KONGRUENCES

Teorija un piemēri 10.-12. klasei, gatavojoties Atklātajai matemātikas olimpiādei 2022./2023. m. g.

Iesakām izlasīt arī teorijas materiālu par dalāmību, kas domāts 5.-9. klašu skolēniem.

Kongruences jēdziens

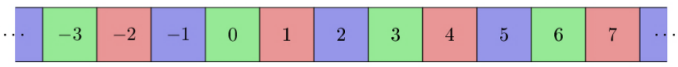
Viens no pazīstamākajiem veselo skaitļu iedalījumiem ir to dalījums pāra un nepāra skaitļos. Katrs vesels skaitlis ir vai nu pāra, vai nepāra, taču neviens nav vienlaikus gan pāra, gan nepāra skaitlis. Tā visi veselie skaitļi tiek sadalīti divās klasēs: skaitļi, kas dalās ar 2 (pāra skaitļi), un skaitļi, 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, atlikumam var būt vērtības $0, 1, 2, \dots, b-1$.

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 $a \equiv b \pmod{m}$ vai $a \equiv_m b$, ja a un b, dalot tos ar m, dod vienādu atlikumu.

Piemēri

- $7 \equiv 3 \pmod{2}$, jo gan 7, gan 3, dalot ar 2, dod atlikumu 1
- $17 \equiv 73 \pmod{14}$, jo gan 17, gan 73, dalot ar 14, dod atlikumu 3
- $71 \equiv 8 \pmod{9}$, jo gan 71, gan 8, dalot ar 9, dod atlikumu 8
- $-2 \equiv 4 \pmod{3}$, jo gan -2, gan 4, dalot ar 3, dod atlikumu 1
- $-6 \equiv 85 \pmod{7}$, 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. $a \equiv b \pmod{m}$ tad un tikai tad, ja starpība $a - b$ dalās ar m.

Piemēri

- $7 \equiv 3 \pmod{2}$, jo starpība $7 - 3 = 4$ dalās ar 2
- $17 \equiv 73 \pmod{14}$, jo starpība $17 - 73 = -56$ dalās ar 14
- $71 \equiv 8 \pmod{9}$, jo starpība $71 - 8 = 63$ dalās ar 9
- $-2 \equiv 4 \pmod{3}$, jo starpība $-2 - 4 = -6$ dalās ar 3
- $-6 \equiv 85 \pmod{7}$, 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 $a \equiv r \pmod{m}$.
2. Ja $a \equiv b \pmod{m}$, tad $ka \equiv kb \pmod{m}$, kur k ir jebkurš vesels skaitlis.
3. Ja $a \equiv b \pmod{m}$, tad $a^n \equiv b^n \pmod{m}$, kur n ir jebkurš naturāls skaitlis.
4. Ja $a \equiv b \pmod{m}$ un $c \equiv d \pmod{m}$, tad
   - $a + c \equiv b + d \pmod{m}$,
   - $a - c \equiv b - d \pmod{m}$,
   - $ac \equiv bd \pmod{m}$.
5. Visiem veseliem a izpildās kongruence $a \equiv a \pmod{m}$ (refleksivitāte).
6. Ja $a \equiv b \pmod{m}$, tad $b \equiv a \pmod{m}$ (simetrija).
7. Ja $a \equiv b \pmod{m}$ un $b \equiv c \pmod{m}$, tad $a \equiv c \pmod{m}$ (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 $a^n \pmod{m}$ 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 $n \equiv 0 \pmod{3}$, tad $n^2 \equiv 0^2 \equiv 0 \pmod{3}$;
- ja $n \equiv 1 \pmod{3}$, tad $n^2 \equiv 1^2 \equiv 1 \pmod{3}$;
- ja $n \equiv 2 \pmod{3}$, tad $n^2 \equiv 2^2 \equiv 4 \equiv 1 \pmod{3}$.

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 $2 \equiv -1 \pmod{3}$, tas ir, ja $n \equiv \pm 1 \pmod{3}$, tad $n^2 \equiv (\pm 1)^2 \equiv 1 \pmod{3}$.

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

Šo informāciju ērti apkopot tabulā:

n	0	1	2	3	4	5	6	7	...
$3^n \pmod 7$	**1**	3	2	6	4	5	**1**	3	...

