Advancēta modulārā aritmētika

Kims Georgs Pavlovs, Kalvis Apsītis

1 Ievads

Šajā nodarbībā aplūkosim sarežģītākus modulārās aritmētikas jēdzienus – Mazo Fermā teorēmu, Vilsona teorēmu, inversos elementus pēc pirmskaitļa moduļa p un ķīniešu atlikumu teorēmu.

2 Mazā Fermā teorēma

2.1 Teorijas fakti

Mazā Fermā teorēma. Katram pirmskaitlim p un katram veselam a, kam $\gcd(a,p) = 1$, izpildās

$$a^{p-1} \equiv 1 \pmod{p}.$$

To var pārrakstīt: $a^p \equiv a \pmod{p}$, šoreiz ieskaitot arī tos a, kas dalās ar p.

Pierādījums. Aplūkosim skaitli a, kurš nedalās ar p un divas skaitļu kopas $A = \{1, 2, \ldots, p-1\}$ un $B = \{a \cdot 1 \pmod{p}, a \cdot 2 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$. Pierādīsim, ka kopas A elementi sakrīt ar kopas B elementiem (citiem vārdiem sakot kopas B elementi ir kaut kāda kopas A elementu permutācija). Pietiek pierādīt, ka kopa B satur $p-1$ dažādus elementus. Pieņemsim pretējo, ka tā nesatur $p-1$ dažādus elementus, tad kādi divi no kopā B esošajiem $p-1$ atlikumiem ir vienādi. Tad atradīsies $i \neq j$, kam $ai \equiv aj \pmod{p}$. Tādā gadījumā:

$$\begin{aligned} ai &\equiv aj \pmod{p} \\ a(i-j) &\equiv 0 \pmod{p} \\ p &\mid a(i-j) \end{aligned}$$

Tā kā a nedalās ar p, tad $i-j$ būtu jādalās ar p. Taču $i \neq j$ un $i, j < p$, tātad $0 < |i-j| < p$, kas nozīmē, ka $i-j$ nevar dalīties ar p – pretruna. Tas nozīmē, ka mūsu sākotnējais pieņēmums ir aplams, līdz ar to kopas A elementi sakrīt ar kopas B elementiem.

Tā kā kopās A un B ir tie paši elementi, tad visu elementu reizinājumi abās kopās ir vienādi:

$$\begin{gathered} 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (a \cdot 1)(a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1)) \pmod{p} \\ (p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod{p} \\ (a^{p-1} - 1) \cdot (p-1)! \equiv 0 \pmod{p} \end{gathered}$$

Tas nozīmē, ka $p \mid (a^{p-1} - 1) \cdot (p-1)!$. Tā kā $p \nmid (p-1)!$, tad secinām, ka $p \mid a^{p-1} - 1$. Līdz ar to $a^{p-1} \equiv 1 \pmod{p}$, kas arī bija jāpierāda. □

Noderīgs fakts. Katram nepāra pirmskaitlim p un katram a, kam $\gcd(a,p) = 1$ izpildās $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ vai $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Pierādījums. No Mazās Fermā teorēmas izriet, ka

$$\begin{gathered} a^{p-1} \equiv 1 \pmod{p} \\ (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p} \\ p \mid (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \end{gathered}$$

Tas nozīmē, ka $p \mid (a^{\frac{p-1}{2}} + 1)$ vai $p \mid (a^{\frac{p-1}{2}} - 1)$, kas ir ekvivalents $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ vai $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, kas arī bija jāpierāda. □

Fermā Ziemassvētku teorēma. Dots naturāls skaitlis x. Visi skaitļa $x^2 + 1$ nepāra pirmreizinātāji ir $1 \pmod 4$.

Pierādījums. Pieņemsim pretējo, ka eksistē tāds pirmskaitlis p, ka $p \mid x^2 + 1$ un $p = 4k + 3$, kur k ir nenegatīvs vesels skaitlis. No Mazās Fermā teorēmas izriet, ka

$$x^{p-1} \equiv 1 \pmod{p} \implies x^{4k+2} \equiv 1 \pmod{p}$$

Taču mēs zinām, ka

$$p \mid x^2 + 1 \implies x^2 \equiv -1 \pmod{p}$$

Kāpinot abas kongruences puses $2k + 1$ pakāpē, iegūstam, ka

$$x^2 \equiv -1 \pmod{p}$$
$$(x^2)^{2k+1} \equiv (-1)^{2k+1} \pmod{p}$$
$$x^{4k+2} \equiv -1 \pmod{p}$$

Esam ieguvuši, ka $1 \equiv x^{4k+2} \equiv -1 \pmod{p}$, kas nozīmē, ka $1 \equiv -1 \pmod{p}$ jeb $2 \equiv 0 \pmod{p}$. Pēdējā kongruence ir aplama, jo p ir nepāra skaitlis – pretruna. Līdz ar to mūsu pieņēmums ir aplams un visi skaitļa $x^2 + 1$ pirmreizinātāji ir $1 \pmod 4$, kas arī bija jāpierāda. □

Citiem vārdiem: Nepāra pirmskaitlim p skaitlis -1 ir kvadrātisks atlikums tad un tikai tad, ja $p \equiv 1 \pmod 4$.
Par Ziemassvētku teorēmu parasti sauc Fermā teorēmu par divu kvadrātu summu – nepāra pirmskaitli p var izteikt kā $p = a^2 + b^2$ tad un tikai tad, ja $p \equiv 1 \pmod 4$.

2.2 Uzdevumu risināšanas piemēri

1.piemērs Doti pieci naturāli skaitļi. Šo skaitļu reizinājums apzīmēts ar R, bet to piekto pakāpju summa ar S. Zināms, ka S dalās ar 1001. Vai ir iespējams, ka R un S ir savstarpēji pirmskaitļi?

Atrisinājums. Ievērosim, ka $11 \mid 1001$. Apzīmēsim dotos naturālos skaitļos ar a, b, c, d, e. Mums ir dots, ka

$$11 \mid a^5 + b^5 + c^5 + d^5 + e^5$$

Pieņemsim, ka neviens no skaitļiem a, b, c, d, e nedalās ar 11. Taču mēs zinām, ka $a^5 \equiv 1 \pmod{11}$ vai $a^5 \equiv -1 \pmod{11}$. Analoģisks rezultāts izpildās katram no atlikušajiem mainīgajiem b, c, d, e. Taču summējot piecus skaitļus, kur katrs no tiem ir 1 vai -1 nevar iegūt 0 pēc moduļa 11. Līdz ar to mūsu pieņēmums ir aplams, kas nozīmē, ka kāds no skaitļiem a, b, c, d, e dalās ar 11.Tādā gadījumā $11 \mid R$ un $11 \mid gcd(R, S)$, kas nozīmē, ka skaitļi R un S nevar būt savstarpēji pirmskaitļi.

