Tartu Ülikooli Teaduskool

Arvuteooria

6. Kongruentsid

Koostanud Maksim Ivanov, TÜ Teaduskool
Retsenseerinud Elts Abel, Tartu Ülikool

Käesolevas vihikus tutvume kongruentsi mõistega, lahendame kongruentse ja kongruentside süsteeme ning lahendame mõningaid jaguvusülesandeid kongruentside abil.

Kongruentsi mõiste

Definitsioon 1. Kaht täisarvu a ja b nimetatakse *kongruentseks* mooduli m järgi, kui arvude a ja b jagamisel positiivse täisarvuga m saame ühe ja sama jäägi (st leiduvad sellised täisarvud q_1, q_2 ja r, et $a = mq_1 + r$ ja $b = mq_2 + r$, kus $0 \leqslant r < m$), ja tähistatakse

$$a \equiv b \pmod{m}.$$

Märkus. Definitsioonist otseselt järeldub, et

- arvu a kongruentsus nulliga mooduli m järgi on samaväärne sellega, et arv a jagub arvuga m, st $m \mid a$ parajasti siis, kui $a \equiv 0 \pmod{m}$;
- täisarvud a ja b on kongruentsed mooduli m järgi parajasti siis, kui $m \mid a - b$ (võib lugeda **alternatiivseks definitsiooniks**);
- täisarvud a ja b on kongruentsed mooduli m järgi siis ja ainult siis, kui üks arv erineb teisest mooduli kordse võrra, st leidub selline täisarv t, et $a = b + mt$ (see on samuti alternatiivne definitsioon);
- kui $m \nmid a - b$, siis täisarvud a ja b ei ole kongruentsed mooduli m järgi, st $a \not\equiv b \pmod{m}$.

Näited definitsiooni kasutamisest:

- kehtivad kongruentsid $0 \equiv 3 \pmod{3}$, $3 \equiv 21 \pmod{3}$ ja $21 \equiv 0 \pmod{3}$, kuna arvud 0, 3 ja 21 annavad sama jäägi 0 arvuga 3 jagamisel;
- kehtivad kongruentsid $2 \equiv 20 \pmod{3}$ ja $200 \equiv 2000 \pmod{3}$, sest kõik arvud 2, 20, 200 ja 2000 annavad jäägi 2 arvuga 3 jagamisel (kõikide nende arvude ristsummad on 2);
- $2 \equiv -1 \pmod{3}$, sest $-1 = 3 \cdot (-1) + 2$;
- $1 \not\equiv -1 \pmod{3}$, sest jäägiga jagamisel saame võrdused $1 = 3 \cdot 0 + 1$ ja $-1 = 3 \cdot (-1) + 2$, kus $1 \neq 2$.

Ülesanne 2. Olgu a, b ja m sellised positiivsed täisarvud, mille korral leiduvad sellised täisarvud q_1, q_2, r_1 ja r_2, et

$$a = mq_1 + r_1 \qquad \text{ja} \qquad b = mq_2 + r_2,$$

kus $0 \leqslant r_1, r_2 < m$. Tõestada, et $a \equiv b \pmod{m}$ parajasti siis, kui $r_1 = r_2$.

Tõestus.

Tarvilikkus. Kehtigu $a \equiv b \pmod{m}$. Tõestame, et $r_1 = r_2$:

Piisavus. Kehtigu nüüd $r_1 = r_2$. Tõestame, et $a \equiv b \pmod{m}$:

Näited alternatiivse definitsiooni kasutamisest:

- kehtib kongruents $543 \equiv 987 \pmod{4}$, sest $987 - 543 = 444$ ja $4 \mid 444$;
- mis tahes täisarvu a korral kehtivad kongruentsid $a \equiv a + 2 \pmod{2}$ ja $a \equiv a - 3 \pmod{3}$, sest $2 \mid (a + 2) - a$ ja $3 \mid a - (a - 3)$.

Ülesanne 3. Põhjendada kas kongruentsi definitsiooni või selle alternatiivse definitsiooni kaudu, et kehtivad järgmised tingimused:

a) $2007 \equiv 7002 \pmod{5}$

b) $2007^2 \equiv 7002^2 \pmod{5}$

c) $2a + 7 \equiv 2 + 7a \pmod{5}$ mis tahes täisarvu a korral

Näide 4. Leiame kõik ühest suuremad positiivsed moodulid, mille järgi on kõik täisarvud 123, 234 ja 345 omavahel kongruentsed.

Olgu a ja b mis tahes kaks nimetatud arvudest ja m otsitav moodul. Kongruentsi alternatiivsest definitsioonist järeldub, et peab kehtima tingimus $m \mid a - b$. Paneme tähele, et mis tahes kahe nimetatud arvu positiivne vahe on kas 111 või $222 = 2 \cdot 111$. Seega moodul m on arvu 222 tegur. Ilmselt m ei tohi olla paarisarv, sest paarisarvuga jagamisel annavad paaris- ja paaritud arvud erinevad jäägid. Seega m on arvu $111 = 3 \cdot 37$ tegur. Järelikult arvu $m > 1$ väärtuseks saab olla kas arv 3 või arv 37. Kuna

$$\begin{aligned} 123 &= 3 \cdot 41 = 37 \cdot 3 + 12; \\ 234 &= 3 \cdot 78 = 37 \cdot 6 + 12; \\ 345 &= 3 \cdot 115 = 37 \cdot 9 + 12, \end{aligned}$$

siis 3 ja 37 ongi kõik võimalikud ühest suuremad positiivsed moodulid, mille järgi on kõik antud arvud omavahel kongruentsed.

Kongruentsi omadused

Lause 5. *Olgu a, b, c ja d täisarvud ning olgu m positiivne täisarv. Siis kehtivad järgmised omadused:*

a) $a \equiv a \pmod{m}$ *(refleksiivsus);*

b) kui $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m}$, *siis* $a \equiv c \pmod{m}$ *(transitiivsus);*

c) kui $a \equiv b \pmod{m}$, *siis* $b \equiv a \pmod{m}$ *(sümmeetrilisus);*

d) kui $a \equiv b \pmod{m}$, *siis* $c \equiv d \pmod{m}$ *parajasti siis, kui* $a + c \equiv b + d \pmod{m}$ *;*

e) kui $a \equiv b \pmod{m}$ *ja* $c \equiv d \pmod{m}$, *siis* $ac \equiv bd \pmod{m}$.

Märkus. Kongruentsid on samaväärsed, kui nende kongruentside lahendite hulgad on võrdsed.

