Baltic Way, Skaitļu teorija (16 no 22)

BW (un līdzīgu reģionālu konkursu) uzdevumi un līdz ar to arī atlases sacensību uzdevumi pēc stila jūtami atšķiras no Latvijas olimpiāžu uzdevumiem. Šī dokumenta mērķis ir atvieglot gatavošanos Baltic Way atlases sacensībām, kas parasti notiek ik gadus septembra vidū, kur uzaicina iepriekšējā gada valsts un atklātajā olimpiādē labāko rezultātu saņēmējus.
Matemātiskie rezultāti BW un IMO stila olimpiādēs parasti nav ļoti dziļi (neviens nesagaida, ka dalībnieki pratīs lietot izsmalcinātus ģeometriskos pārveidojumus, algebrisko lauku teoriju vai Ramzeja teoriju kombinatorikā), bet tie pārklāj visai daudzveidīgas tēmas - no kurām katrā vēlams nedaudz orientēties. Jāprot arī vienā pierādījumā izmantot prasmes no dažādām matemātikas nozarēm (piemēram, kombinatoriku un skaitļu teoriju vai algebru un skaitļu teoriju). Starptautiskos konkursos un to atlases sacensībās svarīgi rūpīgi pierakstīt savu pamatojumu; neļaut noņemt punktus par faktiski izrēķinātu uzdevumu. Par liekiem/nevajadzīgiem pamatojumiem nevienu nesoda, toties pārāk bieži skolēnu darbos izlaisti būtiski soļi; tādēļ labāk uzrakstīt pārāk daudz nekā pārāk maz - it sevišķi tad, ja esat pārliecināti, ka risinājums ir uz pareizā ceļa.
Tēmas atkārtošanai:

- Sākt risināt vieglāku uzdevumu (piemēram, ar mazākiem skaitļiem). Piemēram, vienādojuma $x^{2015} + y^{2015} = z^{2016}$ vietā aplūkot $x^2 + y^2 = z^3$.
- Pirmskaitļu izvietojums. Pirmskaitļu bezgalīgais skaits. Eratostena režģis. Veids, kā konstruēt patvaļīgi garus naturālu skaitļu intervālus, kuros nav neviena pirmskaitļa.
- Eiklīda algoritms divu skaitļu (vai divu polinomu) lielākā kopīgā dalītāja atrašanai. Skaitļu un polinomu dalīšana ar atlikumu.
- Aritmētiskas funkcijas. Eilera funkcija $\varphi(n)$, unikālo pirmreizinātāju skaita funkcija $\omega(n)$, pirmskaitļa indeksa funkcija $\nu_p(n)$.
- Ķīniešu atlikumu teorēma; spēja atrast atrisinājumu lineārām kongruencēm vai kongruenču sistēmām.
- Pretrunas modulis. Kā pierādīt vienādojuma neatrisināmību veselos skaitļos, apskatot abu pušu iespējamos atlikumus, dalot ar kādu speciāli izvēlētu skaitli. Parasti tā, lai analizējamo atlikumu būtu iespējami maz un abās vienādojuma pusēs tie nepārklātos.
- Multiplikatīvas grupas pēc p moduļa (ja p ir pirmskaitlis un arī ja nav). Mazā Fermā teorēma. Eilera teorēma. Primitīvās saknes eksistence pēc p moduļa, ka p ir pirmskaitlis.
- Pakāpes pacelšanas lemmas.
  Lemma 1: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir naturāls skaitlis un p ir nepāru pirmskaitlis tāds, ka $p \mid x - y$, bet ne x ne y nedalās ar p, tad

  $$\nu_p\left(x^n - y^n\right) = \nu_p(x - y) + \nu_p(n),$$

  kur ar $\nu_p(x)$ apzīmēta augstākā p pakāpe, ar kuru tas ietilpst x sadalījumā pirmreizinātājos.
  Lemma 2: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir nepāru naturāls skaitlis un p ir nepāru pirmskaitlis tāds, ka $p \mid x + y$, bet ne x ne y nedalās ar p, tad

  $$\nu_p\left(x^n + y^n\right) = \nu_p(x + y) + \nu_p(n).$$

Lemma 3: Ja x un y ir divi nepāru veseli skaitļi un m ir pāru naturāls skaitlis. Tādā gadījumā:

$$\nu_2(x^m - y^m) = \nu_2(x-y) + \nu_2(x+y) + \nu_2(m) - 1.$$

- Binomiālie un polinomiālie koeficienti. Iekavu atvēršana, kāpinot divus vai vairākus saskaitāmos n-tajā pakāpē.
- Ja diviem n-tās pakāpes polinomiem sakrīt vērtības $n+1$ punktos, tad šie polinomi ir identiski. (Piemērs: Caur 2 punktiem (x_1, y_1) un (x_2, y_2) var novilkt tikai vienu taisni jeb pirmās pakāpes polinomu $P(x) = ax + b$.)
  Ekvivalents apgalvojums: Ja $P(x) = a_n x^n + \ldots + a_0$ pieņem nulles vērtību $n+1$ dažādām argumenta x vērtībām, tad visi a_i ir 0.
- Dirihlē princips (un tam līdzīgi ekstremālā elementa pielietojumi elementu skaita novērtēšanai).
- Monotonas apakšvirknes. Erdeša-Sekereša teorēma.