2.piemērs Atrast visus pirmskaitļu pārus (p, q), kas apmierina vienādojumu:

$$3p^q - 2q^{p-1} = 19.$$

Atrisinājums. Vispirms aplūkosim gadījumu, kad $p = q$. Tādā gadījumā mūsu vienādojums kļūst par

$$3p^p - 2p^{p-1} = 19$$

Tas nozīmē, ka $p \mid 19$, līdz ar to $p = 19$. Viegli redzēt, ka skaitļu pāris $(p, q) = (19, 19)$ nav vienādojuma atrisinājums.
Ja $p \neq q$, tad varam apskatīt abas vienādojuma puses pēc moduļa p un iegūt, ka:

$$-2 \equiv 19 \pmod{p} \implies p \mid 21$$

Tas nozīmē, ka $p = 3$ vai arī $p = 7$. No otras puses, apskatot abas vienādojuma puses pēc moduļa q, varam iegūt, ka:

$$3p \equiv 19 \pmod{q} \implies 3p - 19 \equiv 0 \pmod{q}$$

Šķirojam gadījumus:

- Ja $p = 3$, tad $3p - 19 = -10$. Tā kā $q \mid 10$, tad tas nozīmē, ka $q = 2$ vai $q = 5$.
- Ja $p = 7$, tad $3p - 19 = 21 - 19 = 2$. Tā kā $q \mid 2$, tad secinām, ka $q = 2$.

Līdz ar to vienīgie iespējamie skaitļu pāri (p, q) ir $(7, 2)$, $(3, 2)$ un $(3, 5)$, kuriem pēc pārbaudes var secināt, ka $(3, 5)$ neder.

3.piemērs Atrast visus nepāra pirmskaitļus p, kuriem skaitlis:

$$1^{p-1} + 2^{p-1} + \ldots + 103^{p-1}$$

dalās ar p.

Atrisinājums. Ja $p > 103$, tad visi saskaitāmie ir $i^{p-1} \equiv 1 \pmod{p}$ no mazās Fermā teorēmas. Tad summa kongruenta ar $103 < p$ pēc moduļa p, kas nav kongruents ar 0.
Līdz ar to $p \leq 103$. Uzrakstīsim $103 = kp + r$, kur k – naturāls un $0 \leq r \leq p - 1$. Varam ievērot, ka būs k saskaitāmie, kas dalās ar p, tātad tie kongruenti ar 0 pēc moduļa p, bet visi pārējie saskaitāmie pēc mazās Fermā teorēmas ir kongruenti ar 1. Tātad summa kongruenta ar

$$kp + r - k \equiv r - k \equiv 0 \pmod{p}.$$

Tas nozīmē, ka $r \equiv k \pmod{p}$. Šķirosim gadījumus:

- Ja $k < p$, tad $k = r$ (no kongruences). Varam uzrakstīt $103 = kp + k = k(p + 1)$. Tā kā 103 ir pirmskaitlis, šis var izpildīties tikai tad, ja $p + 1 = 103 \implies p = 102$, taču 102 nav pirmskaitlis - nevar būt.
- Ja $k \geq p$, tad ievērojam, ka $103 = kp + r \geq p^2$. Vienīgie nepāra pirmskaitļi, kam izpildās šī nevienādība, ir $3, 5, 7$. Ievietojot to vērtības izteiksmē $kp + r$, var redzēt, ka $r \equiv k \pmod{p}$ tikai tad, ja $p = 3$, kas arī ir vienīgā atbilde.

4.piemērs Atrisināt veselos skaitļos vienādojumu

$$x^{2010} - 2006 = 4y^{2009} + 4y^{2008} + 2007y.$$

Atrisinājums. Pieskaitīsim abām vienādojuma pusēm 2007. Iegūsim, ka

$$x^{2010} + 1 = 4y^{2009} + 4y^{2008} + 2007y + 2007$$
$$x^{2010} + 1 = 4y^{2008}(y + 1) + 2007(y + 1)$$
$$x^{2010} + 1 = (4y^{2008} + 2007)(y + 1)$$

Ievērosim, ka $4y^{2008} + 2007 \equiv 3 \pmod{4}$. Pierādīsim, ka eksistē tāds pirmskaitlis p ar īpašību, ka $p \mid 4y^{2008} + 2007$ un $p \equiv 3 \pmod{4}$. Ja tas tā nebūtu, tad visi pirmskaitļi, kuri dalītu $y^{2008} + 2007$, būtu $1 \pmod{4}$. Tā kā katrs skaitlis ir visu savu pirmreizinātāju attiecīgo pakāpju reizinājums, tad

secinām, ka $y^{2008} + 2007$ ir jābūt $1 \pmod 4$ – pretruna.

Esam ieguvuši, ka eksistē tāds pirmskaitlis p, ka $p \equiv 3 \pmod 4$ un p dala vienādojuma kreiso pusi. Tas nozīmē, ka p dala arī vienādojuma labo pusi, taču $x^{2010} + 1 = z^2 + 1$, kur $z = x^{1005}$. Tas ir pretrunā ar Fermā Ziemassvētku teorēmu.

5.piemērs Pierādīt, ka visiem naturāliem skaitļiem a, b, c eksistē naturāls skaitlis k ar īpašību, ka skaitļu $a^k + bc$, $b^k + ca$, $c^k + ab$ lielākais kopīgais dalītājs ir lielāks par 1.

Atrisinājums. Vispirms apskatīsim gadījumu, kad skaitlis $abc+1$ ir divnieka pakāpe. Tādā gadījumā skaitļi a, b, c visi ir nepāra. Pierādīsim, ka $k = 1$ apmierina nosacījumu. Ievērosim, ka $a+bc, b+ca, c+ab$ visi ir pāra skaitļi, kas nozīmē, ka to lielākais kopīgais dalītājs ir vismaz 2.

