Advancēta modulārā aritmētika - atrisinājumi

1.uzdevums Dots nepāra pirmskaitlis p. Chuhan un Edgars spēlē spēli, kurā viņi pēc kārtas veic gājienus: viena gājiena laikā var izvēlēties skaitli no kopas $\{1, 2, ..., 2p-3, 2p-2\}$, kuru pirms tam nav izvēlējies neviens no spēlētājiem. Spēle beidzas, kad visi skaitļi ir izvēlēti. Pēc tam katrs spēlētājs aprēķina savu izvēlēto skaitļu reizinājumu un pieskaita tam 1. Uzvar tas spēlētājs, kura iegūtais skaitlis dalās ar p, bet tā pretinieka iegūtais skaitlis nedalās ar p. Pierādīt, ka Chuhan vienmēr var uzvarēt neatkarīgi no tā, kā spēlē Edgars, ja Chuhan veic pirmo gājienu.

Atrisinājums. Tā kā skaitļu pavisam ir $2p-2$, tad katrs spēlētājs spēles gaitā izvēlas $p-1$ skaitļus. Sadalām skaitļus pāros, kas ir kongruenti (mod p):

$$(1, p+1),\ (2, p+2),\ \ldots,\ (p-2, 2p-2).$$

Ievērojam, ka skaitļiem $p-1$ un p nav pāra.

Pāri $(i, p+i)$, no kura neviens skaitlis nav izvēlēts, saucam par *neaiztiktu*; pāri, no kura tieši viens ir izvēlēts, saucam par *aiztiktu*, bet pāri, no kura abi ir izvēlēti, saucam par *pabeigtu*.

Pamatosim, ka Chuhan var izvēlēties skaitli $p-1$ un vēl arī tieši pa vienam skaitlim no katra pāra. Turklāt pēc katra Chuhan gājiena ir ne vairāk kā viens aiztikts pāris. Aprakstīsim viņa stratēģiju:

- Pirmajā gājienā Chuhan izvēlas skaitli $p-1$. (Visi pāri ir neaiztikti, un skaitlis p ir neizvēlēts.)
- Ja Edgars izvēlas skaitli no neaiztikta pāra, tad Chuhan izvēlas otru skaitli no šī paša pāra. Līdz ar to pāris tiek pabeigts. (Aiztikto pāru skaits nemainās.)
- Ja Edgars izvēlas p, tad Chuhan aiztiek kādu jaunu pāri. (Aiztikto pāru skaits aug no 0 līdz 1.)
- Ja Edgars pabeidz kādu jau Chuhan aiztiktu pāri, tad Chuhan aiztiek jaunu pāri. (Aiztikto pāru skaits nemainās – vienu pabeidz, otrs izveidojas.)

Ievērojam, ka spēles gaitā Edgars noteikti ir izvēlējies skaitli p vai nu kaut kad spēles vidū, vai arī pašā pēdējā gājienā, kad visi citi skaitļi jau ir paņemti. Tādēļ Edgara skaitļu reizinājums P_E dalās ar p, bet $P_E + 1$ nedalās ar p.

Savukārt Chuhan ir izvēlējies $p-1$ un vēl pa vienam atlikumam no katras kongruenču klases no 1 līdz $p-2$. Visu Chuhan izraudzīto skaitļu reizinājums $P_C \equiv (p-1)!$ (mod p). Pēc Vilsona teorēmas $P_C + 1 \equiv (p-1)! + 1 \equiv 0$ (mod p).

2.uzdevums Atrast visus naturālu skaitļu trijniekus (a, b, c), kuriem izpildās

$$(a-b)^3(a+b)^2 = c^2 + 2(a-b) + 1.$$

Atrisinājums. Pārveidosim doto vienādojumu

$$(a-b)\left((a-b)^2(a+b)^2 - 2\right) = c^2 + 1$$

Aplūkosim visus iespējamos gadījumus

- Ja $a-b$ ir pāra skaitlis, tad $(a-b)^2(a+b)^2 - 2$ arī ir pāra skaitlis, kas nozīmē, ka vienādojuma kreisā puse dalās ar 4. Taču tādā gadījumā arī vienādojuma labajai pusei ir jādalās ar 4. Tās nozīmē, ka $c^2 \equiv 3 \pmod 4$, kas nav iespējams, jo veselu skaitļu kvadrāti dod tikai atlikumus 0 vai 1, dalot ar 4.

