

1.mājasdarba atrisinājumi

1.uzdevums Atrast visus pirmskaitļus p , kuriem eksistē naturāli skaitļi x, y un z ar īpašību, ka skaitlis $x^p + y^p + z^p - x - y - z$ ir tieši trīs dažādu pirmskaitļu reizinājums.

Atrisinājums. Sākamā izskatīsim gadījumu, kad $p \in \{2, 3, 5\}$.

- Ja $p = 2$, tad pie $x = 1, y = 1, z = 7$ mēs dabūjam, ka

$$x^p + y^p + z^p - x - y - z = 1 + 1 + 49 - 1 - 1 - 7 = 42 = 2 \cdot 3 \cdot 7$$

- Ja $p = 3$, tad pie $x = 1, y = 2, z = 3$ mēs dabūjam, ka

$$x^p + y^p + z^p - x - y - z = 1 + 8 + 27 - 1 - 2 - 3 = 30 = 2 \cdot 3 \cdot 5$$

- Ja $p = 5$, tad pie $x = 1, y = 1, z = 2$ mēs dabūjam, ka

$$x^p + y^p + z^p - x - y - z = 1 + 1 + 32 - 1 - 1 - 2 = 30 = 2 \cdot 3 \cdot 5$$

Tātad pirmskaitļi 2, 3 un 5 apmierina uzdevuma nosacījumus. Palika apskatīt gadījumu, kad $p \geq 7$. Ievērojam, ka skaitļiem x^p un x ir vienāda paritāte, no kā izriet, ka $2 \mid x^p - x$. Veicot līdzīgus spriedumus, secinām, ka

$$2 \mid x^p + y^p + z^p - x - y - z.$$

Tā kā p ir nepāra, tad pierakstot $p = 2k + 1$, iegūstam, ka ja x nedalās ar 3, tad

$$x^p \equiv x \cdot (x^k)^2 \equiv x \cdot 1 \equiv x \pmod{3}$$

no kā izriet, ka $3 \mid x^p - x$. Taču ja x dalās ar 3, tad acīmredzami $3 \mid x^p - x$, tāpēc $3 \mid x^p - x$ visiem naturāliem skaitļiem x . Veicot analogiskus spriedumus skaitļiem y un z , iegūstam, ka

$$3 \mid x^p + y^p + z^p - x - y - z.$$

Tagad apskatīsim divus gadījumus. Ja $p \mid x$, tad $p \mid x^p$, no kā seko, ka $p \mid x^p - x$. Taču ja $p \nmid x$, tad pielietojot Mazo Fermā teorēmu, secinām, ka $x^p \equiv x \pmod{p}$, no kā seko, ka $p \mid x^p - x$. Tātad iegūstam, ka $p \mid x^p - x$ neatkarīgi no skaitļa x vērtības. Veicot analogiskus spriedumus skaitļiem y un z , secinām, ka

$$p \mid x^p + y^p + z^p - x - y - z.$$

Tā kā 2, 3 un p ir trīs dažādi pirmskaitļi, kas dala doto vērtību, tad lai uzdevuma nosacījums izpildītos, mums ir jābūt

$$x^p + y^p + z^p - x - y - z = 2 \cdot 3 \cdot p = 6p$$

Pamanīsim, ka vismaz viens no skaitļiem x, y, z ir lielāks par vienu, no kā izriet, ka

$$6p = x^p + y^p + z^p - x - y - z \geq 2^p - 2,$$

kas nav iespējams visiem $p \geq 7$ (to var viegli pierādīt izmantojot matemātisku indukciju). Līdz ar to, vienīgie pirmskaitļi, kas apmierina uzdevuma nosacījumus ir 2, 3 un 5.

2. uzdevums Atrast visus pirmskaitļus p un q ar īpašību, ka skaitlis $1 + \frac{p^q - q^p}{p+q}$ ir pirmskaitlis.