Tagad aplūkosim gadījumu, kad $abc + 1$ nav divnieka pakāpe. Tas nozīmē, ka eksistē nepāra pirmskaitlis p ar īpašību, ka $p \mid abc + 1$. Ievērosim, ka tādā gadījumā $\gcd(a, p) = \gcd(b, p) = \gcd(c, p) = 1$. Pierādīsim, ka $k = p - 2 > 0$ apmierina uzdevuma nosacījumus.

No Mazās Fermā teorēmas un no tā, ka $abc \equiv -1 \pmod p$, izriet:

$$\begin{aligned} a^{p-1} + abc &\equiv 1 - 1 \equiv 0 \pmod p \\ b^{p-1} + abc &\equiv 1 - 1 \equiv 0 \pmod p \\ c^{p-1} + abc &\equiv 1 - 1 \equiv 0 \pmod p \end{aligned}$$

Citiem vārdiem sakot, tas nozīmē, ka $p \mid a^{p-1} + abc = a(a^{p-2} + bc)$. Tā kā $\gcd(a, p) = 1$, tad secinām, ka $p \mid a^{p-2} + bc$. Analoģiski varam iegūt, ka $p \mid b^{p-2} + ca$, $p \mid c^{p-2} + ab$. Tas nozīmē, ka skaitļu $a^{p-2} + bc, b^{p-2} + ca, c^{p-2} + ab$ lielākais kopīgais dalītājs ir vismaz p.

3 Inversie elementi

3.1 Teorijas fakti

Definīcija. Par vesela skaitļa a *inverso elementu* pēc moduļa m sauc tādu atlikumu x, kam izpildās

$$ax \equiv 1 \pmod{m}. \quad \square$$

To pieraksta $x \equiv a^{-1} \pmod{m}$.

Ja skaitļiem a un m ir kopīgs dalītājs $d > 1$, tad a^{-1} neeksistē, jo $d \mid ax$ un tātad arī $ax \not\equiv 1 \pmod{m}$.

Teorēma. Aplūkosim veselu skaitļus a un m, kam $\gcd(a, m) = 1$. Tad eksistē unikāls inversais elements skaitlim a.

Pierādījums. *Eksistence.* Aplūkosim skaitļu kopu A, kas sastāv no visiem skaitļiem x ar īpašību, ka $\gcd(x, m) = 1$ un $1 \leq x < m$. Aplūkosim veselu skaitli a ar īpašību, ka $\gcd(a, m) = 1$. Tad visi kopas A elementi pareizināti ar a pēc moduļa m ir kopas A elementu permutācija. To parāda tāpat kā Mazās Fermā teorēmas pierādījumā. Ievērosim, ka kopa A satur skaitli 1, līdz ar to $ax \equiv 1 \pmod{m}$ un esam atraduši meklēto skaitli x. Diemžēl, šāds pamatojums nepasaka efektīvu metodi inversā elementa atrašanai, izņemot pilno pārlasi (skatīt papildus informācijas dokumentu, kas tiks publicēts pēc NNV9).
Unikalitāte. Pieņemsim, ka eksistē divi dažādi atlikumu b un c ar īpašību, ka $ab \equiv ac \equiv 1 \pmod{m}$. Tādā gadījumā $a(b - c) \equiv 0 \pmod{m}$. Tā kā $\gcd(a, m) = 1$, tad $m \mid b - c$. Taču $1 \leq b < c \leq m - 1$, līdz ar to $0 < |b - c| < m$, kas nozīmē, ka dalāmība nevar izpildīties. Līdz ar to inversais elements skaitlim a ir unikāls. $\square$

Svarīgi ievērot, ka inversais elements ir atlikums pēc moduļa m, līdz ar to tas ir intervālā no 0 līdz $m - 1$. Vispār dotajam a ($\gcd(a, m) = 1$) eksistē bezgalīgi daudz skaitļu x, kam $ax \equiv 1 \pmod{m}$. Jo, pieskaitot skaitļa m daudzkārtni inversajam elementam a^{-1}, iegūsim jaunus skaitļus, kas apmierina prasīto īpašību.
Līdz ar to $x = a^{-1}$ ir labi definēts lielums – tas ir unikāls un eksistē, ja $\gcd(a, m) = 1$. Atzīmēsim, ka $x = a^{-1}$ ir apzīmējums un **nav** tas pats, kas skaitlis $\frac{1}{a}$. Skaitlis $\frac{1}{a}$ ir daļveida skaitlis, savukārt a^{-1} ir **atlikums** (tas nozīmē vesels skaitlis), kuru, sareizinot ar a, iegūst 1 pēc moduļa m. Taču inversiem elementiem piemīt visas daļām piemītošās īpašības, tāpēc bieži vien ar tiem var operēt kā ar parastām daļām.

Noderīgs fakts. Aplūkosim veselus skaitļus a, b, m ar īpašību, ka $\gcd(a, m) = \gcd(b, m) = 1$. Izpildās sekojošas sakarības

- $a^{-1}b^{-1} = (ab)^{-1} \pmod{m}$
- $a^{-1} + b^{-1} = (a + b)(ab)^{-1} \pmod{m}$

Pierādījums. Aplūkosim pirmo sakarību. Mums ir prasīts pierādīt, ka skaitļa ab inversais elements ir $a^{-1}b^{-1}$ pēc moduļa m. Tā kā inversais elements ir unikāls mums ir pietiekami pārliecināties, ka šo divu skaitļu reizinājums ir 1. Tiešām

$$ab \cdot a^{-1}b^{-1} \equiv aa^{-1}bb^{-1} \equiv 1 \pmod{m}$$

Priekš otras sakarības izmantosim pirmo sakarību

$$(a + b)(ab)^{-1} \equiv (a + b)a^{-1}b^{-1} \equiv aa^{-1}b^{-1} + ba^{-1}b^{-1} \equiv b^{-1} + a^{-1} \pmod{m}$$

Tas pierāda prasīto. $\square$

Ievērosim, ka ja a^{-1} un b^{-1} vietā mēs rakstītu $\frac{1}{a}$ un $\frac{1}{b}$, tad mēs esam pierādījuši labi zināmās īpašības par daļām

$$\frac{1}{a} \cdot \frac{1}{b} = \frac{1}{ab} \quad \text{un} \quad \frac{1}{a} + \frac{1}{b} = \frac{a+b}{ab}$$

Līdz ar to tas pierāda, ka inversie elementi uzvedas kā mums ierastās daļas, līdz ar to bieži vien ir vērts rakstīt a^{-1} vietā $\frac{1}{a}$ un operēt kā ar parastām daļām.