Tõestus. Iga väite tõestamisel kasutame kongruentsi alternatiivset definitsiooni:

$$a \equiv b \pmod{m} \text{ parajasti siis, kui } m \mid a - b.$$

a) Kuna iga positiivse arvu m korral $m \mid 0$, siis $m \mid a - a$, millest saame, et $a \equiv a \pmod{m}$.

b) Tingimustest $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$ järeldub, et $m \mid a-b$ ja $m \mid b-c$. Kuna

$$a-c = a-b+b-c = \underbrace{(a-b)}_{\vdots m} + \underbrace{(b-c)}_{\vdots m},$$

siis $m \mid a-c$ ja definitsiooni põhjal $a \equiv c \pmod{m}$.

c) Kui $a \equiv b \pmod{m}$, siis $m \mid a-b$ ja $m \mid -(a-b) = b-a$, millest $b \equiv a \pmod{m}$.

d) Tingimus $a \equiv b \pmod{m}$ on samaväärne tingimusega $m \mid a-b$. Kuna

$$a+c-(b+d) = \underbrace{(a-b)}_{\vdots m} + (c-d),$$

siis $m \mid a+c-(b+d)$ parajasti siis, kui $m \mid c-d$, millest järeldub, et kongruentsid $c \equiv d \pmod{m}$ ja $a+c \equiv b+d \pmod{m}$ on samaväärsed.

e) Tingimused $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$ on samaväärsed tingimustega $m \mid a-b$ ja $m \mid c-d$. Kuna

$$ac-bd = ac-cb+cb-bd = c\underbrace{(a-b)}_{\vdots m} + b\underbrace{(c-d)}_{\vdots m},$$

siis $m \mid ac-bd$ ja $ac \equiv bd \pmod{m}$. □

Märkus. Olgu k positiivne täisarv ning olgu iga $i \in \{1,2,\ldots,k\}$ korral a_i ja b_i täisarvud. Siis kehtivad järgmised omadused:

- kui $a_i \equiv b_i \pmod{m}$ iga $i \in \{1,2,\ldots,k\}$ korral, siis

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m};$$

- kui $a_i \equiv b_i \pmod{m}$ iga $i \in \{1,2,\ldots,k\}$ korral, siis

$$a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k \pmod{m}.$$

Märkusena sõnastatud omadused on lihtsalt tõestatavad vastavalt lause 5 väidete d) ja e) abil.

Ülesanne 6. Olgu a, b, c ja d täisarvud ning olgu m positiivne täisarv. Tõestada järgmised omadused:

a) kui $a \equiv b \pmod{m}$, siis $c \equiv d \pmod{m}$ parajasti siis, kui $a - c \equiv b - d \pmod{m}$;

b) kui $a \equiv b \pmod{m}$, siis $ak \equiv bk \pmod{m}$ mis tahes täisarvu k korral;

c) kui täisarvud k ja m on ühistegurita, siis $a \equiv b \pmod{m}$ on samaväärne kongruentsiga $ak \equiv bk \pmod{m}$;

d) kui $a \equiv b \pmod{m}$ ja k on selline positiivne täisarv, et $k \mid m$, siis $a \equiv b \pmod{k}$;

e) $a \equiv b \pmod{m}$ parajasti siis, kui $ak \equiv bk \pmod{mk}$ iga positiivse täisarvu k korral;

f) kui $a \equiv b \pmod{m}$, siis $a^k \equiv b^k \pmod{m}$ mis tahes positiivse täisarvu k korral.

Kongruentside lahendamine

Kongruentside teisendamine erineb oluliselt algebraliste võrduste teisendamisest.

- Algebras võrdusest $4a = 4b$ järeldub võrdus $a = b$. Kongruentside keeles väitest $4a \equiv 4b \pmod 6$ ei järeldu väide $a \equiv b \pmod 6$ (vt ülesanne 6 *c*)). Teiselt poolt kongruentsid $4a \equiv 4b \pmod 7$ ja $a \equiv b \pmod 7$ on samaväärsed (vt ülesanne 6 *c*)).
- Algebras võrdusest $ab = 0$ järeldub, et kas $a = 0$ või $b = 0$. Aga kongruentsist $ab \equiv 0 \pmod m$ ei saa järeldada, et kas $a \equiv 0 \pmod m$ või $b \equiv 0 \pmod m$. Näiteks $3 \cdot 5 \equiv 0 \pmod{15}$, aga $3 \not\equiv 0 \pmod{15}$ ja $5 \not\equiv 0 \pmod{15}$.

Lause 7. *Olgu a ja b täisarvud ning olgu k, n, m ja m_i iga $i \in \{1, 2, \ldots, n\}$ korral positiivsed täisarvud. Siis kehtivad järgmised omadused:*

a) $ak \equiv bk \pmod m$ *parajasti siis, kui*

$$a \equiv b \pmod{\frac{m}{S\ddot{U}T(m,k)}};$$

b) $a \equiv b \pmod{m_i}$ *iga* $i \in \{1, 2, \ldots, n\}$ *korral parajasti siis, kui*

$$a \equiv b \pmod{V\ddot{U}K(m_1, m_2, \ldots, m_n)}.$$

Märkus. *$S\ddot{U}T(a,b)$ on täisarvude a ja b suurim ühistegur ja $V\ddot{U}K(a,b)$ on nende vähim positiivne ühiskordne.*

Tõestus.

a) Tingimus $ak \equiv bk \pmod m$ on samaväärne tingimusega

$$m \mid ak - bk = k(a - b),$$

mis jaguvuse definitsiooni põhjal kehtib parajasti siis, kui leidub selline täisarv c, et $k(a - b) = mc$. Kuna $S\ddot{U}T(m,k)$ jagab arve m ja k, siis saame viimase võrdusega samaväärse võrduse

$$\frac{k}{S\ddot{U}T(m,k)}(a - b) = \frac{m}{S\ddot{U}T(m,k)}c,$$

kus $S\ddot{U}T\left(\frac{k}{S\ddot{U}T(m,k)}, \frac{m}{S\ddot{U}T(m,k)}\right) = 1$. Saadud võrdus kehtib parajasti siis, kui $\frac{m}{S\ddot{U}T(m,k)} \mid a - b$ ehk $a \equiv b \pmod{\frac{m}{S\ddot{U}T(m,k)}}$.

b) *Tarvilikkus.* Kuna $a \equiv b \pmod{m_i}$ iga $i \in \{1, 2, \ldots, n\}$ korral, siis $m_i \mid a - b$ samuti iga $i \in \{1, 2, \ldots, n\}$ korral. Seega $a - b$ on arvude m_i ühiskordne, mis alati jagub vähima ühiskordsega, st

$$\text{VÜK}(m_1, m_2, \ldots, m_n) \mid a - b.$$

Piisavus. Kehtigu

$$a \equiv b \pmod{\text{VÜK}(m_1, m_2, \ldots, m_n)}$$

ehk $\text{VÜK}(m_1, m_2, \ldots, m_n) \mid a - b$. Kuna $m_i \mid \text{VÜK}(m_1, m_2, \ldots, m_n)$ iga $i \in \{1, 2, \ldots, n\}$ korral, siis $m_i \mid a - b$ samuti iga $i \in \{1, 2, \ldots, n\}$ korral. □

Märkus. Lause 7 *a*) osa väite põhjal saab kongruentsi pooli jagada.

- Näiteks, kongruentsi $2n \equiv 8 \pmod{6}$ korral jagaja (st arvu 2) ja mooduli (st arvu 6) suurim ühistegur võrdub 2-ga, seega $n \equiv 4 \pmod{3}$ on antud kongruentsiga samaväärne.
- Kongruentsi $2n \equiv 8 \pmod{5}$ korral jagaja on mooduliga ühistegurita, seega sama mooduli korral saab selle kongruentsi pooli 2-ga jagada (st $n \equiv 4 \pmod{5}$), kusjuures lahendite hulk jääb samaks.
- Kuna $6 = \text{VÜK}(2, 3)$, siis lause 7 *b*) osa väite põhjal, näiteks, kongruents $2n \equiv 5 \pmod{6}$ on samaväärne kongruentside süsteemiga

$$\begin{cases} 2n \equiv 5 \pmod{2} \\ 2n \equiv 5 \pmod{3}. \end{cases}$$

Täisarvude a ja b korral kongruentsi $an \equiv b \pmod{m}$ lahendamine täisarvu n suhtes on samaväärne täisarvu n võimalike jääkide leidmisega jagamisel mooduliga m.