Atrisinājums. Pieņemsim, ka

$$1 + \frac{p^q - q^p}{p+q} = r \implies p + q + p^q - q^p = r(p+q)$$

kādam pirmskaitlim r . Ievērojam, ka ja $p = q$, tad

$$p + p + p^p - p^p = r(p+p) \implies 2p = 2pr \implies r = 1,$$

kas nav pirmskaitlis. Līdz ar to $p \neq q$. Tad no Mazas Fermā teorēmas seko, ka

$$q^p \equiv q \pmod{p} \implies p \mid q - q^p.$$

Secinām, ka

$$p \mid p + q + p^q - q^p = r(p+q) \implies p \mid qr.$$

Tā kā $p \neq q$, tad no $p \mid qr$ izriet, ka $p = r$. Dabūjam, ka

$$p + q + p^q - q^p = p(p+q)$$

Apskatot abas vienādojums puses pēc moduļa q un pielietojot Mazo Fermā teorēmu, secinām, ka

$$p + p \equiv p^2 \pmod{q} \implies p(p-2) \equiv 0 \pmod{q} \implies q \mid p-2.$$

Pamanīsim, ka tas ir iespējams tikai tad ja $p > q$ vai $p = 2$.

- Ja $p > q$, tad izmantojot labi zināmo faktu, ka $a^b > b^a$ visiem $b > a \geq 3$, secinām, ka $q < 3$ jeb $q = 2$, jo citādi $p > q \geq 3$, kas nozīmē, ka

$$p^q < q^p \implies p^q - q^p < 0 \implies p(p+q) = p + q + p^q - q^p < p + q,$$

kas ir pretruna. Tā kā $q = 2$, tad

$$p + 2 + p^2 - 2^p = p(p+2) \implies 2^p = 2 - p,$$

kas nav patiess visiem pirmskaitļiem p .

- Ja $p = 2$, tad

$$2 + q + 2^q - q^2 = 2(2+q) \implies 2^q = q^2 + q + 2.$$

Ievērojām, ka $2^q > q^2 + q + 2$ visiem $q > 5$ (to var viegli pierādīt, izmantojot matemātisko indukciju). Līdz ar to $q \leq 5 \implies q \in \{2, 3, 5\}$. Pārbaudot šīs vērtības, iegūtam, ka vienīgais iespējams atrisinājums ir $p = 2$ un $q = 5$.

3. uzdevums Sauksim skaitļu $(1, 2, \dots, n)$ permutāciju (a_1, \dots, a_n) par *rizz*, ja skaitļi $a_1 + a_2 + \dots + a_i$ dod dažādus atlikumus, dalot ar n , visiem $1 \leq i \leq n$. Pierādīt, ka eksistē naturāls skaitlis n ar īpašību, ka eksistē vismaz 2025 skaitļu $(1, 2, \dots, n)$ rizz permutācijas.

Atrisinājums. Vispirms pierādīsim sekojošu apgalvojumu.

Apgalvojums. Ja (a_1, a_2, \dots, a_n) ir skaitļu $(1, 2, \dots, n)$ rizz permutācija, tad jebkuram skaitlim c ar īpašību, ka $\gcd(c, n) = 1$, skaitļu kopa $(ca_1, ca_2, \dots, ca_n) \pmod{n}$ arī ir skaitļu $(1, 2, \dots, n)$ rizz permutācija.

Pierādījums. Pašā materiālā pierādījām, ka $(ca_1, \dots, ca_n) \pmod{n}$ ir skaitļu $(1, 2, \dots, n)$ permutācija. Apzīmēsim ar $s_i = a_1 + a_2 + \dots + a_i$. No pieņēmuma izriet, ka $(s_1, \dots, s_n) \pmod{n}$ ir skaitļu $(1, 2, \dots, n)$ permutācija. Līdz ar to $(cs_1, \dots, cs_n) \pmod{n}$ arī ir skaitļu $(1, 2, \dots, n)$ permutācija, kas nozīmē, ka $(ca_1, ca_2, \dots, ca_n) \pmod{n}$ arī ir skaitļu $(1, 2, \dots, n)$ rizz permutācija.

Līdz ar to, ja mēs varam atrast tādu naturālu skaitli n ar īpašību, ka $\phi(n) \geq 2025$ un skaitlim n eksistē vismaz viena rizz permutācija, tad uzdevums būs atrisināts.