Noderīgs fakts. Aplūkosim veselus skaitļus a, b un m ar īpašību, ka $\gcd(a, m) = 1$. Tad eksistē vesels skaitlis x ar īpašību, ka

$$ax \equiv b \pmod{m}$$

Pierādījums. Skaitlis $x \equiv a^{-1}b \pmod{m}$ apmierina uzdevuma nosacījumus, jo, pirmkārt, a^{-1} eksistē, jo $\gcd(a, m) = 1$, otrkārt,

$$ax \equiv aa^{-1}b \equiv b \pmod{m}$$

Līdz ar to esam atraduši vajadzīgo skaitli. □

Inversie elementi garantē kongruences $ax \equiv b \pmod{m}$ atrisinājuma eksistenci, ja $\gcd(a, m) = 1$. Tas ir visbiežāk izmantotais fakts par inversiem elementiem.

3.2 Uzdevumu risināšanas piemēri

6.piemērs Dots nepāra pirmskaitlis p. Pierādīt, ka eksistē skaitļu $1, 2, \ldots, p$ permutācija $a_1, a_2, \ldots, a_p$ ar īpašību, ka skaitļi a_1, a_1a_2, $a_1a_2a_3$, …, $a_1a_2a_3 \ldots a_p$ dod dažādus atlikumus, dalot ar skaitli p.

Atrisinājums. Paņemsim $a_1 = 1$ un $a_i = (i-1)^{-1} \cdot i \pmod{p}$ visiem $1 < i \leq p$. Ievērosim, ka tādā gadījumā

$$\begin{gathered} a_1 \equiv 1 \pmod{p} \\ a_1a_2 = 1 \cdot (1^{-1} \cdot 2) \equiv 2 \pmod{p} \\ a_1a_2a_3 = 1 \cdot (1^{-1} \cdot 2) \cdot (2^{-1} \cdot 3) \equiv 3 \pmod{p} \\ \ldots \\ a_1a_2 \cdot \ldots \cdot a_i \equiv 1 \cdot (1^{-1} \cdot 2) \cdot \ldots \cdot ((i-1)^{-1} \cdot i) \equiv i \pmod{p} \end{gathered}$$

Līdz ar to mēs iegūsim, ka skaitļi $a_1, a_1a_2, \ldots, a_1a_2 \ldots a_p$ dod atlikumus tieši $1, 2, \ldots, p$, dalot ar p. Atliek pierādīt, ka skaitļi $a_1, a_2, \ldots, a_p$ atbilst dažādiem atlikumiem. Pieņemsim pretējo, ka eksistē tādi $p \geq j > i \geq 2$ ar īpašību, ka $a_i = a_j$. Tādā gadījumā iegūsim, ka

$$\begin{gathered} (i-1)^{-1} \cdot i \equiv (j-1)^{-1} j \pmod{p} \\ i \cdot (j-1) \equiv j \cdot (i-1) \pmod{p} \\ ij - i \equiv ij - j \pmod{p} \\ i - j \equiv 0 \pmod{p} \end{gathered}$$

Pārējā no pirmās rindas uz otro rindu mēs reizinājām abas kongruences abas puses ar $(i-1) \cdot (j-1)$. Ieguvām, ka $p \mid (i-j)$, kas nav iespējams, jo $0 < |i-j| < p$. Līdz ar to esam ieguvuši, ka skaitļi $a_2, \ldots, a_p$ dod dažādus atlikumus dalot ar p. Atliek pierādīt, ka $a_1 \neq a_i$ visiem $p \leq i \leq 2$. Pieņemsim

pretējo, tad iegūsim, ka

$$\begin{gathered} a_1 \equiv a_i \pmod p \\ 1 \equiv (i-1)^{-1} \cdot i \pmod p \\ (i-1) \equiv i \pmod p \\ 1 \equiv 0 \pmod p \end{gathered}$$

Pārējā no otrās uz trešo rindu reizinājām abas kongruences abas puses ar $(i-1)$. Iegūtā kongruence ir acīmredzami aplama. Līdz ar to secinām, ka skaitļi $a_1, a_2, \ldots, a_p$ ir pa pāriem dažādi.

7.piemērs Dots nepāra pirmskaitlis $p \geq 3$. Pierādīt, ka eksistē skaitļu $(1, 2, \ldots, p-1)$ permutācija $(x_1, \ldots, x_{p-1})$ ar īpašību, ka $x_1x_2 + x_2x_3 + \cdots + x_{p-2}x_{p-1} \equiv 2 \pmod p$.

Atrisinājums Izvēlēsimies $x_i = (i-1)^{-1} = \frac{1}{i-1}$. Tādā gadījumā

$$\begin{gathered} x_1x_2 + \ldots + x_{p-2}x_{p-1} = \\ = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{(p-2) \cdot (p-1)} \equiv = \\ = \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \ldots + \left(\frac{1}{p-2} - \frac{1}{p-1}\right) = \\ = 1 - \frac{1}{p-1} = \\ = 1 - (p-1)^{-1} \equiv 1 - (p-1) \equiv 2 \pmod p \end{gathered}$$

Pēdējā rindā izmantojām to, ka $\frac{1}{p-1} = (p-1)^{-1}$, jo skaitļa $(p-1)$ inversais elements ir $(p-1)$, jo $(p-1)^2 \equiv 1 \pmod p$. Līdz ar to esam atraduši vajadzīgo permutāciju.

8.piemērs Dots pirmskaitlis p un naturāls skaitlis n. Atrast četrinieku (a_1, a_2, a_3, a_4) skaitu ar īpašību, ka $a_i \in \{0, 1, \ldots, p^n - 1\}$ visiem $i = 1, 2, 3, 4$ un

$$p^n \mid (a_1a_2 + a_3a_4 + 1).$$

Atrisinājums. Apskatīsim vairākus gadījumus

- Ja $p \nmid a_1$, tad a var izvēlēties $p^n - p^{n-1}$ veidos, jo dotajā intervālā eksistē tikai p^{n-1} skaitļi, kuri dalās ar p. Skaitļus a_3, a_4 var izvēlēties patvaļīgi, un to var izdarīt $p^n \cdot p^n = p^{2n}$ veidos. Tādā gadījumā skaitlis a_2 ir unikāls un ir vienāds

$$\begin{gathered} a_1a_2 + a_3a_4 + 1 \equiv 0 \pmod{p^n} \\ a_1a_2 \equiv (-1 - a_3a_4) \pmod{p^n} \\ a_2 \equiv a_1^{-1}(-1 - a_3a_4) \pmod{p^n} \end{gathered}$$

  Līdz ar to šajā gadījumā eksistē $(p^n - p^{n-1}) \cdot p^{2n} = p^{3n-1}(p-1)$ veidi, kā var izvēlēties vajadzīgos skaitļu četriniekus.

