaké řešení kongruence (65), je třeba pro konstrukci řešení kongruence (64) řešit ještě $\alpha - 1$ už pouze lineárních kongruencí tvaru $ax + b \equiv 0 \bmod p^\beta$, kde $1 \leqq \beta < \alpha$ a $p^\beta | a$, $p^\beta | b$. Obecnou teorií lineárních kongruencí tohoto typu jsme se však nezabývali. Kromě toho zmíněná konstrukce vyžaduje hlubších znalostí některých vlastností polynomů, které však už přesahují rámec této publikace.

Proto se až do konce této knihy omezíme pouze na studium kongruencí vyšších stupňů o jedné neznámé s prvočíselným modulem tvaru (65).

Věta 35. *Budiž p prvočíslo a nechť kongruence n-tého stupně o jedné neznámé*

$$P_n(x) \equiv 0 \bmod p$$

má více než n řešení, která jsou podle modulu p vzájemně inkongruentní.

Potom vztah $P_n(x) \equiv 0 \bmod p$ *platí pro všechna celá čísla* x.

Důkaz provedeme matematickou indukcí podle n. Nechť $n = 1$ a nechť kongruence

$$a_0 x + a_1 \equiv 0 \bmod p$$

má alespoň dvě řešení x_1 a x_2, která jsou inkongruentní podle modulu p. Bude tedy

$$a_0 x_1 + a_1 \equiv 0 \bmod p,$$
$$a_0 x_1 + a_1 \equiv 0 \bmod p.$$

Odečtením těchto kongruencí dostaneme

$$a_0(x_1 - x_2) \equiv 0 \bmod p.$$

Poněvadž však $x_1 - x_2 \not\equiv 0 \bmod p$, bude podle věty 13 $a_0 \equiv 0 \bmod p$. Odtud a ze vztahu $a_0 x_1 + a_1 \equiv 0 \bmod p$ pak plyne, že též $a_1 \equiv 0 \bmod p$. Ježto

$$a_0 \equiv 0 \bmod p,$$
$$a_1 \equiv 0 \bmod p,$$

dostaneme podle věty 17, že pro každé celé číslo x platí

$$a_0 x + a_1 \equiv 0 \bmod p.$$

Tím jsme dokázali, že tvrzení věty je správné pro $n = 1$.

Předpokládejme nyní, že věta 35 platí pro jisté přirozené číslo n. Dokážeme, že z tohoto předpokladu plyne její správnost i pro přirozené číslo $n + 1$.

Nechť

$$P_{n+1}(x) = a_0 x^{n+1} + a_1 x^n + a_2 x^{n-1} + \ldots + a_{n-1} x^2 + a_n x + a_{n+1}$$

a nechť kongruence $(n + 1)$-tého stupně o jedné neznámé

$$P_{n+1}(x) \equiv 0 \bmod p \tag{66}$$

má alespoň $n + 2$ řešení $x_1, x_2, \ldots, x_{n+1}, x_{n+2}$, která jsou vzájemně inkongruentní podle modulu p. Platí tedy

$$P_{n+1}(x_i) \equiv 0 \bmod p \ (i = 1, 2, \ldots, n + 1, n + 2), \tag{67}$$

přičemž pro $i \neq k$ $(i, k = 1, 2, \ldots, n + 1, n + 2)$ bude

$$x_i \not\equiv x_k \bmod p. \tag{68}$$

Poněvadž tedy

$$P_{n+1}(x_{n+2}) \equiv 0 \bmod p,$$

bude pro všechna celá čísla x platit

$$P_{n+1}(x) \equiv P_{n+1}(x) - P_{n+1}(x_{n+2}) \bmod p. \tag{69}$$

Avšak

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = a_0(x^{n+1} - x_{n+2}^{n+1}) + a_1(x^n - x_{n+2}^n) + \\ + a_2(x^{n-1} - x_{n+2}^{n-1}) + \ldots + a_{n-2}(x^3 - x_{n+2}^3) + \\ + a_{n-1}(x^2 - x_{n+2}^2) + a_n(x - x_{n+2}).$$

Poněvadž platí

$$x^{n+1} - x_{n+2}^{n+1} = (x - x_{n+2})(x^n + x_{n+2}x^{n-1} + x_{n+2}^2x^{n-2} + \\ + \ldots + x_{n+2}^{n-1}x + x_{n+2}^n),$$

$$x^n - x_{n+2}^n = (x - x_{n+2})(x^{n-1} + x_{n+2}x^{n-2} + x_{n+2}^2x^{n-3} + \\ + \ldots + x_{n+2}^{n-2}x + x_{n+2}^{n-1}),$$

$$x^{n-1} - x_{n+2}^{n-1} = (x - x_{n+2})(x^{n-2} + x_{n+2}x^{n-3} + x_{n+2}^2x^{n-4} +$$

$$+ \ldots + x_{n+2}^{n-3}x + x_{n+2}^{n-2}),$$
$$\vdots$$
$$x^3 - x_{n+2}^3 = (x - x_{n+2})(x^2 + x_{n+2}x + x_{n+2}^2),$$
$$x^2 - x_{n+2}^2 = (x - x_{n+2})(x + x_{n+2}),$$

můžeme dále psát

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = (x - x_{n+2})[a_0(x^n + x_{n+2}x^{n-1} + x_{n+2}^2x^{n-2} + \ldots + x_{n+2}^{n-1}x + x_{n+2}^n) + a_1(x^{n-1} + x_{n+2}x^{n-2} + x_{n+2}^2x^{n-3} + \ldots + x_{n+2}^{n-2}x + x_{n+2}^{n-1}) + a_2(x^{n-2} + x_{n+2}x^{n-3} + x_{n+2}^2x^{n-4} + \ldots + x_{n+2}^{n-3}x + x_{n+2}^{n-2}) + \ldots + a_{n-2}(x^2 + x_{n+2}x + x_{n+2}^2) + a_{n-1}(x + x_{n+2}) + a_n].$$

Avšak x_{n+2} je známé číslo. Proto výraz v hranaté závorce bude opět polynom v proměnné x. V tomto polynomu najdeme nejvýše n-tou mocninu proměnné x, přičemž koeficient u x^n je a_0. Půjde tedy o polynom n-tého stupně a označíme-li jej $P_n(x)$, dostaneme konečně

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = (x - x_{n+2})\,P_n(x).$$

Po dosazení tohoto výsledku do (69) tedy obdržíme

$$P_{n+1}(x) \equiv (x - x_{n+2})\,P_n(x) \bmod p. \qquad (70)$$

Dosadíme-li do tohoto vztahu za x postupně čísla x_1, x_2, ..., x_{n+1}, dostaneme vzhledem k (67)

$$(x_i - x_{n+2})\,P_n(x_i) \equiv 0 \bmod p \quad (i = 1, 2, \ldots, n+1),$$

odkud vzhledem k (68) podle věty 13 plyne, že

$$P_n(x_i) \equiv 0 \bmod p \quad (i = 1, 2, \ldots, n+1).$$

Z toho vidíme, že kongruence n-tého stupně o jedné neznámé $P_n(x) \equiv 0 \bmod p$ má alespoň $n + 1$ řešení $x_1, x_2, \ldots, x_{n+1}$, která jsou vzájemně inkongruentní podle modulu p. Poněvadž jsme předpokládali, že věta 35 platí pro přirozené číslo n, bude tedy pro všechna celá čísla x platit $P_n(x) \equiv 0 \bmod p$. Ze vztahu (70) pak plyne, že pro všechna celá čísla x platí též

$$P_{n+1}(x) \equiv 0 \bmod p,$$

což jsme chtěli dokázat.

Ukážeme si dva zajímavé důsledky věty 35. Prvním z nich bude

věta 36. *Budiž $P_n(x)$ polynom n-tého stupně a nechť existuje celé číslo x_0 tak, že $P_n(x_0) \not\equiv 0 \bmod p$. Potom kongruence n-tého stupně o jedné neznámé s prvočíselným modulem*

$$P_n(x) \equiv 0 \bmod p$$

má nejvýše n řešení, která jsou vzájemně inkongruentní podle modulu p.

