Skaitļu dalāmība un kongruences

Teorija un piemēri, gatavojoties Novada olimpiādei 2015./2016. mācību gadā

Olimpiādes uzdevumu komplektā katrai klašu grupai tiek iekļauts algebras, ģeometrijas, kombinatorikas un skaitļu teorijas uzdevums. Šogad Novada matemātikas olimpiādē skaitļu teorijas uzdevums 5.-8. klasei būs par tēmu “Dalāmības pazīmes” (skat. 1.-3. lpp.), bet 9.-12. klasei par tēmu “Kongruences” (vecāko klašu skolēniem ieteicams izskatīt visu materiālu).

Skaitļu teorija ir matemātikas apakšnozare, kas pēta veselo skaitļu dalāmību.

Skaitļu dalāmība

Ja a un b ir veseli skaitļi, tad ne vienmēr, dalot a ar b, dalījumā iegūst veselu skaitli. Ja dalījums ir vesels skaitlis, tad saka, ka a dalās ar b, pretējā gadījumā saka, ka a nedalās ar b.

Definīcija. Ja $b \neq 0$ un $a : b = k$, kur a, b, k – veseli skaitļi, tad saka, ka a dalās ar b. Pretējā gadījumā saka, ka a nedalās ar b.

Piemēram, 15 dalās ar 3, bet 15 nedalās ar 2.

Iegaumē! Ja tiek runāts par skaitļu dalāmību, tad runa ir tikai par veseliem skaitļiem.

Dalāmības pazīmes

Noskaidrot, vai viens vesels skaitlis dalās ar otru, tikai ar definīcijas palīdzību, tas ir, izdalot skaitļus, bieži vien ir neparocīgi un laikietilpīgi. Šo uzdevumu atvieglo skaitļu dalāmības pazīmes. Tālāk dotas biežāk lietotās dalāmības pazīmes.

Dalāmības pazīme	Piemēri
Skaitlis dalās ar 2, ja tā pēdējais cipars ir pāra, tas ir, tā pēdējais cipars ir 0, 2, 4, 6 vai 8.	201**6** dalās ar 2, jo tā pēdējais cipars ir pāra
Skaitlis dalās ar 3, ja tā ciparu summa dalās ar 3.	2016 dalās ar 3, jo $2+0+1+6=9$ dalās ar 3
Skaitlis dalās ar 4, ja tā pēdējo divu ciparu veidotais skaitlis dalās ar 4.	20**16** dalās ar 4, jo 16 dalās ar 4
Skaitlis dalās ar 5, ja tā pēdējais cipars ir 0 vai 5.	201**5** dalās ar 5, jo tā pēdējais cipars ir 5
Skaitlis dalās ar 6, ja tas dalās gan ar 2, gan ar 3.	2016 dalās ar 6, jo tas dalās ar 2 un 3
Skaitlis dalās ar 8, ja tā pēdējo trīs ciparu veidotais skaitlis dalās ar 8.	12**800** dalās ar 8, jo 800 dalās ar 8 2**016** dalās ar 8, jo pēdējo trīs ciparu veidotais skaitlis ir 16, kas dalās ar 8
Skaitlis dalās ar 9, ja tā ciparu summa dalās ar 9.	2016 dalās ar 9, jo $2+0+1+6=9$ dalās ar 9
Skaitlis dalās ar 10, ja tā pēdējais cipars ir 0.	15**0** dalās ar 10, jo tā pēdējais cipars ir 0
Skaitlis dalās ar 11, ja tā ciparu summas, kas atrodas nepāra pozīcijās, un ciparu summas, kas atrodas pāra pozīcijās, starpība dalās ar 11.	$\underline{1}0\underline{8}6\underline{4}7$ dalās ar 11, jo $(1+8+4)-(0+6+7)=0$, kas dalās ar 11 $\underline{9}4\underline{8}3\underline{1}$ dalās ar 11, jo $(9+8+1)-(4+3)=11$, kas dalās ar 11

Citas dalāmības pazīmes

- Skaitlis dalās ar 10^n, ja tā pēdējo n ciparu veidotais skaitlis dalās ar 10^n.
- Skaitlis dalās ar 2^n, ja tā pēdējo n ciparu veidotais skaitlis dalās ar 2^n.
- Skaitlis dalās ar 5^n, ja tā pēdējo n ciparu veidotais skaitlis dalās ar 5^n.

