DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

10.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu gredzenos **3**

1.1. Pamatfakti 3

1.2. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa 11

1.3. Lineārs vienādojums ar vienu nezināmo 15

1.4. Vienādojumi atlikumu gredzenos pēc pirmskaitļa moduļa 19

1.5. Vienādojumi atlikumu gredzenos pēc pirmskaitļa pakāpes moduļa 26

2. 10.mājasdarbs **29**

1. Vienādojumu risināšana atlikumu gredzenos

1.1. Pamatfakti

1.1. piezīme. Atrisināt Diofanta vienādojumu pēc moduļa m

$$f(x_1, ..., x_n) \equiv 0 \pmod{\mathrm{m}}$$

vai Diofanta vienādojumu sistēmu pēc moduļa m

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \pmod{m_1} \\ f_2(x_1, ..., x_n) \equiv 0 \pmod{m_2} \\ ... \\ f_k(x_1, ..., x_n) \equiv 0 \pmod{m_k} \end{cases}$$

nozīmē to atrisināt *veselos skaitļos* (gredzenā $\mathbb{Z}$). Šādus vienādojumus un vienādojumu sistēmas sauksim par *modulārām Diofanta sistēmām*.

Parasti kā starprezultāts tiek iegūts kāds rezultāts par nezināmo vērtībām reducējot tos pēc noteiktiem moduļiem. Tādējādi risinot vienādojumu sistēmas atlikumu gredzenos, nezināmie līdz noteiktam brīdim tiek uzskatīti par elementiem atlikumu gredzenos.

1.2. piezīme. Kā zināms, atlikumu klases a (mod m) pārstāvji ir visi veselie x, kuriem izpildās nosacījums

$$x \equiv a \text{ (mod m)}.$$

Visu šādu veselo skaitļu kopu $\mathcal{C}_m(a)$ var interpretēt kā atlikumu klases a inverso attēlu attiecībā uz reducēšanas pēc moduļa m funkciju

$$\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

Tādējādi $\mathcal{C}_m(a) = \pi_m^{-1}(a)$. Pāreju no atlikumu klases uz veselo skaitļu kopu interpretēsim kā redukcijas inverso attēlojumu.

1.3. piezīme. Atzīmēsim vēl vienu lietderīgu funkciju. Ja $k|m$, tad

- ja $a_1 \equiv a_2 \pmod{\text{m}}$, tad $a_1 \equiv a_2 \pmod{\text{k}}$;
- katra ekvivalences klase mod k ir vairāku mod m ekvivalences klašu apvienojums, piemērs - $\bar{0}$ klase mod 2 (pāra skaitļi) ir klašu $\bar{0}$ un $\bar{2}$ mod 4 apvienojums.

Tādējādi ir definēta funkcija

$$\pi_{m,k} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z},$$

kas katrai atlikuma klasei x mod m, kuru pārstāv vesels skaitlis $\tilde{x}$ piekārto $\pi_k(\tilde{x})$. Citiem vārdiem sakot,

$$\pi_{m,k}(x) = \pi_k(\tilde{x}),$$

kur $\tilde{x} \in \pi_m^{-1}(x)$. Šādu funkciju sauksim par *relatīvo redukciju no* m *uz* k. Tāpat kā redukcijas funkcijai, arī relatīvajai redukcijai var interpretēt inverso attēlojumu.

1.1. teorēma.

1. Klases $\pi_{m,k}^{-1}(x)$ dažādo pārstāvju kopa var tikt ņemta vienāda ar
$$\{x, x + k \cdot 1, x + k \cdot 2, ..., x + k \cdot (\frac{m}{k} - 1)\}.$$
2. $|\pi_{m,k}^{-1}(a)| = \frac{m}{k}$.

PIERĀDĪJUMS 1. x klase mod k ir skaitļi formā $x + kt$. Izdalīsim t ar $\frac{m}{k}$:
$$t = q \cdot \frac{m}{k} + r,$$
kur $0 \leq r < \frac{m}{k}$. Redzam, ka
$$x + kt = x + k(q \cdot \frac{m}{k} + r) = x + qm + kr = (x + kr) + qm.$$
Redzam, ka katrs klases $\pi_{m,k}^{-1}(x)$ pārstāvis ir izsakāms vēlamajā formā. Pierādīsim, ka visas klases formā $x + kr$ ir dažādas. Ja
$$x + kr_1 \equiv x + kr_2 \pmod{\text{m}},$$
tad $k(r_1 - r_2) = mt'$, bet $|r_1 - r_2| < \frac{m}{k}$, tātad $t' = 0$ un $r_1 = r_2$.