Důkaz této věty provedeme nepřímo. Kdyby kongruence n-tého stupně o jedné neznámé $P_n(x) \equiv 0 \bmod p$ měla více než n řešení vzájemně inkongruentních podle modulu p, platilo by podle věty 35 $P_n(x) \equiv 0 \bmod p$ pro všechna celá čísla x. To však by byl spor s předpokladem $P_n(x_0) \not\equiv 0 \bmod p$. Proto může daná kongruence mít nejvýše n řešení vzájemně inkongruentních podle modulu p, což jsme měli dokázat.

Druhým důsledkem věty 35 je

věta 37. *Pro každé prvočíslo p platí*

$$(p-1)! + 1 \equiv 0 \bmod p. \tag{71}$$

Důkaz. Pro $p = 2$ je vztah (71) zřejmě správný, neboť $(2-1)! + 1 = 2$ a $2 \equiv 0 \bmod 2$.

Předpokládejme tedy, že p je liché prvočíslo, a utvořme polynom

$$Q(x) = (x-1).(x-2). \ldots .(x-p+1) - x^{p-1} + 1.$$

Snadno nahlédneme, že v tomto polynomu je koeficient u x^{p-1} roven nule a koeficient u x^{p-2} roven číslu $-\frac{p(p-1)}{2}$. Stupeň polynomu $Q(x)$ je tedy $p-2$.

Zvolíme-li za ξ kterékoliv z čísel $1, 2, \ldots, p-1$, dostaneme $Q(\xi) = -\xi^{p-1} + 1$. Pro tato ξ je však podle (38)

$$\xi^{p-1} \equiv 1 \bmod p,$$

takže

$$Q(\xi) \equiv 0 \bmod p.$$

Čísla $1, 2, \ldots, p-1$ tedy představují $p-1$ řešení kongruence $Q(x) \equiv 0 \bmod p$ vzájemně inkongruentních podle tohoto modulu. Poněvadž stupeň kongruence $Q(x) \equiv 0 \bmod p$ je $p-2$, platí podle věty 35 vztah $Q(x) \equiv 0 \bmod p$ pro každé celé číslo x. Položíme-li nyní $x = 0$, dostaneme

$$(-1).(-2). \ldots .(-(p-1)) + 1 \equiv 0 \bmod p.$$

Poněvadž p je liché prvočíslo, plyne z posledního vztahu ihned vztah (71), což jsme měli dokázat.

Vztah (71) bývá v teorii čísel nazýván Wilsonovou

větou. Poprvé byl uveřejněn ve Waringově pojednání *Meditationes Algebraicae* v roce 1770.

Porovnáme-li věty 12 a 13 z kapitoly 2, dále příklad 37 a větu 36 a konečně úlohu 9 (kapitola 3) a větu 37, zjistíme, že věty 13, 36 a 37 jsou charakteristickými pro kongruence s prvočíselnými moduly, neboť neplatí pro kongruence s moduly složenými. Z vět 14 a 36 je mimoto zřejmé, že kongruence s prvočíselnými moduly mají ve srovnání s kongruencemi se složenými moduly další vlastnosti, které jsou analogické s vlastnostmi rovností resp. algebraických rovnic.

V další části této kapitoly se budeme podrobněji zabývat kvadratickými kongruencemi o jedné neznámé s prvočíselným modulem. Celkem jednoduchá a málo zajímavá situace nastává pro $p = 2$. Proto se budeme věnovat pouze studiu kvadratických kongruencí tvaru

$$a_0x^2 + a_1x + a_2 \equiv 0 \bmod p, \tag{72}$$

kde p je liché prvočíslo, přičemž $p \nmid a_0$.

Nejprve budeme studovat speciální kvadratické kongruence tvaru

$$x^2 - a \equiv 0 \bmod p, \tag{73}$$

kde a je dané číslo.

Příklad 38. Vyšetřte kvadratické kongruence o jedné neznámé:

a) $x^2 - 5 \equiv 0 \bmod 11$;

b) $x^2 - 7 \equiv 0 \bmod 11$.

Řešení. Probíhá-li x úplnou soustavou zbytků $\{0, 1, 2, \ldots, 10\}$ podle modulu 11, bude podle tohoto modulu číslo x^2 postupně kongruentní s čísly 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1. Z toho je patrné, že $4^2 - 5 \equiv 0 \bmod 11$,

$7^2 - 5 \equiv 0 \bmod 11$. Dále vidíme, že pro každé celé x z dané úplné soustavy zbytků je $x^2 - 7 \not\equiv 0 \bmod 11$.

Odpověď.

a) Kongruence $x^2 - 5 \equiv 0 \bmod 11$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 10\}$ podle modulu 11 dvě řešení $x_1 = 4$ a $x_2 = 7$.

b) Kongruence $x^2 - 7 \equiv 0 \bmod 11$ nemá žádné řešení.

Předpokládejme, že $p \nmid a$ a že x_1 je řešením kongruence (73). Položme $x_2 = p - x_1$. Protože $x_2^2 = p^2 - 2px_1 + x_1^2$, vidíme, že $x_2^2 \equiv x_1^2 \bmod p$ a tedy též $x_2^2 - a \equiv x_1^2 - a \equiv 0 \bmod p$. Číslo x_2 je proto rovněž řešením kongruence (73). Dokážeme si ještě, že řešení x_1 a x_2 jsou podle modulu p inkongruentní. Kdyby totiž bylo $x_1 \equiv x_2 \bmod p$, měli bychom po dosazení za x_2 $x_1 \equiv p - x_1 \bmod p$, z čehož pak by plynulo $2x_1 \equiv 0 \bmod p$. Protože p je liché prvočíslo, dostali bychom z tohoto vztahu konečně $x_1 \equiv 0 \bmod p$, takže by bylo též $a \equiv x_1^2 \equiv 0 \bmod p$. To by však bylo ve sporu s předpokladem, že $p \nmid a$. Proto řešení x_1 a $x_2 = p - x_1$ jsou podle modulu p inkongruentní.

Jestliže $p \mid a$, přejde kongruence (73) v triviální kongruenci $x^2 \equiv 0 \bmod p$, jejíž jediné řešení v úplné soustavě zbytků $\{0, 1, 2, \ldots, p - 1\}$ je $x_1 = 0$.

Z této úvahy a příkladů 38a) a b) tedy plyne, že kvadratická kongruence (73) nemá buďto žádné řešení, nebo má v každé úplné soustavě zbytků podle modulu p jedno řešení, nebo konečně má v každé úplné soustavě zbytků podle modulu p dvě řešení vzájemně inkongruentní podle tohoto modulu. Z věty 36 pak plyne, že žádná jiná možnost nemůže nastat.

Zabývejme se nyní otázkou, kdy kongruence (73) má řešení. Přitom není třeba vyšetřovat případy, kdy $p|a$, neboť pro $p|a$ má zmíněná kongruence vždy řešení $x_1 \equiv 0 \bmod p$.

Definice 11. *Nechť* $(a, p) = 1$. *Má-li kongruence* (73) *řešení, nazýváme číslo* a *kvadratickým zbytkem podle modulu* p. *Nemá-li kongruence* (73) *řešení, nazýváme číslo* a *kvadratickým nezbytkem podle modulu* p.

Příklad 39. Najděte všechny kvadratické zbytky a všechny kvadratické nezbytky podle modulu 17 z redukované soustavy zbytků $\{0, 1, 2, \ldots, 16\}$ podle tohoto modulu.

Řešení. Necháme-li x probíhat redukovanou soustavou zbytků $\{1, 2, 3, \ldots, 16\}$ podle modulu 17, bude x^2 kongruentní podle modulu 17 postupně s čísly 1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1. Kvadratickými zbytky podle modulu 17 budou tedy čísla 1, 2, 4, 8, 9, 13, 15, 16, kvadratickými nezbytky pak čísla 3, 5, 6, 7, 10, 11, 12 a 14.

Věta 38. *Nechť* p *je liché prvočíslo. Potom v každé redukované soustavě zbytků podle modulu* p *je právě* $\frac{p-1}{2}$ *kvadratických zbytků a* $\frac{p-1}{2}$ *kvadratických nezbytků podle modulu* p.