- Näiteks kongruentsi $2n \equiv 8 \pmod{5}$ lahendamisel saame samaväärse kongruentsi $n \equiv 4 \pmod{5}$. Seega esialgse kongruentsi lahendiks on kõik täisarvud, mis jagamisel arvuga 5 annavad jäägi 4. Lahenditeks sobivad näiteks arvud 14, 99 ja -56 ning kehtivad kongruentsid

$$2 \cdot 14 \equiv 8 \pmod{5}, \quad 2 \cdot 99 \equiv 8 \pmod{5}, \quad 2 \cdot (-56) \equiv 8 \pmod{5}.$$

- Kongruentsi $2n \equiv 8 \pmod 6$ lahendamisel saame samaväärse kongruentsi $n \equiv 4 \pmod 3$ ehk $n \equiv 1 \pmod 3$, millest järeldame, et selle lahenditeks sobivad kõik täisarvud, mis jagamisel arvuga 3 annavad jäägi 1 ehk on mingi täisarvu k korral kujul $3k + 1$. Kuna esialgse kongruentsi mooduliks on arv 6 ning 6-ga jagamisel võivad tekkida jäägid 0 kuni 5, siis peame sellest lõigust otsima kõik 6-ga jagamisel tekkivad jäägid kujul $3k + 1$. Nendeks on arvud 1 ja 4. Järelikult kongruentsi $2n \equiv 8 \pmod 6$ lahenditeks on kõik täisarvud, mis jagamisel arvuga 6 annavad kas jäägi 1 või 4. Teisisõnu,
$$n \equiv 1, 4 \pmod 6.$$

Tõestame nüüd ühe lause, mis on vajalik järgmise teoreemi tõestamiseks.

Lause 8. *Olgu a ja b ühistegurita täisarvud. Siis leiduvad sellised täisarvud s ja t, et*
$$sa + tb = 1.$$

Tõestus. Vaatleme hulka $K = \{ua + vb \mid u \text{ ja } v \text{ on täisarvud}\}$.
Olgu k hulga K vähim positiivne element. Siis leiduvad täisarvud s ja t, mille korral $k = sa + tb$. Kui jagame arvud a ja b arvuga k, siis saame täisarvud q_1, q_2, r_1 ja r_2 nii, et $a = q_1k + r_1$ ja $b = q_2k + r_2$, kus $0 \leqslant r_1, r_2 < k$. Kuna jäägid
$$r_1 = a - q_1k = a - q_1(sa + tb) = (1 - q_1s)a + (-q_1t)b$$
ja
$$r_2 = b - q_2k = b - q_2(sa + tb) = (-q_2s)a + (1 - q_2t)b$$
on hulga K elemendid, siis k valiku ja võrratuse $0 \leqslant r_1, r_2 < k$ põhjal võime järeldada, et $r_1 = r_2 = 0$. Seega $a = q_1k$ ja $b = q_2k$ ehk $k \mid a$ ja $k \mid b$. Kuna a ja b on ühistegurita, siis $k = 1$. □

Anname nüüd tarviliku ja piisava tingimuse selleks, et kongruentsil $an \equiv b \pmod m$ leiduks lahend.

Teoreem 9. *Kongruentsil $an \equiv b \pmod m$ leidub lahend parajasti siis, kui*
$$SÜT(a, m) \mid b.$$

Tõestus. Olgu $d = \text{SÜT}(a, m)$.
Tarvilikkus. Leidugu kongruentsil $an \equiv b \pmod m$ lahend. Siis leidub täisarv t nii, et $an = b + mt$. Kuna $d \mid an$ ja $d \mid mt$, siis ka $d \mid b$.

Piisavus. Kehtigu $d \mid b$. Kuna $\frac{m}{d}$ ja $\frac{a}{d}$ on ühistegurita, siis lause 8 põhjal leiduvad täisarvud s ja t nii, et

$$s \cdot \frac{m}{d} + t \cdot \frac{a}{d} = 1.$$

Olgu $b = dk$ mingi täisarvu k korral. Siis saame eelmise võrdusega samaväärsed võrdused $sm + ta = d$ ja $smk + tak = dk = b$. Seega antud kongruentsiga $an \equiv b \pmod{m}$ on samaväärsed kongruentsid

$$an \equiv smk + tak \pmod{m},$$
$$an \equiv tak \pmod{m},$$
$$n \equiv tk \pmod{\frac{m}{d}},$$

millest järeldubki, et lahend leidub. □

Märkus. Olgu $d = \text{SÜT}(a, m)$. Juhul kui kongruentsil $an \equiv b \pmod{m}$ leidub lahend (st kui $d \mid b$), siis see on samaväärne kongruentsiga $\frac{a}{d}n \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, millel on täpselt üks moodulist väiksem mittenegatiivne lahend r, st

$$n \equiv r \pmod{\frac{m}{d}}, \quad \text{kus} \quad 0 \leqslant r < \frac{m}{d}.$$

Esialgsel kongruentsil $an \equiv b \pmod{m}$ on sellisel juhul täpselt d erinevat moodulist m väiksemat mittenegatiivset lahendit r_i, kus $r_i \in \{1, 2, \ldots, d\}$, st

$$n \equiv r_i \pmod{m}, \quad \text{kus} \quad 0 \leqslant r_i < m.$$

Näide 10. Lahendame põhjalikult kongruentsi $42n \equiv 12 \pmod{90}$, st leiame, millised jäägid võivad tekkida arvu n jagamisel antud mooduliga 90. Jagades kongruentsi läbi 6-ga (vt ülesanne 6 e)), saame samaväärse kongruentsi

$$7n \equiv 2 \pmod{15}.$$

Kuna arvud -2 ja 15 on ühistegurita, siis korrutades kongruentsi mõlemad pooled arvuga -2 (vt ülesanne 6 c)) saame

$$-14n \equiv -4 \pmod{15}.$$

Sellest, et $15n \equiv 15 \pmod{15}$, saame lause 5 d) põhjal antud kongruentsiga samaväärse kongruentsi

$$-14n + 15n \equiv -4 + 15 \pmod{15} \quad \text{ehk} \quad n \equiv 11 \pmod{15}.$$

Seega jagamisel arvuga 90 arvu n võimalikud jäägid on kujul $0 \leqslant 15k + 11 < 90$, kus k on täisarv. Järelikult

$$n \equiv 11, 26, 41, 56, 71, 86 \pmod{90}.$$

Näide 11. Lahendame lühidalt kongruentsid

a) $8n \equiv 3 \pmod{13}$;

b) $8n \equiv 10 \pmod{30}$;

c) $8n \equiv 30 \pmod{60}$.