2. Seko no pirmā apgalvojuma. ■

1.1. piemērs. $\pi_{4,2}(\bar{0}) = \bar{0}$, $\pi_{4,2}(\bar{1}) = \bar{1}$, $\pi_{4,2}(\bar{2}) = \bar{0}$, $\pi_{4,2}(\bar{3}) = \bar{1}$. $\pi_{6,2}^{-1}(\bar{0}) = \{\bar{0}, \bar{2}, \bar{4}\}$, $\pi_{6,2}^{-1}(\bar{1}) = \{\bar{1}, \bar{3}, \bar{5}\}$.

1.4. piezīme. Relatīvā redukcija ir grupu un pat gredzenu homomorfizms (saglabā visas operācijas). Relatīvās redukcijas inverso attēlojumu izmanto, ja atrisinājums tiek tiek atrast pēc kāda moduļa k, bet mūs interesē atrisinājumu pēc moduļa m, kur $k|m$.

1.2. teorēma. Ja vesels skaitlis a apmierina sistēmu

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ ... \\ f_k(x) \equiv 0 \pmod{m_k} \end{cases},$$

tad jebkurš skaitlis a' tāds, ka

$$a \equiv a' \pmod{MKD(m_1, ..., m_k)},$$

arī apmierina šo sistēmu.

PIERĀDĪJUMS Ja $a \equiv a' \pmod{MKD(m_1, ..., m_k)}$, tad katram i izpildās

$$f_i(a) \equiv f_i(a') \pmod{MKD(m_1, ..., m_k)}.$$

Saskaņā ar atlikumu kongruences īpašībām katram m_j izpildās

$$f_i(a) \equiv f_i(a') \equiv 0 \pmod{m_j}.$$

■

1.5. piezīme. Ņemot vērā iepriekšējo teorēmu, var konstatēt, ka modulārās Diofanta sistēmas veselie atrisinājumu veido atlikumu klases pēc moduļa $MKD(m_1, ..., m_k)$. Šī iemesla dēļ dažreiz modulāras sistēmas atrisinājumu definē kā atlikumu klasi pēc šī moduļa.

1.6. piezīme. Pilnīgs analoģisks apgalvojums ir spēkā, ja tiek risināta sistēma ar vairākiem nezināmiem: ja skaitļu virkne $(a_1, ..., a_n)$ apmierina sistēmu

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \pmod{m_1} \\ f_2(x_1, ..., x_n) \equiv 0 \pmod{m_2} \\ ... \\ f_k(x_1, ..., x_n) \equiv 0 \pmod{m_k} \end{cases},$$

tad jebkura virkne $(a'_1, ..., a'_n)$, kur $a_j \equiv a'_j \pmod{MKD(m_1, ..., m_k)}$, arī apmierina šo sistēmu.

1.7. piezīme. Ja sākotnēji vienādojumi ir doti ar veseliem koeficientiem, tad reducējot vienādojumu pēc moduļa m, ērti ir reducēt arī koeficientus, piemēram:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 \equiv$$
$$\overline{a}_n x^n + \overline{a}_{n-1} x^{n-1} + ... + \overline{a}_0 \equiv 0 \pmod{\mathrm{m}}.$$

Šādu operāciju polinomu kopā sauksim par polinoma redukciju pēc moduļa m un apzīmēsim ar $\overline{f}(x)$. Polinomu redukcija ir operācija, kas nemaina atrisinājumu kopu. Polinomu redukcija ir gredzenu homomorfizms

$$\Pi_m : \mathbb{Z}[x_1, ..., x_n] \to \mathbb{Z}/m\mathbb{Z}[x_1, ..., x_n].$$

1.2. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa

1.3. teorēma. Zemāk aprakstītās operācijas saglabā modulāra vienādojuma atrisinājumu kopu:

1. reducēt polinomu koeficientus pēc dotā moduļa;
2. pieskaitīt vienādojuma abām pusēm vienu un to pašu atlikumu klasi;
3. reizināt abas puses ar vienu un to pašu invertējamu atlikumu klasi;
4. reizināt visus locekļus un moduli ar nenulles veselu skaitli k;
5. ja katrs vienādojuma loceklis un modulis dalās ar d, tad var izdalīt visus locekļus un moduli ar d;

PIERĀDĪJUMS 4.-5. Ja $f(x) \equiv 0 \pmod{\mathrm{m}}$, tad $f(x) = mq$, tātad $kf(x) = (mk)q$. Katru $f(x)$ koeficientu var reizināt ar k. Ja katrs $f(x)$ koeficients dalās ar d un m dalās ar d un $f(x) \equiv 0 \pmod{\mathrm{m}}$, tad

$f(x) = mq$ un $d \cdot f_1(x) = d \cdot m_1 q$, tātad $f_1(x) = m_1 q$. Esam ieguvuši vienādojumu $f_1(x) \equiv 0 \pmod{m_1}$. ■

1.2. piemērs. $x + 2 \equiv 0 \pmod 5$ tad un tikai tad, ja $x + 2 - 2 \equiv 0 - 2 \pmod 5$ un $x \equiv 3 \pmod 5$.

$4x + 2 \equiv 0 \pmod 5$ tad un tikai tad, ja $4(4x + 2) \equiv 4 \cdot 0 \pmod 5$ un $x \equiv 2 \pmod 5$.

$2x \equiv 6 \pmod 8$ tad un tikai tad, ja $x \equiv 3 \pmod 4$. Ja gribam izteikt atrisinājumu kā klases mod 8, tad $x \in \pi_{8,4}^{-1}(3) = \{3, 7\}$.

1.8. piezīme. Ja $(x_1, ..., x_n)$ ir vesels atrisinājums vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\text{m}}$$

un $k|m$, tad $(x_1, ..., x_n)$ ir atrisinājums arī vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\text{k}}.$$

Bet ne otrādi. Vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\text{k}}$$

var būt vairāk atrisinājumu nekā sākotnējam vienādojumam. Šo īpašību izmanto kontrapozitīvajā formā: ja nav atrisinājumu mod k, tad nav atrisinājumu mod m.

1.3. piemērs. Vienādojumam $x \equiv 1$ ir viena atrisinājumu klase mod 4 un viena atrisinājumu klase mod 2, kas satur iepriekšējo klasi kā apakškopu. Ja $x^4 + 1 \equiv 0 \pmod{27}$, tad $x^4 + 1 \equiv 0 \pmod{3}$. Pēdējam vienādojumam nav atrisinājumu, tātad to nav arī sākotnējam vienādojumam.

1.3. Lineārs vienādojums ar vienu nezināmo

1.9. piezīme. Vienādojums

$$ax \equiv b \pmod{m},$$

kur $LKD(a, m) = 1$, ir viegli atrisināms, jo eksistē $a^{-1} \pmod{m}$:

$$a^{-1}(ax) \equiv x \equiv a^{-1}b \pmod{m}.$$

Atrisinājumu var uzrakstīt arī izmantojot Eilera teorēmu:

$$x \equiv a^{\varphi(m)-1}b \pmod{m}.$$

1.4. piemērs. Vienādojuma $3x \equiv 2 \pmod{5}$ atrisinājums ir

$$x \equiv 3^3 2 \equiv 4 \pmod{5}.$$

Vienādojuma $3x \equiv 2 \pmod{15}$ atrisinājums ir

$$x \equiv 3^7 2 \equiv 11 \pmod{15}.$$

1.4. teorēma.

1. Vienādojumam
$$ax \equiv b \pmod{m}$$
neeksistē atrisinājumi, ja $b \not\equiv 0 \pmod{d}$, kur $d = LKD(a, m)$.
2. Ja $b \equiv 0 \pmod{d}$, tad vienādojuma
$$ax \equiv b \pmod{m}$$
atrisinājumu kopa ir klase $(\frac{a}{d})^{-1}(\frac{b}{d}) \pmod{(\frac{m}{d})}$.