Důkaz. Budeme hledat kvadratické zbytky ležící v redukované soustavě zbytků $\{1, 2, 3, \ldots, p-1\}$ podle modulu p. Probíhá-li číslo x touto redukovanou soustavou, budou kvadratické zbytky podle modulu p ležet v těch zbytkových třídách podle tohoto modulu, ve kterých leží čísla $1^2, 2^2, 3^2, \ldots, (p-1)^2$. Libovolný reprezentant kterékoliv z těchto tříd bude tedy kvadra-

tickým zbytkem podle modulu p, takže pro stanovení počtu kvadratických zbytků stačí určit, kolik z těchto tříd je navzájem různých.

Snadno nahlédneme, že probíhá-li x postupně čísly $1, 2, 3, \ldots, \frac{p-1}{2}$, bude výraz $p - x$ probíhat až na pořadí zbývajícími čísly redukované soustavy zbytků $\{1, 2, 3, \ldots, p-1\}$. Poněvadž dále $(p-x)^2 \equiv x^2 \bmod p$, leží čísla x^2 a $(p-x)^2$ vždy ve stejné zbytkové třídě podle modulu p (srovnej s příkladem 39), takže se můžeme omezit na stanovení počtu vzájemně různých zbytkových tříd podle modulu p, ve kterých leží čísla

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Dokážeme si, že tyto třídy jsou vzájemně různé.

Předpokládejme, že existují přirozená čísla x_1 a x_2 tak, že

$$x_1^2 \equiv x_2^2 \bmod p, \tag{74}$$

přičemž platí

$$\left.\begin{aligned} 1 \leqq x_1 \leqq \frac{p-1}{2}, \\ 1 \leqq x_2 \leqq \frac{p-1}{2}. \end{aligned}\right\} \tag{75}$$

Z kongruence (74) plyne, že $x_1^2 - x_2^2 \equiv 0 \bmod p$, tj. že

$$(x_1 + x_2)(x_1 - x_2) \equiv 0 \bmod p. \tag{76}$$

Sečtením obou nerovností (75) dostaneme dále

$$2 \leqq x_1 + x_2 \leqq p - 1 < p,$$

takže podle výsledku úlohy 2 bude $p \nmid (x_1 + x_2)$. Z kon-

gruence (76) pak podle věty 13 plyne, že $x_1 \equiv x_2 \bmod p$. Odtud pak vzhledem k nerovnostem (75) dostaneme podle věty 14 rovnost $x_1 = x_2$.

Jestliže tedy čísla x_1 a x_2 vyhovují nerovnostem (75) a je $x_1 \neq x_2$, nemůže být $x_1^2 \equiv x_2^2 \bmod p$, takže zbytkové třídy podle modulu p, ve kterých leží čísla 1^2, 2^2, 3^2, ..., $\left(\frac{p-1}{2}\right)^2$, jsou vzájemně různé. Počet kvadratických zbytků podle modulu p je roven počtu těchto tříd, tj. číslu $\frac{p-1}{2}$. V redukované soustavě zbytků $\{1, 2, 3, \ldots, p-1\}$ je tedy $\frac{p-1}{2}$ kvadratických zbytků podle modulu p. Zbývající čísla této soustavy, kterých je $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$, jsou tudíž kvadratickými nezbytky podle modulu p, čímž máme větu 38 dokázánu.

Při počítání s kvadratickými kongruencemi je třeba umět rychle rozhodnout, zda dané číslo je kvadratickým zbytkem nebo nezbytkem podle modulu p. Existuje řada kritérií, podle kterých lze toto rozhodnutí učinit. Dokážeme si některá z nich.

Věta 39. *Budiž p liché prvočíslo a nechť $p \nmid a$. Potom platí:*

a) Číslo a je kvadratickým zbytkem podle modulu p právě tehdy, je-li

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p. \tag{77}$$

b) Číslo a je kvadratickým nezbytkem podle modulu p právě tehdy, je-li

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p. \tag{78}$$

Důkaz. Vyšetřme nejprve kongruenci

$$u^{p-1} - 1 \equiv 0 \bmod p. \tag{79}$$

Poněvadž pro $u_0 = 0$ je $-1 \not\equiv 0 \bmod p$, má tato kongruence podle věty 36 nejvýše $p - 1$ řešení, která jsou vzájemně inkongruentní podle modulu p. Avšak podle (38) bude řešením kongruence (79) každé z čísel 1, 2, 3, ..., $p - 1$, takže kongruence (79) má právě $p - 1$ řešení, která jsou vzájemně inkongruentní podle modulu p.

Poněvadž p je liché prvočíslo, je číslo $\frac{p-1}{2}$ celé, takže kongruenci (79) můžeme přepsat ve tvaru

$$(u^{\frac{p-1}{2}} - 1)(u^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p.$$

Podle věty 13 tedy pro každé celé číslo u, které vyhovuje tomuto vztahu, platí buďto

$$u^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p, \tag{80}$$

nebo

$$u^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p. \tag{81}$$

Vztahy (80) a (81) nemohou platit současně, neboť v opačném případě bychom jejich odečtením dostali $-2 \equiv 0 \bmod p$, což není možné.

Každé řešení kongruence (79) je tedy řešením právě jedné z kongruencí (80) a (81). To znamená, že každá z těchto kongruencí má právě $\frac{p-1}{2}$ řešení, která jsou vzájemně inkongruentní podle modulu p.

Nechť nyní číslo a je kvadratickým zbytkem podle modulu p. Potom podle definice 11 má kongruence (73) řešení x_1. Poněvadž $p \nmid a$, platí též $p \nmid x_1$, takže podle (38) bude $x_1^{p-1} \equiv 1 \bmod p$. Ze vztahu $x_1^2 \equiv a \bmod p$ pak podle (18) dostaneme $(x_1^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p$. Shrnutím těchto výsledků obdržíme konečně $a^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \bmod p$. Tím jsme dokázali, že pro každý kvadratický zbytek podle modulu p platí vztah (77), tj. každý kvadratický zbytek podle modulu p je řešením kongruence (80). Avšak kongruence (80) má právě tolik řešení, kolik je v dané redukované soustavě kvadratických zbytků podle modulu p (viz větu 38). Z toho plyne, že číslo a je kvadratickým zbytkem podle modulu p právě tehdy, je-li řešením kongruence (80), tj. platí-li vztah (77). Tím jsme dokázali tvrzení a).

Dokažme ještě tvrzení b). Protože každý kvadratický nezbytek podle modulu p je řešením kongruence (79), bude řešením právě jedné z kongruencí (80) a (81). Z dokázaného tvrzení a) plyne, že číslo a je kvadratickým nezbytkem podle modulu p právě tehdy, neplatí-li vztah (77), tj. není-li řešením kongruence (80). To je však možné právě tehdy, je-li řešením kongruence (81), tj. platí-li vztah (78). Tím máme dokázáno i tvrzení b).

Příklad 40. Určete, která z čísel 5, 20, 26 a 30 jsou kvadratickými zbytky a která jsou kvadratickými nezbytky podle modulu 41.

Řešení. Užitím známých pravidel pro počítání s kongruencemi, případně i užitím vztahu (38) dostaneme postupně:

a) $5^{20} = 25^{10}$, $25 \equiv -16 \bmod 41$, takže $5^{20} \equiv (-2^4)^{10} \bmod 41$, tj. $5^{20} \equiv 2^{40} \equiv 1 \bmod 41$;

b) $20^{20} = 2^{40}.5^{20}$, $2^{40} \equiv 1 \bmod 41$, $5^{20} \equiv 1 \bmod 41$, tedy $20^{20} \equiv 1 \bmod 41$;

c) $26^{20} = 2^{20}.13^{20} = 2^{20}.169^{10}$, $169 \equiv 5 \bmod 41$, $169^{10} \equiv 5^{10} \bmod 41$, $5^{10} \equiv (-16)^5 \bmod 41$, takže $26^{20} \equiv 2^{20}.(-16)^5 \bmod 41$, tj. $26^{20} \equiv -2^{40} \equiv -1 \bmod 41$;

d) $30^{20} \equiv (-11)^{20} \bmod 41$, $(-11)^{20} = 121^{10}$ a $121 \equiv -2 \bmod 41$, takže $30^{20} \equiv (-2)^{10} \bmod 41$; avšak $(-2)^{10} = 1024$ a $1024 \equiv -1 \bmod 41$, takže $30^{20} \equiv -1 \bmod 41$.

