

LTE lemma

Kims Georgs Pavlovs

1 Ievads

Šajā materiālā mēs aplūkosim Eilera funkciju un teorēmu, kura vispārina iepriekšējā materiālā aplūkoto mazo Fermā teorēmu, kā arī pēdējos gados popularitāti ieguvušo LTE lemmu, kura ļauj spriest par noteikta veida izteiksmju dalāmību ar pirmskaitļiem.

2 Eilera funkcija un teorēma

2.1 Teorijas fakti

Eilera teorēma ir Mazās Fermā teorēmas vispārinājums priekš saliktiem skaitļiem.

Definīcija. $\varphi(n)$ (Eilera funkcija no n) apzīmē, cik ir veselu skaitļu intervālā $[1; n]$, kuri ir savstarpēji pirmskaitļi ar n .

Pārsteidzošā kārtā, lai noteiktu $\varphi(n)$, pietiek zināt skaitļa n kanonisko reprezentāciju.

Apgalvojums. Eilera funkciju katram naturālam n var izrēķināt, izmantojot kādu no trim gadījumiem:

$$\varphi(n) = \begin{cases} p - 1, & \text{ja } n = p \text{ ir pirmskaitlis,} \\ p^{r-1}(p - 1), & \text{ja } n = p^r \text{ ir pirmskaitļa pakāpe,} \\ \varphi(n_1) \cdot \varphi(n_2) \cdot \dots \cdot \varphi(n_k), & \text{ja } n = n_1 n_2 \dots n_k \text{ ir pirmskaitļu pakāpju } n_i \text{ reizinājums.} \end{cases}$$

Pierādījums. Abas pirmās vienādības var pārbaudīt tieši. Katrai pirmskaitļa pakāpei $n = p^r$ tādu skaitļu, kam ir kopīgi dalītāji ar n (un tātad arī ar p), būs tieši $\frac{1}{p}$, jo katrs p -tais skaitlis dalās ar p . Visu atlikušo skaitļu skaits:

$$\varphi(p^r) = p^r \left(1 - \frac{1}{p}\right) = p^{r-1}(p - 1)$$

Ja n ir vairāku pirmskaitļu pakāpju reizinājums, tad izmantojam faktu, ka $\varphi(n)$ ir *multiplikatīva funkcija*: tā definēta visiem naturāliem skaitļiem, pie tam katriem diviem savstarpējiem pirmskaitļiem a, b izpildās $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Interesenti var iepazīties ar pierādījumu, ka $\varphi(n)$ ir multiplikatīva, internetā, bet šajā materiālā tas netiks pierādīts. Ievērosim, ka no pierādītā izriet, ka, ja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ ir skaitļa n kanoniskā reprezentācija, tad

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} (p_2 - 1)p_2^{\alpha_2 - 1} \dots (p_n - 1)p_n^{\alpha_n - 1}$$

Eilera teorēma Katram naturālam m un katram a , kas ir savstarpējs pirmskaitlis ar m , izpildās kongruence

$$a^{\varphi(n)} \equiv 1 \pmod{m}.$$

Eilera teorēma ir noderīga ar to, ka saliktam skaitlim n un skaitlim a , kam $\text{gcd}(a, n) = 1$, var efektīvi izrēķināt skaitļa a pakāpes pēc moduļa n .

Svarīgs rezultāts. Ja doti naturāli skaitļi a, b, n ar īpašību, ka $\gcd(a, n) = 1$. Tādā gadījumā ir spēkā, ka

$$a^b \equiv a^{b \pmod{\varphi(n)}} \pmod{n}$$

Pierādījums. Pieņemsim, ka $b = q\varphi(n) + r$. Tādā gadījumā no Eilera teorēmas izriet, ka

$$a^b = (a^{\varphi(n)})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}$$

Ievērosim, ka $r \equiv b \pmod{\varphi(n)}$, kas pierāda prasīto.

Šis rezultāts būs noderīgs daudzos uzdevumos.

2.2 Uzdevumu risināšanas piemēri

1.piemērs. Dots naturāls skaitlis $n \geq 3$. Pierādīt, ka

$$1989 \mid n^{n^{n^n}} - n^{n^n}$$

Atrisinājums. Sadalām pirmreizinātājos: $1989 = 3^2 \cdot 13 \cdot 17$. Pierādīsim dalāmību katram no pirmreizinātājiem atsevišķi, jo tad acīmredzami izteiksme dalīsies ar to reizinājumu.

- Vispirms pierādīsim $n^{n^{n^n}} \equiv n^{n^n} \pmod{9}$ visiem naturāliem $n \geq 3$. Ja $3 \mid n$, tad acīmredzami kongruence izpildās. Pretējā gadījumā varētu pierādīt kāpinātāju kongruenci pēc $\phi(9) = 6$, tātad jāpierāda $n^{n^n} \equiv n^n \pmod{6}$, jo tad no Eilera teorēmas varētu sākotnējo izteiksmi vienkāršot uz vienu un to pašu atlikumu. Līdzīgi varam reducēt vēlamo tālāk ar $\phi(6) = 2$, tas ir, pierādīt, ka $n^n \equiv n \pmod{2}$. Taču šī kongruence acīmredzami izpildās, tādēļ, atpakaļgaitā spriežot, varam secināt, ka $n^{n^{n^n}} \equiv n^{n^n} \pmod{9}$.
- Tālāk pierādīsim, ka $n^{n^{n^n}} \equiv n^{n^n} \pmod{13}$. Veicam spriedumus līdzīgā veidā. Ja $13 \mid n$, tad kongruence izpildās; citādi $\phi(13) = 12$, tāpēc vēlamies pierādīt, ka $n^{n^n} \equiv n^n \pmod{12}$. Ievērosim, ka šai kongruencei jāizpildās pēc moduļa 3 un moduļa 4 – tā kā $\gcd(3, 4) = 1$, tad pietiek pierādīt šīs divas mazākās kongruences. Ievērosim, ka $\phi(4) = \phi(3) = 2$, tāpēc jāpierāda $n^n \equiv n \pmod{2}$, kas acīmredzami izpildās.
- Visbeidzot pierādīsim, ka $n^{n^{n^n}} \equiv n^{n^n} \pmod{17}$. Ja $17 \mid n$, tad vajadzīgais izpildās. Pretējā gadījumā $\phi(17) = 16$, tāpēc būtu jāpierāda $n^{n^n} \equiv n^n \pmod{16}$. Ja $n \geq 3$ ir pāra, tad minētā kongruence izpildās. Aplūkojam gadījumu, ja n ir nepāra. Tad $\phi(16) = 8$, un mēs gribētu pierādīt $n^n \equiv n \pmod{8}$. Ievērosim, ka visiem nepāra skaitļiem izpildās $n^2 \equiv 1 \pmod{8}$, tādēļ $n^{n-1} \equiv 1 \pmod{8}$ un attiecīgi $n^n \equiv n \pmod{8}$, kas dod vēlamo.