- Ja $p \mid a_1$, tad skaitli a_1 var izvēlēties p^{n-1} veidos. Ievērosim, ka neviens no skaitļiem a_3, a_4 nedalās ar p. Pretējā gadījumā $p \nmid a_1a_2 + a_3a_4$ un uzdevuma meklētos četriniekus nevar atrast. Skaitli a_2 var izvēlēties patvaļīgi un to var izdarīt p^n veidos. Skaitli a_3 var izvēlēties $p^n - p^{n-1}$ veidos, taču tādā gadījumā skaitli a_4 var izteikt unikālā veidā:

$$\begin{gathered} a_1a_2 + a_3a_4 + 1 \equiv 0 \pmod{p^n} \\ a_3a_4 \equiv (-1 - a_1a_2) \pmod{p^n} \\ a_4 \equiv a_3^{-1}(-1 - a_1a_2) \pmod{p^n} \end{gathered}$$

Līdz ar to šajā gadījumā eksistē $p^{n-1} \cdot p^n \cdot (p^n - p^{n-1}) = p^{3n-2}(p-1)$ veidi, kā var izvēlēties vajadzīgos skaitļu četriniekus.

Secinām, ka kopā meklēto četrinieku skaits ir vienāds ar

$$p^{3n-1}(p-1) + p^{3n-2}(p-1) = p^{3n} - p^{3n-2}$$

Uzdevums atrisināts.

4 Vilsona teorēma

4.1 Teorijas fakti

Vilsona teorēma. Katram pirmskaitlim p izpildās

$$(p-1)! \equiv -1 \pmod{p}.$$

Pierādījums. Ja $p = 2$, tad $1! \equiv -1 \pmod 2$. Tāpēc turpmāk pieņemam, ka p ir nepāra pirmskaitlis. Aplūkosim nenulles atlikumu inversos elementus pēc p moduļa. Pierādīsim, ka vienīgie atlikumi, kas ir paši sev inversie elementi, ir 1 un -1. Pieņemsim, ka atlikums ir pats sev inversais elements. Tad:

$$a^2 \equiv 1 \pmod{p} \implies (a-1)(a+1) \equiv 0 \pmod{p}.$$

Lai šī kongruence izpildītos, nepieciešams lai kāda no iekavām dalītos ar p, kas iespējams tikai tad, ja $a \equiv \pm 1 \pmod p$.
Aprēķināsim $(p-1)!$ doto atlikumu pēc moduļa p. Aplūkojam reizinājumu $2 \cdot 3 \cdot \ldots \cdot (p-2)$. Tajā ir $p-3$ jeb pāra skaits reizinātāju ($p-3$ ir pāra skaitlis nepāra pirmskaitļiem p). Katram reizinātājam eksistē savs inversais elements, pie tam, ja a inversais elements ir b, tad b inversais elements ir a. Tāpēc reizinātājus var sadalīt pāros, kur katrā pārī skaitļu reizinājums ir $\equiv 1 \pmod p$. Tātad $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p$. Piereizinot 1 un $(p-1) \equiv -1 \pmod p$, iegūsim, ka $(p-1)! \equiv -1 \pmod p$, kas pierāda teorēmu. $\square$

Ja n ir salikts skaitlis, tad $(n-1)! \equiv -1 \mod n$ nevar izpildīties, ja $n > 4$. Tas ir tāpēc, ka var izteikt $n = ab$, kur $1 < a, b < n$. Tad viegli pierādīt, ka atradīsies divi dažādi skaitļi starp skaitļiem $1, 2, \ldots, n-1$, ka viens no tiem dalās ar a un otrs dalās ar b. Tas nozīmē, ka $n \mid (n-1)!$ un kogruence $(n-1)! \equiv -1 \pmod n$ ir aplama.

4.2 Uzdevumu risināšanas piemēri

9. piemērs Dots pirmskaitlis p. Pierādīt, ka $(2p-1)! - p$ dalās ar p^2.

Atrisinājums Ievērosim, ka

$$(2p-1)! - p = p\big((1 \cdot 2 \cdot \ldots \cdot (p-1)) \cdot ((p+1) \cdot (p+2) \cdot \ldots (2p-1)) - 1\big)$$

Ievērosim, ka

$$(p+1) \cdot (p+2) \cdot \ldots \cdot (2p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

Līdz ar to no Vilsona teorēmas izriet, ka

$$\begin{gathered}(1 \cdot 2 \cdot \ldots \cdot (p-1)) \cdot ((p+1) \cdot (p+2) \cdot \ldots (2p-1)) - 1) \equiv \\ \equiv \big((1 \cdot 2 \cdot \ldots \cdot (p-1)) \cdot (1 \cdot 2 \cdot \ldots \cdot (p-1)) - 1\big) \equiv \\ \equiv \big(((p-1)!)^2 - 1\big) \equiv \\ \equiv ((-1)^2 - 1) \equiv 0 \pmod{p}\end{gathered}$$

Tas nozīmē, ka skaitli $(2p-1)! - p$ var izteikt kā divu skaitļu reizinājumu, kur katrs no tiem dalās ar p, līdz ar to viss skaitlis dalās sar p^2, kas arī bija jāpierāda.

10.piemērs Pierādīt, ka skaitlis $712! + 1$ ir salikts skaitlis.

Atrisinājums. Ievērosim, ka 719 ir pirmskaitlis, tāpēc no Vilsona teorēmas izriet, ka:

$$\begin{gathered}
718! \equiv -1 \pmod{719} \\
712! \cdot (713 \cdot \ldots \cdot 718) \equiv -1 \pmod{719} \\
712! \cdot ((-1) \cdot (-2) \cdot \ldots \cdot (-6)) \equiv -1 \pmod{719} \\
712! \cdot 6! \equiv -1 \pmod{719} \\
712! \cdot 720 \equiv -1 \pmod{719} \\
712! \equiv -1 \pmod{719} \\
719 \mid 712! + 1
\end{gathered}$$

Līdz ar to dotais skaitlis nav pirmskaitlis.