PIERĀDĪJUMS 1. Ja $d = 1$, tad vienmēr $b \equiv 0 \pmod{d}$. Pieņemsim, ka $d > 1$, $a = a_1 d$, $m = m_1 d$, kur $LKD(a_1, m_1) = 1$. Vienādojums $ax \equiv b \pmod{m}$ ir ekvivalents vienādojumam
$$(a_1 d)x = b + (m_1 d)q$$
ar kādu $q \in \mathbb{Z}$. Redzam, ka $b \equiv 0 \pmod{d}$.

2. Ja $b \equiv 0 \pmod{d}$, tad $b = b_1 d$. Vienādojums
$$ax \equiv b \pmod{m}$$

ir ekvivalents ar vienādojumu

$$(a_1 d)x \equiv b_1 d \pmod{m_1 d}.$$

Izdalot visus locekļus un moduli ar d, iegūsim ekvivalentu vienādojumu

$$a_1 x \equiv b_1 \pmod{m_1}.$$

Tā kā $LKD(a_1, m_1) = 1$, tad šim vienādojumam eksistē viena atrisinājumu klase

$$x \equiv a_1^{-1} b_1 \pmod{m_1}$$

vai

$$x \equiv (\frac{a}{d})^{-1}(\frac{b}{d}) \pmod{(\frac{m}{d})}.$$

■

1.10. piezīme. Ja ir nepieciešamība rakstīt atrisinājumu kopu sākotnējā moduļa m terminos, tad

$$x = \pi^{-1}_{m,\frac{m}{d}}((\frac{a}{d})^{-1}(\frac{b}{d})) =$$
$$\{a_1^{-1}b_1, a_1^{-1}b_1 + m_1, ..., a_1^{-1}b_1 + m_1(d-1)\}.$$

1.5. piemērs. Vienādojumam

$$4x \equiv 5 \pmod 8$$

nav atrisinājumu.

Vienādojums

$$6x \equiv 9 \pmod{15}$$

ir ekvivalents vienādojumam

$$2x \equiv 3 \pmod 5,$$

kura atrisinājums ir

$$x \equiv 2^{-1}3 \equiv 4 \pmod 5 = \{4, 9, 14\} \pmod{15}.$$

1.4. Vienādojumi atlikumu gredzenos pēc pirmskaitļa moduļa

1.11. piezīme. $\mathbb{Z}/p\mathbb{Z}$ ir lauks (visi nenulles elementi ir invertējami). Lauki ir arī, piemēram, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Risināt vienādojumus un vienādojumu sistēmas var līdzīgi kā reālos skaitļos. Piemēram, lineārām sistēmām var izmantot Gausa metodi, ir spēkā Bezū teorēma.

1.12. piezīme. Atgādinājums par Bezū teorēmu: a ir vienādojuma $f(x) = 0$ atrisinājums tad un tikai tad, ja $(x - a)|f(x)$ jeb

$$f(x) = (x - a)g(x).$$

Ar ko $\mathbb{Z}/p\mathbb{Z}$ atšķiras no $\mathbb{Q}$,$\mathbb{R}$ vai $\mathbb{C}$:

- laukā $\mathbb{Z}/p\mathbb{Z}$ ir galīgs skaits elementu - sliktākajā gadījumā var atrast visus atrisināju-mus ar izsmeļošo pārlasi;
- ne vienmēr eksistē saknes - lietderīgi izmantot primitīvās saknes un indeksus.

1.5. teorēma. Ja p ir pirmskaitlis un

$$f_1(x)f_2(x) \equiv 0 \pmod{\text{p}},$$

tad vai nu $f_1(x) \equiv 0 \pmod{\text{p}}$, vai arī $f_2(x) \equiv 0 \pmod{\text{p}}$.

PIERĀDĪJUMS Tas seko no agrāk pierādīta fakta, ka atlikumu gredzenā pēc pirmskaitļa moduļa nav nulles dalītāju - ja $ab \equiv 0 \pmod{\text{p}}$, tad vai nu $a \equiv 0$, vai arī $b \equiv 0$. ■

Polinomu $f(x)$ sauksim par *sadalāmu pēc moduļa p (reducible)*, ja

$$f(x) \equiv \bar{f}(x) \equiv f_1(x)f_2(x) \pmod{\text{p}},$$

kur $f_i(x)$ ir nekonstanti polinomi. Pretējā gadījuma polinomu sauksim par *nesadalāmu (irreducible)*.