Esam pierādījuši, ka prasītā izteiksme dalās ar katru no skaitļa 1989 pirmreizinātājiem (kur ņemta vērā arī pakāpe), tādēļ tā dalās ar 1989.

2.piemērs Pierādīt, ka katram fiksētam naturālam skaitlim n virkne

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \dots \pmod{n}$$

kaut kādā brīdī kļūst konstanta.

Atrisinājums. Definējam skaitļu virkni, ko veido daudzstāvu pakāpes:

$$b_1 = 2, \text{ un } b_{m+1} = 2^{b_m}, \text{ ja } m \geq 1.$$

Pamatojam apgalvojumu ar indukciju.

Bāze $n = 1$. Visiem b_m izpildās $b_m \equiv 0 \pmod{1}$.

Induktīvais pieņēmums. Pieņemsim, ka apgalvojums izpildās **visiem** naturāliem $n \in [1; k]$ līdz kādam skaitlim k . (Dažreiz to sauc par *strong induction*, lai atšķirtu no induktīvās pārejas $k \rightarrow k + 1$.)

Pāreja $[1; k] \rightarrow k + 1$. Pamatosim, ka apgalvojums izpildās arī pie $n = k + 1$. Šķirojam gadījumus:

- Ja $k + 1$ ir nepāra, aprēķinām $\varphi(k + 1)$. Tas ir naturāls skaitlis un pieder intervālam $[1; k]$. Izmantojam induktīvo pieņēmumu un sagaidām brīdi, kad atlikumu virkne pēc $\varphi(k + 1)$ moduļa kļūst konstanta, t.i. $b_{m+1} \equiv b_m \pmod{\varphi(k + 1)}$. Pēc Eilera teorēmas arī $2^{b_{m+1}} \equiv 2^{b_m} \pmod{k + 1}$ jeb $b_{m+2} \equiv b_{m+1} \pmod{k + 1}$, t.i. virkne kļūst konstanta arī pēc $k + 1$ moduļa.
- Ja $k + 1$ ir pāra, izsakām to kā divnieka pakāpes un nepāra skaitļa u reizinājumu $k + 1 = 2^v \cdot u$. Arī $\varphi(u) \in [1; k]$ un var lietot induktīvo pieņēmumu – sagaidīt brīdi, kad $b_{m+1} \equiv b_m \pmod{\varphi(u)}$. Tad pēc Eilera teorēmas līdzīgi kā iepriekš $b_{m+2} \equiv b_{m+1} \pmod{u}$. Ja divnieka kāpinātājs v izteiksmē $2^v \cdot u$ ir liels, tad var gadīties, ka b_{m+1} vai b_{m+2} vēl nedalās ar 2^v . Bet, palielinot m vērtību, virknes b_i locekļi sāks dalīties ar jebkuru divnieka pakāpi, tāpēc izpildīsies arī $b_{m+2} \equiv b_{m+1} \pmod{k + 1}$.

3.piemērs Pierādīt, ka, ja n ir salikts skaitlis, tad

$$\varphi(n) \leq n - \sqrt{n}$$

Atrisinājums. Šķirosim gadījumus:

- Ja n ir pirmskaitļa pakāpe p^k , tad no Apgalvojuma nodaļā 2.1 zināms, ka $\varphi(n) = p^k - p^{k-1}$. Jāpārbauda, vai izpildās novērtējums: $\varphi(n) = n - \sqrt{n}$ jeb $p^k - p^{k-1} \leq p^k - p^{k/2}$. Pēc noīsināšanas: $p^{k/2} \leq p^{k-1}$ jeb (logaritmējot abas puses pēc bāzes p) $k/2 \leq k - 1$. Tā ir patiesība, jo $k \geq 2$.
- Ja n nav pirmskaitļa pakāpe, tad to var izteikt $n = ab$, kur a, b ir savstarpēji pirmskaitļi, $a, b > 1$. Eilera funkcija $\varphi(n)$ nepārsniedz skaitļu skaitu intervālā $[1; n]$, kas nedalās ne ar a , ne ar b . Ar skaitli a dalās tieši b skaitļi; ar skaitli b dalās tieši a skaitļi; ar abiem dalās 1 skaitlis (pats n). Pēc ieslēgšanas-izslēgšanas principa:

$$\varphi(ab) \leq ab - a - b + 1.$$

Pārbaudīsim vai lielums $ab - a - b + 1$ nepārsniedz $n - \sqrt{n}$. Izrakstīsim vairākas nevienādības, kuru patiesums vēl jāpārbauda (apzīmētas ar $\leq^?$):

$$\begin{aligned} ab - a - b + 1 &\leq^? ab - \sqrt{ab}, \\ \sqrt{ab} &\leq^? a + b - 1, \\ \sqrt{ab} + \left(\frac{a+b}{2} - \sqrt{ab}\right) &\leq^? a + b - 1, \\ \frac{a+b}{2} &\leq^? a + b - 1, \\ a + b &\leq^? 2a + 2b - 2, \\ 2 &\leq a + b. \end{aligned}$$

Trešā rinda iegūta, pieskaitot mazākajai pusei nenegatīvu skaitli – vidējā aritmētiskā un vidējā ģeometriskā starpību. Pēdējā nevienādība ir pareiza, jo $a, b > 1$, no tās seko visas iepriekšējās.

3 Orderis

3.1 Teorijas fakti

Ja mēs aplūkojam virkni $a, a^2, a^3, \dots \pmod{n}$, kur $\gcd(a, n) = 1$, tad Eilera teorēma vai Mazā Fermā teorēma pasaka, ka šajā virknē eksistē skaitlis 1, taču bieži vien ir vērts zināt, kad tieši pirmo reizi parādās skaitlis 1, kas motivē ieviest ordera konceptu.

Definīcija. Doti naturāli skaitļi a, m ar īpašību, ka $\gcd(a, m) = 1$. Par skaitļa a orderi pēc moduļa m sauc mazāko naturālo skaitli k ar īpašību, ka $a^k \equiv 1 \pmod{m}$. Parasti apzīmē $k = \text{ord}_m a$

Vispirms aplūkosim pāris skaitliskus piemērus:

- Katram naturālam m : $\text{ord}_m(1) = 1$.
- Katram naturālam m : $\text{ord}_m(-1) = 2$.
- $\text{ord}_7(2) = \text{ord}_7(4) = 3$, jo $(2^1, 2^2, 2^3) \equiv (2, 4, 1) \pmod{7}$ un $(4^1, 4^2, 4^3) \equiv (4, 2, 1) \pmod{7}$.
- Ja $m = 5$, tad $\text{ord}_5(2) = 4$, jo $(2^1, 2^2, 2^3, 2^4) \equiv (2, 4, 3, 1) \pmod{5}$.