2015.g. Atlases Sacensības

Anotācija

2015.gadā BW komandu atlase notika 4 dienas (divas nedēļas nogales pēc kārtas); katru dienu piedāvāja 4 uzdevumus. No 4.dienas četriem uzdevumiem trīs bija par skaitļu teoriju; bez tam uz skaitļu teoriju var attiecināt arī pa vienam 1. un 2. dienas uzdevumam.

Uzdevums 1.1 (BwTst2015.Day1.3): Pierādīt, ka neeksistē polinoms $P(x)$ ar veseliem koeficientiem un naturāls skaitlis m, tādi, ka

$$x^m + x + 2 = P(P(x))$$

izpildās visiem veseliem skaitļiem x.

Atrisinājums. Tā kā $x^m + x + 2$ un $P(P(x))$ abi ir polinomi, tad viņu sakrišana bezgalīgi daudzos punktos (visām veselām x vērtībām) nozīmē to, ka abi polinomi ir identiski visiem reāliem x; viņu attiecīgie koeficienti sakrīt. T.i. $x^m + x + 2 = P(P(x))$ ir algebriska identitāte (nevis tikai vienādība, kas izpildās veseliem x).

Apgalvojums A: Polinoms $P(x)$, kuram $P(P(x)) = x^m + x + 2$ nevar būt 1. pakāpes poplinoms.

Pamatojums: 1. pakāpes polinomiem $P(x) = a_1 x + a_0$ identitāte nevar būt spēkā, jo $P(P(x))$ arī sanāktu 1. pakāpes polinoms jeb $x^m + x + 2 = x^1 + x + 2 = 2x + 2$, bet

$$P(P(x)) = a_1(a_1 x + a_0) + a_0 = a_1^2 x + a_1 a_0 + a_0.$$

Nevienam veselam a_1 koeficients pie x nevar būt $a_1^2 = 2$, jo sakne no 2 nav vesels skaitlis. □

Apgalvojums B: Polinoms $P(x)$ ar pakāpi $n > 1$, kuram $P(P(x)) = x^m + x + 2$ ir jāizpildās $m = n^2$. Turklāt polinoma vecākais koeficients pie x^n ir 1 vai -1.

Pamatojums: Polinomiem $P(x) = a_n x^n + \ldots + a_0$, kuru pakāpe $n > 1$, $P(P(x))$ būs polinoms ar pakāpi n^2, t.i. $m = n^2$, un koeficients pie šī vecākā locekļa ir a_n^{n+1}. No otras puses, zināms, ka koeficients pie vecākā locekļa x^m ir 1. T.i. $a_n = 1$ ja n ir pāru, $a_n = \pm 1$, ja n ir nepāru. □

Apgalvojums C: Pieņemsim, ka eksistē polinoms $P(x)$ ar pakāpi $n > 1$, kuram $P(P(x)) = x^m + x + 2$ un $m = n^2$. Tad tas ir uzrakstāms formā $a_n x^n + c$, kur $a_n = \pm 1$.

Pamatojums: Induktīvi pierādīsim, ka koeficienti a_{n-i}, kur $i = 1, \ldots, n-1$ (izņemot vecāko koeficientu a_n un jaunāko koeficientu a_0) ir vienādi ar 0.

- Ja $i = 1$, pierādīsim, ka $a_{n-1} = 0$. Ievietosim n-tās pakāpes polinomu $P(x)$ izteiksmē $P(P(x))$, ņemot vērā Apgalvojumus A un B, ka $n > 1$ un $m = n^2$

$$\begin{aligned} P(P(x)) &= a_n(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0)^n + a_{n-1}(a_n x^n + \ldots + a_0)^{n-1} + \ldots + a_0 = \\ &= a_n(a_n)^n x^n + a_n \binom{n}{1} (a_n)^{n-1} a_{n-1}^1 x^{n-1} + \ldots \\ &= x^{n^2} + x + 2. \end{aligned} \tag{1}$$