Odpověď. Čísla 5 a 20 jsou kvadratickými zbytky a čísla 26 a 30 kvadratickými nezbytky podle modulu 41.

Abychom nemuseli obšírně vypisovat „kvadratický zbytek podle modulu p" nebo „kvadratický nezbytek podle modulu p", zavádíme v teorii kvadratických kongruencí tzv. Legendreův symbol.

Definice 12. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Potom definujeme Legendreův symbol $\left(\frac{a}{p}\right)$ takto: Je-li a kvadratickým zbytkem podle modulu p, klademe $\left(\frac{a}{p}\right) = 1$. Je-li a kvadratickým nezbytkem podle modulu p, klademe $\left(\frac{a}{p}\right) = -1$.*

Z věty 39 a definice 12 plyne okamžitě

věta 40. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Potom*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p. \qquad (82)$$

Zavedením Legendreova symbolu můžeme tedy shrnout vzorce (77) a (78) do jediného vztahu (82). Pomocí tohoto vztahu si nyní dokážeme některá pravidla pro počítání s Legendreovým symbolem.

Věta 41. *Budiž p liché prvočíslo a nechť $(a, p) = (b, p) = 1$. Potom platí:*

a) Je-li $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, *je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

b) Je-li $a \equiv b \bmod p$, *je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

c)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \tag{83}$$

$$\left(\frac{a^2}{p}\right) = 1, \tag{84}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{85}$$

Důkaz tvrzení a). Poněvadž $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, bude prvočíslo p dělitelem výrazu $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right)$. Absolutní hodnota tohoto výrazu je však nejvýše rovna dvěma a protože $p > 2$, plyne z výsledku úlohy 2 a věty 2 (kapitola 1), že $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) = 0$. Tím jsme dokázali tvrzení a).

Důkaz tvrzení b). Z kongruence $a \equiv b \bmod p$ podle (18) plyne, že též $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \bmod p$. Podle (82) je však

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p,$$

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \bmod p.$$

Podle (11) tedy dostaneme $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, z čehož užitím tvrzení a) plyne správnost tvrzení b).

Důkaz tvrzení c). Poněvadž $(a, p) = (b, p) = 1$, bude i $(ab, p) = 1$, takže podle (82) bude

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \bmod p.$$

Avšak $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} . b^{\frac{p-1}{2}}$ a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$, $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \bmod p$, takže podle (17) dostaneme též

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

Shrnutím nalezených výsledků obdržíme pak podle (11), že platí $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p$. Odtud zcela stejně, jako při důkazu tvrzení a), plyne vztah (83).

Položíme-li v (83) speciálně $b = a$, dostaneme (84), neboť $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1$.

Vztah (85) dokážeme konečně ze vztahu (82) zcela stejně, jako jsme dokazovali tvrzení a).

Ukážeme si nyní na příkladě, jak lze věty 41 užít k určení hodnoty Legendreova symbolu.

Příklad 41. Určete a) $\left(\frac{2}{139}\right)$; b) $\left(\frac{35}{139}\right)$.

Řešení.

a) $$\left(\frac{2}{139}\right) = \left(\frac{2}{139}\right)^7 = \left(\frac{128}{139}\right) = \left(\frac{-11}{139}\right) =$$

$$= \left(\frac{-1}{139}\right) \cdot \left(\frac{11}{139}\right) = -\left(\frac{11}{139}\right) = -\left(\frac{150}{139}\right) =$$

$$= -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right) \cdot \left(\frac{25}{139}\right) = -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right), \text{ tj.}$$

$$\left(\frac{2}{139}\right) = -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right).$$

Z tohoto vztahu tedy vypočteme $\left(\frac{3}{139}\right) = -1$. Dále pak bude

$$\left(\frac{2}{139}\right) = \left(\frac{2}{139}\right) \cdot \left(\frac{4}{139}\right) = \left(\frac{8}{139}\right) = \left(\frac{147}{139}\right) =$$

$$= \left(\frac{3}{139}\right) \cdot \left(\frac{49}{139}\right) = \left(\frac{3}{139}\right) = -1.$$

b) $$\left(\frac{35}{139}\right) = \left(\frac{35}{139}\right) \cdot \left(\frac{4}{139}\right) = \left(\frac{140}{139}\right) = \left(\frac{1}{139}\right) = 1.$$

Odpověď. a) $\left(\frac{2}{139}\right) = -1$; b) $\left(\frac{35}{139}\right) = 1$.

Dokážeme si ještě jedno kritérium, podle něhož lze principiálně velmi jednoduše rozhodnout, zda číslo a z redukované soustavy zbytků podle modulu p je kvadratickým zbytkem či kvadratickým nezbytkem podle

tohoto modulu. Při zápisu opět s výhodou použijeme Legendreova symbolu.

Věta 42. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Buďte dále $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{\frac{p-1}{2}}$ absolutně nejmenší zbytky při dělení prvočíslem p utvořené postupně k číslům $1.a$, $2.a$, $3.a$, $\ldots$, $\frac{p-1}{2}.a$. Nechť konečně ν značí počet záporných čísel ležících v systému $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{\frac{p-1}{2}}$.*

Potom

$$\left(\frac{a}{p}\right) = (-1)^{\nu}. \tag{86}$$

Důkaz. Nechť k je některé z čísel $1, 2, 3, \ldots, \frac{p-1}{2}$. Podle věty 5 existují k danému číslu k celá čísla ξ_k a ϱ_k tak, že platí

$$k.a = \xi_k p + \varrho_k,$$

$$-\frac{p}{2} \leqq \varrho_k < \frac{p}{2}.$$

Bude tedy

$$ak \equiv \varrho_k \bmod p \quad \left(k = 1, 2, 3, \ldots, \frac{p-1}{2}\right). \tag{87}$$

Poněvadž p je liché prvočíslo, budou celá čísla ϱ_k splňovat dokonce ostré nerovnosti $-\frac{p}{2} < \varrho_k < \frac{p}{2}$, takže

$$|\varrho_k| < \frac{p}{2} \quad \left(k = 1, 2, 3, \ldots, \frac{p-1}{2}\right). \tag{88}$$

Předpokládejme, že $1 \leqq h \leqq \frac{p-1}{2}$, $1 \leqq k \leqq \frac{p-1}{2}$ a že $|\varrho_h| = |\varrho_k|$. Z této rovnosti plyne, že též $\varrho_h^2 = \varrho_k^2$, takže vzhledem ke vztahům (87) dostaneme dále $a^2h^2 \equiv a^2k^2 \bmod p$. Ježto $p \nmid a$, můžeme podle věty 11 v této kongruenci krátit číslem a^2, takže dostaneme $h^2 \equiv k^2 \bmod p$, tj. $h^2 - k^2 \equiv 0 \bmod p$. Avšak poslední kongruenci můžeme psát ve tvaru

$$(h + k)(h - k) \equiv 0 \bmod p. \tag{89}$$

Sečteme-li dále nerovnosti pro čísla h a k, dostaneme

$$2 \leqq h + k \leqq p - 1 < p,$$

takže musí platit $p \nmid (h + k)$. Podle věty 13 pak z kongruence (89) plyne, že $h - k \equiv 0 \bmod p$ neboli $h \equiv k \bmod p$. Odtud podle věty 14 dostaneme $h = k$.