Lemma par orderi. Doti naturāli skaitļi a, m ar īpašību, ka $\gcd(a, m) = 1$ un $k = \text{ord}_m a$. Ja kaut kādam naturālam skaitlim b izpildās $a^b \equiv 1 \pmod{m}$, tad $k \mid b$.

Pierādījums. Pieņemsim pretējo, ka $k \nmid b$, tad eksistē tāds naturāli skaitļi q un r ar īpašību, ka $b = kq + r$, kur $0 < r < k$. Ievērosim, ka no dotā izriet, ka

$$1 \equiv a^b \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{m}$$

Bet tādā gadījumā mēs esam atraduši mazāku naturālu skaitli par k , kuram izpildās $a^r \equiv 1 \pmod{m}$, kas ir pretrunā ar ordera definīciju.

Olimpiādē var izmantot šo lemmu bez pierādījuma, atsaucoties uz to, kā uz lemma par orderi. Skolēniem bieži vien ir grūti saprast, kādos uzdevumos un kāpēc ir jāizmanto orderis, tāpēc šeit ir pāris vispārīgi padomi. Galvenokārt, tas noder uzdevumos, kuros parādās izteiksmes $a^n - 1, a^n + 1, a^n - b^n, a^n + b^n$. Ja mums ir dota izteiksme, $d \mid a^c \pm b^c$, tad ar ordera palīdzību mēs varam pateikt kaut ko par skaitļa d pirmreizinātāju struktūru vai īpašībām, kas savukārt var mums pateikt kādas globālas īpašības pieder skaitlim d . Tas tiks ilustrēts vairākos piemēros. Bet pirms tam aplūkosim vēl vienu svarīgu konceptu.

Definīcija. Dots pirmskaitlis p . Par primitīvo sakni sauc tādu atlikumu g pēc moduļa p , ka $\text{ord}_p g = p - 1$.

Primītīva sakne pēc jebkura pirmskaitļa moduļa eksistē un to var olimpiādē izmantot bez pierādījuma. Šajā materiālā tas netiks pierādīts, bet nākamā lemma ir noderīgāks veids, kā izmantot primitīvo sakni olimpiāžu uzdevumos.

Lemma par primitīvo sakni Ja g ir primitīvā sakne pēc moduļa p , tad skaitļu kopa $\{g, g^2, \dots, g^{p-1}\}$ pēc moduļa p ir kopas $\{1, 2, \dots, p-1\}$ permutācija.

Pierādījums. Mums pietiek pierādīt, ka kopas $\{g, g^2, \dots, g^{p-1}\}$ ir pa pāriem dažādi. Pieņemsim pretējo, ka tas tā nav, tad eksistē divi indeksi $i \neq j$ ar īpašību, ka

$$g^i \equiv g^j \pmod{p} \implies g^{i-j} \equiv 1 \pmod{p}$$

Taču $0 < |i - j| < p - 1$, kas ir pretrunā ar to, ka $p - 1 = \text{ord}_p g$.

Izmantojot lemmu par primitīvo sakni varam pierādīt Vilsona teorēmu, kura apgalvo, ka $(p - 1)! \equiv -1 \pmod{p}$. Aplūkosim primitīvo sakni g pēc moduļa p . No lemmas par primitīvo sakni izriet, ka kopas $\{g, g^2, \dots, g^{p-1}\}$ elementi pēc moduļa p ir kopas $\{1, 2, \dots, p - 1\}$ permutācija. Tas nozīmē, ka abu kopu visu elementu reizinājums pēc moduļa p ir vienāds, līdz ar to

$$\begin{aligned} (p - 1)! &\equiv g \cdot g^2 \cdot \dots \cdot g^{p-1} \equiv \\ &\equiv g^{1+2+\dots+(p-1)} \equiv \\ &\equiv g^{\frac{p(p-1)}{2}} \equiv \\ &\equiv (g^{\frac{p-1}{2}})^p \equiv \\ &\equiv (-1)^p \equiv -1 \pmod{p} \end{aligned}$$

Pēdējā rindā mēs izmantojam to, ka $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, taču tas nevar būt vienāds ar 1, jo tas būtu pretrunā ar primitīvas saknes definīciju, līdz ar to $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Tas pierāda Vilsona teorēmu.

3.2 Uzdevumu risināšanas piemēri

1.piemērs Dots naturāls skaitlis $n \geq 2$. Pierādīt, ka skaitlis n nedala skaitli **a)** $2^n - 1$ **b)** $3^n - 2^n$

Atrisinājums. **a)** Pieņemsim pretējo, ka skaitlis n dala skaitli $2^n - 1$. Tas nozīmē, ka $2^n \equiv 1 \pmod{n}$. Aplūkosim mazāko pirmskaitli p , ar ko dalās skaitlis n . Ievērosim, ka

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

No Mazās Fermā teorēmas izriet, ka $2^{p-1} \equiv 1 \pmod{p}$. Aplūkosim $k = \text{ord}_p 2$ (ievērosim, ka $\text{gcd}(2, p) = 1$, līdz ar to tas eksistē). No lemmas par orderi izriet, ka $k \mid n$ un $k \mid p - 1$. Ievērosim, ka $k \leq p - 1 < p$, kas nozīmē, ja $k > 1$, tad esam atraduši mazāko naturālu skaitli par p ar īpašību, ka $k \mid n$ – pretruna ar p minimalitāti. Līdz ar to $k = 1$, kas nozīmē $1 \equiv 2^k \equiv 2^1 \pmod{p}$, kas neizpildās nevienam pirmskaitlim p .

b) Pieņemsim pretējo, ka skaitlis n dala skaitli $3^n - 2^n$. Tas nozīmē, ka $3^n \equiv 2^n \pmod{n}$. Aplūkosim mazāko pirmskaitli p , ar ko dalās skaitlis n . Tādā gadījumā

$$p \mid n \mid 3^n - 2^n \implies 3^n \equiv 2^n \pmod{p} \implies (3 \cdot 2^{-1})^n \equiv 1 \pmod{p}$$

Pēdējā solī mēs pareizinājam abas kongruences puses ar skaitļa 2 inverso elementu n tajā pakāpē, tas ir, skaitli $(2^{-1})^n$. Aplūkosim $k = \text{ord}_p(3 \cdot 2^{-1})$. No Mazās Fermā teorēmas izriet, ka $(3 \cdot 2^{-1})^{p-1} \equiv 1 \pmod{p}$. No lemmas par orderi izriet, ka $k \mid p - 1$ un $k \mid n$. Ievērosim, ka $k \leq p - 1 < p$, kas nozīmē, ja $k > 1$, tad esam atraduši mazāko naturālu skaitli par p ar īpašību, ka $k \mid n$ – pretruna ar p minimalitāti. Līdz ar to $k = 1$, kas nozīmē

$$1 \equiv (3 \cdot 2^{-1})^k \equiv (3 \cdot 2^{-1}) \pmod{p} \implies 3 \equiv 2 \pmod{p},$$

kas neizpildās nevienam pirmskaitlim p .