Redzam, ka virkne $3^n \pmod 7$ ir periodiska ar perioda garumu 6. Tā kā $3^6 \equiv 1 \pmod 7$, tad secinām, ka $3^{50} \equiv 3^{6\cdot 8+2} \equiv 3^2 \equiv 2 \pmod 7$. 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 $n \equiv 0 \pmod 9$, tad $n^2 \equiv 0^2 \equiv 0 \pmod 9$;
- ja $n \equiv 1 \pmod 9$, tad $n^2 \equiv 1^2 \equiv 1 \pmod 9$;
- ja $n \equiv 2 \pmod 9$, tad $n^2 \equiv 2^2 \equiv 4 \pmod 9$;
- ja $n \equiv 3 \pmod 9$, tad $n^2 \equiv 3^2 \equiv 9 \equiv 0 \pmod 9$;
- ja $n \equiv 4 \pmod 9$, tad $n^2 \equiv 4^2 \equiv 16 \equiv 7 \pmod 9$;
- ja $n \equiv 5 \equiv -4 \pmod 9$, tad $n^2 \equiv (-4)^2 \equiv 4^2 \equiv 7 \pmod 9$;
- ja $n \equiv 6 \equiv -3 \pmod 9$, tad $n^2 \equiv (-3)^2 \equiv 3^2 \equiv 0 \pmod 9$;
- ja $n \equiv 7 \equiv -2 \pmod 9$, tad $n^2 \equiv (-2)^2 \equiv 2^2 \equiv 4 \pmod 9$;
- ja $n \equiv 8 \equiv -1 \pmod 9$, tad $n^2 \equiv (-1)^2 \equiv 1^2 \equiv 1 \pmod 9$.

Šo informāciju ērti apkopot tabulā:

$n \pmod 9$	0	1	2	3	4	5	6	7	8
$n^2 \pmod 9$	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:

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

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

- ja $n \equiv 6 \equiv -1 \pmod 7$, tad $n^3 \equiv (-1)^3 \equiv -1 \pmod 7$.

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.

$a^3 \pmod 7$ / $b^3 \pmod 7$	-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 $3 \equiv -4 \pmod 7$ 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:

$n \pmod 9$	0	1	2	3	4	5	6	7	8
$n^3 \pmod 9$	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

$$p^2 \equiv 1 \pmod 8 \text{ un } p^2 \equiv 1 \pmod 3,$$

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 $p^2 \equiv 1 \pmod 8$. 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:

$p \pmod 8$	1	3	5	7
$p^2 \pmod 8$	1	$9 \equiv 1$	$25 \equiv 1$	$49 \equiv 1$

Redzam, ka šādiem pirmskaitļiem p izpildās $p^2 \equiv 1 \pmod 8$, tas ir, $p^2 - 1$ dalās ar 8.

2) Pamatosim, ka $p^2 \equiv 1 \pmod 3$. 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:

$p \pmod 3$	1	2
$p^2 \pmod 3$	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 $(\pm a^2) \equiv a^2 \pmod n$.
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 $3^3-3, 5^5-5, 7^7-7, \ldots, 2015^{2015}-2015$ 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 $n\equiv \pm 1 \pmod 3$, līdz ar to $n^{n-1}-1\equiv (\pm 1)^{2k}-1\equiv 0 \pmod 3$; 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 $5\equiv -3 \pmod 8$ un $7\equiv -1 \pmod 8$, kas nozīmē, ka $n\equiv \pm 1 \pmod 8$ vai arī $n\equiv \pm 3 \pmod 8$.

   Ievērosim, ka $(\pm 1)^2 \equiv 1 \pmod 8$ un $(\pm 3)^2 \equiv 9\equiv 1 \pmod 8$. Tātad $n^2\equiv 1 \pmod 8$ un
$$n^{n-1}-1\equiv (n^2)^k-1\equiv 1^k-1\equiv 0 \pmod 8.$$
   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.

Citi avoti

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 NMS mājas lapā sadaļā Arhīvs.

Uzdevumi

1. Pierādīt, ka

a) no pieciem naturāliem skaitļiem vienmēr var izvēlēties vairākus (vismaz divus), kuru summa dalās ar 4;

b) var atrast četrus tādus naturālus skaitļus, ka no tiem nevar izvēlēties vairākus (vismaz divus), kuru summa dalās ar 4.

2. Pierādīt, ka no jebkuriem trim naturālu skaitļu kvadrātiem var izvēlēties divus tā, ka to summa vai starpība dalās ar 5.

3. Pierādīt, ka starp jebkuriem pieciem naturālu skaitļu kvadrātiem var atrast divus tādus, ka to summa vai starpība dalās ar 13.

4. Atrast visu skaitļu, kas pierakstāmi formā a^4-b^4, kur $a>b>5$ un a un b ir pirmskaitļi, lielāko kopīgo dalītāju!

Uzdevumu atrisinājumi doti nākamajā lapā.

Uzdevumu atrisinājumi

1. Pierādīt, ka

a) no pieciem naturāliem skaitļiem vienmēr var izvēlēties vairākus (vismaz divus), kuru summa dalās ar 4;

b) var atrast četrus tādus naturālus skaitļus, ka no tiem nevar izvēlēties vairākus (vismaz divus), kuru summa dalās ar 4.