Aplūkosim skaitli $n = 2^k$ un permutāciju $(a_1, a_2, \dots, a_n) = (n, 1, 2, \dots, n-1)$. Tādā gadījumā $s_i = a_1 + a_2 + \dots + a_i = n + \frac{i(i-1)}{2}$. Pieņemsim, ka eksistē skaitļi i un j ar īpašību, ka s_i un s_j dot vienādus atlikumus dalot ar 2^k . Tādā gadījumā $2^k \mid \frac{i(i-1)}{2} - \frac{j(j-1)}{2}$, kas nozīmē, ka $2^{k+1} \mid i(i-1) - j(j-1) = (i-j)(i+j-1)$. Ievērosim, ka skaitļiem $i-j$ un $i+j-1$ ir dažāda paritāte. Līdz ar to $2^{k+1} \mid i-j$ vai $2^{k+1} \mid i+j-1$. Ievērosim, ka $|i-j| < 2^k$, tāpēc pirmajā gadījumā iegūstam, ka $i=j$. Otrajā gadījumā ievērosim, ka $0 < i+j-1 \leq 2^k + 2^k - 1 - 1 = 2^{k+1} - 2$, līdz ar to dalāmība arī nevar izpildīties. Secinām, ka permutācija $(n, 1, \dots, n-1)$ ir rizz.

Atliek izvēlēties tādu skaitli k , ka $\phi(2^k) \geq 2025$, taču $k = 12$ apmierina šīs prasības, jo $\phi(2^{12}) = 2^{11} = 2048$.

4. uzdevums Atrast visus naturālos skaitļus (m, n) ar īpašību, ka skaitlis $m^2 - mn + n^2 + 1$ dala gan skaitli $3^{m+n} + (m+n)!$, gan skaitli $3^{m^3+n^3} + m + n$.

Atrisinājums. Vispirms pierādīsim sekojošu apgalvojumu.

Apgalvojums. Skaitlis $m^2 - mn + n^2 + 1$ ir pirmskaitlis.

Pierādījums. Pieņemsim pretējo, ka skaitlis $m^2 - mn + n^2 + 1$ ir salikts skaitlis. Tad tam eksistē dalītājs ar d ar īpašību, ka tas nav lielāks par $\sqrt{m^2 - mn + n^2 + 1} < m + n$. Tas nozīmē, ka $d \mid (m+n)!$, līdz ar to secinām, ka

$$d \mid m^2 - mn + n^2 + 1 \mid 3^{m+n} + (m+n)! \implies d \mid 3^{m+n}.$$

No šejienes iegūstam, ka $3 \mid d \mid m^2 - mn + n^2 + 1$. Ievērosim, ka $m^2 - mn + n^2 + 1 = (m+n)^2 - 3mn + 1$, tāpēc $3 \mid (m+n)^2 + 1$. Taču reāla skaitļa kvadrāti dod tikai atlikumus 0 vai 1, dalot ar 3, tāpēc $(m+n)^2 + 1$ ar 3 nedalās – pretruna.

Apzīmēsim $m^2 - mn + n^2 + 1 = p$, kur p ir pirmskaitlis. Pieņemsim, ka $p > 3$. Ievērosim, ka no Mazās Fermā teorēmas tādā gadījumā izriet, ka

$$1 \equiv 3^{p-1} = 3^{m^2 - mn + n^2} \pmod{p} \implies 1 \equiv 1^{m+n} \equiv 3^{m^3 + n^3} \pmod{p}$$

Secinām, ka

$$1 + m + n \equiv 3^{m^3 + n^3} + m + n \equiv 0 \pmod{p}$$

Citiem vārdiem sakot, esam ieguvuši, ka $p = m^2 - mn + n^2 + 1 \mid m + n + 1$. Tas nozīmē, ka

$$\begin{aligned} m + n + 1 &\geq m^2 - mn + n^2 + 1 \\ 2m + 2n &\geq (m - n)^2 + m^2 + n^2 \\ 2 &\geq (m - n)^2 + (m - 1)^2 + (n - 1)^2 \end{aligned}$$

Secinām, ka $m, n \leq 2$. Pārbaudot visus iespējamus gadījumus iegūstam, ka vienīgais atrisinājums ir $(2, 2)$.

Atliek apskatīt gadījumu, kad $m^2 - mn + n^2 + 1 = 2$ vai 3 . Mēs iepriekš pierādījām, ka $3 \nmid m^2 - mn + n^2 + 1$, tāpēc otrais variants atkrīt. Ievērosim, ka pirmā gadījumu vienādojumu var pārveidot sekojoši

$$m^2 - mn + n^2 + 1 = 2 \implies (2m - n)^2 + 3n^2 = 4$$

Vienīgais iespējamais atrisinājums ir, kad $n = 1$ un $2m - n = 1$, kas nozīmē, ka $m = 1$, taču viegli pārbaudīt, ka šis pāris neapmierina uzdevuma nosacījumus.