  Atverot iekavas izteiksmē $P(P(x))$, mums interesē tikai koeficienti pie x^n un x^{n-1} (kas rodas atverot pirmās iekavas, kas kāpinātas n-tajā pakāpē), visus pārējos esam aizstājuši ar daudzpunktu. Tādā gadījumā pietiek aplūkot tikai pirmās iekavas jeb $(P(x))^n$, jo visas zemākās pakāpes, sākot ar $(P(x))^{n-1}$, rada koeficientus pie x pakāpēm, kas nepārsniedz $n(n-1) = n^2 - n$. Pielīdzinām koeficientus pie x^{n-1} abiem polinomiem – $P(P(x))$ un $x^m + x + 2$. Iegūstam:

$$a_n \binom{n}{1} (a_n)^{n-1} a_{n-1}^1 = 0 \text{ jeb } a_{n-1} = 0.$$

- Pieņemsim, ka visi a_{n-i} ir 0, ja $i = 1, 2, \ldots, k$. Pamatosim, ka $a_{n-(k+1)}$ arī ir 0. Tāpat kā iepriekš atvērsim iekavas izteiksmē $P(P(x))$ un pielīdzināsim koeficientus. Arī šoreiz pietiek apskatīt tikai pirmo saskaitāmo: $a_n(P(x))^n$, jo visi citi saskaitāmie, sākot ar $a_{n-1}(P(x))^{n-1}$, rada koeficientus pie x pakāpēm, kas nepārsniedz $n(n-1) = n^2 - n$. Iegūstam:

$$\begin{aligned} P(P(x)) &= a_n(a_n x^n + a_{n-(k+1)}x^{n-(k+1)} + \ldots + a_0)^n + \ldots = \\ &= a_n(a_n)^n x^n + a_{n-(k+1)} \binom{n}{1} (a_n)^{n-1} a_{n-(k+1)}^1 x^{n-(k+1)} + \ldots \\ &= x^{n^2} + x + 2. \end{aligned} \tag{2}$$

  Atkal, pielīdzinot koeficientus abos polinomos pie $x^{n-(k+1)}$, iegūstam $a_{n-(k+1)} = 0$. Ievērosim, ka kāpinātājs $n - (k+1) > n^2 - n$, tādēļ darījām pareizi, ignorējot $P(x)^{n-1}$ un visus tālākos saskaitāmos.

Apgalvojums D: Polinoms formā $P(x) = a_n x^n + c$ nevar apmierināt identitāti $P(P(x)) = x^m + x + 2$.
Pamatojums: Atveram iekavas $P(P(x))$. Aplūkojam koeficientu pie $x^{n(n-1)}$.

$$\begin{aligned} P(P(x)) &= a_n(a_n x^n + c)^n + c = \\ &= a_n(a_n)^n x^n + \binom{n}{1} (a_n)^{n-1} c^1 x^{n^2-n} + \ldots \\ &= x^{n^2} + x + 2. \end{aligned} \tag{3}$$

Pielīdzinot koeficientus, iegūstam $c = 0$. Tas tomēr nav iespējams, jo šajā gadījumā $P(P(x)) = x^{n^2}$ nevis $x^{n^2} + x + 2$. □

Pieņēmums, ka $P(P(x)) = x^m + x + 2$ eksistē, vairāku apgalvojumu gaitā noveda pie arvien lielākiem ierobežojumiem par to, kāds var būt $P(x)$ un visbeidzot – pie pretrunas. Tādēļ šāds polinoms neeksistē. ■

Uzdevums 1.2 (BwTst2015.Day2.4): Dots fiksēts racionāls skaitlis q. Skaitli x sauksim par *harizmātisku*, ja var atrast tādu naturālu skaitli n un veselus skaitļus $\alpha_1, \alpha_2, \ldots, \alpha_n$, ka

$$x = (q+1)^{\alpha_1} \cdot (q+2)^{\alpha_2} \cdot \ldots \cdot (q+n)^{\alpha_n}.$$

(A) Pierādīt, ka var atrast tādu q, kam visi pozitīvie racionālie skaitļi ir harizmātiski.

(B) Vai tiesa, ka visiem q, ja skaitlis x ir harizmātisks, tad arī $x+1$ ir harizmātisks?

Uzdevums 1.3 (BwTst2015.Day4.1): Vai eksistē tādi pozitīvi reāli skaitļi a un b, ka $\lfloor an+b \rfloor$ ir pirmskaitlis visām naturālām n vērtībām. Ar $\lfloor x \rfloor$ apzīmē skaitļa veselo daļu – lielāko veselo skaitli, kas nepārsniedz x.