Kombinējot iepriekš dotās pazīmes, var iegūt arī pazīmes dalāmībai ar citiem skaitļiem. Piemēram, skaitlis dalās ar 12, ja tas dalās ar 3 un 4; skaitlis dalās ar 90, ja tas dalās ar 9 un 10 jeb skaitļa ciparu summa dalās ar 9 un tā pēdējais cipars ir nulle. Šādi pazīmes veido, doto dalītāju sadalot reizinātājos, kas ir savstarpēji pirmskaitļi un pārbaudot dalāmību ar katru no tiem.

Definīcija. Par savstarpējiem pirmskaitļiem sauc skaitļus, kam lielākais kopīgais dalītājs ir skaitlis 1.

Piemērs. Ja skaitlis dalās ar 2 un 6, mēs nevaram apgalvot, ka tas dalās arī ar $2 \cdot 6 = 12$, piemēram, 18 dalās gan ar 2, gan ar 6, bet 18 nedalās ar 12. Tāpēc ir ļoti svarīgi, lai reizinātāji būtu savstarpēji pirmskaitļi.

Teorēma. Ja b un c ir savstarpēji pirmskaitļi un a dalās ar b un a dalās ar c, tad a dalās ar bc.

Uzdevumu piemēri

1. Vienādi burti apzīmē vienādus ciparus, dažādi – dažādus. Zināms, ka trīsciparu skaitlis $\overline{ASS}$ dalās ar 5, bet nedalās ar 4. Vai skaitlis $\overline{OLA}$ var dalīties ar 5?

Piezīme. Ar $\overline{abc}$ apzīmē trīsciparu skaitli, kura pirmais cipars ir a, otrais – b, trešais – c.

Atrisinājums. Tā kā skaitlis $\overline{ASS}$ dalās ar 5, tad $S = 0$ vai $S = 5$.

1. Ja $S = 0$, tad iegūstam skaitli $\overline{A00}$, kas dalās ar 4, bet tā ir pretruna ar doto, ka $\overline{ASS}$ nedalās ar 4. Tātad S nevar būt 0.
2. Apskatīsim gadījumu, kad $S = 5$. Lai skaitlis $\overline{OLA}$ dalītos ar 5, tad vai nu $A = 0$, vai $A = 5$. Tā kā dažādiem burtiem atbilst dažādi cipari, tad A nevar būt 5 un tāpēc $A = 0$. Bet tad skaitlis $\overline{ASS}$ nebūtu trīsciparu skaitlis, jo tā pirmais cipars būtu 0. Tātad S nevar būt arī 5.

Esam ieguvuši, ka skaitlis $\overline{OLA}$ nevar dalīties ar 5.

2. Naturālā vienpadsmitciparu skaitlī vienādus ciparus aizstāja ar vienādiem burtiem, bet dažādus – ar dažādiem; ieguva pierakstu $PĀRSTEIGUMS$. Zināms, ka šis skaitlis dalās ar 18. Noteikt, kurš cipars aizstāts ar burtu S.

Atrisinājums. Vārdā $PĀRSTEIGUMS$ pavisam ir 11 burti, no tiem pirmie 10 dažādi, tātad pirmie 10 burti apzīmē visus desmit ciparus. Tad

$$P + \bar{A} + R + S + T + E + I + G + U + M + S = 0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + S = 45 + S$$

Tā kā dotais vienpadsmitciparu skaitlis dalās ar 18, tad tas dalās ar 2 un 9. Tas nozīmē, ka tas ir pāra skaitlis un tā ciparu summa dalās ar 9. Tātad S ir pāra cipars un $45 + S$ dalās ar 9. Tā kā $45 + S$ jādalās ar 9 un skaitlis 45 dalās ar 9, tad arī S jādalās ar 9. Tātad ar burtu S ir aizstāts cipars 0.

Piezīme. Lai noteiktu, kurš cipars aizstāts ar burtu S, izteiksmē $45 + S$ var arī ievietot visas iespējamās S vērtības – 0, 2, 4, 6, 8 – un pārbaudīt katru no šiem gadījumiem.