Jestliže tedy $|\varrho_h| = |\varrho_k|$, je nutně $h = k$. Z toho pak plyne, že pro $h \neq k$ bude též $|\varrho_h| \neq |\varrho_k|$. Proto čísla $|\varrho_1|, |\varrho_2|, |\varrho_3|, \ldots, |\varrho_{\frac{p-1}{2}}|$ budou vzájemně různá. Žádné z nich nebude rovno nule, neboť v opačném případě bychom podle (87) dostali, že buďto $p|a$, nebo $p|k$, což by odporovalo předpokladu o číslech a a k. Vzhledem k nerovnostem (88) bude tedy $\frac{p-1}{2}$ čísel $|\varrho_1|$, $|\varrho_2|$, $|\varrho_3|$, $\ldots$, $|\varrho_{\frac{p-1}{2}}|$ nabývat až na pořadí hodnot $1, 2, 3, \ldots, \frac{p-1}{2}$, takže bude

$$\varrho_1\varrho_2\varrho_3 \ldots \varrho_{\frac{p-1}{2}} = (-1)^{\left(\frac{p-1}{2}\right)}!. \tag{90}$$

Znásobíme-li nyní mezi sebou všechny kongruence (87), dostaneme

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \varrho_1\varrho_2\varrho_3 \ldots \varrho_{\frac{p-1}{2}} \bmod p;$$

dosadíme-li do této kongruence podle (90), obdržíme

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\nu}\left(\frac{p-1}{2}\right)! \bmod p.$$

Poněvadž $p \nmid \left(\frac{p-1}{2}\right)!$, můžeme podle věty 11 v této kongruenci krátit číslem $\left(\frac{p-1}{2}\right)!$, takže dostaneme

$$a^{\frac{p-1}{2}} \equiv (-1)^{\nu} \bmod p.$$

Odtud vzhledem k (82) plyne, že

$$\left(\frac{a}{p}\right) \equiv (-1)^{\nu} \bmod p,$$

z čehož stejným postupem, jako při důkazu tvrzení a) věty 41, dostaneme dokazovaný vztah (86).

Větu, kterou jsme právě dokázali, nazýváme v teorii čísel Gaussovým lematem.

Příklad 42. Užitím Gaussova lematu určete a) $\left(\frac{5}{41}\right)$; b) $\left(\frac{26}{41}\right)$.

Řešení. a) Pro $a = 5$ budeme hledat absolutně nejmenší zbytky při dělení číslem 41 postupně k číslům 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100. Tyto zbytky budou rovny číslům 5, 10, 15, 20, —16, —11, —6, —1, 4, 9, 14, 19, —17, —12, —7, —2, 3, 8, 13 a 18. Je tedy $\nu = 8$, takže podle (86) bude $\left(\frac{5}{41}\right) = 1$.

b) Podobně pro $a = 26$ budeme hledat absolutně nejmenší zbytky při dělení číslem 41 postupně pro čísla 26, 52, 78, 104, 130, 156, 182, 208, 234, 260, 286, 312, 338, 364, 390, 416, 442, 468, 494, 520. Tyto zbytky budou rovny číslům —15, 11, —4, —19, 7, —8, 18, 3, —12, 14, —1, —16, 10, —5, —20, 6, —9, 17, 2 a —13. V tomto případě je $\nu = 11$, takže podle (86) dostaneme $\left(\frac{26}{41}\right) = -1$.

Odpověď. a) $\left(\frac{5}{41}\right) = 1$; b) $\left(\frac{26}{41}\right) = -1$.

Doposud jsme se zabývali otázkou, kdy má kongruence (73) řešení. Tuto otázku dovedeme úplně zodpovědět, neboť pro $p \nmid a$ umíme určit hodnotu Legendreova symbolu $\left(\frac{a}{p}\right)$ a tím i rozhodnout o existenci řešení kongruence (73), a pro $p|a$ umíme dokonce toto řešení přímo napsat.

Obraťme nyní pozornost k otázce, jak v případě, kdy kongruence (73) má řešení, lze toto řešení zkonstruovat. Na rozdíl od kvadratických rovnic je u kvadratických kongruencí tento problém v obecném případě mnohem komplikovanější. Avšak v některých speciálních případech už nám vyložená teorie stačí k tomu, abychom řešení kongruence (73) sestrojili.

Jeden dosti obecný případ, ve kterém dovedeme řešení kongruence (73) sestrojit, popisuje

věta 43. *Nechť* $p \equiv 3 \bmod 4$ *a nechť* $\left(\frac{a}{p}\right) = 1$. *Potom pro řešení* x_1 *kvadratické kongruence* (73) *platí*

$$x_1 \equiv a^{\frac{p+1}{4}} \bmod p. \tag{91}$$

Důkaz. Exponent $\frac{p+1}{4}$ je celé číslo, neboť z předpokladu $p \equiv 3 \bmod 4$ plyne, že $p + 1 \equiv 0 \bmod 4$. Podle (91) je dále $x_1^2 - a \equiv a^{\frac{p+1}{2}} - a \bmod p$. Avšak

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

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

Poněvadž z (82) plyne, že $a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right) \equiv 0 \bmod p$, dostaneme shrnutím těchto výsledků $x_1^2 - a \equiv 0 \bmod p$. Vidíme, že číslo x_1 definované vztahem (91) je skutečně řešením kongruence (73).

Druhé řešení x_2 kongruence (73) určíme pak snadno ze vztahu $x_2 \equiv p - x_1 \bmod p$.

Příklad 43. Vyšetřte kvadratickou kongruenci

$$x^2 - 35 \equiv 0 \bmod 59.$$

Řešení. Především zjistíme, zda daná kongruence má řešení. K tomu musíme určit hodnotu Legendreova symbolu $\left(\frac{35}{59}\right)$. Podle věty 41 postupně dostaneme

$$\left(\frac{35}{59}\right) = \left(\frac{-24}{59}\right) = \left(\frac{-6}{59}\right)\cdot\left(\frac{4}{59}\right) = \left(\frac{-6}{59}\right) =$$

$$= \left(\frac{-6}{59}\right)\cdot\left(\frac{9}{59}\right) = \left(\frac{-54}{59}\right) = \left(\frac{5}{59}\right) = \left(\frac{64}{59}\right) = \left(\frac{1}{59}\right) = 1.$$

Daná kongruence má tedy v každé redukované soustavě zbytků podle modulu 59 dvě řešení.

Poněvadž $59 \equiv 3 \bmod 4$, bude podle (91)

$$x_1 \equiv 35^{15} \bmod 59.$$

Avšak $35^{15} = 5^{15}.7^{15}$, $5^3 \equiv 7 \bmod 59$, $5^{15} \equiv 7^5 \bmod 59$, takže $x_1 \equiv 35^{15} \equiv 7^{20} \bmod 59$. Dále je $7^2 \equiv -10 \bmod 59$ a tedy $7^{20} \equiv 10^{10} \bmod 59$. Poněvadž $10^3 \equiv -3 \bmod 59$, dostaneme konečně $x_1 \equiv 7^{20} \equiv 10^{10} \equiv 10.(-3)^3 \equiv 25 \bmod 59$.

Pro druhé řešení dané kongruence pak dostaneme $x_2 \equiv 59 - 25 \bmod 59$, tj. $x_2 \equiv 34 \bmod 59$.

Odpověď. Kvadratická kongruence $x^2 - 35 \equiv 0 \bmod 59$ má v redukované soustavě zbytků $\{1, 2, 3, \ldots, 58\}$ podle modulu 59 dvě řešení, $x_1 = 25$ a $x_2 = 34$.

Věta 43 nám umožňuje konstruovat řešení kvadratické kongruence (73) pro prvočíselné moduly tvaru $p = 4m + 3$ (m celé). Postupu, jehož jsme při konstrukci řešení užili, lze však někdy užít i v případě, že prvočíslo p má tvar $p = 4m + 1$.

Nechť $p \equiv 1 \bmod 4$ a nechť $\left(\frac{a}{p}\right) = 1$. Hledejme nejmenší přirozené číslo k, pro které platí $a^k \equiv 1 \bmod p$. Víme už, že takové číslo jistě existuje. Podle věty 29 bude dokonce $k \mid (p - 1)$.

Je-li číslo k liché, bude $k + 1$ sudé a položíme-li

$$x_1 \equiv a^{\frac{k+1}{2}} \bmod p, \tag{92}$$

dostaneme $x_1^2 - a \equiv a^{k+1} - a \bmod p$. Avšak $a^{k+1} - a = a(a^k - 1)$ a $a^k - 1 \equiv 0 \bmod p$, takže konečně obdržíme $x_1^2 - a \equiv 0 \bmod p$. Vidíme-li, že číslo x_1 definované vztahem (92) je opět řešením kongruence (73).

Je-li však číslo k sudé, nelze tohoto postupu užít.