Atrisinājums. Ja šādi pozitīvi reāli skaitļi eksistētu, tad ar formulas $p_n = \lfloor an+b \rfloor$ palīdzību varētu iegūt bezgalīgi augošu pirmskaitļu virkni, turklāt attālums starp pirmskaitļiem šajā virknē nepārsniegtu $p_{n+1} - p_n$:

$$\lfloor a(n+1)+b \rfloor - \lfloor an+b \rfloor \leq (a(n+1)+b) - ((an+b)-1) = a+1.$$

Mēģināsim pamatot, ka pirmskaitļi starp lieliem skaitļiem ir sastopami arvien retāk, un tāda pirmskaitļu virkne, kur attālums starp jebkuriem blakus esošiem pirmskaitļiem nepārsniedz fiksētu skaitli $a+1$ neeksistē. Izvēlamies naturālu skaitli $N > a+1$. Atradīsim N pēc kārtas sekojošus saliktus skaitļus, kas visi ir lielāki par $a+b$. Tā kā virkne p_n nevar "pārlēkt" pāri N saliktiem skaitļiem, būsim ieguvuši, ka vismaz viens p_n loceklis ir salikts skaitlis, kas būtu pretruna.
Izvēlamies naturālu m, kas ir lielāks gan apr $a+b$, gan par N. Aplūkojam šādus skaitļus:

$$\begin{aligned} m!+2 &= 2(m!/2+1) \\ m!+3 &= 3(m!/3+1) \\ &\dots \\ m!+m &= m(m!/m+1) \end{aligned} \tag{4}$$

Labajā pusē visās iekavās ir veseli skaitļi, jo $m! = 1 \cdot 2 \cdot \ldots \cdot m$ dalās ar 2, ar 3 utt. un ar m. Tādēļ visi naturālie skaitļi x intervālā $m!+2 \leq x \leq m!+m$ ir salikti skaitļi. Tā kā $m > N$, esam ieguvuši vismaz N pēc kārtas sekojošus saliktus skaitļus. Turklāt visi tie ir lielāki par virknes p_n pirmo locekli $a+b$, kas nozīmē, ka virkne p_n saturēs kādu no šiem skaitļiem, kas nav pirmskaitlis.

Uzdevums 1.4 (BwTst2015.Day4.2): Ar $S(a)$ apzīmēsim skaitļa a ciparu summu. Kādām naturālām R vērtībām var atrast tādu naturālu n, ka

$$\frac{S(n^2)}{S(n)} = R?$$

Atrisinājums. Izvēloties $n = 1, 11, 111, \ldots, 111111111$, iegūstam ka R var būt $1, 2, \ldots, 9$. Izvēloties vēl lielāku vienīnieku skaitu, ievērojam, ka kāpinot kvadrātā ar reizināšanu stabiņā, sāk rasties pārnesumi, kuri neļauj tālāk paaugstināt R vērtību. Lai konstruētu piemēru patvaļīgam naturālam R, vieniniekus rakstīsim pamīšus ar vienu vai vairākām nullēm tā, lai iespējami izvairītos no pārnesumiem.
Mūsu konstrukcijā, lai iegūtu attiecību $S(n^2)/S(n)$ vienādu ar iepriekš uzdotu naturālu skaitli R, izvēlēsimies skaitli n, kura decimālpierakstā ir tieši R vienīnieki; turklāt tie rakstīti pozīcijās, kuras, skaitot no labās puses, atrodas divnieka pakāpēs. T.i. cipars "1" atradīsies pirmajā, otrajā, ceturtajā, astotajā, utt. pozīcijā, skatoties no labās puses. Pierakstot formulas veidā:

$$n = 1 \cdot 10^0 + 1 \cdot 10^1 + 1 \cdot 10^3 + \ldots + 1 \cdot 10^{2^{R-1}-1} = \sum_{j=0}^{R-1} 10^{2^j-1}.$$

Pamatosim, ka $S(n^2)/S(n) = R$. Atvērsim iekavas izteiksmē

$$\left(1 \cdot 10^0 + 1 \cdot 10^1 + 1 \cdot 10^3 + \ldots + 1 \cdot 10^{2^{R-1}-1}\right)^2,$$

iegūstot summu ar dažādiem desmitnieka pakāpju savstarpējiem reizinājumiem.

Apgalvojums. Neeksistē divi dažādi saskaitāmie augšminētajā izteiksmē (t.i. četri kāpinātāji (j_1, j_2) un (j_3, j_4), kur (j_1, j_2) atšķiras no (j_3, j_4) un arī no (j_4, j_3)), kam būtu spēkā:

$$10^{2^{j_1}-1} \cdot 10^{2^{j_2}-1} = 10^{2^{j_3}-1} \cdot 10^{2^{j_4}-1}.$$

Tik tiešām, pieņemsim, ka dažādiem pāriem (j_1, j_2) un (j_3, j_4) abi reizinājumi sakrīt. Ieviešam apzīmējumus tā, lai $j_1 \geq j_2$ un $j_3 \geq j_4$; turklāt $j_1 \geq j_3$. Šajā gadījumā $(2^{j_1} - 1) + (2^{j_2} - 1) = (2^{j_3} - 1) + (2^{j_4} - 1)$. Ja $j_1 > j_3$, tad saskaitāmais $2^{j_1} - 1$ viens pats ir lielāks par $(2^{j_3} - 1) + (2^{j_4} - 1)$, jo tur abi saskaitāmie abi ir mazāki par pusi no $2^{j_1} - 1$. Tādēļ atliek gadījums $j_1 = j_3$. Viegli redzēt, ka tad arī $j_2 = j_4$ un abi pāri sanāk vienādi. □