a) Kuna arvud 8 ja 13 on ühisteguriteta, siis kongruents $8n \equiv 3 \pmod{13}$ on samaväärne järgmiste kongruentsidega:

$$\begin{aligned} 5 \cdot 8n &\equiv 5 \cdot 3 && \pmod{13}, \\ 40n &\equiv 15 && \pmod{13}, \\ 40n - 13 \cdot 3n &\equiv 15 && \pmod{13}, \\ n &\equiv 15 && \pmod{13}, \\ n &\equiv 15 - 13 && \pmod{13}, \\ n &\equiv 2 && \pmod{13}. \end{aligned}$$

b) Kuna $\text{SÜT}(8, 30) = 2$, siis kongruentsil $8n \equiv 10 \pmod{30}$ leidub 2 lahendit ja see on samaväärne järgmiste kongruentsidega:

$$\begin{aligned} 8n : 2 &\equiv 10 : 2 && \pmod{30 : 2}, \\ 4n &\equiv 5 && \pmod{15}, \\ 4 \cdot 4n &\equiv 4 \cdot 5 && \pmod{15}, \\ 16n &\equiv 20 && \pmod{15}, \\ 16n - 15n &\equiv 20 - 15 && \pmod{15}, \\ n &\equiv 5 && \pmod{15}. \end{aligned}$$

Seega $n = 15k + 5$ mingi täisarvu k korral. Arvestades võrratusega $0 \leqslant n < 30$, saame, et

$$n \equiv 5, 20 \pmod{30}.$$

c) Teoreemist 9 teame, et kongruentsil $an \equiv b \pmod{m}$ leidub lahend parajasti siis, kui kehtib tingimus

$$\text{SÜT}(a, m) \mid b.$$

Kuna $\text{SÜT}(a, m) = \text{SÜT}(8, 60) = 4$, $b = 30$ ja $4 \nmid 30$, siis sellel kongruentsil lahend puudub.

Ülesanne 12. Lahendada kongruentsid

a) $55n \equiv 35 \pmod 9$

b) $55n \equiv 35 \pmod{75}$

c) $55n \equiv 36 \pmod{75}$

Näide 13. Lahendame kongruentside süsteemi

$$\begin{cases} 5a + 7b \equiv 3 \pmod{17} \\ 2a + 3b \equiv -2 \pmod{17}. \end{cases}$$

Kuna arvud 2 ja -5 on arvuga 17 ühistegurita, siis esimese kongruentsi mõlemad pooled võime korrutada arvuga 2 ja teise kongruentsi mõlemad pooled korrutada arvuga -5. Saame esialgsega samaväärse süsteemi

$$\begin{cases} 10a + 14b \equiv 6 \pmod{17} \\ -10a - 15b \equiv 10 \pmod{17}. \end{cases}$$

Liites kongruentside vastavad pooled saame kongruentsi $-b \equiv 16 \pmod{17}$, millest $b \equiv 1 \pmod{17}$. Seega antud süsteem on samaväärne süsteemiga

$$\begin{cases} b \equiv 1 \pmod{17} \\ 2a + 3b \equiv -2 \pmod{17}. \end{cases}$$

Kuna $b \equiv 1 \pmod{17}$, siis asendades teises kongruentsis b väärtuse arvuga 1, saame kongruentsi

$$2a + 3 \equiv -2 \pmod{17} \quad \text{ehk} \quad 2a \equiv -5 \pmod{17}.$$

Et arvud 9 ja 17 on ühistegurita, siis korrutades viimasena saadud kongruentsi 9-ga, saame kongruentsi

$$18a \equiv -45 \pmod{17}.$$

Lahutades viimasest $17a \equiv -51 \pmod{17}$, saame $a \equiv 6 \pmod{17}$. Järelikult antud süsteemi lahendiks on

$$\begin{cases} a \equiv 6 \pmod{17} \\ b \equiv 1 \pmod{17}. \end{cases}$$

Ülesanne 14. Lahendada kongruentside süsteem

$$\begin{cases} 8a + 5b \equiv 1 \pmod{13} \\ 4a + 3b \equiv 3 \pmod{13}. \end{cases}$$

Lahendus.

Näide 15. Tööpäeva jooksul ettevõte toodab teatud arvu tooteid. Pakkijad panid tähele, et kui nende seas 2, 3, 4, 5 või 6 toodet osutub praagiks, siis vastavalt 1, 2, 3, 4 või 5 toodet jääb pakkimata. Kui leidub 7 praaktoodet, siis kõiki tooteid õnnestub karpidesse pakkida. Leiame, kui palju tooteid saab ettevõte toota ühe tööpäeva jooksul, kui on teada, et neid on kokku vähem kui 1000.

Olgu n toodete arv. Siis lause *"kui nende seas* 2, 3, 4, 5 *või* 6 *toodet osutub praagiks, siis vastavalt* 1, 2, 3, 4 *või* 5 *toodet jääb pakkimata"* on samaväärne kongruentsidega

$$n \equiv -1 \pmod{2,3,4,5,6},$$

mis on omakorda samaväärne kongruentsiga

$$n \equiv -1 \pmod{\text{VÜK}(2,3,4,5,6)}$$

ehk

$$n \equiv -1 \pmod{60}.$$

Lause *"kui leidub 7 praaktoodet, siis kõiki tooteid õnnestub karpidesse pakkida"* on samaväärne kongruentsiga

$$n \equiv 0 \pmod{7}.$$

Seega peame lahendama kongruentside süsteemi

$$\begin{cases} n \equiv -1 \pmod{60} \\ n \equiv 0 \pmod{7}. \end{cases}$$

Kongruentsist $n \equiv -1 \pmod{60}$ järeldub, et leidub täisarv k nii, et $n = 60k - 1$. Seega

$$\begin{aligned} 60k - 1 &\equiv 0 \pmod{7}, \\ 60k &\equiv 1 \pmod{7}, \\ 120k &\equiv 2 \pmod{7}, \\ 120k - 17 \cdot 7k &\equiv 2 \pmod{7}, \\ k &\equiv 2 \pmod{7}, \end{aligned}$$

millest järeldub, et leidub täisarv l nii, et $k = 7l + 2$. Kokkuvõttes saame, et

$$n = 60k - 1 = 60(7l + 2) - 1 = 420l + 119$$

ehk $n \equiv 119 \pmod{420}$. Kui $l \geqslant 3$, siis $n > 1000$. Võttes l väärtusteks arvud 0 kuni 2 saame, et n võimalikeks väärtusteks on arvud 119, 539 ja 959.

Näide 16. Olgu antud jadad $1, 4, 7, 10, \ldots$ ja $9, 16, 23, 30, \ldots$. Olgu S_1 ja S_2 vastavate jadade 1000-st esimesest liikmest koosnevad hulgad. Leiame, mitu võrdset elementi leidub nendes hulkades.

Paneme tähele, et kõik hulga S_1 elemendid on kongruentsed 1-ga mooduli 3 järgi ja kõik hulga S_2 elemendid on kongruentsed 2-ga mooduli 7 järgi. Seega lahendame kongruentside süsteemi

$$\begin{cases} n \equiv 1 \pmod 3 \\ n \equiv 2 \pmod 7. \end{cases}$$

Esimesest kongruentsist järeldub, et leidub täisarv k nii, et $n = 3k + 1$. Seega kongruents $n \equiv 2 \pmod 7$ on samaväärne järgmiste kongruentsidega

$$\begin{aligned} 3k + 1 &\equiv 2 \pmod 7 \\ 3k &\equiv 1 \pmod 7 \\ 6k &\equiv 2 \pmod 7 \\ -k &\equiv 2 \pmod 7 \\ k &\equiv 5 \pmod 7, \end{aligned}$$

millest järeldub, et leidub täisarv m nii, et $k = 7m + 5$. Kokkuvõttes saame, et

$$n = 3k + 1 = 3(7m + 5) + 1 = 21m + 16.$$

Kuna hulga S_1 suurim element on $1 + 3 \cdot 999 = 2998$, siis $0 \leqslant 21m + 16 \leqslant 2998$ parajasti siis, kui $0 \leqslant m \leqslant 142$ ehk hulkades S_1 ja S_2 leidub 143 võrdset elementi.