2.mājasdarba atrisinājumi

1.uzdevums Dota naturālu skaitļu kopa $\{a_1, a_2, \dots, a_n\}$. Pierādīt, ka eksistē tāds naturāls skaitlis b , ka visi skaitļi kopā $\{ba_1, ba_2, \dots, ba_n\}$ ir veselu skaitļu pakāpes (iespējamās dažādas), kuras ir lielākas par 1.

Atrisinājums. Apzīmēsim visus pirmskaitļus, kas dala kaut vienu no a_i ar p_1, p_2, \dots, p_r kādam naturālam skaitlim r . Tad katru no a_i var piekārstīt kā

$$a_i = p_1^{\alpha_{i,1}} \cdot p_2^{\alpha_{i,2}} \cdot \dots \cdot p_r^{\alpha_{i,r}},$$

kur $\alpha_{i,j}$ ir nenegatīvs vesels skaitlis katram $1 \leq i \leq n$ un $1 \leq j \leq r$. Tagad apskatīsim skaitli

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_r^{\beta_r},$$

kur β_j ir nenegatīvs vesels skaitlis katram $1 \leq j \leq r$. Ievērojam, ka ba_i ir vesela skaitļa pakāpe, kas ir lielāka par viens tad un tikai tad, ja

$$\gcd(\alpha_{i,1} + \beta_1, \alpha_{i,2} + \beta_2, \dots, \alpha_{i,r} + \beta_r) > 1$$

Apskatīsim patvaļīgus dažādus pirmskaitļus q_1, q_2, \dots, q_n . Ievērojam, ka, izmantojot Ķīniešu atlikumu teorēmu, katram $1 \leq j \leq r$ mēs varam konstruēt tādu β_j , ka

$$\beta_j \equiv -\alpha_{1,j} \pmod{q_1}$$

$$\beta_j \equiv -\alpha_{2,j} \pmod{q_2}$$

...

$$\beta_j \equiv -\alpha_{n,j} \pmod{q_n}$$

Tas nozīmē, ka $q_i \mid \alpha_{i,j} + \beta_j$ visiem $1 \leq i \leq n$ un $1 \leq j \leq r$. Tādā gadījumā, katram $1 \leq i \leq n$ izpildās

$$\gcd(\alpha_{i,1} + \beta_1, \alpha_{i,2} + \beta_2, \dots, \alpha_{i,r} + \beta_r) \geq q_i > 1,$$

kas nozīmē, ka ba_i ir vesela skaitļa pakāpe, kas ir lielāka par viens visiem $1 \leq i \leq n$, kas dod prasīto.

2. uzdevums Atrast visus naturālo skaitļus n ar īpašību, ka skaitļus no 1 līdz $2n$ var sadalīt 2 grupās (a_1, a_2, \dots, a_n) , (b_1, b_2, \dots, b_n) tā, ka katrs skaitlis ir tieši vienā grupā un $2n \mid a_1 a_2 \cdots a_n + b_1 b_2 \cdots b_n - 1$.

Atrisinājums. Vispirms pierādīsim sekojošu apgalvojumu.

Apgalvojums. Skaitlis n ir divnieka pakāpe.

Pierādījums. Pieņemsim pretējo, tad eksistē nepāra pirmskaitlis p ar īpašību, ka $p \mid n$. Ievērosim, ka skaitlim $a_1 a_2 \cdots a_n + b_1 b_2 \cdots b_n$ jābūt nepāra, kas nozīmē, ka viens no skaitļiem $a_1 a_2 \cdots a_n$ un $b_1 b_2 \cdots b_n$ jābūt nepāra. Nezaudējot vispārīgumu, pieņemsim, ka $a_1 a_2 \cdots a_n$ ir nepāra, tad skaitļu kopa (a_1, a_2, \dots, a_n) ir skaitļu kopas $(1, 3, \dots, 2n - 1)$ permutācija. Viegli pamanīt, ka tādā gadījumā $p \mid a_1 a_2 \cdots a_n$, jo p ir nepāra pirmskaitlis un $p < n$. No otras puses, tādā gadījumā skaitļu kopa (b_1, b_2, \dots, b_n) ir skaitļu kopas $(2, 4, \dots, 2n)$ permutācija. Tā kā $2p < 2n$, tad secinām, ka $p \mid b_1 b_2 \cdots b_n$, taču tādā gadījumā $p \mid a_1 a_2 \cdots a_n + b_1 b_2 \cdots b_n - 1$ – pretruna.