Piezīme. Šis ir ilustratīvs piemērs, kurā parādās ordera noderīgums. No lemmas par orderi izriet, ka $k \mid n$ un $k \mid p - 1$, kas pasaka ļoti daudz par pirmreizinātāja p īpašībām. Konkrētāk, ja p ir mazākais pirmreizinātājs, tad iegūtās sakarības pierāda tā neeksistenci. Atzīmēsim, ka **b)** daļā ir svarīgi pareizināt ar inverso elementu, lai panāktu to, ka kongruences labajā pusē ir 1, citādi nevar pielietot lemmu par orderi.

2.piemērs Pierādīt, ka neeksistē naturāls skaitlis $n > 1$ ar īpašību, ka $n \mid 2^{n-1} + 1$.

Atrisinājums. Pieņemsim pretējo, ka eksistē tāds naturāls skaitlis n ar īpašību, ka $n \mid 2^{n-1} + 1$. Tas nozīmē, ka

$$2^{n-1} \equiv -1 \pmod{n} \implies 2^{2(n-1)} \equiv 1 \pmod{n}$$

Pēdēja solī mēs kāpinājām abas kongruences puses kvadrātā. Tas tika darīts ar mērķi, lai mēs varētu pielietot lemmu par orderi kaut kādā brīdī, jo priekš tās mums ir vajadzīgs, lai skaitļa pakāpe ir kongruenta ar 1, nevis -1 pēc kaut kāda moduļa. Aplūkosim patvaļīgu skaitļa n pirmreizinātāju (ne obligāti mazāko). Tādā gadījumā

$$2^{2(n-1)} \equiv 1 \pmod{p} \quad \text{un} \quad 2^{p-1} \equiv 1 \pmod{p}$$

Apzīmēsim $d = \text{ord}_p 2$, tad no lemmas par orderi izriet, ka $d \mid p - 1$ un $d \mid n - 1$.

Apgalvojums. Izpildās $\nu_2(d) = \nu_2(n - 1) + 1$.

Pierādījums. Ievērosim, ka no uzdevuma nosacījumiem izriet, ka n ir nepāra skaitlis, līdz ar to pirmskaitlis p arī ir nepāra. Aplūkosim skaitļa $n - 1$ kanonisko reprezentāciju, tas ir

$$n - 1 = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Tā kā $d \mid n - 1$, tad skaitli d var uzrakstīt formā

$$d = 2^{\beta_0} p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

kur $\beta_i \leq \alpha_i$ katram $1 \leq i \leq k$ un $0 \leq \beta_0 \leq \alpha_0 + 1$. Pieņemsim, ka $\beta_0 \neq \alpha_0 + 1$, tad $0 \leq \beta_0 \leq \alpha_0$. No ordera definīcijas izriet, ka

$$2^d \equiv 1 \pmod{p} \implies 2^{n-1} \equiv 1 \pmod{p},$$

kur pēdējā solī mēs kāpinājām abas puses kongruences puses pakāpē $2^{\gamma_0} p_1^{\gamma_1} \dots p_k^{\gamma_k}$, kur $\gamma_i = \alpha_i - \beta_i$ visiem $0 \leq i \leq k$. Taču no uzdevuma nosacījumiem $2^{n-1} \equiv -1 \pmod{p}$, kas ir pretruna gadījumos, kad $p \neq 2$. Līdz ar to secinām, ka $\beta_0 = \alpha_0 + 1$, kas nozīmē, ka $\nu_2(d) = \nu_2(n - 1) + 1$.

No lemmas par orderi izriet, ka $d \mid p - 1$, kas nozīmē, ka $2^{\nu_2(n-1)+1} \mid p - 1$ jeb $p \equiv 1 \pmod{2^{\nu_2(n-1)+1}}$. Tā kā tas izpildās visiem skaitļa n pirmreizinātājiem, tad secinām, ka $n \equiv 1 \pmod{2^{\nu_2(n-1)+1}}$, kas nozīmē, ka

$$2^{\nu_2(n-1)+1} \mid n - 1,$$

kas ir pretrunā ar valuācijas definīciju.

Piezīme. Vēl viens ilustratīvs piemērs, kurā mums orderis palīdzēja pateikt kaut ko par skaitļa n pirmreizinātājiem – konkrētāk to, ka viņi ir 1 pēc moduļa $2^{\nu_2(n-1)+1}$. Tas savukārt mums ļauj pateikt globāli kaut ko par skaitli n , jo mēs zinām vienu konkrētu lietu par katra tā pirmreizinātāju. Ievērosim, ka uzdevuma sākumā ir jāizkāpina abas puses kvadrātā, lai panāktu, ka kongruences labajā pusē ir 1, citādi nevar pielietot lemmu par orderi.

3.piemērs Sauksim naturālu skaitli n par *latvisku*, ja var atrast tādu naturālu skaitli m un pirmskaitļus $1 < p < q$, ka $q - p \mid m$ un

$$\begin{aligned} p &\mid n^m + 1 \\ q &\mid n^m + 1. \end{aligned}$$

Atrast visus n , kas ir *latviski*.

Atrisinājums. Pierādīsim, ka visi nepāra skaitļi $n > 1$ ir *latviski*. Izvēlēsimies $p = 2$ un kaut kādu nepāra pirmskaitli q ar īpašību, ka $q \mid n^2 + 1$. Tāds eksistē, jo $n^2 + 1 \equiv 2 \pmod{4}$, līdz ar to skaitlis $n^2 + 1$ nav divnieka pakāpe. Piedevām paņemsim, ka $m = 2(q - 2)$, tad viegli redzēt, ka

$$n^2 \equiv -1 \pmod{q} \implies n^{2(q-2)} \equiv (-1)^{q-2} \equiv -1 \pmod{q} \implies q \mid n^m + 1$$

Savukārt tā kā n ir nepāra skaitlis, tad $2 \mid n^m + 1$, līdz ar to secinām, ka visi nepāra $n > 1$ ir *latviski*. Ja $n = 1$, tad vienīgie iespējamie pirmskaitļi ir $p = q = 2$, kas neizpilda uzdevuma nosacījumus, tādēļ šī vērtība neder.