- Ja $a-b$ ir nepāra skaitlis, tad $a+b = (a-b) + 2b$ arī ir nepāra skaitlis. Nepāra skaitļu kvadrāti ir $1 \pmod 4$, līdz ar to varam iegūt, ka

  $$(a-b)^2(a+b)^2 - 2 \equiv 1 \cdot 1 - 2 \equiv 3 \pmod 4$$

  Ja $(a-b)^2(a+b)^2 - 2 \neq \pm 1$, tad mēs varam atrast nepāra pirmreizinātāju p ar īpašību, ka $p \mid (a-b)^2(a+b)^2 - 2$ un $p \equiv 3 \pmod 4$. Ja tāds pirmskaitlis neeksistētu, tad visi skaitļa pirmreizinātāji būtu $1 \pmod 4$, kas nozīmētu, ka pats skaitlis arī ir $1 \pmod 4$ – pretruna. Bet tādā gadījumā $p \mid c^2 + 1$, kas nav iespējams pēc Fermā Ziemassvētku teorēmas.

Esam ieguvuši, ka $(a-b)(a+b)^2 - 2 = \pm 1$. Ievērosim, ka $(a-b)^2(a+b)^2 \neq 3$, līdz ar to $(a-b)^2(a+b)^2 = 1$. No šī varam iegūt atrisinājumus $(a, b) = (1, 0)$, $(0, 1)$, $(-1, 0)$ un $(0, -1)$, taču visos gadījumos kāds no skaitļiem nav naturāls. Varam secināt, ka naturālos skaitļos prasītie skaitļu trijnieki neeksistē.

3.uzdevums Dots pirmskaitlis $p \geq 2$. Kristaps un Armands spēlē spēli, kurā viņi pēc kārtas veic gājienus: viena gājiena laikā spēlētājs izvēlas indeksu i no kopas $\{0, 1, 2, \ldots, p-1\}$, kuru neviens no spēlētājiem nebija izvēlējies pirms tam, un izvēlas kādu skaitli no kopas $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, izvēlēto skaitli apzīmējot ar a_i. Kristaps veic pirmo gājienu. Spēlē beidzas, kad visi indeksi ir izvēlēti. Pēc tam tiek aprēķināts skaitlis

$$M = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_{p-1} \cdot 10^{p-1} = \sum_{i=0}^{p-1} a_i \cdot 10^i.$$

Kristapa mērķis ir panākt to, ka skaitlis M dalās ar p, bet Armanda mērķis ir panākt to, ka skaitlis M nedalās ar p. Pierādīt, ka Kristapam ir uzvaroša stratēģija.

Atrisinājums. Pamanīsim, ja $p = 2$ vai $p = 5$, tad Kristapam pietiek pirmajā gājienā izvēlēties $a_0 = 0$, ar ko viņš garantēs, ka $p \mid 10 \mid M$, kas nodrošina viņam uzvaru.

Tagad apskatīsim gadījumu, kad $p \notin \{2, 5\}$. Tādā gadījumā no Fermā teorēmas izriet, ka $10^{p-1} \equiv 1 \pmod{p}$, kas nozīmē, ka $10^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Izveidosim sekojošus skaitļu pārus:

$$\left(1, \frac{p-1}{2} + 1\right), \left(2, \frac{p-1}{2} + 2\right), ..., \left(\frac{p-1}{2}, p-1\right)$$

Pieņemsim, ka Kristaps ar pirmo gājienu izvēlas $a_0 = 0$. Aplūkosim visus iespējamos gadījumus