Atrisinājums. a) Naturāls skaitlis, dalot ar 4, dod atlikumu 0, 1, 2 vai 3, pāra skaitļi dod atlikumu 0 vai 2, nepāra – atlikumu 1 vai 3.

1. Ja starp dotajiem pieciem skaitļiem ir divi, kas, dalot ar 4, abi dod atlikumu 0 vai abi dod atlikumu 2, tad šo divu skaitļu summa dalās ar 4, jo $0+0 \equiv 0 \pmod 4$ vai $2+2 \equiv 4 \equiv 0 \pmod 4$, tad varam ņemt šos. Pretējā gadījumā ir ne vairāk kā divi pāra skaitļi, tātad ir vismaz trīs nepāra skaitļi.
2. Ja starp nepāra skaitļiem ir gan tāds, kas, dalot ar 4, dod atlikumu 1, gan tāds, kas dod atlikumu 3, tad šo abu summa dalās ar 4 un mēs varam ņemt šos. Pretējā gadījumā mums visi nepāra skaitļi dod vienu un to pašu atlikumu (1 vai 3), dalot ar 4.
3. Ja kāds no skaitļiem, dalot ar 4, dod atlikumu 2, tad tas summā ar diviem nepāra skaitļiem (kuri abi dod atlikumu 1 vai 3, dalot ar 4) dalās ar 4, jo $2+1+1 \equiv 4 \equiv 0 (\mathrm{mod}\ 4)$ vai $2+3+3 \equiv 8 \equiv 0 (\mathrm{mod}\ 4)$, tad varam ņemt šos trīs skaitļus. Pretējā gadījumā ir ne vairāk kā viens pāra skaitlis (kurš dod atlikumu 0, dalot ar 4).
4. Ja ir ne vairāk kā viens pāra skaitlis, tad ir vismaz četri nepāra skaitļi, kas visi dod vienādus atlikumus, dalot ar 4, tad to summa dalās 4.

b) Līdzīgi kā a) gadījumā varam secināt, ka neder divi pāra skaitļi, kas dod vienādus atlikumus, dalot ar 4, divi nepāra skaitļi, kas dod dažādus atlikumus, dalot ar 4, un neder arī viens pāra skaitlis, kas dod atlikumu 2, dalot ar 4. Tādējādi nonākam pie atlikumiem 0, 1, 1, 1 vai 0, 3, 3, 3, kas abi der.

Ņemsim jebkurus skaitļus, kas, dalot ar 4, dod attiecīgi atlikumus 0, 1, 1, 1. Tad vairāku no tiem atlikumu summa būs vismaz 1, bet ne lielāka kā 3 (ja mēs sasummējam visus), tātad tā var pieņemt tikai vērtības 1, 2 vai 3. Līdz ar to nekādu vairāku no tiem summa nedalīsies ar 4. Šādi skaitļi ir, piemēram, 4, 1, 5, 9 (to, ka tie der, var pārbaudīt arī, aprēķinot visas 11 iespējamās vairāku no tiem summas).

2. Pierādīt, ka no jebkuriem trim naturālu skaitļu kvadrātiem var izvēlēties divus tā, ka to summa vai starpība dalās ar 5.

Atrisinājums. Vispirms noskaidrosim, ar ko var būt kongruents naturāla skaitļa kvadrāts pēc moduļa 5.

$n \pmod 5$	0	1	2	3	4
$n^2 \pmod 5$	0	1	4	4	1

Tātad naturāla skaitļa kvadrāts pēc moduļa 5 var būt kongruents ar 0, 1 vai 4. iespējami divi gadījumi.

- Ja divi kvadrāti dod vienādu atlikumu, dalot ar 5, tad to starpība dalās ar 5.
- Ja nekādi divi no šiem trim kvadrātiem nav kongruenti pēc moduļa 5, tad tie pēc moduļa 5 pieņem visas iespējamās vērtības 0, 1 un 4. Tā kā $1+4=5$, tad atbilstošo kvadrātu summa dalīsies ar 5.

3. Pierādīt, ka starp jebkuriem pieciem naturālu skaitļu kvadrātiem var atrast divus tādus, ka to summa vai starpība dalās ar 13.

Atrisinājums. Vispirms noskaidrosim, ar ko var būt kongruents naturāla skaitļa kvadrāts pēc moduļa 13.

$n \pmod{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12
$n^2 \pmod{13}$	0	1	4	9	3	12	10	10	12	3	9	4	1

Tātad naturāla skaitļa kvadrāts pēc moduļa 13 var būt kongruents ar 0, 1, 3, 4, 9, 10 vai 12. Iespējami divi gadījumi.