Näide 17. Leiame vähima positiivse täisarvu n väärtuse, mille korral kehtib kongruentside süsteem

$$\begin{cases} n \equiv 7 \pmod{37} \\ n^2 \equiv 12 \pmod{37^2}. \end{cases}$$

Teame, et kongruents $n \equiv 7 \pmod{37}$ kehtib parajasti siis, kui leidub selline täisarv k, et $n = 37k + 7$. Seega järgmised kongruentsid on kongruentsiga $n^2 \equiv 12 \pmod{37^2}$ samaväärsed:

$$\begin{aligned} (37k + 7)^2 &\equiv 12 \pmod{37^2} \\ (37k)^2 + 14 \cdot 37k + 49 &\equiv 12 \pmod{37^2} \\ 14 \cdot 37k &\equiv -37 \pmod{37^2} \\ 14k &\equiv -1 \pmod{37} \\ 112k &\equiv -8 \pmod{37} \\ 112k - 37 \cdot 3k &\equiv -8 \pmod{37} \\ k &\equiv 29 \pmod{37}. \end{aligned}$$

Seega leidub täisarv l nii, et $k = 37l + 29$. Kokkuvõttes saame, et

$$n = 37k + 7 = 37(37l + 29) + 7 = 1369l + 1080,$$

millest järeldub, et 1080 ongi vähim positiivne täisarv, mis rahuldab ülesande tingimust.

Näide 18. Leiame kõik sellised täisarvud n, mille korral kehtib kongruentside süsteem

$$\begin{cases} n \equiv 3 \pmod 7 \\ n^2 \equiv 44 \pmod{7^2} \\ n^3 \equiv 111 \pmod{7^3}. \end{cases}$$

a) Kongruentsi $n \equiv 3 \pmod 7$ kehtivus tähendab, et leidub selline täisarv k, et $n = 7k + 3$.

b) Eelmist punkti arvestades saame, et kongruents $n^2 \equiv 44 \pmod{7^2}$ on samaväärne järgmiste kongruentsidega:

$$\begin{aligned} (7k+3)^2 &\equiv 44 \pmod{7^2} \\ 7^2k^2 + 42k + 9 &\equiv 44 \pmod{7^2} \\ 42k &\equiv 35 \pmod{7^2} \\ 6k &\equiv 5 \pmod 7 \\ -k &\equiv 5 \pmod 7 \\ k &\equiv 2 \pmod 7. \end{aligned}$$

Seega leidub selline täisarv l, et $k = 7l + 2$, millest saame, et

$$n = 7k + 3 = 7(7l + 2) + 3 = 7^2l + 17.$$

c) Saadud tulemust $n = 7^2l + 17$ ja kongruentsi $17^3 \equiv 111 \pmod{7^3}$ kasutades saame, et $n^3 \equiv 111 \pmod{7^3}$ on samaväärne järgmiste kongruentsidega:

$$\begin{aligned} (7^2l + 17)^3 &\equiv 111 \pmod{7^3} \\ 7^6l^3 + 3 \cdot 17 \cdot 7^4l^2 + 3 \cdot 17^2 \cdot 7^2l + 17^3 &\equiv 111 \pmod{7^3} \\ 3 \cdot 17^2 \cdot 7^2l &\equiv 0 \pmod{7^3} \\ 7^2l &\equiv 0 \pmod{7^3} \\ l &\equiv 0 \pmod 7, \end{aligned}$$

millest saame, et $l = 7m$ mingi täisarvu m korral. Seega

$$n = 7^2l + 17 = 7^2 \cdot 7m + 17 = 7^3m + 17 = 343m + 17.$$

Näiteks süsteemi lahendiks sobivad arvud 17, 360, 703, 1046 jne.

Jaguvusülesannete lahendamine kongruentside abil

Kasutame nüüd eespool tõestatud kongruentside omadusi jaguvusülesannete lahendamisel.

Näide 19. Tõestame, et kehtivad järgmised tingimused:

a) $7 \mid 123 \cdot 124 \cdot 125 - 125^2$,

b) $8 \mid 321^{320} - 1$,

c) $123 \mid 1 \cdot 2 \cdot \ldots \cdot 61 + 62 \cdot 63 \cdot \ldots \cdot 122$,

d) $7 \mid 2222^{5555} + 5555^{2222}$.

a) Kõigepealt leiame, millise jäägi annab arv 123 jagamisel arvuga 7. Võrdusest $123 = 7 \cdot 17 + 4$ saame, et

$$123 \equiv 4 \pmod 7, \quad 124 \equiv 5 \pmod 7 \quad \text{ja} \quad 125 \equiv 6 \pmod 7,$$

millest järeldub, et

$$\begin{aligned} 123 \cdot 124 \cdot 125 - 125^2 &\equiv 4 \cdot 5 \cdot 6 - 6^2 \pmod 7, \\ 4 \cdot 5 \cdot 6 - 6^2 &\equiv 84 \pmod 7, \\ 84 &\equiv 0 \pmod 7. \end{aligned}$$

Seega $123 \cdot 124 \cdot 125 - 125^2 \equiv 0 \pmod 7$, mis on väitega *a*) samaväärne.
b) Sellest, et $321 \equiv 1 \pmod 8$, saame, et

$$\begin{aligned} 321^{320} - 1 &\equiv 1^{320} - 1 \pmod 8, \\ 1^{320} - 1 &\equiv 0 \pmod 8, \end{aligned}$$

millest järeldub $321^{320} - 1 \equiv 0 \pmod 8$ ehk $8 \mid 321^{320} - 1$.
c) Paneme tähele, et kehtivad kongruentsid $62 \equiv -61 \pmod{123}$, $63 \equiv -60 \pmod{123}$ jne kuni $122 \equiv -1 \pmod{123}$. Seega

$$\begin{aligned} 1 \cdot 2 \cdot \ldots \cdot 61 \; + \; & 62 \cdot 63 \cdot \ldots \cdot 122 \equiv \\ \equiv \; & 1 \cdot 2 \cdot \ldots \cdot 61 + (-61) \cdot (-60) \cdot \ldots \cdot (-1) \equiv 0 \pmod{123}, \end{aligned}$$

millest järeldubki antud avaldise jaguvus arvuga 123.
d) Et $2222 \equiv 3 \pmod 7$ ja $5555 \equiv 4 \pmod 7$, siis