3. Kādi cipari var būt burtu a un b vietā, lai piecciparu skaitlis $\overline{a543b}$ dalītos ar 36?

Atrisinājums. Lai skaitlis $\overline{a543b}$ dalītos ar 36, tam jādalās gan ar 9, gan ar 4. Lai skaitlis $\overline{a543b}$ dalītos ar 4, tā pēdējo divu ciparu veidotajam skaitlim jādalās ar 4. Tātad pēdējo divu ciparu veidotajam skaitlim jābūt vai nu 32, vai 36, līdz ar to $b = 2$ vai $b = 6$. Lai dotais skaitlis dalītos ar 9, tā ciparu summai jādalās ar 9.

- Ja $b = 2$, tad skaitļa ciparu summa ir $a + 5 + 4 + 3 + 2 = 14 + a$. Der $a = 4$, jo $14 + 4 = 18$, kas dalās ar 9. Tā kā a ir cipars, tad citus skaitļus, kas dalās ar 9, iegūt nevar.
- Ja $b = 6$, tad skaitļa ciparu summa ir $a + 5 + 4 + 3 + 6 = 18 + a$. Vērtība $a = 0$ neder, jo a ir skaitļa pirmais cipars. Der $a = 9$, jo $18 + 9 = 27$, kas dalās ar 9. Tā kā a ir cipars, tad citus skaitļus, kas dalās ar 9, iegūt nevar.

Tātad esam ieguvuši, ka $a = 4, b = 2$ vai $a = 9, b = 6$ ir vienīgās iespējamās vērtības.

4. Kāda ir mazākā iespējamā ciparu summa desmitciparu skaitlim, kas dalās ar 33?

Atrisinājums. Mazākā iespējamā ciparu summa desmitciparu skaitlim, kas dalās ar 33, ir 6, piemēram, skaitlim 3300000000.

Pierādīsim, ka ciparu summa nevar būt mazāka kā 6. Lai naturāls skaitlis dalītos ar 33, tam jādalās ar 3 un ar 11. Tā kā skaitlim jādalās ar 3, tad arī tā ciparu summai jādalās ar 3. Tas nozīmē, ka ir jāpierāda, ka ciparu summa nevar būt 3. Apzīmēsim skaitļa ciparu summu nepāra pozīcijās ar a un pāra pozīcijās – ar b, tad, lai skaitlis dalītos ar 11, $a-b$ jādalās ar 11. Pieņemsim, ka $a \geq b$, otru gadījumu aplūko analogi. Iespējami 2 gadījumi:

- $a-b=0$, tad $a=b$ un skaitļa ciparu summa ir $a+b$, kas ir pāra skaitlis, tātad tā nevar būt 3;
- $a-b \geq 11$, tad $a \geq 11$ un skaitļa ciparu summa ir lielāka kā 11, tātad tā nevar būt 3.

Piezīme. Uzdevumu var atrisināt arī, pārbaudot visus iespējamos gadījumus, kādus ciparus var saturēt desmitciparu skaitlis, kura ciparu summa ir 3: skaitlī ir viens (pirmais) cipars 3 un deviņas nulles; skaitlī ir viens cipars 1, viens cipars 2 un astoņas nulles; skaitlī ir trīs cipari 1 un septiņas nulles.

Tālāk dotais materiāls paredzēts 9.-12. klašu skolēniem.

Kongruences jēdziens

Lai pilnvērtīgāk apgūtu tematu par kongruencēm, ļoti ieteicams patstāvīgi risināt, piemēram, grāmatā A. Bērziņa, A. Bērziņš "Diferencēti uzdevumi skaitļu teorijā" dotos vingrinājumus un uzdevumus. Grāmata pieejama arī elektroniski: http://nms.lu.lv/wp-content/uploads/2014/06/BerzinsBerzina_DiferencetiUzdSkT.pdf

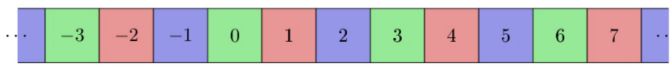
Viens no pazīstamākajiem veselo skaitļu iedalījumiem ir to dalījums pāra un nepāra skaitļos. Katrs vesels skaitlis ir vai nu pāra, vai nepāra, taču neviens nav vienlaikus gan pāra, gan nepāra skaitlis. Tā visi veselie skaitļi tiek sadalīti divās klasēs: skaitļi, kas dalās ar 2 (pāra skaitļi), un skaitļi, kas nedalās ar 2 (nepāra skaitļi).

