Ettevalmistus matemaatikaolümpiaadiks (ülemaste)

Arvuteooria II

Koostanud Maksim Ivanov
TÜ Teaduskool

27. august 2014. a.

Sissejuhatus

Käesolev õppematerjal on ülemastme arvuteooria ülesannete lahendamismeetodite harjutamiseks mõeldud teine töövihik. Selles on palju kongruentsidega seotud ülesandeid (neist suur osa on ka täieliku lahendusega).

Kongruentsid

Definitsioon 1. Kaht täisarvu a ja b nimetatakse *kongruentseks* mooduli m järgi (ehk modulo m), 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 $a \not\equiv b \pmod{m}$.

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

Lahendus.

Ülesanne 3. Kaks sõpra mängivad "tikumängu", mille reeglid on järgmised: tikutoosis on 50 tikku, iga mängija võib korraga ära võtta 1 kuni 5 tikku, käiakse kordamööda ning kaotab see, kes võtab tikutoosist viimase tiku. Kongruentsi mõistet kasutades kirjeldage esimese mängija võitvat strateegiat.

Lahendus.

Lause 4. *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 $a \equiv b \pmod{m}$*, siis* $c \equiv d \pmod{m}$ *parajasti siis, kui* $ac \equiv bd \pmod{m}$.

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

Tõestus. Iga väite tõestamisel kasutame 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

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

Need omadused on lihtsalt tõestatavad lause 4 väidete $d)$ ja $e)$ abil.

Ülesanne 5. Olgu a, b, c ja d täisarvud ning olgu m positiivne täisarv. Tõestage 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.

Tõestus.

Märkus. Kongruentside lahendamine oluliselt erineb 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 5 c)). Teiselt poolt kongruentsid $4a \equiv 4b \pmod{7}$ ja $a \equiv b \pmod{7}$ on samaväärsed (vt ülesanne 5 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 6. *Olgu a ja b täisarvud ning olgu k, m ja m_i iga $i \in \{1, 2, \ldots, k\}$ korral positiivsed täisarvud. Siis kehtivad järgmised omadused:*

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

$$a \equiv b \pmod{\frac{m}{\text{SÜT}(m,k)}};$$

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

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

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 $\text{SÜT}(m, k)$ jagab arve m ja k, siis saame viimase võrdusega samaväärse võrduse

$$\frac{k}{\text{SÜT}(m,k)}(a - b) = \frac{m}{\text{SÜT}(m,k)}c,$$

kus $\text{SÜT}\left(\frac{k}{\text{SÜT}(m,k)}, \frac{m}{\text{SÜT}(m,k)}\right) = 1$. Saadud võrdus kehtib parajasti siis, kui $\frac{m}{\text{SÜT}(m,k)} \mid a - b$ ehk $a \equiv b \pmod{\frac{m}{\text{SÜT}(m,k)}}$. *Veenduge selles!*

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

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

Piisavus. Kehtigu

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

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

Märkus. Lause 6 *a*) osa väite põhjal saab kongruentsi pooli jagada.

- Näiteks, kongruentsi $2n \equiv 8 \pmod 4$ korral jagaja (st arvu 2) ja mooduli (st arvu 4) suurim ühistegur võrdub 2-ga, seega $n \equiv 4 \pmod 2$ 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 $35 = \text{VÜK}(5,7)$, siis lause 6 *b*) osa väite põhjal, näiteks, kongruents $2n \equiv 9 \pmod{35}$ on samaväärne kongruentside süsteemiga

$$\begin{cases} 2n \equiv 9 \pmod 5 \\ 2n \equiv 9 \pmod 7. \end{cases}$$

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.

Näide 7. Lahendame 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 5 *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 5 *c*)) saame

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

Sellest, et $15n \equiv 15 \pmod{15}$, lause 4 *d*) põhjal saame antud kongruentsiga samaväärse kongruentsi

$$n \equiv 11 \pmod{15}.$$

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

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

Ülesanne 8. Lahendage kongruentsid

a) $55n \equiv 35 \pmod 9$; b) $55n \equiv 35 \pmod{75}$; c) $55n \equiv 36 \pmod{75}$.

Lahendus.