Ja reiz nevienā desmitnieku pozīcijā nenonāk vairāk nekā divi reizinājumi $10^{2^{j_1}-1} \cdot 10^{2^{j_2}-1}$ (t.i. atbilstoši pārim (j_1, j_2) un atbilstoši tam pašam pārim pretējā secībā: (j_2, j_1)), tad arī pārnesumi uz nākamo desmitnieku pozīciju neveidojas. Esam ieguvuši, ka visi R^2 saskaitāmie būs redzami reizinājuma rezultātā, un tādēļ $S(n^2) = R^2$, kas nozīmē, ka $S(n^2)/S(n) = R^2/R = R$. Reizināšanas piemērs ($R = 4$) ilustrē šo konstrukciju:

```
       10001011
*      10001011
---------------
       10001011
      10001011
     00000000
    10001011
   00000000
  00000000
 00000000
10001011
---------------
100020221022121
```

Uzdevums 1.5 (BwTst2015.Day4.3): Ar $\omega(n)$ apzīmēsim dažādo pirmskaitļu skaitu, ar ko dalās n. Pierādīt, ka ir bezgalīgi daudz tādu naturālu skaitļu n, kuriem $\omega(n) < \omega(n+1) < \omega(n+2)$.

Atrisinājums. Pieaugot skaitlim n, izredzes, ka tas dalīsies ar lielāku skaitu pirmskaitļu arī palielinās. Skaitlim $6 = 2 \cdot 3$ ir divi šādi dalītāji, $30 = 2 \cdot 3 \cdot 5$ ir trīs dalītāji, $210 = 2 \cdot 3 \cdot 5 \cdot 7$ – četri dalītāji, utt. No otras puses, divu vai trīs blakusesošu skaitļu dalītāju skaits reti kad padodas kaut kādām viegli aprakstāmām likumsakarībām. Tādēļ konstruēsim bezgalīgi augošu naturālu skaitļu virkni n_k (kurai izpildās $\omega(n_k) < \omega(n_k + 1) < \omega(n_k + 2)$). Konstruēsim šos skaitļus īpatnējā formā (izlaižot daudzus citus derīgus piemērus), lai pamatojums būtu "viendabīgs" katram virknes loceklim, lai nebūtu bezgalīgi daudzi skaitļi dažnedažādos veidos jācenšas dalīt pirmreizinātājos.

Lai uzminētu likumsakarības, sākam ar eksperimentēšanu - pārbaudot (ne pārāk daudzos) skaitļus $n \in [1, 200]$, kam $\omega(n) = 3$. Pirmie 3 trijnieki, kuri apmierina uzdevuma nosacījumu ir sekojoši:

$$\begin{aligned}
(64, 65, 66) &= \left(2^6,\ \ 5 \cdot 13,\ \ 2 \cdot 3 \cdot 11\right) \\
(103, 104, 105) &= \left(103,\ \ 2^3 \cdot 13,\ \ 3 \cdot 5 \cdot 7\right) \\
(128, 129, 130) &= \left(2^7,\ \ 3 \cdot 43,\ \ 2 \cdot 5 \cdot 13\right)
\end{aligned} \tag{5}$$

Redzam, ka daži šādi trijnieki sākas ar divnieka pakāpēm 2^k. Turpmāk meklēsim visus trijniekus tieši šādā formā $(2^k, 2^k + 1, 2^k + 2)$. Tas ir izdevīgi arī tādēļ, ka k-tajā skaitļu trijniekā ietilpst divkāršots skaitlis no iepriekšējā skaitļu trijnieka:

$$2^k + 2 = 2 \cdot \left(2^{k-1} + 1\right).$$

Varam redzēt, ka $\omega\left(2^k+2\right) = \omega\left(2^{k-1}+1\right)+1$, jo nepāra skaitli piereizinot ar 2, tam rodas viens dalītājs-pirmskaitlis vairāk.
Definējam virkni: $o_k = \omega(2^k+1)$. Ja kādam k izrādās, ka $1 < o_k \leq o_{k-1}$, tad skaitļu trijnieks $(2^k, 2^k+1, 2^k+2)$ atbilst uzdevuma nosacījumiem, jo attiecīgās ω vērtības ir:

$$\begin{cases} \omega(2^k) & = & 1 \\ \omega(2^k+1) & = & o_k \\ \omega(2^k+2) & = & o_{k-1}+1 \end{cases}$$