Ja dalītāju 2 aizvieto ar 3, tad līdzīgi var runāt par skaitļiem, kas dalās vai nedalās ar 3. Tomēr izrādās, ka lietderīgāk ir veselos skaitļus sadalīt klasēs atkarībā no tā, kādu atlikumu tie dod, dalot ar 3. Arī pāra un nepāra skaitļus var uztvert kā skaitļus, kas, dalot ar 2, dod attiecīgi atlikumu 0 vai 1. Ja nomainām 2 ar 3, tad veselos skaitļus mēs sadalām trīs klasēs – šķirojot gadījumus, vai skaitlis, dalot ar 3, dod atlikumu 0, 1 vai 2.

Teorēma par dalīšanu ar atlikumu. Ja a ir vesels skaitlis un b ir naturāls skaitlis, tad noteikti var atrast tādus veselus skaitļus q un r, ka $a=b \cdot q+r$, turklāt $0 \leq r < b$.

Iegaumē! Atlikums nekad nav mazāks kā 0 un vienmēr ir mazāks nekā skaitlis, ar kuru dala, tas ir, dalot ar b, atlikumam var būt vērtības $0, 1, 2, \ldots, b-1$.

Skaitļu sadalīšanu klasēs var salīdzināt ar "skaitļu krāsošanu". Pieņemsim, ka visi veselie skaitļi sarakstīti uz bezgalīgas rūtiņu lentes. Ja vēlamies veselos skaitļus sašķirot klasēs atkarībā no tā, piemēram, kādus atlikumus tie dod, dalot ar 3, tad grafiski var iztēloties, ka katram skaitlim atbilstošā rūtiņa tiek nokrāsota vienā no trim krāsām: tie skaitļi, kas dalās ar trīs, tiek krāsoti vienā krāsā, tie skaitļi, kas, dalot ar 3, dod atlikumu 1 – citā krāsā, un skaitļi, kas, dalot ar 3, dod atlikumu 2 – vēl citā krāsā. Tādējādi visi skaitļi tiek nokrāsoti kādā no trim krāsām, turklāt katrs skaitlis tiek nokrāsots tieši vienā krāsā:



1. att.

Lai šos spriedumus vispārinātu un lietotu uzdevumu risināšanā, definē kongruences jēdzienu.

Definīcija. Doti veseli skaitļi a un b un naturāls skaitlis $m \geq 2$. Skaitļi a un b ir kongruenti pēc moduļa m un pieraksta $a \equiv b\ (mod\ m)$ vai $a \equiv_m b$, ja a un b, dalot tos ar m, dod vienādu atlikumu.

Piemēri

- $7 \equiv 3\ (mod\ 2)$, jo gan 7, gan 3, dalot ar 2, dod atlikumu 1
- $17 \equiv 73\ (mod\ 14)$, jo gan 17, gan 73, dalot ar 14, dod atlikumu 3
- $71 \equiv 8\ (mod\ 9)$, jo gan 71, gan 8, dalot ar 9, dod atlikumu 8
- $-2 \equiv 4\ (mod\ 3)$, jo gan -2, gan 4, dalot ar 3, dod atlikumu 1
- $-6 \equiv 85\ (mod\ 7)$, jo gan -6, gan 85, dalot ar 7, dod atlikumu 1

Bieži vien, lai pārbaudītu, vai skaitļi ir kongruenti pēc kāda moduļa, ir ērti lietot tālāk doto teorēmu.

Teorēma. $a \equiv b\ (mod\ m)$ tad un tikai tad, ja starpība $a - b$ dalās ar m.

Piemēri

- $7 \equiv 3\ (mod\ 2)$, jo starpība $7 - 3 = 4$ dalās ar 2
- $17 \equiv 73\ (mod\ 14)$, jo starpība $17 - 73 = -56$ dalās ar 14
- $71 \equiv 8\ (mod\ 9)$, jo starpība $71 - 8 = 63$ dalās ar 9
- $-2 \equiv 4\ (mod\ 3)$, jo starpība $-2 - 4 = -6$ dalās ar 3
- $-6 \equiv 85\ (mod\ 7)$, jo starpība $-6 - 85 = -91$ dalās ar 7

Kongruenču īpašības

Lai kongruences jēdzienu varētu lietot dažādu uzdevumu risināšanā, var izmantot kongruenču īpašības, kas ļauj daudzus aprēķinus veikt ievērojami vienkāršāk.