Pierādīsim, ka visiem skaitļiem $n = 2^k$, kur $k > 1$, skaitļus var sadalīt uzdevuma prasītā veidā. Sadalīsim skaitļus grupās $(a_1, a_2, \dots, a_n) = (1, 3, \dots, 2^k - 1)$ un $(b_1, b_2, \dots, b_n) = (2, 4, \dots, 2^k)$. Ievērosim, ka $2^{k+1} \mid b_1 b_2 \cdots b_n$, tāpēc atliek pierādīt, ka $a_1 a_2 \cdots a_n \equiv 1 \pmod{2^{k+1}}$.

Apgalvojums. Katram nepāra skaitlim $a < 2^{k+1}$ eksistē unikāls nepāra skaitlis $a \neq b < 2^{k+1}$ ar īpašību, ka $ab \equiv -1 \pmod{2^{k+1}}$.

Pierādījums. Eksistence ir pierādīta materiālā ("noderīgs fakts" 6. lapaspuse). Lai pierādītu unikalitāti, tad pieņemsim, ka eksistē 2 dažādi nepāra skaitļi ar prasīto īpašību b, c , tad $ab \equiv ac \equiv -1 \pmod{2^{k+1}}$, tad $a(b - c) \equiv 0 \pmod{2^{k+1}}$, kas nozīmē, ka $2^{k+1} \mid b - c$, kas ir iespējams tad un tikai tad, ja $b = c$ – pretruna. Atliek pierādīt, ka $a \neq b$. Pieņemsim pretējo, tad $ab \equiv a^2 \equiv -1 \pmod{2^{k+1}}$, kas nozīmē, ka $4 \mid 2^{k+1} \mid a^2 + 1$, kas nav iespējams, jo veselu skaitļu kvadrāti dod tikai atlikumus 0 vai 1, dārot ar 4.

No apgalvojuma mēs secinām, ka skaitļus, ka katru skaitli no kopas $(1, 3, \dots, 2n - 1)$ mēs varam sagrupēt kopā ar unikālu citu skaitli no šīs kopas tā, lai to reizinājums būtu $-1 \pmod{2^{k+1}}$. Līdz ar to $a_1 a_2 \cdots a_n \equiv (-1)^{n/2} \equiv (-1)^{2^k} \equiv 1 \pmod{2^{k+1}}$, kas arī bija jāpierāda.

Priekš $n = 2$ pilnā pārlase pasaka mums, ka prasīto nevar izdarīt.

3.uzdevums Atrast visas funkcijas $f : \mathbb{N} \rightarrow \mathbb{N}$, kurām visiem naturāliem skaitļiem n un pirmskaitļiem p izpildās

$$p \mid f(n)f(p-1)! + n^{f(p)}.$$

Atrisinājums. Ar $P(2, 2)$ apzīmēsim doto sakarību. Ievērosim, ka no $P(2, 2)$ izriet, ka $2 \mid f(1)f(1)! + 1$. Ja $f(1) > 1$, tad $f(1)!$ ir pāra skaitlis un $f(1)f(1)! + 1$ attiecīgi nepāra skaitlis – pretruna. Līdz ar to $f(1) = 1$. No $P(1, p)$ izriet, ka

$$p \mid f(p-1)! + 1 \implies f(p-1)! \equiv -1 \pmod{p}$$

Uzdevuma doto sakarību var pārrakstīt kā

$$0 \equiv n^{f(p)} + f(n)f(p-1)! \equiv n^{f(p)} - f(n) \pmod{p}$$

Secinām, ka $p \mid n^{f(p)} - f(n)$.

Apgalvojums. Skaitlis $f(p)$ ir p pakāpe.

Pierādījums. Pieņemsim pretējo, tad eksistē pirmskaitlis $q \neq p$ ar īpašību, ka $q \mid f(p)$. Ievērosim, ka $q \mid n^{f(q)} - f(n)$. Ievietojot n vietā p , iegūsim, ka $q \mid p^{f(q)} - f(p)$, no kurienes izriet, ka $q \mid p^{f(q)}$, līdz ar to $q = p$ – pretruna.