1.6. piemērs. $x^2 + 1 \equiv (x+1)^2 \pmod 2$. $x^2 + x + 1 \pmod 2$ ir nesadalāms, bet $x^2 + x + 1 \equiv (x+2)^2 \pmod 3$.

$x^2 + x + 3 \equiv (x+2)(x+4) \pmod 5$.

Par polinoma $f(x) = \sum_{i=1}^{n} a_i x^i$ *Fermā redukciju ar moduli* p sauksim polinomu

$$\hat{f}_p(x) = \sum_{i=1}^{n} a_i x^{i \bmod p-1}.$$

1.7. piemērs. Ja $f(x) = x^6 + x^5 + x + 1$, tad

$$\hat{f}_3(x) = x^0 + x^1 + x + 1 \equiv 2x + 2.$$

1.6. teorēma. Jebkurš algebrisks vienādojums ar vienu nezināmo pēc moduļa p ir ekvivalents vienādojumam, kura pakāpe nepārsniedz $p-1$.

PIERĀDĪJUMS Pieņemsim, ka $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$. Ja $a_0 \not\equiv 0 \pmod{\text{p}}$, tad $x \not\equiv 0 \pmod{\text{p}}$ un

$$x^i \equiv x^{i \bmod \text{p-1}} \bmod \text{p}.$$

Redzam, ka

$$f(x) \equiv \hat{f}(x) \pmod{\text{p}}.$$

Ja $a_0 \equiv 0 \pmod{\text{p}}$, tad

$$f(x) \equiv x^r g(x),$$

kur polinoma $g(x)$ brīvais loceklis nav kongruents ar nulli. $f(x)$ atrisinājumu kopa ir 0 un $\hat{g}(x) \equiv 0$ atrisinājumu kopas apvienojums, tāpēc vienādojums $f(x) \equiv 0 \pmod{\text{p}}$ ir ekvivalents ar vienādojumu $x\hat{g}(x) \equiv 0 \pmod{\text{p}}$, kura pakāpe nepārsniedz $p-1$. ■

1.13. piezīme. Algoritms vienādojuma $f(x) \equiv 0 \pmod{\text{p}}$ risināšanai:

1. veikt polinoma $f(x)$ pārveidošanu par ekvivalentu polinomu
$$\tilde{f}(x) = x^s \cdot g(x),$$
kur $s \in \{0, 1\}$ $g(0) \not\equiv 0 \pmod{\text{p}}$ un $g(x)$ pakāpe nepārsniedz $p - 2$;
2. mēģināt sadalīt reizinātājos $g(x) \pmod{\text{p}}$ - izteikt to formā
$$g(x) \equiv g_1(x)...g_l(x) \pmod{\text{p}};$$
3. katram i atrisināt vienādojumu
$$g_i(x) \equiv 0 \pmod{\text{p}}$$
un atrast visu atrisinājumu apvienojumu.

1.8. piemērs. Atrisināsim vienādojumu

$$x^7 + 8x^5 - 2x^3 + x - 1 = 0 \pmod 5.$$

Reducējot koeficientus mod 5, iegūsim

$$x^7 + 3x^5 + 3x^3 + x + 4 = 0 \pmod 5.$$

Pielietojot Fermā redukciju, iegūsim ekvivalento vienājumu

$$x^3 + 3x + 3x^3 + x + 4 \equiv 4x^3 + 4x + 4 \equiv x^3 + x + 1 \equiv 0 \pmod 5.$$

Sadalīsim kreiso pusi reizinātājos:

$$x^3 + x + 1 \equiv (x+1)(x^2 + 4x + 2) \equiv 0 \pmod 5.$$

Redzam, ka saskaņā ar Bezū teorēmu ir viena sakne $x \equiv 4$ (mod 5). Veselos skaitļos atrisinājumu kopa ar $\{5t + 4 | t \in \mathbb{Z}\}$.

1.14. piezīme. Algoritms lineāras modulāru vienādojumu sistēmas atrisināšanai ar fiksētu moduli p - pielietot Gausa metodi.