1. Ja a, dalot ar m, dod atlikumu r, tad $a \equiv r\ (mod\ m)$.
2. Ja $a \equiv b\ (mod\ m)$, tad $ka \equiv kb\ (mod\ m)$, kur k ir jebkurš vesels skaitlis.
3. Ja $a \equiv b\ (mod\ m)$, tad $a^n \equiv b^n\ (mod\ m)$, kur n ir jebkurš naturāls skaitlis.
4. Ja $a \equiv b\ (mod\ m)$ un $c \equiv d\ (mod\ m)$, tad
    - $a + c \equiv b + d\ (mod\ m)$,
    - $a - c \equiv b - d\ (mod\ m)$,
    - $ac \equiv bd\ (mod\ m)$.
5. Visiem veseliem a izpildās kongruence $a \equiv a\ (mod\ m)$ (refleksivitāte).
6. Ja $a \equiv b\ (mod\ m)$, tad $b \equiv a\ (mod\ m)$ (simetrija).
7. Ja $a \equiv b\ (mod\ m)$ un $b \equiv c\ (mod\ m)$, tad $a \equiv c\ (mod\ m)$ (transitivitāte).

Uzdevumos par veselu skaitļu pakāpēm ar mainīgu vai lielu kāpinātāju var noderēt nākamā teorēma.

Teorēma. Virkne $x_n = a^n$ pēc moduļa m ir periodiska.

Perioda garumu un tajā ietilpstošos skaitļus var atrast, rakstot pēc kārtas skaitļus a^n pēc moduļa m. Tiklīdz virknē $a^n\ (mod\ m)$ parādās kāds jau bijis skaitlis, ir atrasts periods. Perioda garums nepārsniedz m.

Tā kā kongruence pēc moduļa m sadala visus veselos skaitļus m klasēs, kur katrā klasē ietilpst skaitļi, kas dod vienādus atlikumus pēc moduļa m (skat., piemēram, 1. att., kur $m = 3$ un vienā krāsā ir nokrāsoti skaitļi, kas ir vienā klasē), tad īpašību, kas jāpierāda visiem veseliem skaitļiem, pietiek pierādīt katras klases skaitļiem atsevišķi.

Uzdevumu piemēri

1. Kādu atlikumu var iegūt, vesela skaitļa kvadrātu dalot ar 3?

Atrisinājums. Ievērojam, ka veselu skaitli n, dalot ar 3, var iegūt atlikumu 0, 1 vai 2:

- ja $n \equiv 0 \ (mod\ 3)$, tad $n^2 \equiv 0^2 \equiv 0 \ (mod\ 3)$;
- ja $n \equiv 1 \ (mod\ 3)$, tad $n^2 \equiv 1^2 \equiv 1 \ (mod\ 3)$;
- ja $n \equiv 2 \ (mod\ 3)$, tad $n^2 \equiv 2^2 \equiv 4 \equiv 1 \ (mod\ 3)$.

Tātad vesela skaitļa kvadrātu, dalot ar 3, var iegūt atlikumu 0 vai 1.

Piezīmes

1. Uzdevumu varēja atrisināt arī aplūkojot gadījumus $n = 3k$, $n = 3k + 1$ un $n = 3k + 2$, kur k – vesels skaitlis.
2. Aplūkotajā risinājumā pēdējos divus gadījumus varēja apvienot, ievērojot, ka $2 \equiv -1 \ (mod\ 3)$, tas ir, ja $n \equiv \pm 1 \ (mod\ 3)$, tad $n^2 \equiv (\pm 1)^2 \equiv 1 \ (mod\ 3)$.

2. Kādu atlikumu dod skaitlis 3^{50}, dalot to ar 7?

Atrisinājums. Virkne 3^n, $n = 0, 1, 2, \ldots$, ir periodiska pēc moduļa 7, apskatīsim šīs virknes pirmos locekļus:

- ja $n = 0$, tad $3^0 \equiv \mathbf{1} \ (mod\ 7)$;
- ja $n = 1$, tad $3^1 \equiv 3 \ (mod\ 7)$;
- ja $n = 2$, tad $3^2 \equiv 9 \equiv 2 \ (mod\ 7)$;
- ja $n = 3$, tad $3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \ (mod\ 7)$;
- ja $n = 4$, tad $3^4 \equiv 3^3 \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv 4 \ (mod\ 7)$;
- ja $n = 5$, tad $3^5 \equiv 3^4 \cdot 3 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \ (mod\ 7)$;
- ja $n = 6$, tad $3^6 \equiv 3^5 \cdot 3 \equiv 5 \cdot 3 \equiv 15 \equiv \mathbf{1} \ (mod\ 7)$;
- ja $n = 7$, tad $3^7 \equiv 3^6 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \ (mod\ 7)$;
- ...