Nicméně i pro tyto případy lze řešení kongruence (73) zkonstruovat $\left(\text{přirozeně za předpokladu, že } \left(\frac{a}{p}\right) = 1\right)$. Konstrukce je však příliš komplikovaná a přesahuje rámec této knihy. Proto se jí nebudeme zabývat a omezíme se v těchto případech na stanovení řešení dané kvadratické kongruence jen zkusmo.

Obecně tedy dovedeme zkonstruovat řešení kvadratické kongruence (73) jen v těch případech, kdy buďto $p \equiv 3 \bmod 4$, nebo mezi lichými děliteli čísla $p - 1$ existuje takové číslo k, pro které je $a^k \equiv 1 \bmod p$.

Příklad 44. Vyšetřte kvadratickou kongruenci

$$x^2 - 28 \equiv 0 \bmod 53.$$

Řešení. Nejprve budeme zkoumat, zda daná kongruence má řešení. Zřejmě bude

$$\left(\frac{28}{53}\right) = \left(\frac{81}{53}\right) = 1,$$

takže kongruence má v každé redukované soustavě zbytků podle modulu 53 dvě řešení.

Poněvadž $53 \equiv 1 \bmod 4$, budeme hledat mezi lichými děliteli čísla $53 - 1 = 52$ číslo k takové, že $28^k \equiv 1 \bmod 53$. Lichými děliteli čísla 52 jsou však pouze čísla 1 a 13. Postupně určíme

$28^2 \equiv -11 \bmod 53,$

$28^4 \equiv 121 \equiv 15 \bmod 53,$

$28^6 \equiv -11.15 \equiv -6 \bmod 55,$

$28^{12} \equiv 36 \bmod 53,$

$28^{13} \equiv 36.28 \equiv 1 \bmod 53.$

Podle (92) tedy bude

$$x_1 \equiv 28^7 \equiv -6.28 \equiv 6.25 \equiv 44 \bmod 53.$$

Položíme-li ještě $x_2 = 53 - 44 = 9$, vidíme, že daná kongruence má v redukované soustavě zbytků $\{1, 2, 3, \ldots, 52\}$ podle modulu 53 dvě řešení, $x_1 = 44$ a $x_2 = 9$.

Příklad 45. Najděte všechna řešení kvadratické kongruence $x^2 \equiv 20 \bmod 41$ v úplné soustavě zbytků $\{0, 1, 2, \ldots, 40\}$ podle modulu 41.

Řešení. V příkladu 40 jsme zjistili, že $\left(\frac{20}{41}\right) = 1$. Daná kongruence bude proto mít ve zvolené úplné soustavě zbytků dvě inkongruentní řešení. (Tato řešení budou dokonce z odpovídající redukované soustavy.)

Poněvadž $41 \equiv 1 \bmod 4$, nelze ke konstrukci těchto řešení užít věty 43. Lichými děliteli čísla $41 - 1 = 40$ jsou pouze čísla 1 a 5. Přitom

$$20^2 \equiv -10 \bmod 41,$$

$$20^4 \equiv 100 \equiv 18 \bmod 41,$$

$$20^5 \equiv 18.20 \equiv -9 \bmod 41,$$

$$20^{10} \equiv 81 \equiv -1 \bmod 41,$$

$$20^{20} \equiv 1 \bmod 41.$$

Vidíme, že $20^5 \not\equiv 1 \bmod 41$. Poněvadž přirozenými děliteli čísla 40 jsou pouze čísla 1, 2, 4, 5, 8, 10 a 20 a poněvadž $20^8 \equiv 324 \equiv -4 \bmod 41$, je číslo $k = 20$ nejmenším přirozeným číslem, pro které platí $20^k \equiv 1 \bmod 41$.

Nelze tedy užít ani vztahu (92) a řešení dané kongruence bude proto třeba hledat zkusmo. Studujme

prvky zbytkové třídy podle modulu 41, ve které leží číslo 20. Zřejmě bude

$$20 \equiv 61 \equiv 102 \equiv 143 \equiv 184 \equiv 225 \bmod 41,$$

takže bude též $x^2 \equiv 225 \bmod 41$, tj. $x^2 \equiv 15^2 \bmod 41$. Jedno řešení vyšetřované kongruence bude tedy $x_1 = 15$, druhé pak dostaneme ze vztahu $x_2 = 41 - 15 = 26$.

Odpověď. Hledaná řešení kongruence $x^2 \equiv 20 \bmod 41$ jsou $x_1 = 15$, $x_2 = 26$.

Ke konstrukci řešení některých speciálních kvadratických kongruencí lze někdy užít i jiných vět, které jsme si vyložili. Jako ukázku si uvedeme příklad, kde ke konstrukci řešení využijeme Wilsonovy věty (věta 37).

Příklad 46. Nechť p je prvočíslo tvaru $p = 4m + 1$. Užitím Wilsonovy věty dokažte, že kongruence $x^2 + 1 \equiv 0 \bmod p$ má řešení

$$x_{1,2} \equiv \pm(2m)! \bmod p.$$

Řešení. Protože

$(2m)! = 1.2.3. \ldots .2m = (-1).(-2).(-3). \ldots . (-2m)$ a pro $k = 1, 2, 3, \ldots, 2m$ platí

$$-k \equiv p - k \bmod p,$$

dostaneme vynásobením všech těchto kongruencí

$$(2m)! \equiv (p-1).(p-2).(p-3). \ldots .(p-2m) \bmod p.$$

Znásobíme-li tuto kongruenci číslem $(p - 2m - 1)!$, dostaneme

$$(2m)!.(p - 2m - 1)! \equiv (p-1)! \bmod p.$$

Avšak $p - 2m - 1 = 4m + 1 - 2m - 1 = 2m$, takže bude

$$((2m)!)^2 \equiv (p-1)! \bmod p.$$

Odtud užitím vztahu (71) dostaneme

$$((2m)!)^2 \equiv -1 \bmod p$$

neboli

$$((2m)!)^2 + 1 \equiv 0 \bmod p.$$

Poněvadž $x_1^2 \equiv x_2^2 \equiv ((2m)!)^2 \bmod p$, obdržíme konečně

$$x_1^2 + 1 \equiv 0 \bmod p,$$
$$x_2^2 + 1 \equiv 0 \bmod p.$$

Čísla x_1 a x_2 budou tedy skutečně řešeními kongruence $x^2 + 1 \equiv 0 \bmod p$, což jsme měli dokázat.

Závěrem této kapitoly se ještě stručně zmíníme o obecné kvadratické kongruenci s prvočíselným modulem

$$a_0x^2 + a_1x + a_2 \equiv 0 \bmod p, \qquad (72)$$

kde p je liché prvočíslo, $p \nmid a_0$. Postup, jehož při studiu takovéto kongruence užíváme, je zcela obdobný s postupem užívaným při řešení kvadratických rovnic.

Poněvadž p je liché prvočíslo a $p \nmid a_0$, platí též, že $p \nmid 4a_0$. Vynásobíme-li tedy kongruenci (72) číslem $4a_0$, dostaneme ekvivalentní kongruenci

$$4a_0^2x^2 + 4a_0a_1x + 4a_0a_2 \equiv 0 \bmod p.$$

Doplníme-li levou stranu této kongruence na úplný čtverec a označíme-li $D = a_1^2 - 4a_0a_2$ diskriminant kvadratického trojčlenu $a_0x^2 + a_1x + a_2$, dostaneme po jednoduché úpravě kongruenci

$$(2a_0x + a_1)^2 - D \equiv 0 \bmod p,$$

která je rovněž ekvivalentní s kongruencí (72). Položme ještě

$$2a_0x + a_1 \equiv z \mod p. \tag{93}$$

Dostaneme tak kvadratickou kongruenci

$$z^2 - D \equiv 0 \mod p, \tag{94}$$

která už má tvar (73). Ze vztahu (93) plyne, že každému řešení kongruence (72) odpovídá právě jedno řešení kongruence (94). Poněvadž však $p \nmid 2a_0$, lze i obráceně z lineární kongruence (93) ke každému řešení kongruence (94) najít právě jedno řešení kongruence (72).