- $10^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Ja Armands savā gājienā izvēlas a_i, tad Kristapam jāizvēlas indekss, kas ir vienā pārī ar i (apzīmēsim to ar j), un tāds skaitlis, lai $a_i + a_j = 9$. Tādā gaidījumā spēlēs beigās sanāk, ka

$$M = \sum_{i=0}^{p-1} a_i \cdot 10^i = a_0 + \sum_{i=1}^{\frac{p-1}{2}} (a_i \cdot 10^i + a_{\frac{p-1}{2}+i} \cdot 10^{\frac{p-1}{2}+i}) \equiv \sum_{i=1}^{\frac{p-1}{2}} (a_i \cdot 10^i + (9 - a_i) \cdot 1 \cdot 10^i) =$$

$$= 9(10 + 10^2 + \cdots 10^{\frac{p-1}{2}}) = 9\left(10\left(\frac{10^{\frac{p-1}{2}} - 1}{10 - 1}\right)\right) = 10(10^{\frac{p-1}{2}} - 1) \equiv 10(1 - 1) \equiv 0 \pmod{p}$$

- $10^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Ja Armands savā gājienā izvēlas a_i, tad Kristapam jāizvēlas indekss, kas ir vienā pārī ar i (apzīmēsim to ar j), un tāds skaitlis, lai $a_i = a_j$. Tādā gaidījumā spēlēs beigās sanāk, ka

$$M = \sum_{i=0}^{p-1} a_i \cdot 10^i = a_0 + \sum_{i=1}^{\frac{p-1}{2}} (a_i \cdot 10^i + a_{\frac{p-1}{2}+i} \cdot 10^{\frac{p-1}{2}+i}) \equiv \sum_{i=1}^{\frac{p-1}{2}} (a_i \cdot 10^i + a_i \cdot (-1) \cdot 10^i) \equiv$$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}} a_i (10^i - 10^i) \equiv \sum_{i=1}^{\frac{p-1}{2}} a_i \cdot 0 \equiv 0 \pmod{p}$$

Abos gadījumos Kristaps var panākt, ka spēles beigās $M \equiv 0 \pmod{p}$, līdz ar ko Kristapam vienmēr ir uzvaroša stratēģija, kas bija jāpierāda.

4.uzdevums Doti naturāli skaitļi c un n, pie tam $n > c$. Rūdis izvēlas n naturālus skaitļus (ne obligāti dažādus). Pierādīt, ka eksistē Rūda izvēlēto skaitļu permutācija $a_1, \ldots, a_n$, kurai skaitlis

$$(a_1 - a_2) \cdot (a_2 - a_3) \cdots (a_{n-1} - a_n) \cdot (a_n - a_1)$$

dod atlikumu 0 vai c, dalot ar n.

Atrisinājums. Ievērosim, ka, ja starp dotajiem skaitļiem eksistē divi skaitļi, kuri dod vienādus atlikumus, dalot ar n, tad mēs varam izvēlēties tādu skaitļu $a_1, a_2, \ldots, a_n$ permutāciju, ka $a_1 \equiv a_n \pmod{n}$. Tādā gadījumā skaidrs, ka

$$(a_1 - a_2) \cdot (a_2 - a_3) \cdots (a_n - a_1) \equiv 0 \pmod{n}$$

Līdz ar to varam pieņemt, ka izvēlētie skaitļi dod pa pāriem dažādus atlikumus pēc moduļa n. Aplūkosim divus iespējamos gadījumus

- Skaitlis n ir vienāds ar pirmskaitli p. Izvēlēsimies tādu permutāciju, ka $a_i \equiv i \pmod{p}$ visiem $1 \leq i \leq p$. Tādā gadījumā

$$\begin{gathered}(a_1 - a_2) \cdot (a_2 - a_3) \cdots (a_{n-1} - a_n) \cdot (a_n - a_1) \equiv \\ \equiv (1-2) \cdot (2-3) \cdots ((p-1) - p) \cdot (p-1) \equiv R \pmod{p},\end{gathered}$$

  kur ir R ir kaut kāds no nulles atšķirīgs atlikums. No inverso elementu īpašībām eksistē tāds atlikums k, kam $R \cdot k \equiv c \pmod{p}$, kur $k \equiv R^{-1} \cdot c \pmod{p}$. Tādā gadījumā aizstājot $a_1, a_2, \ldots, a_p$ ar $ka_1, ka_2, \ldots ka_n$ mēs iegūsim vajadzīgo atlikumu. Taču teorijas materiālā mēs pierādījām, ka $ka_1, ka_2, \ldots, ka_n$ pēc moduļa p ir kopas $\{1, 2, \ldots, p\}$ permutācija, līdz ar to esam atraduši vajadzīgo permutāciju.