Šo informāciju ērti apkopot tabulā:

n	0	1	2	3	4	5	6	7	...
$3^n (mod\ 7)$	**1**	3	2	6	4	5	**1**	3	...

Redzam, ka virkne $3^n (mod\ 7)$ ir periodiska ar perioda garumu 6.

Tā kā $3^6 \equiv 1 \ (mod\ 7)$, tad secinām, ka

$$3^{50} \equiv 3^{6 \cdot 8 + 2} \equiv 3^2 \equiv 2 \ (mod\ 7).$$

Tātad skaitlis 3^{50} dod atlikumu 2, dalot ar 7.

3. Trīs veselu skaitļu kvadrātu summa dalās ar 9. Pierādiet, ka var izvēlēties divus no šiem kvadrātiem tā, ka to starpība dalās ar 9.

Atrisinājums. Vispirms noskaidrosim, ar ko var būt kongruenti veselu skaitļu kvadrāti pēc moduļa 9:

- ja $n \equiv 0 \ (mod\ 9)$, tad $n^2 \equiv 0^2 \equiv 0 \ (mod\ 9)$;
- ja $n \equiv 1 \ (mod\ 9)$, tad $n^2 \equiv 1^2 \equiv 1 \ (mod\ 9)$;
- ja $n \equiv 2 \ (mod\ 9)$, tad $n^2 \equiv 2^2 \equiv 4 \ (mod\ 9)$;
- ja $n \equiv 3 \ (mod\ 9)$, tad $n^2 \equiv 3^2 \equiv 9 \equiv 0 \ (mod\ 9)$;
- ja $n \equiv 4 \ (mod\ 9)$, tad $n^2 \equiv 4^2 \equiv 16 \equiv 7 \ (mod\ 9)$;
- ja $n \equiv 5 \equiv -4 \ (mod\ 9)$, tad $n^2 \equiv (-4)^2 \equiv 4^2 \equiv 7 \ (mod\ 9)$;
- ja $n \equiv 6 \equiv -3 \ (mod\ 9)$, tad $n^2 \equiv (-3)^2 \equiv 3^2 \equiv 0 (mod\ 9)$;
- ja $n \equiv 7 \equiv -2 \ (mod\ 9)$, tad $n^2 \equiv (-2)^2 \equiv 2^2 \equiv 4 \ (mod\ 9)$;
- ja $n \equiv 8 \equiv -1 \ (mod\ 9)$, tad $n^2 \equiv (-1)^2 \equiv 1^2 \equiv 1 \ (mod\ 9)$.

Šo informāciju ērti apkopot tabulā:

$n\ (mod\ 9)$	0	1	2	3	4	5	6	7	8
$n^2\ (mod\ 9)$	0	1	4	0	7	7	0	4	1

Tātad veselu skaitļu kvadrāti pēc moduļa 9 var būt kongruenti ar 0, 1, 4 vai 7. Pārbaudām, ka trīs dažādi atlikumi nevar dot summā skaitli, kas dalās ar 9:

- $0 + 1 + 4 \equiv 5\ \not\equiv 0\ (mod\ 9)$;
- $0 + 1 + 7 \equiv 8\ \not\equiv 0\ (mod\ 9)$;
- $0 + 4 + 7 \equiv 2\ \not\equiv 0\ (mod\ 9)$;
- $1 + 4 + 7 \equiv 3\ \not\equiv 0\ (mod\ 9)$.

Tātad vismaz divi no atlikumiem ir vienādi, bet tas nozīmē, ka šo kvadrātu starpība dalās ar 9.