11.piemērs Kopa A satur 20 pēc kārtas secīgus veselus skaitļus, kuru summa un reizinājums nedalās ar 23. Pierādīt, ka kopas A elementu reizinājums nav vesela skaitļa kvadrāts.

Atrisinājums. Apzīmēsim kopas A elementus ar $i, i+1, \ldots, i+19$. Ja skaitlis i dalot ar 23 dod atlikumu, kas ir vismaz 4 vai 0, tad acīmredzami, ka kāds no kopas A elementiem dalās ar 23, līdz ar to visu elementu reizinājums dalās ar 23. Tas nozīmē, ka skaitlis i dalot ar 23 dod atlikumu $1, 2$ vai 3. Aplūkosim kopas A elementu summu

$$i + (i+1) + (i+2) + \ldots + (i+19) = \frac{(2i+19)20}{2} = 10(2i+19)$$

Mēģināsim atrast kādiem i kopas A elementu summa dalās ar 23. Tas nozīmē, ka $2i \equiv -19 \pmod{23}$. Reizinot abas kongruences puses ar 12, iegūsim, ka

$$24i \equiv i \equiv -19 \cdot 12 = -228 \equiv -228 + 230 \equiv 2 \pmod{23}$$

Līdz ar to secinām, ka skaitlis i nevar dod atlikumu 2 dalot ar 23. Aplūkosim atlikušos gadījumus:

- Ja skaitlis $i \equiv 1 \pmod{23}$, tad kopas A elementu reizinājums ir vienāds ar $1 \cdot 2 \cdot \ldots \cdot 20 \equiv 20! \pmod{23}$. No Vilsona teorēmas izriet, ka

$$\begin{gathered}
22! \equiv -1 \pmod{23} \\
20! \cdot 21 \cdot 22 \equiv -1 \pmod{23} \\
20! \cdot (-2) \cdot (-1) \equiv -1 \pmod{23} \\
20! \cdot 2 \equiv -1 \pmod{23} \\
20! \cdot 24 \equiv -12 \pmod{23} \\
20! \equiv 11 \pmod{23}
\end{gathered}$$

- Ja skaitlis $i \equiv 3 \pmod{23}$, tad kopas A elementu reizinājums ir vienāds ar $R = 3 \cdot 4 \cdot \ldots \cdot 22 \pmod{23}$. Ievērosim, ka no Vilsona teorēmas izriet, ka

$$\begin{gathered}
22! \equiv -1 \pmod{23} \\
2R \equiv -1 \pmod{23} \\
24R \equiv -12 \pmod{23} \\
R \equiv 11 \pmod{23}
\end{gathered}$$

Abos gadījumos esam ieguvuši, ka kopas A elementu reizinājums ir vienāds ar 11 pēc moduļa 23. Taču viegli pārliecināties, ka naturālu skaitļu kvadrāti dod tikai atlikumus $1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6$ dalot ar 23. Redzam, ka starp tiem nav 11, līdz ar to kopas A elementu reizinājums nav vesela skaitļa kvadrāts.

12.piemērs Pirmskaitlim p ar S_p apzīmēsim kopu $\{1, 2, \ldots, p-1\}$. Atrast visus pirmskaitļus p, kuriem eksistē funkcija $f : S_p \to S_p$ ar īpašību, ka

$$n \cdot f(n) \cdot f(f(n)) - 1 \quad \text{dalās ar} \quad p$$

katram $n \in S_p$.

Atrisinājums. Vispirms pierādīsim sekojošu apgalvojumu.

Apgalvojums. Kopas $\{f(1), f(2), \ldots, f(p)\}$ elementi ir kopas $\{1, 2, \ldots, p\}$ permutācija.
Pierādījums. Pieņemsim pretējo, ka tas tā nav, tad kopā

$$\{f(1), f(2), \ldots, f(p)\}$$

eksistē divi vienādi elementi. Pieņemsim, ka $f(a) = f(b)$, kur $1 \leq a < b \leq p-1$. Tādā gadījumā $f(f(a)) = f(f(b))$. No uzdevuma nosacījumiem izriet, ka

$$p \mid af(a)f(f(a)) - 1 \quad \text{un} \quad p \mid bf(b)f(f(b)) - 1$$

Tas nozīmē, ka

$$\begin{gathered} p \mid af(a)f(f(a)) - 1 - (bf(b)f(f(b)) - 1) \\ p \mid af(a)f(f(a)) - bf(b)f(f(b)) \\ p \mid f(a)f(f(a))(a-b) \end{gathered}$$

Tā kā $p \nmid f(a)$ un $p \nmid f(f(a))$, tad $p \mid a-b$, taču $0 < |a-b| < p-1$, līdz ar to dalāmība nevar izpildīties.

Ievērosim, ka tā kā kopa $\{f(1), f(2), \ldots, f(p-1)\}$ elementi ir kopas $\{1, 2, \ldots, p\}$ permutācija, tad kopas $\{f(f(1)), f(f(2)), \ldots, f(f(p-1))\}$ elementi ir kopas $\{1, 2, \ldots, p-1\}$ permutācija.

No uzdevuma nosacījumiem izriet, ka

$$\begin{gathered} 1 \cdot f(1) \cdot f(f(1)) \equiv 1 \pmod{p} \\ 2 \cdot f(2) \cdot f(f(2)) \equiv 1 \pmod{p} \\ \ldots \\ (p-1) \cdot f(p-1) \cdot f(f(p-1)) \equiv 1 \pmod{p} \end{gathered}$$

Sareizināsim kopā visas $p-1$ dotās kongruences. Ievērosim, ka visu kopas $\{f(1), f(2), \ldots, f(p-1)\}$ un $\{f(f(1)), f(f(2)), \ldots, f(f(p-1))\}$ elementu reizinājums ir tāds pats kā kopas $\{1, 2, \ldots, p-1\}$ reizinājums un abi ir vienādi ar $(p-1)!$. Tas nozīmē, ka

$$\begin{gathered} (p-1)! \cdot (p-1)! \cdot (p-1)! \equiv 1 \pmod{p} \\ (-1)^3 \equiv 1 \pmod{p} \\ -1 \equiv 1 \pmod{p} \\ 2 \equiv 0 \pmod{p} \end{gathered}$$

Pēdējā kongruence izpildās tad un tikai tad, ja $p = 2$. Līdz ar to visiem pirmskaitļiem $p > 2$ funkcija f neeksistē. Priekš $p = 2$ kopa $S_p = \{1\}$ un funkcija $f(1) = 1$ apmierina uzdevuma nosacījumus.