- Skaitlis n ir salikts skaitlis. Tādā gadījumā eksistē tādu naturāli skaitļi $1 < a, b < n$ ar īpašību, ka $ab = n$. Izvēlēsimies $a_1 \equiv a + 1 \pmod{n}$, $a_2 \equiv 1 \pmod{n}$ un $a_3 \equiv b + 2 \pmod{n}$ un $a_4 \equiv 2 \pmod{n}$. Tādā gadījumā $(a_1 - a_2)(a_3 - a_4) \equiv ab \equiv 0 \pmod{n}$. Tas nozīmē, ka

$$(a_1 - a_2) \cdot (a_2 - a_3) \cdots (a_n - a_1) \equiv 0 \pmod{n}$$

  Atliek pārliecināties, ka a_1, a_2, a_3, a_4 ir pa pāriem dažādi, taču tas ir acīmredzami, jo $1 < 2 < a + 1 < b + 2$, ja mēs pieņemam, ka $a \leq b$.

Visos gadījumos Rūdis var panākt vajadzīgo.

5.uzdevums Ar $\mathbb{P}$ apzīmēsim visu pirmskaitļu kopu. Kopa M sastāv no vismaz 3 dažādiem pirmskaitļiem un tai piemīt īpašība, ka ikvienai M apakškopai A, kas nav vienāda ar M, visi skaitļa

$$\Big(\prod_{p\in A} p\Big) - 1$$

pirmreizinātāji arī pieder kopai M. Pierādīt, ka $M = \mathbb{P}$. (*Ar* $\prod$ *apzīmē visu norādīto skaitļu reizinājumu.*)

Atrisinājums. Atrisinājums sastāvēs no vairākiem soļiem.

1.solis Skaitļi $2, 3, 5, 7 \in M$.
Pierādījums. Sākotnēji kopa satur 3 pirmskaitļus a, b, c. Ja kāds no tiem ir pāra, tad $2 \in M$. Pretējā gadījumā tie visi ir nepāra skaitļi, līdz ar to $ab-1$ ir pāra, kas nozīmē, ka $2 \in M$. Ja kāds no dotajiem skaitļiem dalās ar 3, tad $3 \in M$. Pretējā gadījumā skaitļi a, b, c, dod atlikumus 1 vai 2, dalot ar 3. Pēc Dirihlē principa diviem skaitļiem, teiksim a, b ir vienāds atlikums, dalot ar 3, kas nozīmē, ka $3 \mid ab-1$ jeb $3 \in M$. Ievērosim, ka arī $2\cdot 3-1 = 5$ un $3\cdot 5-1 = 14$, kas nozīmē, ka $5, 7 \in M$, kas arī bija jāpierāda.

2.solis Kopa M ir bezgalīga.
Pierādījums. Pieņemsim pretējo, ka kopa M ir galīga un visi tās elementi ir $p_1 = 2, p_2 = 3, \ldots, p_k$. Ievērosim, ka no uzdevuma nosacījumiem skaitļa

$$p_2 p_3 \cdots p_k - 1$$

pirmreizinātāji arī ir kopā M. Acīmredzami, ka $p_i \nmid p_2 p_3 \cdots p_k - 1$ visiem $2 \le i \le k$. Tā kā kopa M satur tikai skaitļus $p_1, \ldots, p_k$, tad secinām, ka

$$p_2 p_3 \cdots p_k - 1 = 2^x,$$

kur x ir kaut kāds naturāls skaitlis. Taču $7 \mid p_2 p_3 \cdots p_k$, kas nozīmē, ka $2^x \equiv -1 \pmod 7$. Viegli pārbaudīt, ka divnieka pakāpes dod tikai atlikumus $2, 4, 1$, dalot ar 7.