Lause 9. *Olgu a ja b ühistegurita täisarvud ning m positiivne täisarv. 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 positiivsed 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

$$r_1 = a - q_1k = a - q_1(sa + tb) = (1 - q_1s)a + (-q_1t)b \in K$$

ja

$$r_2 = b - q_2k = b - q_2(sa + tb) = (-q_2s)a + (1 - q_2t)b \in K,$$

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 $k = 1$. $\square$

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

Lause 10. *Kongruentsil $an \equiv b \pmod{m}$ leidub lahend parajasti siis, kui*

$$S\ddot{U}T(a, m) \mid b.$$

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 9 põhjal leiduvad täisarvud s ja t nii, et

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

Olgu $b = dk$ mingi täisarvu k korral. Siis saame eelmise võrdusega samaväärsed võrdused $sm + ta = d$ ja $smk + tak = dk = b$. Seega

$$an \equiv smk + tak \pmod{m},$$

$$an \equiv tak \pmod{m},$$

$$n \equiv tk \pmod{\frac{m}{d}},$$

millest järeldubki, et lahend leidub. □

Näide 11. 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 2-ga ja teise kongruentsi mõlemad pooled korrutada -5-ga. Saame samaväärse süsteemi

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

Liites kongruentside vastavad pooled saame $-b \equiv 16 \pmod{17}$, 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 $2a + 3 \equiv -2 \pmod{17}$, mis on samaväärne kongruentsiga $2a \equiv -5 \pmod{17}$. Et ervud 9 ja 17 on ühistegurita, siis $18a \equiv -45 \pmod{17}$. Lahutades viimasest $17a \equiv -51 \pmod{17}$ saame $a \equiv 6 \pmod{17}$.

Ülesanne 12. Lahendage kongruentside süsteem

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

Lahendus.

Kasutame nüüd eespool tõestatud kongruentside omadusi jaguvusülesannete lahendamisel.

Näide 13. Näitame, et

a) $7 \mid 2006 \cdot 2007 \cdot 2008 - 2008^2$ ja

b) $8 \mid 2009^{2008} - 1$.

Kõigepealt leiame, millise jäägi annavad arvud 2006, 2007 ja 2008 jagamisel 7-ga. Saame

$$2006 \equiv 4 \pmod{7}, \quad 2007 \equiv 5 \pmod{7} \quad \text{ja} \quad 2008 \equiv 6 \pmod{7},$$

millest järeldub, et

$$\begin{aligned} 2006 \cdot 2007 \cdot 2008 - 2008^2 &\equiv 4 \cdot 5 \cdot 6 - 6^2 \pmod{7}, \\ 4 \cdot 5 \cdot 6 - 6^2 &\equiv 84 \pmod{7}, \\ 84 &\equiv 0 \pmod{7}. \end{aligned}$$

Seega $2006 \cdot 2007 \cdot 2008 - 2008^2 \equiv 0 \pmod{7}$, mis on väitega samaväärne.

Sellest, et $2009 \equiv 1 \pmod 8$, saame

$$\begin{aligned} 2009^{2008} - 1 &\equiv 1^{2008} - 1 \pmod 8, \\ 1^{2008} - 1 &\equiv 0 \pmod 8 \end{aligned}$$

millest järeldub $2009^{2008} - 1 \equiv 0 \pmod 8$ ehk $8 \mid 2009^{2008} - 1$.

Ülesanne 14. Tõestage, et

a) $2007 \mid 1 \cdot 2 \cdot \ldots \cdot 1003 + 1004 \cdot 1005 \cdot \ldots \cdot 2006$ ja

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

Tõestus.

Ülesanne 15. Tõestage, et kui positiivsete täisarvude a ja b korral $ab + 1$ jagub arvuga 24, siis jagub ka $a + b$ arvuga 24.

Tõestus.
Tõestamiseks piisab näidata, et $a + b$ jagub arvudega 3 ja 8 (vt ülesanne 5 *b*)) ehk $a + b \equiv 0 \pmod 3$ ja $a + b \equiv 0 \pmod 8$.

a) Kuna $ab + 1 \equiv 0 \pmod 3$, siis $ab \equiv -1 \equiv 2 \pmod 3$. Viimasest järeldub, et peaks kehtima kas

$$\begin{cases} a \equiv 1 \pmod 3 \\ b \equiv 2 \pmod 3 \end{cases}$$

või

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

Mõlemal juhul $a + b \equiv 3 \equiv 0 \pmod 3$.

b) Juhtumit $a + b \equiv 0 \pmod 8$ tõestage ise!

Näide 16. Tõestame, et mis tahes positiivse täisarvu n korral

$$N = 17^n - 12^n - 24^n + 19^n$$

jagub arvuga 35. Kuna $35 = \text{VÜK}(5,7)$, siis võime eraldi näidata, et $5 \mid N$ ja $7 \mid N$:

- $5 \mid N$, sest

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

- $7 \mid N$, sest

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

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

Tõestus.

Näide 18. Tõestame, et mis tahes positiivse täisarvu n korral

$$13 \mid 3^{n+2} + 4^{2n+1}.$$

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

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

Ülesanne 19. Tõestage, et mis tahes positiivse täisarvu n korral

a) $27 \mid 2^{5n+1} + 5^{n+2}$,

b) $43 \mid 6^{n+2} + 7^{2n+1}$.