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7.$$

Võrdusest

$$3^{5555} + 4^{2222} = (3^5)^{1111} + (4^2)^{1111} = (3^5)^{1111} + 16^{1111}$$

ja kongruentsidest $3^5 \equiv 3^2 \cdot 3^3 \equiv 2 \cdot (-1) \equiv 5 \pmod 7$ ja $16 \equiv 2 \equiv -5 \pmod 7$ saame, et

$$2222^{5555} + 5555^{2222} \equiv 5^{1111} + (-5)^{1111} \equiv 0 \pmod 7.$$

Näide 20. Leiame, millise jäägi annab

a) arv 6^{123} jagamisel arvuga 37;

b) arv $2^{123} + 1$ jagamisel arvuga 17.

a) Kuna $37 = 6^2 + 1$, millest $6^2 \equiv -1 \pmod{37}$, siis

$$\begin{aligned} 6^{123} &\equiv 6 \cdot 6^{122} \pmod{37}, \\ &\equiv 6 \cdot \left(6^2\right)^{61} \pmod{37}, \\ &\equiv 6 \cdot (-1)^{61} \pmod{37}, \\ &\equiv 6 \cdot (-1) \equiv -6 \equiv 31 \pmod{37}. \end{aligned}$$

b) Kuna $17 = 2^4 + 1$, millest $2^4 \equiv -1 \pmod{17}$, siis

$$2^{123} + 1 \equiv 2^3 \cdot \left(2^4\right)^{30} + 1 \equiv 8 \cdot (-1)^{30} + 1 \equiv 9 \pmod{17}.$$

Näide 21. Tõestame, et arv $53^{103} + 103^{53}$ jagub arvuga 39.
Paneme tähele, et kehtivad kongruentsid

$$\begin{aligned} 53 &\equiv 14 \pmod{39}, \\ 103 &\equiv -14 \pmod{39}, \\ 14^2 &\equiv 1 \pmod{39}. \end{aligned}$$

Järelikult

$$\begin{aligned} 53^{103} + 103^{53} &\equiv 14^{103} + (-14)^{53} \pmod{39}, \\ &\equiv 14^{103} - 14^{53} \pmod{39}, \\ &\equiv 14^{53}\left(14^{50} - 1\right) \pmod{39}, \\ &\equiv 14^{53}\left(\left(14^2\right)^{25} - 1\right) \pmod{39}, \\ &\equiv 14^{53}\left(1^{25} - 1\right) \pmod{39}, \\ &\equiv 0 \pmod{39}. \end{aligned}$$

Näide 22. Tõestame, et mis tahes positiivse täisarvu n korral

a) $35 \mid 17^n - 12^n - 24^n + 19^n$,

b) $13 \mid 3^{n+2} + 4^{2n+1}$,

c) $27 \mid 2^{5n+1} + 5^{n+2}$.

a) Olgu $N = 17^n - 12^n - 24^n + 19^n$. Kuna $35 = \text{VÜK}(5,7)$, siis võime eraldi näidata, et $5 \mid N$ ja $7 \mid N$:

- $5 \mid N$, sest mis tahes positiivse täisarvu n korral

$$\begin{aligned} N &\equiv 17^n - 12^n - 24^n + 19^n \pmod 5 \\ &\equiv 2^n - 2^n - 4^n + 4^n \equiv 0 \pmod 5. \end{aligned}$$

- $7 \mid N$, sest mis tahes positiivse täisarvu n korral

$$\begin{aligned} N &\equiv 17^n - 12^n - 24^n + 19^n \pmod 7 \\ &\equiv 3^n - 5^n - 3^n + 5^n \equiv 0 \pmod 7. \end{aligned}$$

b) Paneme tähele, et mis tahes positiivse täisarvu n korral

$$3^{n+2} \equiv 9 \cdot 3^n \equiv -4 \cdot 3^n \pmod{13}$$

ja

$$4^{2n+1} \equiv 4 \cdot 16^n \equiv 4 \cdot 3^n \pmod{13}.$$

Kokkuvõttes saame, et

$$3^{n+2} + 4^{2n+1} \equiv -4 \cdot 3^n + 4 \cdot 3^n \equiv 0 \pmod{13}.$$

c) Astmete omadusi kasutades, saame

$$2^{5n+1} + 5^{n+2} \equiv 2 \cdot 32^n + 25 \cdot 5^n \equiv 2 \cdot 5^n + 25 \cdot 5^n \equiv 27 \cdot 5^n \equiv 0 \pmod{27}.$$

Näide 23. Tõestame, et mis tahes positiivse täisarvu n korral arv $5^{2n} + 3 \cdot 2^{5n-2}$ jagub arvuga 7.
Paneme tähele, et $2n$ on paarisarv. Seega mis tahes positiivse täisarvu n korral kehtivad kongruentsid

$$5^{2n} \equiv (5-7)^{2n} \equiv (-2)^{2n} \equiv 2^{2n} \equiv 4 \cdot 2^{2n-2} \pmod 7$$

ja

$$\begin{aligned} 3 \cdot 2^{5n-2} &\equiv 3 \cdot 2^{3n} \cdot 2^{2n-2} \equiv 3 \cdot 8^n \cdot 2^{2n-2} \pmod 7 \\ &\equiv 3 \cdot 1^n \cdot 2^{2n-2} \equiv 3 \cdot 2^{2n-2} \pmod 7. \end{aligned}$$

Kokkuvõttes saame, et

$$5^{2n} + 3 \cdot 2^{5n-2} \equiv 4 \cdot 2^{2n-2} + 3 \cdot 2^{2n-2} \equiv 7 \cdot 2^{2n-2} \equiv 0 \pmod 7.$$

Ülesanne 24. Tõestada, et mis tahes paaritu positiivse täisarvu n korral summa $5^n + 11^n + 17^n$ jagub arvuga 33.

Tõestus. Märgime, et $33 = 3 \cdot 11$. Kõigepealt tõestame, et $3 \mid 5^n + 11^n + 17^n$ mis tahes positiivse täisarvu n korral:

Tõestame nüüd, et $11 \mid 5^n + 11^n + 17^n$ mis tahes paaritu positiivse täisarvu n korral:

Näide 25. Olgu $a_0 = 2$ ja $b_0 = 3^{a_0}$ ning $a_k = 2^{b_{k-1}}$ ja $b_k = 3^{a_k}$, kui $k \geqslant 1$. Tõestame, et iga $k = 0, 1, 2, \ldots$ korral jagub arv $13^{a_k} + 23^{b_k}$ arvuga 24.

Ülesande tingimustest järeldub, et mis tahes $k = 0, 1, 2, \ldots$ korral on a_k paarisarv ja b_k paaritu arv. Seega iga $k = 0, 1, 2, \ldots$ korral leiduvad positiivsed täisarvud m_k ja n_k nii, et $a_k = 2m_k$ ja $b_k = 2n_k + 1$. Siis

$$13^{a_k} + 23^{b_k} = 13^{2m_k} + 23^{2n_k+1} = 169^{m_k} + 23 \cdot 23^{2n_k}.$$

Et $169 \equiv 1 \pmod{24}$ ja $23 \equiv -1 \pmod{24}$, siis saame

$$13^{a_k} + 23^{b_k} \equiv 169^{m_k} + 23 \cdot 23^{2n_k} \equiv 1^{m_k} + (-1) \cdot (-1)^{2n_k} \equiv 0 \pmod{24}.$$

Järgmiste ülesannete eesmärgiks on leida mingi täisarvu kas viimane number või mingi arv viimaseid numbreid. Nende ülesannete lahendamisel kasutame nn *viimase numbri leidmise meetodit*: et leida antud arvu näiteks $k \geqslant 1$ viimast numbrit, tuleb kongruentside abil leida jääk, millise annab see arv jagamisel 10^k-ga.