3.solis Kopa $M = \mathbb{P}$.
Pierādījums. Aplūkosim patvaļīgu pirmskaitli q. Ja eksistē tāds pirmskaitlis kopā M, kurš dod atlikumu 0, dalot ar q, tad tas nozīmē, ka $q \in M$. Pretējā gadījumā visi kopas M elementi dod tikai atlikumus $1, 2, \ldots, q-1$, dalot ar q. Tā kā kopa M ir bezgalīga, tad eksistē kaut kādi pirmskaitļi $a_1, a_2, \ldots, a_{q-1}$, kas visi dod atlikumu r, dalot ar q. Tādā gadījumā no Mazās Fermā teorēmas izriet, ka

$$a_1 a_2 \cdots a_{q-1} \equiv r^{q-1} - 1 \equiv 0 \pmod q,$$

kas nozīmē, ka $q \in M$. Prasītais pierādīts.

6.uzdevums Atrast visas funkcijas $f : \mathbb{N} \to \mathbb{N}$, kurām izpildās

$$n! + f(m)! \mid f(n)! + f(m!)$$

visiem naturāliem skaitļiem m, n.

Atrisinājums. Ar $P(m, n)$ apzīmēsim doto sakarību. Risinājums sastāvēs no vairākiem soļiem.

1. solis. $f(1) = 1$.
Pierādījums. Ievērosim, ka no $P(1, 1)$ izriet, ka

$$1 + f(1)! \mid f(1)! + f(1) \implies 1 + f(1)! \mid (f(1)! + f(1)) - (f(1)! + 1) = f(1) - 1$$

Ievērosim, ka $f(1)! \geq f(1)$, līdz ar to $f(1)! + 1 \geq f(1) + 1 > f(1) - 1$, līdz ar to vienīgais veids, kā var izpildīties dalāmība ir, ja $f(1) - 1 = 0$ jeb $f(1) = 1$.

Ievērosim, ka no $P(n, 1)$ izriet, ka

$$n! + 1 \mid f(n)! + 1$$

Tas nozīmē, ka $f(n)! + 1 \geq n! + 1$ jeb $f(n)! \geq n!$, no kurienes izriet, ka $f(n) \geq n$.

2.solis. Visiem pirmskaitļiem p ir spēkā, ka $f(p - 1) = p - 1$.
Pierādījums. No $P(p - 1, 1)$ izriet, ka

$$(p - 1)! + 1 \mid f(p - 1)! + 1$$

No Vilsona teorēmas izriet, ka $p \mid (p - 1)! + 1$. Pirms tam ieguvām, ka $f(p - 1) \geq p - 1$. Pieņemsim, ka $f(p - 1) \geq p$, tad $f(p - 1)!$ dalās ar p. Taču tādā gadījumā skaitlis $f(p - 1)! + 1$ ar p dalīties nevar, bet tam ir jādalās, jo

$$p \mid (p - 1)! + 1 \mid f(p - 1)! + 1$$

Līdz ar to mūsu pieņēmums ir aplams, kas nozīmē, ka $f(p - 1) = p - 1$ visiem pirmskaitļiem p.

3.solis. Visiem naturāliem skaitļiem m ir spēkā, ka $f(m)! = f(m!)$.
Pierādījums. Aplūkosim $P(p - 1, m)$, kur p ir patvaļīgs pirmskaitlis un m ir fiksēts skaitlis. Tādā gadījumā varam iegūt, ka

$$\begin{gathered}(p - 1)! + f(m)! \mid f(p - 1)! + f(m!) \\ (p - 1)! + f(m)! \mid (p - 1)! + f(m!) \\ (p - 1)! + f(m)! \mid ((p - 1)! + f(m!)) - ((p - 1)! + f(m)!) \\ (p - 1)! + f(m)! \mid f(m!) - f(m)!\end{gathered}$$

Tā kā pirmskaitļu ir bezgalīgi daudz, tad mēs varam atrast tādu pirmskaitli p ar īpašību, ka $(p - 1)! + f(m)! > |f(m!) - f(m)!|$. Līdz ar to iegūtā dalāmība var izpildīties tikai tad, ja $f(m!) = f(m)!$.