Tagad aplūkosim gadījumu, kad n ir pāra skaitlis, tad $n^m + 1$ ir nepāra skaitlis, līdz ar to p un q ir nepāra pirmskaitļi. Ievērosim, ka

$$n^m \equiv -1 \pmod{p} \implies n^{2m} \equiv 1 \pmod{p}$$

Apzīmēsim $d = \text{ord}_p n$ (mazākais naturālais skaitlis d , kam izpildās $n^d \equiv 1 \pmod{p}$), tad mēs zinām, ka, tā kā $n^{p-1} \equiv 1 \pmod{p}$, tad $d \mid 2m$ un $d \mid p - 1$.

Pierādīsim, ka d nevar būt m dalītājs. Pieņemsim, ka tas tā ir, tad eksistē naturāls skaitlis k ar īpašību, ka $dk = m$, līdz ar to

$$n^d \equiv 1 \pmod{p} \implies -1 \equiv n^m = n^{dk} = 1^k \equiv 1 \pmod{p} \implies 2 \equiv 0 \pmod{p} \implies p = 2,$$

kas ir acīmredzama pretruna. Līdz ar to d nav m dalītājs, taču $d \mid 2m$, kas nozīmē $\nu_2(d) = \nu_2(2m) = \nu_2(m) + 1$. Tā kā $d \mid p - 1$, tad secinām, ka $\nu_2(p - 1) \geq \nu_2(m) + 1$ (šeit ar $\nu_2(n)$ tiek apzīmēta augstākā skaitļa 2 pakāpe, ar ko dalās n , jeb t.s. valuācija).

Veicot analogiskus spriedumus, varam iegūt, ka $\nu_2(q - 1) \geq \nu_2(m) + 1$. Tādā gadījumā secinām, ka

$$\nu_2(q - p) = \nu_2(q - 1 - (p - 1)) \geq \min(\nu_2(q - 1), \nu_2(p - 1)) \geq \nu_2(m) + 1.$$

No otras puses mēs zinām, ka, tā kā $q - p \mid m$, tad $\nu_2(m) \geq \nu_2(q - p) \geq \nu_2(m) + 1$, kas ir pretruna.

4.piemērs Pierādīt, ka visiem naturāliem skaitļiem $a > 1$ un n izpildās, ka $n \mid \varphi(a^n - 1)$

Atrisinājums. Ievērosim, ka $\text{gcd}(a^n - 1, a) = 1$, tāpēc varam aplūkot $\text{ord}_{a^n - 1}(a) = r$. Tā kā $a^n - 1 \equiv 0 \pmod{a^n - 1}$, tad $r \leq n$. Pieņemsim, ka $r < n$. Tādā gadījumā $a^r - 1 \equiv 0 \pmod{a^n - 1}$. Ņemot vērā, ka $a > 1$, tad izpildās $0 < a^r - 1 < a^n - 1$, kas dod pretrunu ar kongruenci. Tā kā $r \leq n$, vienīgā iespēja ir $r = n$ jeb $\text{ord}_{a^n - 1}(a) = n$.

Aplūkojam $a^{\phi(a^n - 1)} \equiv 1 \pmod{a^n - 1}$ pēc Eilera teorēmas. No ordera īpašībām mums ir zināms, ka $\text{ord}_{a^n - 1}(a) \mid \phi(a^n - 1)$. Tā kā $\text{ord}_{a^n - 1}(a) = n$, secinām, ka $n \mid \phi(a^n - 1)$, kas dod prasīto.

5.piemērs Pierādīt, ka pirmskaitlim p :

$$1^n + 2^n + \dots + (p-1)^n \pmod{p} \equiv \begin{cases} -1, & \text{ja } p-1 \mid n \\ 0, & \text{atlikušajos gadījumos} \end{cases}$$

Atrisinājums. Sākotnēji aplūkojam gadījumu $p-1 \mid n$ jeb $n = k(p-1)$. Tādā gadījumā katram $1 \leq i \leq p-1$ saskaitāmais $i^n \equiv (i^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}$ no mazās Fermā teorēmas. Kopā ir $p-1$ saskaitāmie, tādēļ to summa būs $1+1+\dots+1 = p-1 \equiv -1 \pmod{p}$, kas pierāda prasīto šim gadījumam.

Tālāk aplūkosim gadījumu, kad $p-1 \nmid n$. Tā kā p ir pirmskaitlis, tad eksistē primitīvā sakne g pēc moduļa p . Atcerēsimies no primitīvās saknes īpašībām, ka g, g^2, \dots, g^{p-1} pieņem visus nenulles atlikumus pēc moduļa p , pie tam katru tieši vienu reizi. Tādēļ pārrakstīsim prasītajā summā dotos saskaitāmos kā $g^n, g^{2n}, \dots, g^{(p-1)n}$ kaut kādā secībā. Tad no ģeometriskās progresijas formulām

$$1^n + 2^n + \dots + (p-1)^n = g^n + g^{2n} + \dots + g^{(p-1)n} = g^n + (g^n)^2 + \dots + (g^n)^{p-1} = \frac{g^n(g^{(p-1)n} - 1)}{g^n - 1}.$$

Ievērosim, ka $p-1 \nmid n$, tādēļ $n \equiv r \pmod{p-1}$, kur $1 \leq r < p-1$, kas nozīmē, ka $g^n \equiv g^r \not\equiv 1 \pmod{p}$ no primitīvās saknes definīcijas, tādēļ $g^n - 1$ nedalās ar p .

Toties $g^{(p-1)n} \equiv (g^{p-1})^n \equiv 1^n \equiv 1 \pmod{p}$, tātad $g^{(p-1)n} - 1$ dalās ar p . No tā varam secināt, ka iegūtā ģeometriskās progresijas summa dalās ar p un attiecīgi arī uzdevumā prasītā izteiksme dalās ar p jeb dod atlikumu 0.

4 LTE lemma

4.1 Teorijas fakti

LTE lemma ir noderīgs rīks, ar kura palīdzību mēs varam noteikt $\nu_p(a^n \pm b^n)$, ja izpildās kaut kādi nosacījumi.

LTE lemma priekš nepāra pirmskaitļa. Dots nepāra pirmskaitlis p un veseli skaitļi a, b ar īpašību, ka $p \nmid a$ un $p \nmid b$.