Pieņemsim, ka $f(p) = p^k$ (ievērosim, ka dažādām p vērtībām var būt dažādās k vērtības). Ievērosim, ka no Mazās Fermā teorēmas izriet, ka $n^p \equiv n \pmod{p}$. Kāpinot abas sakarības puses p -tajā pakāpē, iegūsim, ka $n^{p^2} \equiv n^p \equiv n$. Atkārtojot šo procesu induktīvi, iegūstam, ka $n^{p^k} \equiv n \pmod{p}$. Secinām, ka

$$0 \equiv n^{f(p)} - f(n) \equiv n - f(n) \pmod{p}$$

Citiem vārdiem sakot, izpildās $p \mid n - f(n)$. Izvēlēties pirmskaitli p ar īpašību, ka $p > |n - f(n)|$, tad $f(n) - n = 0$, kas nozīmē, ka $f(n) = n$. Viegli pārbaudīt, ka šī funkcija der.

4. uzdevums Pierādīt, ka katram pirmskaitlim p eksistē naturāls skaitlis n ar īpašību, ka

$$1^n + 2^{n-1} + 3^{n-2} + \dots + n^1 \equiv 2020 \pmod{p}.$$

Atrisinājums. Ja $p = 2$, tad pie $n = 3$ mēs dabūjam, ka

$$1^3 + 2^2 + 3^1 \equiv 0 \equiv 2020 \pmod{2}.$$

Tagad apskatīsim gadījumu, kad $p \geq 3$. Pierādīsim, ka visiem pirmskaitļiem $p \geq 3$ skaitlis $n = ap(p-1) - 1$, kur a ir naturāls skaitlis ar īpašību, ka $p \mid a + 2020$, apmierina uzdevuma nosacījumus. Apzīmēsim kreiso vienādības pusi ar S . Tā kā $p \mid ap(p-1) = n + 1$, tad

$$S = 1^n + 2^{n-1} + 3^{n-2} + \dots + n^1 = \sum_{k=1}^n (n+1-k)^k \equiv \sum_{k=1}^n (-k)^k \equiv \sum_{k=1}^{n+1} (-k)^k \pmod{p},$$

kur mēs izmantojam to, ka $(-(n+1))^{n+1} \equiv 0 \pmod{p}$. Sadalīsim iegūto summu $a(p-1)$ daļās. Sanāk, ka katrā no tām ir tieši p saskaitāmie:

$$\sum_{k=1}^{n+1} (-k)^k = \sum_{k=1}^{ap(p-1)} (-k)^k = \sum_{k=1}^p (-k)^k + (-k-p)^{k+p} + \dots + (-k-p(a(p-1)-1))^{k+p(a(p-1)-1)}.$$

Pamanīsim, ka iegūtajā summā pie $k = p$ visi saskaitāmie dalās ar p , līdz ar to

$$S \equiv \sum_{k=1}^{p-1} (-k)^k + (-k-p)^{k+p} + \dots + (-k-p(a(p-1)-1))^{k+p(a(p-1)-1)} \pmod{p}.$$

Izmantojot Mazo Fermā teorēmu katram saskaitāmajam, iegūstam, ka

$$S \equiv \sum_{k=1}^{p-1} (-k)^k + (-k)^{k+1} + \dots + (-k)^{k+(a(p-1)-1)} \pmod{p},$$

kur mēs katra saskaitāma kapinātajam atņemam $p-1$ attiecīgo reižu skaitu. Pamanīsim, ka skaitļi $k, k+1, \dots, k+a(p-1)-1$ ir $a(p-1)$ pēc kārtas esošie skaitļi. Tādējādi šie skaitļi reducējas uz visu iespējamo atlikumu pēc moduļa $p-1$ kopas a kopijām:

$$S \equiv a \cdot \sum_{k=1}^{p-1} (-k)^1 + (-k)^2 + \dots + (-k)^{p-1} \equiv a \cdot \sum_{k=1}^{p-1} k^1 + k^2 + \dots + k^{p-1} \pmod{p},$$

kur mēs izmantojam to, ka kopas $\{-1, -2, \dots, -(p-1)\}$ un $\{1, 2, \dots, p-1\}$ ir vienādas pēc moduļa $p-1$. Pārkārtojot saskaitāmos, dabūjam, ka

$$S \equiv a \cdot \sum_{k=1}^{p-1} k^1 + k^2 + \dots + k^{p-1} = a \cdot \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} k^l.$$

Izmantojot labi zināmo faktu, ka $\sum_{l=1}^{p-1} k^l \equiv 0 \pmod{p}$, ja k nedalās ar $p-1$ un $\sum_{l=1}^{p-1} k^l \equiv -1 \pmod{p}$, ja k dalās ar $p-1$. Līdz ar to

$$S \equiv a(0 + 0 + \dots + 0 - 1) = -a \equiv 2020 \pmod{p},$$

kas dod prasīto.