5 Ķīniešu atlikumu teorēma

5.1 Teorijas fakti

Ķīniešu atlikumu teorēma: Doti naturāli skaitļi $m_1, m_2, \ldots, m_k$, kas ir pa pāriem savstarpēji pirmskaitļi. To reizinājumu apzīmējam ar $M = m_1 m_2 \ldots m_k$. Tad jebkurām naturālām vērtībām $(a_1, a_2, \ldots, a_k)$ var atrisināt kongruenču sistēmu

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Tās atrisinājums ir tieši viena kongruenču klase pēc moduļa M.

Nekonstruktīvs pierādījums. Lai parādītu kongruenču sistēmas atrisinājuma eksistenci, ievērojam, ka ikvienu kongruenci $x \equiv b \pmod{M}$ var sadalīt k dažādās kongruencēs – dalot skaitli b ar visiem m_i un apzīmējot dalīšanas atlikumus ar a_i. Šādi definētiem a_i izpildās kongruenču sistēma:

$$\begin{cases} b \equiv a_1 \pmod{m_1} \\ b \equiv a_2 \pmod{m_2} \\ \ldots \\ b \equiv a_k \pmod{m_k} \end{cases}$$

Funkciju, kas no atlikuma b iegūst k atlikumu vektoru $(a_1, a_2, \ldots, a_k)$, apzīmējam ar f:

$$f : \{0, \ldots, M-1\} \mapsto \{0, \ldots, m_1 - 1\} \times \{0, \ldots, m_2 - 1\} \times \ldots \times \{0, \ldots, m_k - 1\}.$$

Pamatojam, ka f ir injektīva – dažādiem b atbilst dažādi vektori $(a_1, \ldots, a_k)$. Pieņemsim no pretējā, ka ir divi dažādi $b' \neq b''$ intervālā $[0; M-1]$, kuriem atbilst viens un tas pats atlikumu vektors $(a_1, \ldots, a_k)$. Atņemam visas kongruences $b' \equiv a_i \pmod{m_i}$ un $b'' \equiv a_i \pmod{m_i}$ vienu no otras. Iegūstam:

$$b' - b'' \equiv 0 \pmod{m_i}.$$

Bet tas nozīmē arī, ka $b' \equiv b'' \pmod{M}$, jo M ir visu m_i reizinājums. Esam ieguvuši pretrunu, jo intervālā $[0; M-1]$ nevar būt divi atšķirīgi skaitļi, kuri ir kongruenti pēc M moduļa.
Pēc Dirihlē principa funkcija f ir arī bijekcija – katram vektoram $(a_1, \ldots, a_k)$ atbilst cits b un var iegūt inverso funkciju f^{-1}, kas ļauj no vektora $(a_1, \ldots, a_k)$ atjaunot b. Šāds pamatojums ir nekonstruktīvs, jo tas neparāda praktisku veidu, kā no $(a_1, \ldots, a_k)$ iegūt kongruenču klasi $b \pmod{M}$. □

Konstruktīvs pierādījums. Aprakstām algebrisku konstrukciju, kā izveidot atlikumu klasi b pēc M moduļa, kas apmierina visas kongruences vienlaikus.
Visiem naturāliem $i \in [1; k]$ apzīmējam:

- $M_i = M/m_i$, t.i. M_i ir visu m_j reizinājums, izņemot pašu m_i.
- $b_i = M_i^{-1} \pmod{m_i}$, t.i. b_i ir skaitļa M_i multiplikatīvi inversais pēc m_i moduļa. Tāds noteikti eksistē, jo visi $m_1, m_2, \ldots, m_k$ ir pa pāriem savstarpēji pirmskaitļi; tāpēc arī m_i un M_i (visu pārējo m_j reizinājums) ir savstarpēji pirmskaitļi.

Šajos apzīmējumos varam rakstīt atrisinājumu:

$$b = (a_1 M_1 b_1 + a_2 M_2 b_2 + \ldots + a_k M_k b_k) \bmod M.$$

Ievērojam, ka ikviens $x \equiv b \pmod{M}$ apmierinās sakarību $x \equiv a_i \pmod{m_i}$. No vienas puses, $M_j \equiv 0 \pmod{m_i}$, ja $j \neq i$. No otras puses, $M_i b_i \equiv 1 \pmod{m_i}$, jo M_i un b_i ir savstarpēji inversi. Visbeidzot, $a_i M_i b_i \equiv a_i \pmod{m_i}$. □

Praksē šo izteiksmi parasti neizmanto, jo nelieliem skaitļiem atlikumu klasi b var sameklēt empīriski, pārlasot elementus – parasti sāk ar lielāko m_i, izraksta visus skaitļus, kas dod vajadzīgo atlikumu a_i, dalot ar m_i. Tad izvēlas nākamo m_j, un no izrakstītajiem skaitļiem atrod to, kurš dod vajadzīgo atlikumu, dalot ar m_j, utt.

5.2 Uzdevumu risināšanas piemēri

Ķīniešu atlikumu teorēma (turpmāk apzīmēta ar CRT) ir noderīgs rīks, ar ko var konstruēt skaitļus, kuriem piemīt noteiktas īpašības. Šīs īpašības bieži vien ir izteiktas ar kongruenču sistēmu. Līdz ar to uzdevumos, kuros ir prasīts pierādīt, kaut kāda skaitļa eksistenci ir vērts aizdomāties, vai to nevar uzkonstruēt ar CRT palīdzību. Ilustrēsim to vairākos piemēros.

13.piemērs Dots naturāls skaitlis n. Pierādīt, ka eksistē n pēc kārtas ejoši naturāli skaitļi ar īpašību, ka
a) katrs no tiem dalās ar kāda vesela skaitļa kvadrātu, kas ir lielāks par 1.
b) neviens no tiem nav vesela skaitļa pakāpe, kas ir lielāka par 1.
c) katrs no tiem dalās ar vismaz 2 atšķirīgiem pirmskaitļiem.