- Ja $p \mid a - b$, tad katram naturālam skaitlim n ir spēkā, ka

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n)$$

- Ja $p \mid a + b$, tad katram **nepāra** skaitlim n ir spēkā, ka

$$\nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n)$$

Līdzīgs rezultāts izpildās arī priekš $p = 2$.

LTE lemma priekš $p = 2$. Doti veseli skaitļi a, b ar īpašību, ka $2 \nmid a, 2 \nmid b$.

- Katram **pāra** skaitlim n ir spēkā, ka

$$\nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(a + b) + \nu_2(n) - 1$$

- Katram **nepāra** skaitlim n ir spēkā, ka

$$\nu_2(a^n - b^n) = \nu_2(a - b)$$

- Katram **pāra** skaitlim n ir spēkā, ka

$$\nu_2(a^n + b^n) = 1$$

- Katram **nepāra** skaitlim n ir spēkā, ka

$$\nu_2(a^n + b^n) = \nu_2(a + b)$$

Šie rezultāti netiks pierādīti, bet interesenti var iepazīties ar to pierādījumiem internetā. Šos rezultātus var izmantot olimpiādēs bez pierādījuma, bet atsaucoties uz tiem kā LTE lemmu.

No pirmā acu uzmetiena liekas, ka ir daudz formulu, kuras ir jāgaumē. Īstenībā pēdējās trīs formulas, var viegli iegūt olimpiādē, ja ir piemirsušās, izmantojot smadzeņu pamatdarbības principus.

Ja n ir nepāra skaitlis un a, b ir nepāra skaitļi, tad

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

Ievērosim, ka otrs pirmreizinātājs sastāv no n nepāra skaitļu summas, līdz ar to ir nepāra. Tas nozīmē, ka

$$\nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) = \nu_2(a - b),$$

kas arī bija jāpierāda.

Ja n ir pāra skaitlis un a, b ir nepāra skaitļi, tad $a^n \equiv 1 \pmod{4}$ un $b^n \equiv 1 \pmod{4}$, kas nozīmē, ka $a^n + b^n \equiv 2 \pmod{4}$ jeb $\nu_2(a^n + b^n) = 1$.

Ja n ir nepāra skaitlis un a, b ir nepāra skaitļi, tad

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1})$$

Ievērosim, ka otrs pirmreizinātājs sastāv no n nepāra skaitļu summas, līdz ar to ir nepāra. Tas nozīmē, ka

$$\nu_2(a^n + b^n) = \nu_2(a + b) + \nu_2(a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1}) = \nu_2(a + b),$$

kas arī bija jāpierāda.

Līdz ar to, izmantojot smadzeņu pamatdarbības principus, olimpiādē varam ātri iegūt pēdējās 3 sakarības. Savukārt pirmās trīs sakarības ir jāiemācās no galvas.

LTE lemmai nav pielietojums tikai olimpiāžu matemātikā, bet arī skaitļošanā un programmēšanā. Piemēram, lai izrēķinātu, ar kādu lielāko pirmskaitļa 3 pakāpi dalās skaitlis $4^{54} - 1$, tad var lietot LTE lemmu, jo $3 \nmid 4$, $3 \nmid 1$ un $3 \mid 4 - 1$, iegūstot

$$\nu_3(4^{54} - 1) = \nu_3(4 - 1) + \nu_3(54) = 1 + 3 = 4.$$

Interesenti šajā video var iepazīt programmēšanas olimpiādes uzdevumu, kurā noderēja LTE lemma.

4.2 Uzdevumu risināšanas piemēri

Tagad apskatīsim piemērus, kuros vēlams lietot LTE lemmu. Pirms ķeraties klāt uzdevumu izpētei, lūdzu pārliecinieties, ka Jums ir laba izpratne par orderi un tā izmantošanu.

1.piemērs Dots naturāls skaitlis x un nepāra pirmskaitlis p . Pierādīt, ka visi skaitļa $\frac{x^p-1}{x-1}$ pirmreizinātāji ir $\equiv 1 \pmod{p}$ vai arī vienādi ar p .

Atrisinājums. Aplūkosim pirmskaitli q ar īpašību, ka $q \mid \frac{x^p-1}{x-1}$. Tādā gadījumā $q \mid x^p - 1$, kas nozīmē, ka

$$x^p \equiv 1 \pmod{q} \quad \text{un} \quad x^{q-1} \equiv 1 \pmod{q}$$

Apzīmēsim ar $d = \text{ord}_q x$. Tādā gadījumā no lemmas par orderi izriet, ka $d \mid p$ un $d \mid q - 1$. Tā kā $d \mid p$, tad $d = 1$ vai $d = p$. Ja $d = p$, tad esam ieguvuši, ka $p \mid q - 1$, kas nozīmē, ka $q \equiv 1 \pmod{p}$.

Aplūkosim gadījumu, kad $d = 1$. Tādā gadījumā $x^d \equiv x \equiv 1 \pmod{q}$ jeb, citiem vārdiem sakot, $q \mid x - 1$. Tas nozīmē, ka mēs varam pielietot LTE lemmu

$$\begin{aligned} \nu_q \left(\frac{x^p - 1}{x - 1} \right) &= \\ &= \nu_q(x^p - 1) - \nu_q(x - 1) = \\ &= \nu_q(x - 1) + \nu_q(p) - \nu_q(x - 1) = \\ &= \nu_q(p) \end{aligned}$$

Taču mēs aplūkojam tādu pirmskaitli q , ka $q \mid \frac{x^p-1}{x-1}$, kas nozīmē, ka $\nu_q \left(\frac{x^p-1}{x-1} \right) = \nu_q(p) \geq 1$. Tas var izpildīties tad un tikai tad, ja $q = p$, kas arī bija jāpierāda.

Piezīme. Ievērosim, ka šajā uzdevumā ir prasīts pierādīt par skaitļa $\frac{x^p-1}{x-1}$ pirmreizinātāju struktūru vai īpašībām, līdz ar to bija vērts apskatīt orderi. Vienā no gadījumiem ieguvām prasīto, taču otrā gadījumā ieguvām, ka $q \mid x - 1$, kas ir vajadzīgais nosacījums, lai pielietotu LTE lemmu, kas šajā gadījumā arī iedeva prasīto.

2.piemērs Doti pozitīvi reāli skaitļi a, b ar īpašību, ka skaitlis $a^n - b^n$ ir vesels skaitlis katram naturālam skaitlim n . Pierādīt, ka skaitļi a un b ir veseli.

Vispirms pierādīsim šādu apgalvojumu.

Apgalvojums. Skaitļi a, b ir racionāli.