- Ja divi kvadrāti dod vienādu atlikumu, dalot ar 13, tad to starpība dalās ar 13.
- Ja nekādi divi no šiem pieciem kvadrātiem nav kongruenti pēc moduļa 13, tad sadalām šo kvadrātu iespējamās vērtības pēc moduļa 13 četrās grupās: {0}, {1; 12}, {3; 10}, {4; 9}. Tā kā ir jāizvēlas pieci naturālu skaitļu kvadrāti, tad vismaz divi no tiem būs vienā grupā (Dirihlē princips). Šo divu skaitļu summa dalās ar 13.

4. Atrast visu skaitļu, kas pierakstāmi formā $a^4 - b^4$, kur $a > b > 5$ un a un b ir pirmskaitļi, lielāko kopīgo dalītāju!

Atrisinājums. Ievērojam, ka $a^4 - b^4 = (a^2 - b^2)(a^2 + b^2) = (a - b)(a + b)(a^2 + b^2)$.
Tā kā

$$11^4 - 7^4 = 4 \cdot 18 \cdot (121 + 49) = 2^4 \cdot 3^2 \cdot 5 \cdot 17 = 240 \cdot 51$$

un

$$13^4 - 11^4 = 2 \cdot 24 \cdot (169 + +121) = 2^4 \cdot 3 \cdot 5 \cdot 29 = 240 \cdot 29,$$

tad meklētais lielākais kopīgais dalītājs d nevar būt lielāks kā 240. Pamatosim, ka visi skaitļi dalās ar 240, līdz ar to būs pierādīts, ka $d = 240$. Ievērosim, ka $240 = 16 \cdot 3 \cdot 5$; tā kā visi reizinātāji ir savstarpēji pirmskaitļi, tad pietiekami parādīt, ka katrs no dotajiem skaitļiem dalās gan ar 16, gan ar 3, gan ar 5.

- Tā kā jebkurš pirmskaitlis p, kas lielāks nekā 5, ir nepāra skaitlis, tad, to dalot ar pāra skaitli, nevar iegūt atlikumu, kas ir pāra skaitlis, līdz ar to var rasties tikai nepāra atlikums: 1, 3, 5, 7, 9, 11, 13 vai 15. Tātad p var būt kongruents ar $\pm 1, \pm 3, \pm 5$ vai ± 7 pēc moduļa 16. Noskaidrosim, ar ko var būt kongruenta pirmskaitļa ceturtā pakāpe pēc moduļa 16:
  - $p^4 \equiv (\pm 1)^4 \equiv 1 \pmod{16}$;
  - $p^4 \equiv (\pm 3)^4 \equiv 81 \equiv 1 \pmod{16}$;
  - $p^4 \equiv (\pm 5)^4 \equiv 25 \cdot 25 \equiv 9 \cdot 9 \equiv 81 \equiv 1 \pmod{16}$;
  - $p^4 \equiv (\pm 7)^4 \equiv 49 \cdot 49 \equiv 1 \cdot 1 \equiv 1 \pmod{16}$.

  Tātad $p^4 \equiv 1 \pmod{16}$.
- Pirmskaitli $p > 5$, dalot ar 3, var iegūt tikai atlikumu 1 vai 2, tāpēc pēc moduļa 3 šāds pirmskaitlis p var pieņemt tikai vērtības ± 1 un $p^4 \equiv 1 \pmod{3}$.
- Pirmskaitli $p > 5$, dalot ar 5, var iegūt tikai atlikumu 1, 2, 3 vai 4, tāpēc pēc moduļa 5 šāds pirmskaitlis p var pieņemt tikai vērtības ± 1 un ± 2. Tad $p^4 \equiv (\pm 1)^4 \equiv 1 \pmod{5}$ vai $p^4 \equiv (\pm 2)^4 \equiv 16 \equiv 1 \pmod{5}$. Tātad $p^4 \equiv 1 \pmod{5}$.

Līdz ar to $p^4 \equiv 1 \pmod{240}$ un tāpēc $a^4 - b^4 \equiv 1 - 1 \equiv 0 \pmod{240}$ jeb $a^4 - b^4$ dalās ar 240. Esam pierādījuši, ka visu skaitļu, kas pierakstāmi formā $a^4 - b^4$, kur $a > b > 5$ un a un b ir pirmskaitļi, lielākais kopīgais dalītājs ir 240.

Piezīme. Pamatot to, ka $a^4 - b^4$ dalās ar 16, var, ievērojot, ka jebkuriem nepāra skaitļiem a un b to kvadrātu summa dalās ar 2, bet kvadrātu starpība dalās ar 8.