4. Vai var atrast tādus divus veselus skaitļus, kuru kubu summa, dalot ar 7, dod atlikumu 3?

Atrisinājums. Vispirms noskaidrosim, ar ko var būt kongruenti veselu skaitļu kubi pēc moduļa 7:

- ja $n \equiv 0\ (mod\ 7)$, tad $n^3 \equiv 0^3 \equiv 0\ (mod\ 7)$;
- ja $n \equiv 1\ (mod\ 7)$, tad $n^3 \equiv 1^3 \equiv 1\ (mod\ 7)$;
- ja $n \equiv 2\ (mod\ 7)$, tad $n^3 \equiv 2^3 \equiv 8 \equiv 1\ (mod\ 7)$;
- ja $n \equiv 3\ (mod\ 7)$, tad $n^3 \equiv 3^3 \equiv 27 \equiv 6 \equiv -1\ (mod\ 7)$;
- ja $n \equiv 4 \equiv -3\ (mod\ 7)$, tad $n^3 \equiv (-3)^3 \equiv -3^3 \equiv -(-1) \equiv 1\ (mod\ 7)$;
- ja $n \equiv 5 \equiv -2\ (mod\ 7)$, tad $n^3 \equiv (-2)^3 \equiv -2^3 \equiv -1\ (mod\ 7)$;
- ja $n \equiv 6 \equiv -1\ (mod\ 7)$, tad $n^3 \equiv (-1)^3 \equiv -1\ (mod\ 7)$.

Tātad veselu skaitļu kubi ir kongruenti ar 0 vai ± 1 pēc moduļa 7. Aplūkosim, ar ko var būt kongruenta divu veselu skaitļu kubu summa pēc moduļa 7.

$a^3\ (mod\ 7)$ \ $b^3\ (mod\ 7)$	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

Esam ieguvuši, ka divu šādu skaitļu summa pēc moduļa 7 var pieņemt jebkuru no vērtībām -2, -1, 0, 1, 2, taču nekādas citas. Tā kā $3 \equiv -4\ (mod\ 7)$ neparādās starp šīm vērtībām, tad divu veselu skaitļu kubu summa nevar dot atlikumu 3, dalot ar 7.

Piezīme. Tabulā -1 vietā varēja aplūkot tam pēc moduļa 7 kongruentu skaitli 6.

5. Pierādīt: ja trīs veselu skaitļu kubu summa dalās ar 9, tad šo skaitļu reizinājums dalās ar 3.

Atrisinājums. Vispirms noskaidrosim, ar ko var būt kongruenti veselu skaitļu kubi pēc moduļa 9:

$n\ (mod\ 9)$	0	1	2	3	4	5	6	7	8
$n^3 (mod\ 9)$	0	1	-1	0	1	-1	0	1	-1

Pieņemsim pretējo, ka doto trīs skaitļu reizinājums nedalās ar 3; tad arī neviens no šiem skaitļiem nedalās ar 3, līdz ar to katra skaitļa kubs ir kongruents ar 1 vai -1 pēc moduļa 9. Secinām, ka visu doto skaitļu kubu summa pēc moduļa 9 ir pierakstāma formā $\pm 1 \pm 1 \pm 1$.

Ievērosim, ka tas ir nepāra skaitlis, kas pēc absolūtās vērtības nepārsniedz 3, tātad nevar būt kongruents ar 0 pēc moduļa 9. Taču tā ir pretruna ar to, ka doto skaitļu kubu summa dalās ar 9. Līdz ar to pieņēmums bijis aplams un doto skaitļu reizinājums dalās ar 3.

6. Pierādīt apgalvojumu: ja $p > 3$ ir pirmskaitlis, tad skaitlis p^2, dalot 24, dod atlikumu 1.

Atrisinājums. Ievērosim, ka $24 = 8 \cdot 3$. Tā kā 8 un 3 ir savstarpēji pirmskaitļi, tad pietiekami parādīt, ka visiem pirmskaitļiem $p \geq 5$ izpildās kongruences

$$p^2 \equiv 1\ (mod\ 8) \text{ un } p^2 \equiv 1\ (mod\ 3),$$

jo tas nozīmēs, ka $p^2 - 1$ dalās gan ar 8, gan ar 3, tātad $p^2 - 1$ dalās ar $8 \cdot 3 = 24$.

1) Pamatosim, ka $p^2 \equiv 1\ (mod\ 8)$. Tā kā visi pirmskaitļi $p \geq 5$ ir nepāra skaitļi, tad pēc moduļa 8 šāds skaitlis p var pieņemt tikai vērtības 1, 3, 5 vai 7 (var arī teikt, ka p pēc moduļa 8 var pieņemt tikai vērtības ± 1 vai ± 3). Pārbaudām, ka visu šo vērtību kvadrāti ir kongruenti ar 1 pēc moduļa 8:

$p\ (mod\ 8)$	1	3	5	7
$p^2 (mod\ 8)$	1	$9 \equiv 1$	$25 \equiv 1$	$49 \equiv 1$

Redzam, ka šādiem pirmskaitļiem p izpildās $p^2 \equiv 1\ (mod\ 8)$, t.i., $p^2 - 1$ dalās ar 8.