Nechť dvěma řešením x_1 a x_2 kongruence (72) odpovídají řešení z_1 a z_2 kongruence (94). Bude tedy

$$2a_0x_1 + a_1 \equiv z_1 \mod p,$$
$$2a_0x_2 + a_1 \equiv z_2 \mod p.$$

Je-li $x_1 \equiv x_2 \mod p$, plyne z těchto vztahů, že i $z_1 \equiv z_2 \mod p$. Je-li obráceně $z_1 \equiv z_2 \mod p$, bude $2a_0x_1 + a_1 \equiv 2a_0x_2 + a_1 \mod p$, takže $2a_0x_1 \equiv 2a_0x_2 \mod p$. Poněvadž $(2a_0, p) = 1$, plyne z této kongruence podle věty 11, že $x_1 \equiv x_2 \mod p$. Tím jsme dokázali, že řešení x_1 a x_2 kongruence (72) jsou kongruentní podle modulu p právě tehdy, jsou-li podle tohoto modulu kongruentní odpovídající řešení z_1 a z_2 kongruence (94).

Z provedených úvah vyplývá, že kvadratické kongruence (72) a (94) jsou ekvivalentní. Postup, který jsme si právě popsali, nám tedy vždy umožní rozhodnout o existenci řešení kongruence (72) a určit počet inkongruentních řešení této kongruence. V těch případech, kdy dovedeme najít řešení kongruence (94), jím dokonce dostaneme řešení kongruence (72). V ně-

kterých konkrétních případech však můžeme tento postup ještě značně zjednodušit.

Příklad 47. Vyšetřte kvadratickou kongruenci

$$57x^2 + 149x + 362 \equiv 0 \bmod 211.$$

Řešení. Pro diskriminant D kvadratického trojčlenu $57x^2 + 149x + 362$ dostaneme $D = 149^2 - 4.57.362$. Snadno zjistíme, že $149^2 - 4.57.362 \equiv (-62)^2 + 17.60 \bmod 211$, tj. $D \equiv 3844 + 1020 \equiv 11 \bmod 211$. Dostaneme tedy ekvivalentní kongruenci

$$z^2 - 11 \equiv 0 \bmod 211.$$

Abychom rozhodli o existenci řešení této kongruence, určíme hodnotu Legendreova symbolu $\left(\frac{11}{211}\right)$. Podle známých pravidel bude

$$\left(\frac{11}{211}\right) = \left(\frac{-200}{211}\right) = \left(\frac{-2}{211}\right)\cdot\left(\frac{100}{211}\right) = \left(\frac{-2}{211}\right) =$$

$$= \left(\frac{-2}{211}\right)\cdot\left(\frac{81}{211}\right) = \left(\frac{-162}{211}\right) = \left(\frac{49}{211}\right) = 1,$$

takže kongruence $z^2 - 11 \equiv 0 \bmod 211$ bude mít dvě řešení inkongruentní podle modulu 211. Poněvadž $211 \equiv 3 \bmod 4$, bude podle věty 43

$$z_1 \equiv 11^{53} \bmod 211.$$

Postupně vypočteme

$11^2 \equiv -90 \bmod 211$,

$11^4 \equiv 8100 \equiv 82 \bmod 211$,

$11^8 \equiv 6724 \equiv -28 \bmod 211$,

$11^{16} \equiv 784 \equiv -60 \bmod 211$,

$11^{48} \equiv -216\,000 \equiv 64 \bmod 211$,

$11^{52} \equiv 64.82 \equiv -27 \bmod 211$ a

$11^{53} \equiv -27.11 \equiv 125 \bmod 211$.

Řešení kongruence $z^2 - 11 \equiv 0 \bmod 211$ tedy budou $z_1 \equiv 125 \bmod 211$ a $z_2 \equiv 211 - 125 \equiv 86 \bmod 211$. Podle (93) dostaneme pro řešení původní kongruence

$$114x_1 + 149 \equiv 125 \bmod 211,$$
$$114x_2 + 149 \equiv 86 \bmod 211.$$

Po úpravě a zkrácení šesti resp. třemi dostaneme dále

$$19x_1 \equiv -4 \bmod 211, \quad 38x_2 \equiv -21 \bmod 211.$$

Znásobíme-li první kongruenci jedenácti, dostaneme $209x_1 \equiv -44 \bmod 211$ neboli $-2x_1 \equiv -44 \bmod 211$, z čehož po zkrácení číslem -2 plyne ihned $x_1 \equiv 22 \bmod 211$. Druhou kongruenci můžeme přepsat ve tvaru $38x_2 \equiv 190 \bmod 211$, z čehož po zkrácení číslem 38 plyne $x_2 \equiv 5 \bmod 211$.

Odpověď. Kongruence $57x^2 + 149x + 362 \equiv 0 \bmod 211$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 210\}$ podle modulu 211 dvě řešení, $x_1 = 22$ a $x_2 = 5$.

Ukážeme si ještě jiný způsob řešení této kongruence. Řešme nejprve lineární kongruenci $57u \equiv 1 \bmod 211$. Podle (46) dostaneme pro její řešení $u_1 \equiv 57^{209} \bmod 211$. Postupně vypočteme

$57^2 \equiv 84 \bmod 211$,

$57^4 \equiv 7056 \equiv 93 \bmod 211$,

$57^8 \equiv 8649 \equiv -2 \bmod 211$,

$57^{40} \equiv -32 \bmod 211$,

$57^{80} \equiv 1024 \equiv -31 \bmod 211,$

$57^{160} \equiv 961 \equiv -94 \bmod 211,$

$57^{200} \equiv (-32).(-94) \equiv 54 \bmod 211,$

$57^{208} \equiv -2.54 \equiv 103 \bmod 211$ a

$57^{209} \equiv 57.103 \equiv -37 \bmod 211.$

Řešení lineární kongruence $57u \equiv 1 \bmod 211$ bude tedy $u_1 \equiv -37 \bmod 211$.

Znásobme nyní původní kvadratickou kongruenci $57x^2 + 149x + 362 \equiv 0 \bmod 211$ číslem -37. Dostaneme tak kvadratickou kongruenci s ní ekvivalentní

$$-2109x^2 - 5513x - 13\,394 \equiv 0 \bmod 211.$$

Tuto kongruenci můžeme podle věty 17 psát v ekvivalentním tvaru

$$x^2 - 27x - 101 \equiv 0 \bmod 211$$

nebo ještě výhodněji ve tvaru

$$x^2 + 184x - 101 \equiv 0 \bmod 211,$$

neboť v této kongruenci můžeme bez dalších úprav doplnit její levou stranu na úplný čtverec. Dostaneme tak

$$(x + 92)^2 - 92^2 - 101 \equiv 0 \bmod 211$$

nebo po úpravě

$$(x + 92)^2 - 125 \equiv 0 \bmod 211.$$

Tato kongruence je zřejmě ekvivalentní s kongruencí původní, a položíme-li ještě $x + 92 = v$, dostaneme opět kvadratickou kongruenci tvaru (73)

$$v^2 - 125 \equiv 0 \bmod 211.$$

Pro Legendreův symbol $\left(\frac{125}{211}\right)$ dostaneme snadno

$$\left(\frac{125}{211}\right) = \left(\frac{5}{211}\right)^3 = \left(\frac{5}{211}\right) = \left(\frac{5}{211}\right)\cdot\left(\frac{9}{211}\right) =$$
$$= \left(\frac{45}{211}\right) = \left(\frac{256}{211}\right) = \left(\frac{16}{211}\right)^2 = 1,$$

takže kongruence $v^2 - 125 \equiv 0 \bmod 211$ má dvě inkongruentní řešení. Podle věty 43 dostaneme jedno z těchto řešení ve tvaru

$$v_1 \equiv 125^{53} \bmod 211.$$

Postupně vypočteme

$125^2 \equiv 11 \bmod 211,$
$125^4 \equiv 121 \equiv -90 \bmod 211,$
$125^8 \equiv 8100 \equiv 82 \bmod 211,$
$125^{12} \equiv -90.82 \equiv 5 \bmod 211,$
$125^{48} \equiv 625 \equiv -8 \bmod 211,$
$125^{52} \equiv (-8).(-90) \equiv 87 \bmod 211$ a
$125^{53} \equiv 125.87 \equiv 114 \bmod 211.$

Bude tedy $v_1 \equiv 114 \bmod 211$ a $v_2 \equiv 211 - 114 \equiv 97 \bmod 211$. Ze vztahu $x + 92 = v$ určíme nyní už snadno řešení původní kvadratické kongruence $x_1 \equiv 114 - 92 \equiv 22 \bmod 211$ a $x_2 \equiv 97 - 92 \equiv 5 \bmod 211$.