1.9. piemērs. Atrisināsim sistēmu

$$\begin{cases} x_1 - x_2 - x_3 \equiv 1 \pmod 3 \\ 2x_1 + x_2 - 2x_3 \equiv 2 \pmod 3 \\ 2x_1 - 2x_2 - x_3 \equiv 2 \pmod 3 \end{cases},$$

Šo pašu sistēmu var atrisināt pēc cita moduļa, piemēram, 2 un iegūt citu rezultātu.

1.15. piezīme. Spēle *All Lights*.

1.16. piezīme. Nelineāras vienādojumu sistēmas pēc fiksēta pirmskaitļa moduļa risināt ir grūti, tāpat kā reālos skaitļos. Ja nekas cits neatliek, var izmantot izsmeļošo pārlasi.

1.5. Vienādojumi atlikumu gredzenos pēc pirmskaitļa pakāpes moduļa

1.17. piezīme. Modulāros vienādojumus pēc pirmskaitļa pakāpes p^α moduļa risināsim izmantojot šādu faktu: ja $a \equiv b \pmod{m}$ un $m'|m$, tad $a \equiv b \pmod{m'}$. Konkrētāk, risināsim modulāros vienādojumus sākot no mazām p pakāpēm: no sākuma pēc moduļa p, pēc tam pēc p^2 u.t.t.

Risinot kongruenču vienādojumus, ir lietderīgi izmantot jau minētu atlikumu kongruences īpašību: ja $d|a$, $d|b$ un $d|m$, tad kongruences $a \equiv b \pmod{m}$ un $(\frac{a}{d}) \equiv (\frac{b}{d}) \pmod{(\frac{m}{d})}$ ir ekvivalentas.

1.18. piezīme. No iepriekšējās piezīmes seko algoritms vienādojuma $f(x) \equiv 0 \pmod{p^\alpha}$ risināšanai:

1. Atrisināsim vienādojumu

$$f(x) \equiv 0 \pmod{p},$$

iegūsim atrisinājumu kopu S_1.

2. Katram $s \in S_1$ ievietosim $x = s + px'$ vienādojumā

$$f(x) \equiv 0 \pmod{p^2},$$

atrisināsim iegūto vienādojumu attiecībā uz x', iegūsim atrisinājumu kopu S_2;

3. ...

1.10. piemērs. Atrisināsim vienādojumu $3x^2 + x - 1 \equiv 0 \pmod{27}$.

1. Jebkurš atrisinājums x apmierina vienādojumu
$$3x^2 + x - 1 \equiv 0 \pmod{3},$$
šim vienādojumam ir viens atrisinājums $x \equiv 1 \pmod{3}$.

2. Ievietosim iegūto atrisinājumu $x = 1 + 3x'$ vienādojumā
$$3x^2 + x - 1 \equiv 0 \pmod{9}.$$
Iegūsim vienādojumu $3x' + 3 \equiv 0 \pmod{9}$. Izdalīsim visu ar 3, iegūsim vienādojumu $x' + 1 \equiv 0 \pmod{3}$, kura atrisinājums ir $x' \equiv 2 \pmod{3}$. Tātad $x \equiv 1 + 3 \cdot 2 = 7 \pmod{9}$.

3. Ievietosim iegūto atrisinājumu $x = 7 + 9x''$ vienādojumā
$$3x^2 + x - 1 \equiv 0 \pmod{27}.$$
Iegūsim vienādojumu $9x'' + 18 \equiv 0 \pmod{27}$. Izdalīsim visu ar 9, iegūsim vienādojumu $x'' + 2 \equiv 0 \pmod{3}$, kura atrisinājums ir $x'' \equiv 1 \pmod{3}$.

Atbilde ir $x \equiv 7 + 9 \cdot 1 = 16 \pmod{27}$.

2. 10.mājasdarbs

1. Atrisiniet vienādojumus
   (a) $15x \equiv 40 \pmod{35}$;
   (b) $44x \equiv 77 \pmod{33}$;
   (c) $1215x \equiv 560 \pmod{2755}$.
2. Atrodiet visus naturālos x, kas apmierina vienādojumus
   (a) $395 \equiv 267 \pmod{2x}$;
   (b) $244 \equiv 100 \pmod{x^2}$.