Turpmākais pierādījums ir par to, kā garantēti atrast bezgalīgi daudzas "interesantas" k vērtības, kurām $o_k > 1$, bet $o_{k-1} \geq o_k$. Šīs vērtības izmantosim, lai veidotu virkni. Tālākais ir šī risināšanas plāna atsevišķie soļi.
Apgalvojums A: Skaitļi formā 2^k+1 var būt pirmskaitļi vienīgi tad, ja $k = 2^N$, t.i. $2^{2^N}+1$. (**Piezīme:** Skaitļus, kas izsakāmi formā $2^{2^N}+1$, sauc par Fermā skaitļiem. Ne visi tie ir pirmskaitļi, piemēram, $2^{2^5}+1 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417$.)
Pamatojums: Ņemot vērā algebrisku identitāti:

$$a^{2m+1}+b^{2m+1} = (a+b)\left(a^{2m}-a^{2m-1}b+a^{2m-2}b^2-\ldots+a^2b^{2m-2}-ab^{2m-1}+b^{2m}\right),$$

izteiksmi 2^k+1 var sadalīt reizinātājos (kas abi lielāki par 1) visos tajos gadījumos, kad skaitlim k ir kāds nepāru dalītājs. Piemēram, $2^{12}+1 = (2^4)^3+1^3 = (2^4+1)(2^8-2^4+1)$. Tādēļ Fermā skaitļi var būt pirmskaitļi vienīgi tad, ja kāpinātājs pats ir divnieka pakāpe ($k = 2^N$), kam nav neviena nepāru reizinātāja: $2^k+1 = 2^{2^N}+1$. □

k	2^k+1		$\omega(2^k+1)$	k	2^k+1		$\omega(2^k+1)$
1	2		1	9	513	$= 3^3 \cdot 19$	2
2	5		1	10	1025	$= 5^2 \cdot 41$	2
3	9	$= 3^2$	1	11	2049	$= 3 \cdot 683$	2
4	17		1	12	4097	$= 17 \cdot 241$	2
5	33	$= 3 \cdot 11$	2	13	8193	$= 3 \cdot 2731$	2
6	65	$= 5 \cdot 13$	2	14	16385	$= 5 \cdot 29 \cdot 113$	3
7	129	$= 3 \cdot 43$	2	15	32769	$= 3^2 \cdot 11 \cdot 331$	3
8	257		1	16	65537		1

Apgalvojums B1: Pieņemsim, ka p ir nepāru pirmskaitis un kongruenču vienādojumam $2^k+1 \equiv 0 \pmod{p}$ eksistē atrisinājums; turklāt k_1 ir mazākais šāds atrisinājums. Tad visi citi k, kas apmierina šo kongruenci ir izsakāmi formā $k = nk_1$, kur n ir nepāru skaitlis.
Pamatojums: Vērtībām $k = 1, 2, \ldots$ aprēķinām kongruenču klasi, kurai pieder $2^k \pmod{p}$. Iespējami divi gadījumi:

- Kongruenču klase 1 parādās pirms kongruenču klases -1. Šajā gadījumā 2^k veidotais kongruenču cikls ir noslēdzies bez -1 un tādēļ vienādojumam $2^k+1 \equiv 0 \pmod{p}$ neeksistē atrisinājums. (Tāds ir, piemēram, pirmskaitlis 7.)
- Kongruenču klase -1 parādās pirms kongruenču klases 1 pie $k = k_1$. Šajā gadījumā kongruenču vienādojumam eksistē atrisinājums (un pēc konstrukcijas mazākais ir tieši k_1, jo mēs pārbaudījām visus pēc kārtas). Šajā gadījumā

  $$2^{2k_1} \equiv (2^{k_1})^2 \equiv (-1)^2 \equiv 1 \pmod{p}.$$

  Tādēļ piereizinot kongruencē $2^{k_1} \equiv -1$ abas puses ar $2^{2k_1} \equiv 1$, iegūsim, ka $k = k_1+2k_1$ arī ir atrisinājums; un šādi piereizinot m reizes, iegūsim, ka arī $k = k1+2mk_1 = k_1(2m+1)$ ir atrisinājumi jebkuram $m \in \mathbb{N}$. (Šāds, piemēram ir pirmskaitlis $p = 3$, kam $k_1 = 1$ un $p = 5$, kam $k_1 = 2$.)

Citu atrisinājumu, izņemot $k = k_1(2m+1)$ kongruenču vienādojumam nav. Pretējā gadījumā mēs iegūtu, ka divu dažādu atrisinājumu $k_i < k_j$ starpība $a = k_j - k_i < 2k_1$. Izdalot 2^{k_j} ar 2^{k_i} iegūsim attiecību $2^{k_j-k_i} = 2^a \equiv 1$. Mums ir zināms, ka $a > k_1$, jo virknē 2^k $(k = 1, 2, \ldots)$ atlikums -1 parādījās vispirms. Bet tad $2^a/2^{k_1} = 2^{a-k_1} \equiv 1/(-1) = -1$. Bet tad esam ieguvuši, ka kongruenču vienādojumam ir arī atrisinājums $a - k_1 < k_1$, kas ir pretruna ar to, ka k_1 ir mazākais pozitīvais atrisinājums. □