Näide 26. Leiame arvu 7^{7^7} viimase numbri.
Arvu 7^{7^7} viimase numbri leidmiseks otsime, millise jäägi annab see arv jagamisel 10-ga. Kõigepealt uurime, kas leidub arvu 7 aste, mis jagamisel 10-ga annaks jäägi 1:

$$7^2 \equiv -1 \pmod{10}, \quad 7^3 \equiv 3 \pmod{10}, \quad 7^4 \equiv 1 \pmod{10}.$$

Järelikult $7^4 \equiv 1 \pmod{10}$ ja mis tahes positiivse täisarvu k korral

$$\left(7^4\right)^k \equiv 1^k \equiv 1 \pmod{10}.$$

Seega peame leidma, millise jäägi annab arvu 7 astendaja 7^7 jagamisel 4-ga. Kasutades kongruentsi $7^2 \equiv 1 \pmod{4}$, saame

$$7^7 \equiv \left(7^2\right)^3 \cdot 7 \equiv 1^3 \cdot 7 \equiv 7 \equiv 3 \pmod{4}.$$

Seega leidub selline täisarv k, et $7^7 = 4k + 3$. Nüüd võime leida arvu 7^{7^7} viimase numbri:

$$7^{7^7} \equiv 7^{4k+3} \equiv \left(7^4\right)^k \cdot 7^3 \equiv 1^k \cdot 3 \equiv 3 \pmod{10}.$$

Näide 27. Leiame arvu 777^{777} kaks viimast numbrit.
Viime arvu 777^{777} kujule $(770 + 7)^{777}$ ja rakendame selle jaoks binoomvalemit:

$$(770 + 7)^{777} = 770^{777} + 777 \cdot 770^{776} \cdot 7 + \ldots + 777 \cdot 770 \cdot 7^{776} + 7^{777}.$$

Saadud võrduse paremal poolel olevatest liidetavatest ainult kaks viimast ei jagu arvuga 100. Seega

$$777^{777} \equiv 777 \cdot 770 \cdot 7^{776} + 7^{777} \equiv 7^{777}(111 \cdot 770 + 1) \pmod{100}.$$

Kuna $7^4 = 2401$, siis $7^4 \equiv 1 \pmod{100}$ ja mis tahes täisarvu k korral

$$7^{4k} \equiv 1 \pmod{100}.$$

Kuna $777 = 4 \cdot 194 + 1$, siis $7^{777} \equiv 7 \pmod{100}$. Järelikult

$$777^{777} \equiv 7^{777}(111 \cdot 770 + 1) \equiv 7 \cdot (111 \cdot 770 + 1) \equiv 97 \pmod{100}.$$

Näide 28. Leiame arvude 99^{34} ja 9^{43} kolm viimast numbrit.
Ülesande mõlema osa lahendamisel kasutame binoomvalemit järgmiselt:

$$\begin{aligned} 99^{34} &= (100-1)^{34} = 100^{34} - \ldots + \binom{34}{32} \cdot 100^2 \cdot 1^{32} - 34 \cdot 100 \cdot 1^{33} + 1^{34} = \\ &= \left[100^{34} - \ldots + \binom{34}{32} \cdot 100^2 \cdot 1^{32}\right] - 34 \cdot 100 \cdot 1^{33} + 1^{34}; \end{aligned}$$

$$\begin{aligned} 9^{43} &= (10-1)^{43} = \\ &= 10^{43} - \ldots + \binom{43}{40} \cdot 10^3 \cdot 1^{40} - \binom{43}{41} \cdot 10^2 \cdot 1^{41} + 43 \cdot 10 \cdot 1^{42} - 1^{43} = \\ &= \left[10^{43} - \ldots + \binom{43}{40} \cdot 10^3 \cdot 1^{40}\right] - \binom{43}{41} \cdot 10^2 \cdot 1^{41} + 43 \cdot 10 \cdot 1^{42} - 1^{43}. \end{aligned}$$

Kuna nurksulgudes olevate avaldiste kõik liidetavad jaguvad arvuga 1000, siis mooduli 1000 järgi kehtivad järgmised kongruentsid:

$$99^{34} \equiv -34 \cdot 100 \cdot 1^{33} + 1^{34} \equiv -3400 + 1 \equiv 601 \pmod{1000}$$

ja

$$\begin{aligned} 9^{43} &\equiv -\binom{43}{41} \cdot 10^2 \cdot 1^{41} + 43 \cdot 10 \cdot 1^{42} - 1^{43} \equiv \\ &\equiv -90300 + 430 - 1 \equiv 129 \pmod{1000} \end{aligned}$$

Ülesanne 29. Näidata, et

a) arvu 3^{123} viimane number on 7;

b) arvu 3^{1000} kaks viimast numbrit on 01.

Mõnede ülesannete lahendamisel on tarvis kasutada järgmist väga lihtsat väidet: iga arv on kongruentne enda numbrite summaga mooduli 9 järgi.

Näide 30. Arvu 2^{29} kümnendesituses on 9 erinevat numbrit ja iga number esineb selles kümnendesituses ainult ühe korra. Leiame, mis number puudub.

Märkame, et ühelt poolt kõigi numbrite summa

$$0+1+2+\ldots+9=45$$

jagub 9-ga. Teiselt poolt, kasutades kongruentsi $2^3 \equiv -1 \pmod 9$, saame

$$2^{29} \equiv 2^2 \cdot \left(2^3\right)^9 \equiv 4 \cdot (-1)^9 \equiv -4 \pmod 9.$$

Seega arvu 2^{29} kümnendesituses puudub number 4.

Näide 31. Nimetame 8-kohalist positiivset täisarvu huvitavaks, kui selle numbriteks on kõik erinevad numbrid 1 kuni 8 mingis järjekorras ja see jagub arvuga 1111. Leiame kõige suurema huvitava arvu.

Teame, et iga arv on kongruentne enda numbrite summaga mooduli 9 järgi. Kuna

$$1+2+\ldots+8 \equiv 0 \pmod 9,$$

siis huvitav 8-kohaline arv n jagub arvuga 9. Kuna 9 ja 1111 on ühistegurita, siis $9999 \mid n$.

Olgu a ja b sellised 4-kohalised arvud, et $n = \overline{ab}$. Siis

$$0 \equiv n \equiv 10^4 \cdot a + b \equiv a + b \pmod{9999}.$$

Kuna $0 < a+b < 2 \cdot 9999$, siis $a+b = 9999$. Nüüd on lihtne näha, et suurimaks huvitavaks arvuks on arv 87651234.

Ülesanne 32. Olgu n positiivne täisarv ja m arvu n numbrite ümberjärjestamisel saadud positiivne täisarv. Tõestada, et $n-m$ alati jagub 9-ga.

Põhjendame, et arvud m ja n on kongruentsed mooduli 9 järgi:

Näitame, et vahe $n-m$ alati jagub 9-ga:

Näide 33. Leiame 10 erinevat positiivset täisarvu, mille summa on 740 ja mille ristsummad on samad.

Kuna arvude keskmine on $\frac{740}{10} = 74$, siis vähemalt üks arvudest on 74-st väiksem ja selle ristsumma ei ületa arvu 15 (arvu 69 ristsumma on 15).

