Kongruences

Matemātikā bieži ir jāpierāda īpašības, kas ir spēkā bezgalīgi daudziem skaitļiem. Šādā gadījumā nevar prasīto pierādīt tikai dažiem skaitļiem un secināt, ka tas izpildīsies visiem pārējiem skaitļiem. Izdevīgi ir skaitļus apvienot grupās un pierādīt īpašību visiem vienas grupas skaitļiem, ērtam pierakstam skaitļu grupēšanai izmanto kongruences jēdzienu. Kongruence pēc moduļa m sadala visus veselos skaitļus m klasēs, kur katrā klasē ietilpst skaitļi, kas dod vienādus atlikumus pēc moduļa m.

Skaitļu dalāmība

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

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.

Kongruences jēdziens

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, var iegūt atlikumu $0, 1, 2, \ldots, b-1$.

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
- $71 \equiv 8 \ (mod\ 9)$, 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

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).

Piemērs. 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 var risināt aplūkojot gadījumus $n = 3k$; $n = 3k + 1$; $n = 3k + 2$, 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 $n^2 \equiv (\pm 1)^2 \equiv 1 \ (mod\ 3)$.

Pretrunas modulis

Viena metode, kā pierādīt, ka uzdevumā prasītais nav iespējams, ir iegūt pretrunu.

Ja jārisina algebrisks vienādojums ar veseliem koeficientiem, kuram atrisinājums jāmeklē veselo vai naturālo skaitļu kopā, tad bieži izmanto šādu ideju:

ja var pierādīt, ka vienādojuma abas puses, dalot ar kādu šim vienādojumam īpaši izvēlētu skaitli, noteikti dod dažādus atlikumus, tad vienādojumam nav atrisinājuma.

Ievēro! Ja vienādojuma abas puses dalās ar kādu skaitli, tad no tā nevar secināt, ka vienādojumam ir atrisinājums veselos skaitļos.

Piemērs. Pierādīt, ka vienādojumam $x^2 + y^2 = 2015$ nav atrisinājuma naturālos skaitļos!
Atrisinājums. Naturāla skaitļa kvadrāts, dalot ar 4, var dot tikai atlikumu 0 vai 1. Tāpēc $x^2 + y^2$, dalot ar 4, var dot tikai atlikumu $0 + 0$, $0 + 1$, $1 + 0$ vai $1 + 1$, tas ir, atlikumu 0, 1 vai 2. Taču skaitlis 2015 dod atlikumu 3, dalot ar 4. Tāpēc dotajam vienādojumam nav atrisinājuma naturālos skaitļos.

Uzdevumi no matemātikas sacensībām

1. 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.

2. 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.

3. Pitagora trijstūrī visu malu garumi ir lielāki nekā 5. Vai var gadīties, ka tā **a)** trīs malu, **b)** divu malu garumi ir pirmskaitļi? *Piezīme.* Pitagora trijstūris ir taisnleņķa trijstūris, kam visi malu garumi ir naturāli skaitļi.

Atrisinājums

a) Nē, trīs malu garumi nevar būt pirmskaitļi. Taisnleņķa trijstūrī malu garumus a, b un c saista Pitagora teorēma $a^2 + b^2 = c^2$. Tā kā visu malu garumiem jābūt pirmskaitļiem, kas lielāki nekā 5, tad visu malu garumi ir nepāra skaitļi, tātad arī a^2 un b^2 ir nepāra skaitļi, bet divu nepāra skaitļu summa ir pāra skaitlis – pretruna ar to, ka c^2 ir nepāra skaitlis.

Piezīme. Principā risinājumā tika izmantota kongruence pēc moduļa 2.

b) Jā, divu malu garumi var būt pirmskaitļi. Piemēram, der malu garumi 11, 60, 61, jo divi no tiem ir pirmskaitļi un tiem izpildās Pitagora teorēmas nosacījums, tas ir, $11^2 + 60^2 = 61^2$ jeb $121 + 3600 = 3721$.

4. Atrast visus tādus pirmskaitļus p, ka $3^{p^2-1}+20$ arī ir pirmskaitlis!

Atrisinājums

Ja $p=2$, tad skaitlis $3^3+20=47$ ir pirmskaitlis.

Ja $p=3$, tad skaitlis $3^8+20=6581$ arī ir pirmskaitlis (noteikt, vai šis skaitlis ir pirmskaitlis, var pārbaudot dalāmību ar visiem pirmskaitļiem līdz $\sqrt{6581}<82$).

Pieņemsim, ka $p\geq 5$. Tad $p\equiv \pm 1\ (mod\ 3)$ un $p^2-1\equiv(\pm 1)^2-1\equiv 0\ (mod\ 3)$.

Turklāt p ir nepāra, tātad p^2-1 ir pāra, kas dalās ar 3. Secinām, ka $p^2-1=6m$ kādam naturālam m.

Taču $3^6\equiv(3^2)^3\equiv 9^3\equiv 2^3\equiv 8\equiv 1\ (\mathrm{mod}\ 7)$, līdz ar to

$$3^{p^2-1}+20\equiv 3^{6m}+20\equiv(3^6)^m+6\equiv 1^m+6\equiv 0\ (\mathrm{mod}\ 7).$$

un $3^{p^2-1}+20$ dalās ar 7, tātad nevar būt pirmskaitlis (jo acīmredzami $3^{p^2-1}+20>7$). Secinām, ka vienīgās derīgās p vērtības ir $p=2$ un $p=3$.

Literatūra

- A. Andžāns "Algebra 10.-12. klasei Profilkursam", II daļa – Rīga, 1998.
- A. Bērziņa, A. Bērziņš "Diferencēti uzdevumi skaitļu teorijā". Grāmata pieejama arī elektroniski: http://nms.lu.lv/wp-content/uploads/2014/06/BerzinsBerzina_DiferencetiUzdSkT.pdf
- Atklātās matemātikas olimpiādes (2015./2016. m.g.) tēma "Vienādojumi veselos skaitļos" http://nms.lu.lv/wp-content/uploads/2016/03/teorija_AMO_1516.pdf
- Mazās matemātikas universitātes nodarbība "Kongruences" http://nms.lu.lv/wp-content/uploads/2015/12/MMU-2015_2_kongruences.pdf
- Mazās matemātikas universitātes nodarbība "Kongruences un to lietojumi" http://nms.lu.lv/wp-content/uploads/2013/02/MMU6_kongruences.pdf
- Novada matemātikas olimpiādes (2015./2016. m.g.) tēma "Dalāmība un kongruences" http://nms.lu.lv/wp-content/uploads/2016/08/teorija_Skaitludalamiba_Kongruences.pdf