Atrisinājums **a)** Ar $p_1, p_2, \ldots, p_n$ apzīmēsim pirmos n dažādos pirmskaitļus. Aplūkosim sekojošu kogruenču sistēmu

$$\begin{aligned} x+1 &\equiv 0 \pmod{p_1^2} \\ x+2 &\equiv 0 \pmod{p_2^2} \\ x+3 &\equiv 0 \pmod{p_3^2} \\ &\ldots \\ x+n &\equiv 0 \pmod{p_n^2} \end{aligned}$$

No CRT teorēmas šai sistēmai eksistē atrisinājums, jo $\gcd(p_i^2, p_j^2) = 1$ visiem $1 \leq i < j \leq n$. Tādā gadījumā viegli redzēt, ka skaitļi $x+1, x+2, \ldots, x+n$ apmierina uzdevuma nosacījumus.

b) Ar $p_1, p_2, \ldots, p_n$ apzīmēsim pirmos n dažādos pirmskaitļus. Aplūkosim sekojošu kogruenču sistēmu

$$\begin{aligned} x+1 &\equiv p_1 \pmod{p_1^2} \\ x+2 &\equiv p_2 \pmod{p_2^2} \\ x+3 &\equiv p_3 \pmod{p_3^2} \\ &\ldots \\ x+n &\equiv p_n \pmod{p_n^2} \end{aligned}$$

No CRT teorēmas šai sistēmai eksistē atrisinājums, jo $\gcd(p_i^2, p_j^2) = 1$ visiem $1 \leq i < j \leq n$. Ievērosim, ka $x+i$ tādā gadījumā dalās ar p_i, bet nedalās ar p_i^2, kas nozīmē, ka skaitlis $x+i$ nav vesela skaitļa pakāpe, kura ir lielāka par 1, jo pretējā gadījumā skaitlis $x+i$ dalītos vismaz ar p_i^2.

c) Ar $p_1, p_2, \ldots, p_{2n}$ apzīmēsim pirmos $2n$ dažādos pirmskaitļus. Aplūkosim sekojošu kogruenču sistēmu

$$\begin{aligned} x+1 &\equiv 0 \pmod{p_1 p_2} \\ x+2 &\equiv 0 \pmod{p_3 p_4} \\ x+3 &\equiv 0 \pmod{p_5 p_6} \\ &\ldots \\ x+n &\equiv 0 \pmod{p_{2n-1} p_{2n}} \end{aligned}$$

No CRT teorēmas šai sistēmai eksistē atrisinājums, jo $\gcd(p_i p_{i+1}, p_j p_{j+1}) = 1$ visiem $1 \leq i < i+1 < j \leq n$. Tādā gadījumā viegli redzēt, ka skaitļi $x+1, x+2, \ldots, x+n$ apmierina uzdevuma nosacījumus.

14.piemērs Pierādīt, ka katram pirmskaitlim p un veselam skaitlim c var atrast tādu naturālu skaitli x ar īpašību, ka $x^x \equiv c \pmod{p}$.

Atrisinājums. Ja $p \mid c$, tad $x = p$ apmierina uzdevuma nosacījumus. Ievērosim, ja $x \equiv 1 \pmod{p-1}$, tad $x = k(p-1)+1$ un no Mazās Fermā teorēmas izriet, ka

$$x^{k(p-1)+1} = (x^{p-1})^k \cdot x \equiv 1^k \cdot x \equiv x \pmod{p}$$

Līdz ar to mēs būsim atraduši vajadzīgo skaitli x, ja tam piemīt sekojošas īpašības

$$x \equiv 1 \pmod{p-1}$$
$$x \equiv c \pmod{p}$$

No CRT tāds skaitlis x eksistē, jo $\gcd(p, p-1) = 1$. Līdz ar to esam atraduši meklēto skaitli x.

15.piemērs Dots fiksēts pirmskaitlis p. Aplūkosim virkni $a_n = 2^n - n$. Pierādīt, ka virkne satur bezgalīgi daudz locekļus, kas dalās ar p.

Atrisinājums. Līdzīgi kā iepriekšējā uzdevumā viegli pārbaudīt, ka visi n, kuriem izpildās

$$n \equiv 1 \pmod{p-1}$$
$$n \equiv 2 \pmod{p}$$

apmierina uzdevuma nosacījums. No CRT tāds skaitlis n eksistē, jo $\gcd(p, p-1) = 1$. Bet mēs iegūtajam skaitlim varam pieskaitīt skaitļa $p(p-1)$ daudzkārtni un saglabāt visas vajadzīgas īpašības. Tas mums ļauj uzkonstruēt bezgalīgi daudz naturālu skaitļu ar vajadzīgo īpašību.

16.piemērs Doti naturāli skaitļi a, b ar īpašību, ka $b^n + n$ dalās ar $a^n + n$ katram naturālam skaitlim n. Pierādīt, ka $a = b$.

Atrisinājums. Aplūkosim pirmskaitli p ar īpašību, ka $p \nmid a, b$. Ievērosim, ka no uzdevuma nosacījumiem izriet, ka

$$a^n + n \mid b^n + n \implies a^n + n \mid b^n - a^n$$

Vai mēs varam panākt to, ka $a^n + n$ dalās ar mūsu izvēlēto pirmskaitli p? Jā, pietiek atrast n ar īpašību, ka

$$n \equiv 1 \pmod{p-1}$$
$$n \equiv -a \pmod{p}$$

No CRT tāds skaitlis n eksistē, jo $\gcd(p, p-1) = 1$. Līdz ar to esam ieguvuši, ka

$$p \mid a^n + n \quad \text{un arī} \quad a^n + n \mid b^n - a^n$$

Taču mēs izvēlējāmies tādu n, ka $n \equiv 1 \pmod{p-1}$, līdz ar to secinām, ka $0 \equiv a^n - b^n \equiv a - b \pmod{p}$. Citiem vārdiem sakot, ka $p \mid a - b$. Tā kā pirmskaitļu ir bezgalīgi daudz, tad eksistē tāds pirmskaitlis p, ka $p > |a - b|$. Līdz ar to vienīgais veids, kā iegūtā dalāmība var izpildīties, ja $a - b = 0$ jeb $a = b$, kas arī bija jāpierāda.