Apgalvojums B2: Pieņemsim, ka p ir nepāru pirmskaitis un kongruenču vienādojumam $2^k + 1 \equiv 0 \pmod{p}$ eksistē atrisinājums; turklāt k_1 ir mazākais šāds atrisinājums, tad $2^{k_1} + 1 \not\equiv 0 \pmod{p^2}$. T.i. $2^{k_1} + 1$ dalās ar p, bet ne ar p^2.
Pamatojums: Apgalvojums nav patiess. Eksistē t.s. A.Viferiha pirmskaitļi (Wieferich primes). Viens no šādiem skaitļiem ir $p = 1093$, kuram $k_1 = 182$. Šim skaitlim $2^{k_1} + 1$ dalās uzreiz ar p^2. □

Apgalvojums B3 (Pakāpes pacelšanas lemma): Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir nepāru naturāls skaitlis un p ir nepāru pirmskaitlis tāds, ka $p \mid x + y$, bet ne x ne y nedalās ar p, tad

$$\nu_p\left(x^n + y^n\right) = \nu_p(x + y) + \nu_p(n),$$

kur ar $\nu_p(x)$ apzīmēta augstākā p pakāpe, ar kuru tas ietilpst x sadalījumā pirmreizinātājos.
Pamatojums: Šī apgalvojuma pierādījumu sk. [1]. □

Apgalvojums B4: Ja $k > 3$, tad $2^k + 1$ nevar būt pirmskaitļa pakāpe, kas augstāka par pirmo.
Pamatojums: Ir spēkā vienādība $2^3 + 1 = 3^2$. Mums jāpamato, ka lielākām divnieka pakāpēm $2^k + 1$ nevarēs būt p^n, kur $n > 1$. Jāpiebilst, ka pie $n = 1$, ir iespējams, ka $2^k + 1 = p$ – tie ir Fermā pirmskaitļi no iepriekšējā apgalvojuma.
Ja vispār eksistē tāds k, kuram $2^k + 1$ dalās ar p, tad ar k_1 apzīmējam mazāko no tiem. Apzīmējam arī $x = 2^{k_1}$ un $y = 1$. Katram nepāru n iegūstam, ka

$$\nu_p\left(x^n + y^n\right) = \nu_p(x + y) + \nu_p(n),$$

t.i. pats mazākais nepāru n, kuram $(2^{k_1})^n + 1$ dalās ar p^2 būs tāds, kur $\nu(n) \geq 1$. Mazākais tāds n ir $n = p$.
Esam ieguvuši, ka $(2^{k_1})^p + 1 > (2^1)^p = 2^p$ ir mazākais skaitlis, kurš varētu dalīties ar p^2. Aplūkosim divus gadījumus:

- Ja $p = 3$, tad $2^p + 1 = p^2$ (t.i. $8 + 1 = 9$).
- Ja $p > 3$, tad $2^p > p^2$ un tātad arī $2^p + 1 > p^2$. Par to var pārliecināties, aprēķinot no abām pusēm naturālo logaritmu:

  $$p\ln(2) > 2\ln(2) \text{ jeb } \frac{\ln(2)}{2} > \frac{\ln(p)}{p}.$$

  Ievērojam, ka funkcija $f(x) = \frac{\ln(x)}{x}$ pieņem vienādas vērtības pie $x = 2$ un $x = 4$ un tā dilst visiem $x > e$. Pārbaudām atvasinājumu:

  $$f'(x) = \left(\frac{\ln(x)}{x}\right)' = \frac{\frac{1}{x}x - 1 \cdot \ln(x)}{x^2} = \frac{1 - \ln(x)}{x^2}.$$

  Acīmredzot $1 - \ln(x) < 0$, ja $x > e$, t.i. funkcija dilst visiem $x > e$ un tādēļ katram pirmskaitlim $p > 3$ tās vērtība $f(p)$ būs mazāka nekā $f(4) = f(2)$.

Varam secināt, ka vienīgais skaitlis formā $2^k + 1$, kas vienāds ar nepāru pirmskaitļa pakāpi ir $2^3 + 1 = 9$.
Aplūkojot vēl lielākas pirmskaitļu pakāpes mēs atkal varam izmantot pakāpes pacelšanas lemmu tiem pašiem skaitļiem $x = 2^{k_1}$ un $y = 1$. Mēs iegūtu, ka mazākais nepāru n, kuram $(2^{k_1})^n + 1$ dalās ar p^3 būs tāds, kur $\nu(n) \geq 2$. Mazākais tāds n ir $n = p^2$. Pamatosim, ka visiem nepāru pirmskaitļiem $2^{p^2} > p^3$. Pie $p = 3$, acīmredzot, $2^9 > 3^3$ jeb $512 > 27$. Arī lielākiem p izpildīsies nevienādība $2^{p^2} > p^3$, jo to var iegūt no augstāk pamatotas nevienādības $2^p > p^2$, to pareizinot ar citu nevienādību: $2^{p^2-p} > p$, kas ir spēkā, jo $p^2 - p > p$, un pēc katras piereizināšanas ar 2, pakāpe 2^n palielinās vismaz par 1.
Līdzīgi varam spriest arī augstākām p pakāpēm. Piemēram $2^{p^3} > p^4$, jo to var iegūt no $2^{p^2} > p^3$, piereizinot abas puses ar citu nevienādību: $2^{p^3-p^2} > p$, utt. Esam ieguvuši, ka skaitļi formā $2^k + 1$ var