Příklad 48. Vyšetřte kvadratickou kongruenci

$$6x^2 - 5x + 21 \equiv 0 \bmod 97.$$

Řešení. Diskriminant kvadratického trojčelnu $6x^2 -$

$-5x + 21$ je $D = 25 - 4.6.21 = -479$, tedy $D \equiv 6 \bmod 97$. Snadno zjistíme, že

$$\left(\frac{6}{97}\right) = \left(\frac{6}{97}\right) \cdot \left(\frac{16}{97}\right) = \left(\frac{96}{97}\right) = \left(\frac{-1}{97}\right) = 1.$$

Kongruence $z^2 - 6 \equiv 0 \bmod 97$ i kongruence původní budou tedy mít dvě inkongruentní řešení.

Poněvadž $97 \equiv 1 \bmod 4$, nemůžeme ke konstrukci řešení kvadratické kongruence $z^2 - 6 \equiv 0 \bmod 97$ užít věty 43. Nelze však užít ani vztahu (92), neboť $6^2 \equiv 36 \bmod 97$, $6^3 \equiv 22 \bmod 97$, $6^4 \equiv 35 \bmod 97$, $6^6 \equiv -1 \bmod 97$, $6^8 \equiv -36 \bmod 97$ a $6^{12} \equiv 1 \bmod 97$, takže nejmenší přirozené číslo k, pro které platí $6^k \equiv 1 \bmod 97$, je sudé.

Znásobíme-li kongruenci $z^2 - 6 \equiv 0 \bmod 97$ šestnácti, dostaneme ekvivalentní kongruenci $16z^2 - 96 \equiv 0 \bmod 97$, kterou můžeme napsat ve tvaru $(4z)^2 \equiv -1 \bmod 97$. Protože jsme zjistili, že $6^6 \equiv -1 \bmod 97$, můžeme dále psát

$$(4z)^2 \equiv (6^3)^2 \bmod 97,$$

z čehož dostaneme $4z_1 \equiv 216 \bmod 97$, $4z_2 \equiv -216 \bmod 97$. Po zkrácení čtyřmi tedy bude $z_1 \equiv 54 \bmod 97$, $z_2 \equiv -54 \equiv 43 \bmod 97$. Tím jsme našli obě inkongruentní řešení kongruence $z^2 - 6 \equiv 0 \bmod 97$.

Abychom určili řešení x_1 a x_2 původní kvadratické kongruence, budeme řešit ještě dvě lineární kongruence. Podle (93) bude

$$12x_1 - 5 \equiv 54 \bmod 97, \quad 12x_2 - 5 \equiv 43 \bmod 97,$$

tj.

$$12x_1 \equiv 59 \bmod 97, \quad 12x_2 \equiv 48 \bmod 97.$$

Násobíme-li první kongruenci osmi, dostaneme $96x_1 \equiv$

$\equiv 472 \bmod 97$ neboli $-x_1 \equiv -13 \bmod 97$, takže bude $x_1 \equiv 13 \bmod 97$. Krátíme-li ve druhé kongruenci dvanácti, dostaneme ihned $x_2 \equiv 4 \bmod 97$.

Odpověď. Kvadratická kongruence $6x^2 - 5x + 21 \equiv 0 \bmod 97$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 96\}$ podle modulu 97 dvě řešení, $x_1 = 13$ a $x_2 = 4$.

Příklad 49. Vyšetřte kvadratickou kongruenci

$$73x^2 - 115x + 48 \equiv 0 \bmod 113.$$

Řešení. Diskriminant daného kvadratického trojčlenu bude $D = 115^2 - 4.73.48$. Snadno zjistíme, že $D \equiv 2^2 + 47.48 \equiv 0 \bmod 113$, takže kvadratická kongruence (94) má v každé úplné soustavě zbytků podle modulu 113 jediné řešení $z_1 \equiv 0 \bmod 113$. Kongruence (93) má v tomto případě tvar $146x_1 - 115 \equiv 0 \bmod 113$ neboli $33x_1 \equiv 2 \bmod 113$. Podle (46) dostaneme řešení této lineární kongruence ve tvaru $x_1 \equiv 2.33^{111} \bmod 113$. Postupně tedy vypočteme

$33^2 \equiv -41 \bmod 113$,

$33^4 \equiv 1681 \equiv -14 \bmod 113$,

$33^8 \equiv 196 \equiv -30 \bmod 113$,

$33^{16} \equiv 900 \equiv -4 \bmod 113$,

$33^{32} \equiv 16 \bmod 113$,

$33^{64} \equiv 256 \equiv 30 \bmod 113$,

$33^{96} \equiv 16.30 \equiv 28 \bmod 113$,

$33^{104} \equiv -30.28 \equiv -49 \bmod 113$,

$33^{108} \equiv (-14).(-49) \equiv 8 \bmod 113$,

$33^{110} \equiv -41.8 \equiv 11 \bmod 113$,

$33^{111} \equiv 33.11 \equiv 24 \bmod 113$,

z čehož dostaneme $x_1 \equiv 2.33^{111} \equiv 48 \bmod 113$.

Odpověď. Vyšetřovaná kongruence má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 112\}$ podle modulu 113 jediné řešení $x_1 = 48$.

Příklad 50. Vyšetřte kvadratickou kongruenci

$$68x^2 - 291x - 50 \equiv 0 \bmod 53.$$

Řešení. Podle věty 17 vyšetříme ekvivalentní kvadratickou kongruenci

$$15x^2 - 26x + 3 \equiv 0 \bmod 53.$$

Diskriminant kvadratického trojčlenu $15x^2 - 26x + 3$ je $D = 26^2 - 4.15.3 = 676 - 180 = 496$, takže $D \equiv$ $\equiv 19 \bmod 53$. Podle (82) je $\left(\frac{19}{53}\right) \equiv 19^{26} \bmod 53$ a poněvadž $19^{26} = (19^2)^{13} = 361^{13}$ a $361 \equiv -10 \bmod 53$, určíme postupně

$10^3 \equiv -7 \bmod 53$,

$10^6 \equiv 49 \equiv -4 \bmod 53$,

$10^{12} \equiv 16 \bmod 53$ a

$10^{13} \equiv 160 \equiv 1 \bmod 53$.

Dostaneme tedy

$$\left(\frac{19}{53}\right) \equiv 361^{13} \equiv (-10)^{13} \equiv -10^{13} \equiv -1 \bmod 53.$$

Vidíme, že diskriminant D je kvadratickým nezbytkem podle modulu 53.

Odpověď. Kvadratická kongruence $68x^2 - 291x - 50 \equiv 0 \bmod 53$ nemá žádné řešení.

Úlohy

21. Určete hodnoty Legendreových symbolů: a) $\left(\frac{322}{307}\right)$; b) $\left(\frac{623}{179}\right)$; c) $\left(\frac{62}{83}\right)$; d) $\left(\frac{-10}{659}\right)$.

V následujících příkladech vyšetřte kvadratické kongruence:

22. $x^2 \equiv 43 \bmod 109$.

23. $x^2 - 90 \equiv 0 \bmod 83$.

24. $x^2 + 48 \equiv 0 \bmod 59$.

25. $67x^2 - 91x + 35 \equiv 0 \bmod 71$.

26. $177x^2 - 47x + 928 \equiv 0 \bmod 353$.

27. $196x^2 + 1456x + 2753 \equiv 0 \bmod 571$.

28. Užitím Gaussova lematu dokažte, že pro liché prvočíslo p platí

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

29. Nechť $p > 2$ je prvočíslo a nechť $p \mid m$. Dokažte, že kongruence $(p-1)$-tého stupně o jedné neznámé

$$x^{p-1} + 1 \equiv 0 \bmod m$$

nemá žádné řešení.