Kõik otsitavad arvud on kongruentsed ühe ja sama arvuga mooduli 9 järgi. Oletame, et see arv on k. Siis

$$k \equiv k + 9k \equiv 10k \equiv 740 \equiv 2 \pmod 9,$$

millest järeldub, et nende arvude ristsumma on mingi täisarvu l korral kujul $k = 9l + 2$. Kuna $k \leqslant 15$, siis iga arvu ristsumma on kas 2 või 11.

Juhul kui iga arvu ristsumma on 2, siis sobivad ainult arvust 740 väiksemad arvud 2, 11, 20, 101, 110 ja 200. Seega nende seas ei leidu 10 erinevat arvu, mille summa on 740.

Juhul kui iga arvu ristsumma on 11, siis vaatleme selle omadusega 10 väiksemat täisarvu:

$$29,\ 38,\ 47,\ 56,\ 65,\ 74,\ 83,\ 92,\ 119,\ 128.$$

Nende arvude summa on 731. Järgmine arv on 137, mis on arvust 128 täpselt 9 võrra suurem. Seega ülesande tingimusi täidavad järgmised 10 täisarvu:

$$29,\ 38,\ 47,\ 56,\ 65,\ 74,\ 83,\ 92,\ 119 \text{ ja } 137.$$

Lahendame nüüd mõned raskemad jaguvusülesanded kongruentside abil.

Näide 34. Tõestame, et arv $2^{100} - 1$ jagub arvuga 41.

Kuna $2^5 \equiv 32 \equiv -9 \pmod{41}$, siis

$$2^{100} - 1 \equiv (2^5)^{20} - 1 \equiv (-9)^{20} - 1 \equiv 9^{20} - 1 \pmod{41}.$$

Kuna $9^2 \equiv 81 \equiv -1 \pmod{41}$, siis

$$2^{100} - 1 \equiv 9^{20} - 1 \equiv (9^2)^{10} - 1 \equiv (-1)^{10} - 1 \equiv 0 \pmod{41}.$$

Näide 35. Tõestame, et $641 \mid 2^{32} + 1$.

Paneme tähele, et

$$641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4.$$

Seega ühelt poolt $2^7 \cdot 5 \equiv -1 \pmod{641}$ ja teiselt poolt $5^4 \equiv -2^4 \pmod{641}$. Saadud kongruentside abil leiame arvu $2^{32} + 1$ jäägi mooduli 641 järgi:

$$\begin{aligned} 2^{32} + 1 &\equiv 2^4 \cdot 2^{28} + 1 \equiv -5^4 \cdot 2^{28} + 1 \pmod{641} \\ &\equiv -\left(5 \cdot 2^7\right)^4 + 1 \equiv -(-1)^4 + 1 \pmod{641} \\ &\equiv -1 + 1 \equiv 0 \pmod{641}. \end{aligned}$$

Järgmisena vaatleme näiteid, mis on seotud faktoriaali mõistega. Siinjuures paneme tähele, et kui n ja m on positiivsed täisarvud, siis $m \mid n!$ iga $n \geqslant m$ korral.

Näide 36. Leiame, millise jäägi annab jagamisel arvuga 12 arv

$$1! + 2! + 3! + 4! + \ldots + 99! + 100!$$

Paneme tähele, et

$$4! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \equiv 24 \equiv 0 \pmod{12}.$$

Seega iga täisarvu $n \geqslant 4$ korral

$$n! \equiv 4! \cdot 5 \cdot 6 \cdot \ldots \cdot n \equiv 0 \cdot 5 \cdot 6 \cdot \ldots \cdot n \equiv 0 \pmod{12}.$$

Kuna $1! + 2! + 3! = 9$, siis

$$1! + 2! + 3! + 4! + \ldots + 99! + 100! \equiv 9 \pmod{12}.$$

Näide 37. Tõestame, et $357! + 358!$ jagub algarvuga 359.
Vaatleme arvu 357 faktoriaali:

$$\begin{aligned} 357! &= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 356 \cdot 357 = \\ &= (359 - 358) \cdot (359 - 357) \cdot (359 - 356) \cdot \ldots \cdot (359 - 3) \cdot (359 - 2). \end{aligned}$$

Saadud võrdusest saame järeldada, et

$$\begin{aligned} 357! &\equiv (-358) \cdot (-357) \cdot (-356) \cdot \ldots \cdot (-3) \cdot (-2) \equiv \\ &\equiv (-1)^{357} \cdot 358! \equiv -358! \pmod{359}. \end{aligned}$$

Järelikult

$$357! + 358! \equiv -358! + 358! \equiv 0 \pmod{359},$$

mida oligi vaja tõestada.

Järgmised ülesanded lahendame matemaatilise induktsiooni meetodi abil.

Näide 38. Tõestame, et iga $n \geqslant 1$ korral

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}.$$

Kõigepealt kontrollime induktsiooni baasi kehtivust $n = 1$ korral. Sellisel juhul saame

$$\begin{aligned} (-13)^{n+1} &\equiv (-13)^2 \equiv 169 \equiv -12 \pmod{181} \\ (-13)^n + (-13)^{n-1} &\equiv -13 + 1 \equiv -12 \pmod{181}. \end{aligned}$$

Seega $n = 1$ korral kongruents kehtib.

Oletame nüüd, et väide kehtib mingi positiivse täisarvu $n = k$ korral, st

$$(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181},$$

ning näitame, et väide kehtib ka järgmise täisarvu $n = k+1$ korral, st

$$(-13)^{k+2} \equiv (-13)^{k+1} + (-13)^k \pmod{181}.$$

Selleks teisendame avaldist $(-13)^{k+2}$ järgmiselt:

$$\begin{aligned}(-13)^{k+2} &\equiv -13 \cdot (-13)^{k+1} \equiv -13 \cdot ((-13)^k + (-13)^{k-1}) \equiv \\ &\equiv (-13)^{k+1} + (-13)^k \pmod{181}.\end{aligned}$$

Seega oleme ülesandes sõnastatud väite tõestanud matemaatilise induktsiooni abil.

Näide 39. Tõestame, et mis tahes täisarvu $n \geqslant 1$ korral ja mis tahes paaritu täisarvu a korral

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

Kontrollime induktsiooni baasi $n = 1$ korral. Sellisel juhul peab mis tahes paaritu täisarvu a korral kehtima kongruents $a^2 \equiv 1 \pmod 8$. Teame, et mis tahes paaritu täisruut annab 8-ga jagamisel jäägi 1, seega induktsiooni baas kehtib.

Oletame nüüd, et $n = k$ korral kehtib seos $a^{2^k} \equiv 1 \pmod{2^{k+2}}$. Siis leidub sellime täisarv m, et kehtib võrdus

$$a^{2^k} = 2^{k+2}m + 1.$$

Jääb tõestada, et $n = k+1$ korral kehtib seos

$$a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}.$$

Kehtib võrdus

$$a^{2^{k+1}} = \left(a^{2^k}\right)^2 = \left(2^{k+2}m + 1\right)^2 = \left(2^{k+2}m\right)^2 + 2^{k+3}m + 1.$$

Kuna $\left(2^{k+2}m\right)^2 + 2^{k+3}m \equiv 0 \pmod{2^{k+3}}$, siis $a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$.