Lahendus.

Selleks, et leida antud arvu näiteks $k \geqslant 1$ viimast numbrit, piisab kongruentside abil leida, millise jäägi annab see arv jagamisel 10^k-ga.

Näide 20. Leiame arvu 7^{7^7} viimase numbri. Selleks otsime, millise jäägi annab see arv jagamisel 10-ga. Kõigepealt uurime, kas leidub arvu 7 aste, mis jagamisel 10-ga annaks jäägi 1:

$$\begin{aligned} 7^2 &\equiv -1 \pmod{10}, \\ 7^3 &\equiv 3 \pmod{10}, \\ 7^4 &\equiv 1 \pmod{10}. \end{aligned}$$

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:

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

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

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

Ülesanne 21. Leidke arvu

a) 777^{777}

b) $\left(\left(\left(\left((7^7)^7\right)^7\right)^7\right)^7\right)^7$

viimane number.

Lahendus.

Ülesanne 22. Leidke

a) arvu 3^{2009} viimane number,

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

Lahendus.

a) Lahendage ise!

b) Et leida arvu 3^{1000} kaks viimast numbrit, peame leidma arvu 3^{1000} jäägi modulo 100. Sellest, et $3^2 = 9 = 10 - 1$, järeldub

$$3^{1000} \equiv 9^{500} \equiv (10-1)^{500} \pmod{100}.$$

Kasutades binoomvalemit saame

$$(10-1)^{500} \equiv 10^2 \cdot (\ldots) - 500 \cdot 10 + 1 \equiv 1 \pmod{100}.$$

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

Ülesanne 23. Leidke arvu $14^{14^{14}}$ viimane number.

Lahendus.

Näide 24. Leiame, millise jäägi annab arv $2^{2009}+1$ jagamisel 17-ga. Kuna $17 = 2^4+1$, millest $2^4 \equiv -1 \pmod{17}$, siis

$$2^{2009}+1 \equiv 2\cdot\left(2^4\right)^{502}+1 \equiv 2\cdot(-1)^{502}+1 \equiv 3 \pmod{17}.$$

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

Näide 25. 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 $2^3 \equiv -1 \pmod{9}$, 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.

Ülesanne 26. Olgu n positiivne täisarv ja m arvu n numbrite ümberjärjestamisel saadud positiivne täisarv. Tõestage, et $n-m$ alati jagub 9-ga.

Lahendus.

Näide 27. 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

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

Ülesanne 28. Olgu $a_1 = 0$, $a_2 = 1$ ja $a_k = 5a_{k-1} - a_{k-2}$, kui $n > 2$. Milliste positiivsete täisarvude k korral jagub arv a_k

a) arvuga 5; b) arvuga 15.

Lahendus.

a) Leiame mõnede esimeste arvude a_k jagamisel 5-ga tekkivad jäägid, kasutades järeldust võrdusest $a_k = 5a_{k-1} - a_{k-2}$:
kui $a_{k-2} \equiv p \pmod 5$ ja $a_{k-1} \equiv q \pmod 5$, kus p ja q on täisarvud nii, et $0 \leqslant p, q < 5$, siis $a_k \equiv 5q - p \pmod 5$.

k	1	2	3	4	5	6	...
$a_k \pmod 5$	0	1	0	4	0	1	...

Et a_k jagamisel arvuga 5 tekkiv jääk on üheselt määratud arvude a_{k-1} ja a_{k-2} jagamisel 5-ga tekkivate jääkidega, siis tekib tsükkel pikkusega 4. Seega võime väita, et a_k jagub 5-ga parajasti siis, kui k on positiivne paaritu täisarv.

b) Lahendage ise!

Näide 29. Olgu antud jadad $1, 4, 7, 10, \ldots$ ja $9, 16, 23, 30, \ldots$. Olgu S_1 ja S_2 vastavate jadade 2008 esimesest liikmest koosnevad hulgad. Leiame, mitu võrdset elementi leidub nendes hulkades. Paneme tähele, et kõik hulga S_1 elemendid on kongruentsed 1-ga modulo 3 ja kõik hulga S_2 elemendid on kongruentsed 2-ga modulo 7. Seega lahendame kongruentside süsteemi

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

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

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

millest järeldub, et leidub täisarv t nii, et $s = 7t + 5$. Kokkuvõttes saame, et $a = 3s + 1 = 3(7t + 5) + 1 = 21t + 16$. Kuna hulga S_1 suurim element on $1 + 3 \cdot 2007 = 6022$, siis $0 \leqslant 21t + 16 \leqslant 6022$ parajasti siis, kui $0 \leqslant t \leqslant 286$ ehk hulkades S_1 ja S_2 leidub 287 võrdset elementi.