2) Pamatosim, ka $p^2 \equiv 1\ (mod\ 3)$. Neviens pirmskaitlis $p \geq 5$ nedalās ar 3. Tātad pēc moduļa 3 šāds pirmskaitlis p var pieņemt tikai vērtības 1, 2 (jeb tikai vērtības ± 1). Pārbaudām, ka šo vērtību kvadrāti ir kongruenti ar 1 pēc moduļa 3:

$p\ (mod\ 3)$	1	2
$p^2 (mod\ 3)$	1	$4 \equiv 1$

Secinām, ka visiem pirmskaitļiem $p > 3$ skaitlis $p^2 - 1$ dalās gan ar 8, gan ar 3, tātad $p^2 - 1$ dalās 24, kas nozīmē, ka p^2, dalot ar 24, dod atlikumu 1.

Piezīmes

1. Pēc moduļa 8 varēja aplūkot arī vērtības ± 1 un ± 3, bet pēc moduļa 3 – vērtības ± 1 un ņemt vērā, ka $(\pm a^2) \equiv a^2\ (mod\ n)$.
2. Ievērojot, ka p ir nepāra skaitlis un $p^2 - 1 = (p-1)(p+1)$ ir divu viens otram sekojošu pāra skaitļu reizinājums (no kuriem viens noteikti dalās ar 2, bet otrs – ar 4), var secināt, ka $p^2 - 1$ dalās ar 8.

7. Atrast skaitļu $3^3 - 3$, $5^5 - 5$, $7^7 - 7$, ..., $2015^{2015} - 2015$ lielāko kopīgo dalītāju!

Atrisinājums. Ievērosim, ka $3^3 - 3 = 24$, tātad meklētais lielākais kopīgais dalītājs d nevar būt lielāks kā 24. Pamatosim, ka visi skaitļi dalās ar 24, līdz ar to būs pierādīts, ka $d = 24$. Ievērosim, ka $24 = 8 \cdot 3$. Tā kā 8 un 3 ir savstarpēji pirmskaitļi, tad pietiekami parādīt, ka katrs no dotajiem skaitļiem dalās gan ar 3, gan ar 8.

Ievērosim, ka visi apskatāmie skaitļi ir formā $n^n - n = n\,(n^{n-1} - 1)$, turklāt n ir nepāra skaitlis, tas ir, $n = 2k + 1$.

1) Pamatosim, ka visi skaitļi dalās ar 3.
   - Ja n dalās ar 3, tad arī reizinājums $n\,(n^{n-1} - 1)$ dalās ar 3.
   - Ja n nedalās ar 3, tad $n \equiv \pm 1\ (mod\ 3)$, līdz ar to $n^{n-1} - 1 \equiv (\pm 1)^{2k} - 1 \equiv 0\ (mod\ 3)$; taču tad reizinājums $n\,(n^{n-1} - 1)$ dalās ar 3.
2) Pamatosim, ka visi skaitļi dalās ar 8. Tā kā n ir nepāra skaitlis, tad n pēc moduļa 8 pieņem vērtības 1, 3, 5, 7. Ērti ir izmantot faktu $5 \equiv -3\ (mod\ 8)$ un $7 \equiv -1\ (mod\ 8)$, kas nozīmē, ka $n \equiv \pm 1\ (mod\ 8)$ vai arī $n \equiv \pm 3\ (mod\ 8)$.

   Ievērosim, ka $(\pm 1)^2 \equiv 1\ (mod\ 8)$ un $(\pm 3)^2 \equiv 9 \equiv 1\ (mod\ 8)$. Tātad $n^2 \equiv 1\ (mod\ 8)$ un
   $$n^{n-1} - 1 \equiv (n^2)^k - 1 \equiv 1^k - 1 \equiv 0\ (mod\ 8).$$
   Taču tas nozīmē, ka skaitlis $n^{n-1} - 1$ un arī reizinājums $n\,(n^{n-1} - 1)$ dalās ar 8.

Esam pierādījuši, ka nepāra skaitļiem n skaitlis $n^n - n = n\,(n^{n-1} - 1)$ dalās gan ar 3, gan ar 8, tātad doto skaitļu lielākais kopīgais dalītājs ir 24.