Pierādījums. Ievērosim, ka no uzdevuma nosacījumiem izriet, ka $a - b$ un $a^2 - b^2$ ir veseli skaitļi. Tas savukārt nozīmē, ka $a + b = \frac{a^2 - b^2}{a - b}$ ir racionāls skaitlis. Līdz ar to $2a = (a - b) + (a + b)$ un $2b = (a + b) - (a - b)$ ir racionāli skaitļi, no kurienes izriet, ka a, b ir racionāli skaitļi.

Pieņemsim, ka $a = \frac{x}{z}$ un $b = \frac{y}{z}$ (mēs vienādojām saucējus skaitļiem a, b un skaitlis z ir mazākais iespējamais). Tādā gadījumā no uzdevuma nosacījumiem izriet, ka

$$a^n - b^n = \frac{x^n - y^n}{z^n} \in \mathbb{Z} \implies z^n \mid x^n - y^n.$$

Ja mēs pierādīsim, ka $z = 1$, tad tas nozīmē, ka $a = x$ un $b = y$ ir veseli skaitļi, kas arī bija jāpierāda. Pieņemsim pretējo, ka $z > 1$ un ka eksistē tāds nepāra pirmskaitlis p , ka $z \mid p$. Tādā gadījumā ievērosim, ka $p \mid z \mid x - y$ (pielietojot uzdevuma dotu pie $n = 1$). Ievērosim, ka ja $p \mid x$, tad arī $y \mid p$, taču tādā gadījumā skaitļus x, y, z var aizstāt $\frac{x}{p}, \frac{y}{p}, \frac{z}{p}$, kas ir pretrunā ar z minimalitāti. Tas nozīmē, ka $p \nmid x$ un $p \nmid y$, līdz ar to mēs varam izmantot LTE lemmu. Tā kā $z^n \mid x^n - y^n$, tad

$$\begin{aligned} \nu_p(x^n - y^n) &\geq \nu_p(z^n) \\ \nu_p(x - y) + \nu_p(n) &\geq n\nu_p(z) \end{aligned}$$

Tā kā tas izpildās visiem naturāliem skaitļiem n , tad $n = p^k$, kas nozīmē, ka

$$\begin{aligned} \nu_p(x - y) + \nu_p(p^k) &\geq n\nu_p(z) \\ \nu_p(x - y) + k &\geq p^k \nu_p(z) \\ k &\geq p^k \nu_p(z) - \nu_p(x - y) \end{aligned}$$

Taču pēdējā nevienādība ir aplama pietiekami lieliem k , jo $\nu_p(z)$ un $\nu_p(x - y)$ ir konstantes un eksponentfunkcija aug ātrāk par lineāro funkciju.

Atliek aplūkot gadījumu, kad z ir divnieka pakāpe. Tādā gadījumā $2 \mid z \mid x - y$ un mēs varam pielietot LTE lemmu. Tā kā $z^n \mid x^n - y^n$, tad

$$\begin{aligned} \nu_2(x^n - y^n) &\geq \nu_2(z^n) \\ \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1 &\geq n\nu_2(z) \end{aligned}$$

Tā kā tas izpildās visiem naturāliem skaitļiem n , tad $n = 2^k$, kas nozīmē, ka

$$\begin{aligned} \nu_2(x - y) + \nu_2(x + y) + \nu_2(2^k) - 1 &\geq 2^k \nu_2(z) \\ \nu_2(x - y) + \nu_2(x + y) + k - 1 &\geq 2^k \nu_2(z) \\ k - 1 &\geq 2^k \nu_2(z) - (\nu_2(x - y) + \nu_2(x + y)) \end{aligned}$$

Taču pēdējā nevienādība ir aplama pietiekami lieliem k , jo $\nu_p(z)$ un $\nu_p(x - y), \nu_p(x + y)$ ir konstantes un eksponentfunkcija aug ātrāk par lineāro funkciju. Secinām, ka $z = 1$, kas atrisina uzdevumu.

Piezīme. Šajā uzdevumā izmantojot parastos novērojumus viegli iegūt, ka $z^n \mid x^n - y^n$. Šeit ir svarīgi saprast, ka uz šo dalāmību ir vērts skatīties, nevis **globāli**, bet no viena konkrēta skaitļa z pirmreizinātāja skatpunkta jeb **lokāli**. Ievērosim, ka tādā gadījuma $n = 1$ dod mums vajadzīgu nosacījumu priekš LTE lemmas. Tālāk ir svarīgi izmantot to, ka uzdevuma dotais izpildās **visiem** naturāliem

skaitļiem n , kas dod mums iespēju izvēlēties tādus skaitļus, kuri mums dos aplamu nevienādību (mēs dalāmības nosacījumu translējām uz nevienādību ar valuācijām).

3.piemērs Dots naturāls skaitlis n . Pierādīt, ka eksistē naturāls skaitlis m ar īpašību, ka

$$7^n \mid 3^m + 5^m - 1$$

Atrisinājums. Izvēlēsimies $m = 7^{n-1}$. No LTE lemmas izriet, ka

$$\begin{aligned}\nu_7(3^{7^n} + 4^{7^n}) &= \nu_7(3 + 4) + \nu_7(7^{n-1}) = n \\ \nu_7(2^{7^n} + 5^{7^n}) &= \nu_7(2 + 5) + \nu_7(7^{n-1}) = n\end{aligned}$$

Tas nozīmē, ka

$$\begin{aligned}3^{7^n} &\equiv -4^{7^n} \pmod{7^{n+1}} \\ 5^{7^n} &\equiv -2^{7^n} \pmod{7^{n+1}}\end{aligned}$$

Tas nozīmē, ka

$$3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv -4^{7^{n-1}} - 2^{7^{n-1}} - 1 \pmod{7^n}$$

Ja mēs apzīmējam, $2^{7^{n-1}} = a$, tad $4^{7^{n-1}} = a^2$. Ievērosim, ka tādā gadījumā

$$-4^{7^{n-1}} - 2^{7^{n-1}} - 1 = -(a^2 + a + 1) = -\frac{a^3 - 1}{a - 1} = -\frac{8^{7^{n-1}} - 1}{2^{7^{n-1}} - 1}$$

Ievērosim, ka no kogrueču tabulas $2^x - 1$ dalās ar 7 tad un tikai tad, ja x dalās ar 3. Līdz ar to $2^{7^{n-1}} - 1$ nedalās ar 7. Ievērosim, ka no LTE lemmas izriet, ka

$$\nu_7(8^{7^{n-1}} - 1) = \nu_7(8 - 1) + \nu_7(7^{n-1}) = 1 + n - 1 = n$$

Ta nozīmē, ka $-\frac{8^{7^{n-1}} - 1}{2^{7^{n-1}} - 1} \equiv 0 \pmod{7^n}$. Līdz ar to secinām, ka

$$3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv 0 \pmod{7^n},$$

kas arī bija jāpierāda.