4.solis Visiem naturāliem skaitļiem n ir spēkā, ka $f(n) = n$.
Pierādījums. Aplūkosim $P(n, p - 1)$, kur p ir patvaļīgs pirmskaitlis

$$\begin{gathered}n! + f(p - 1)! \mid f(n)! + f((p - 1)!) \\ n! + (p - 1)! \mid f(n)! + f(p - 1)! \\ n! + (p - 1)! \mid f(n)! + (p - 1)! \\ n! + (p - 1)! \mid (f(n)! + (p - 1)!) - (n! + (p - 1!)) \\ n! + (p - 1)! \mid f(n)! - n!\end{gathered}$$

Tā kā pirmskaitļu ir bezgalīgi daudz, tad mēs varam atrast tādu pirmskaitli p ar īpašību, ka $(p-1)!+n! > |f(n)! - n!|$. Līdz ar to vienīgais veids, kā iegūtā dalāmība var izpildīties, ir, ja $f(n)! = n!$, kas nozīmē, ka $f(n) = n$.

Viegli pārbaudīt, ka iegūtā funkcija tiešām apmierina uzdevuma nosacījumus.

7.uzdevums Par *kvadrātbrīvu* sauc naturālu skaitli, kurš nedalās ar neviena pirmskaitļa kvadrātu. Pierādīt, ka katram kvadrātbrīvam naturālam skaitlim $n > 1$ eksistē pirmskaitlis p un naturāls skaitlis m ar īpašību, ka

$$p \mid n \quad \text{un} \quad n \mid p^2 + p \cdot m^p.$$

Atrisinājums. Pieņemsim, ka $n = p_1 p_2 \dots p_k$ un $p_k = \max(p_1, \dots, p_k)$. Izvēlēsimies, ka $p = p_k$ un konstruēsim prasīto skaitli m.

Acīmredzami, ka $p_k \mid n$ un $p_k \mid p_k^2 + p_k \cdot m^{p_k}$. Aplūkosim $p_i \mid n$, kur $i \neq k$, tad mēs vēlamies pierādīt, ka $p_i \mid p(p + m^p)$. Tam ekvivalenti ir pierādīt to, ka eksistē naturāls skaitlis m, kam

$$\begin{aligned} m^p &\equiv -p \pmod{p_1} \\ m^p &\equiv -p \pmod{p_2} \\ &\dots \\ m^p &\equiv -p \pmod{p_{k-1}} \end{aligned}$$

Izvēlēsimies skaitli m formā c^l, kur c un l ir naturāli skaitļi, kurus mēs noteiksim pēc brīža.

Apgalvojums. Eksistē tāds naturāls skaitlis l, ka $pl \equiv 1 \pmod{(p_1 - 1)(p_2 - 1) \dots (p_{k-1} - 1)}$.
Pierādījums. Tas izriet no inversā elementa eksistences, ja mēs pierādām, ka $\gcd(p, (p_1 - 1)(p_2 - 1) \dots (p_{k-1} - 1)) = 1$. Taču $p = p_k = \max(p_1, \dots, p_k)$, līdz ar to tas ir savstarpējs pirmskaitlis ar jebkuru naturālu skaitli, kurš ir mazāks par par to. Līdz ar to $\gcd(p, p_1 - 1) = \gcd(p, p_2 - 1) = \dots = \gcd(p, p_{k-1} - 1) = 1$, kas nozīmē, ka $\gcd(p, (p_1 - 1)(p_2 - 1) \dots (p_{k-1} - 1)) = 1$. Prasītais ir pierādīts.

Apzīmēsim $P = (p_1 - 1)(p_2 - 1) \dots (p_{k-1} - 1)$. Ievērosim, ka $m^p = c^{pl} \equiv c \pmod{p_i}$ visiem $i \neq k$, jo $pl = aP + 1 \equiv 1 \pmod{p_i - 1}$ visiem $i \neq k$, kur a ir naturāls skaitlis. Līdz ar to mums vajag atrast tādu naturālu skaitli c, ka

$$\begin{aligned} c &\equiv -p \pmod{p_1} \\ c &\equiv -p \pmod{p_2} \\ &\dots \\ c &\equiv -p \pmod{p_{k-1}} \end{aligned}$$

Tāds c eksistē no ķīniešu atlikumu teorēmas, jo $\gcd(p_i, p_j) = 1$ visiem $1 \leq i < j \leq k - 1$. Līdz ar to esam atraduši meklēto m, kas atrisina uzdevumu.