Piezīme. Intuitīvi skaidrs, ka ja mēs gribam izmantot LTE lemmu un pierādīt, ka skaitlis dalās 7^n , tad ir vērts izvēlēties kā skaitli m septiņnieka pakāpi. Problēma ir tajā, ka dotā izteiksme nav tādā formā, lai pielietotu LTE lemmu. Acīgi var pamanīt, ka 3^m un 5^m var aizstāt -4^m un -2^m , ja m ir atbilstoša 7 pakāpe.

4.piemērs. Atrodiet visus naturālu skaitļu pārus $a, b > 1$, kuriem $a^b - 1$ dalās ar b^a .

Atrisinājums. Pierādīsim, ka skaitlis b ir pāra skaitlis. Pieņemsim pretējo, tad skaitlim b eksistē tā mazākais nepāra pirmreizinātājs p .

Apskatīsim gadījumu, kad p dala $a - 1$. Tādā gadījumā no LTE lemmas izriet, ka

$$\nu_p(a^b - 1) = \nu_p(a - 1) + \nu_p(b)$$

Lai izpildītos dalāmības nosacījums, ir jābūt spēkā, ka

$$\begin{aligned}\nu_p(a^b - 1) &\geq \nu_p(b^a) \\ \nu_p(a - 1) + \nu_p(b) &\geq a\nu_p(b) \\ \nu_p(a - 1) &\geq \nu_p(b)(a - 1) \geq a - 1 \\ \log_p(a - 1) &\geq \nu_p(a - 1) \geq \nu_p(b)(a - 1) \geq a - 1 \\ \log_p(a - 1) &\geq a - 1 \\ a - 1 &\geq p^{(a-1)}\end{aligned}$$

Pēdējā sakarība ir aplama, jo $f(x) = p^x$ naturālos skaitļos aug ātrāk nekā funkcija $g(x) = x$. Līdz ar to skaitlis p nedala $a - 1$. Ievērosim, ka mēs izmantojam novērtējumu, ka $\log_p(a - 1) \geq \nu_p(a - 1)$, kas ir noderīgs arī daudzos citos uzdevumos gadījumos, kad jānovērtē valuācija no augšas.

No Fermā mazās teorēmas izriet, ka $a^{p-1} \equiv 1 \pmod{p}$, kā arī no dotā $a^b \equiv 1 \pmod{p}$. Apzīmēsim $\text{ord}_p a = d$. No lemmas par orderi izriet, ka $d \mid p - 1$, $d \mid b$. Pēc pieņēmuma b ir nepāra skaitlis. Tas nozīmē, ka skaitlis d dalās ar kādu nepāra naturālu skaitli, kas ir mazāks par p . Ievērosim, ka $d \neq 1$, jo $a - 1$ ar p nedalās. Līdz ar to b satur kādu pirmreizinātāju, kas mazāks par p . Tā ir pretruna ar p minimalitāti.

Secinām, ka mūsu pieņēmums ir aplams, līdz ar to b ir pāra skaitlis, kas nozīmē, ka a ir nepāra skaitlis. Pielietojot LTE lemmu, iegūsim, ka

$$\nu_2(a^b - 1) = \nu_2(a - 1) + \nu_2(a + 1) + \nu_2(b) - 1$$

Lai izpildītos dalāmības nosacījums, ir jābūt spēkā, ka

$$\begin{aligned} \nu_2(a^b - 1) &\geq \nu_2(b^a) \\ \nu_2(a - 1) + \nu_2(a + 1) + \nu_2(b) - 1 &\geq a\nu_2(b) \\ \nu_2(a - 1) + \nu_2(a + 1) - 1 &\geq \nu_2(b)(a - 1) \geq a - 1 \\ \nu_2(a - 1) + \nu_2(a + 1) - 1 &\geq a - 1 \end{aligned}$$

Ievērosim, ka $a - 1, a + 1$ ir divi pēc kārtas sekojoši pāra skaitļi, tāpēc viens no tiem dalās ar 2, bet nedalās ar 4. Apskatām visus iespējamus gadījumus

- Ja $\nu_2(a + 1) = 1$, tad iegūsim, ka:

$$\begin{aligned} \nu_2(a - 1) + \nu_2(a + 1) - 1 &\geq a - 1 \\ \nu_2(a - 1) &\geq a - 1 \\ \log_2(a - 1) &\geq \nu_2(a - 1) \geq a - 1 \\ \log_2(a - 1) &\geq a - 1 \\ a - 1 &\geq 2^{a-1} \end{aligned}$$

Pēdējā sakarība ir aplama, jo funkcija $f(x) = 2^x$ naturālos skaitļos aug ātrāk nekā $g(x) = x$. Līdz ar to šāds gadījums nav iespējams.

- Ja $\nu_2(a - 1) = 1$, tad iegūsim, ka:

$$\begin{aligned} \nu_2(a - 1) + \nu_2(a + 1) - 1 &\geq a - 1 \\ \nu_2(a + 1) &\geq a - 1 \\ \log_2(a + 1) &\geq \nu_2(a + 1) \geq a - 1 \\ \log_2(a + 1) &\geq a - 1 \\ a + 1 &\geq 2^{a-1} \end{aligned}$$

Pēdējā sakarība ir aplama visiem naturāliem skaitļiem $a > 3$, jo funkcija $f(x) = 2^x$ naturālos skaitļos aug straujāk nekā funkcija $g(x) = x + 2$ visiem $x > 2$. Secinām, ka $a = 3$ un $\nu_2(b) = 1$

Esam ieguvuši, ka $a = 3$ un $b = 2c$, kur c ir nepāra skaitlis. Dalāmības nosacījums kļūst par $9^c - 1$ dalās ar $8c^3$. Pieņemsim, ka skaitlim c eksistē kaut kāds mazākais nepāra pirmreizinātājs p , tad no mazās Fermā teorēmas izriet, ka

$$9^{p-1} \equiv 1 \pmod{p} \quad \text{un} \quad 9^c \equiv 1 \pmod{p}$$

Ja mēs apskatām mazāko naturālo skaitli $d = \text{ord}_p 9$, tad no lemmas par orderi izriet, ka $d \mid p - 1$ un $d \mid c$. Acīmredzami $d \neq 1$ un d ir nepāra skaitlis, taču tādā gadījumā esam atraduši vēl mazāku pirmreizinātāju skaitlim c , jo $d \leq p - 1 < p$. Tas nozīmē, ka $c = 1$. Līdz ar to vienīgais derīgais skaitļu pāris (a, b) ir $(3, 2)$.