dalīties ar patvaļīgi augstām nepāra pirmskaitļu p pakāpēm, bet tie nekad nav vienādi ar šīm pirmskaitļu pakāpēm, atskaitot gadījumu $2^3+1=3^2$. □

Apgalvojums C: Ja $k \geq 2$, tad eksistē tāds m, kam $2^k < m < 2^{k+1}-1$, kuram $\omega(2^m+1) \geq \omega(2^{m+1}+1)$.
Pamatojums: Ja $k=2$, tad var izvēlēties $m=5$, jo $\omega(2^5+1)=\omega(33)=\omega(3\cdot 11)=2$.
Ja $k>2$, pierādām no pretējā. Iedomāsimies, ka $\omega(m)$ veido stingri augošu apakšvirkni:

$$\omega\left(2^{2^k+1}+1\right) < \omega\left(2^{2^k+2}+1\right) < \ldots < \omega\left(2^{2^{k+1}-1}+1\right).$$

Šajā apakšvirknē ir $2^{k+1}-(2^k+1)=2^k-1$ locekļi. Ja pieņemam, ka pirmais loceklis ir vismaz 2 (tas nevar būt 1, jo ir spēkā Apgalvojums A un Apgalvojums B4 - t.i. pirmais loceklis nevar būt nedz pirmskaitlis, nedz pirmskaitļa pakāpe), tad pēdējais loceklis ir vismaz $2+(2^k-2)=2^k$. T.i. iegūstam, ka $\omega\left(2^{2^{k+1}-1}+1\right)$ ir vismaz 2^k.
No otras puses, mazākais naturālais skaitlis n, kuram $\omega(n) \geq 2^k$ ir pirmo 2^k pirmskaitļu reizinājums:

$$n = \underbrace{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot \ldots \cdot p_{2^k}}_{2^k \text{ reizinātāji}}.$$

Pamatosim, ka $n > 2^{2^{k+1}}$. Reizinājumā, kas veido skaitli n, visi pirmskaitļi, sākot ar 13 ir lielāki par 4. Savukārt $2\cdot 3\cdot 5\cdot 7\cdot 11 > 4^5 = 1024$. Tātad pirmo 2^k pirmskaitļu reizinājums n būs lielāks par $2^{2^{k+1}} = 4^{2^k}$, jo abās pusēs ir tieši 2^k reizinātāji, bet gan pirmie pieci pirmskaitļi, gan arī katrs no pārējiem pirmskaitļiem ir lielāks par attiecīga skaita četrinieku reizinājumu.
Esam ieguvuši pretrunu: $\omega\left(2^{2^{k+1}-1}+1\right)$ nevar būt vismaz 2^k. Tādēļ stingri augošā apakšvirkne neeksistē. Un tādēļ eksistēs tāds m intervālā $[2^k+1, 2^{k+1}-2]$ kam $\omega(2^m+1) \geq \omega(2^{m+1}+1)$. □

Visbeidzot varam konstruēt bezgalīgu virkni n_k, kurai izpildās $\omega(n_k) < \omega(n_k+1) < \omega(n_k+2)$. Katram $k \geq 2$ izvēlamies tādu $m \in [2^k+1, 2^{k+1}-2]$ no Apgalvojuma C, kuram $\omega(2^m+1) \geq \omega(2^{m+1}+1)$. Definējam $n_k = 2^{m+1}$. Šajā gadījumā $\omega(n_k)=1$, $\omega(n_k+1)=\omega(2^{m+1}+1)$ (šis skaitlis ir lielāks par 1 saskaņā ar Apgalvojumiem A un B4), bet $\omega(n_k+2) = 1+\omega(2^m+1) > \omega(2^{m+1}+1)$ (saskaņā ar m izvēli).
Mūsu konstruētā virkne n_k ($k \geq 2$) ļoti strauji aug, jo katrā intervālā starp skaitļiem 2^{2^N} un $2^{2^{N+1}}$ mēs izvēlamies vienu elementu:

$$n_2 = 2^{4+2} = 64, \;\; n_3 = 2^{8+2} = 1024 \;\; n_4 = 2^{16+3} = 524288, \; \ldots.$$

■

2015.g. BW Olimpiāde

Uzdevums 1.6 (Bw2015.16): Ar $P(n)$ apzīmējam lielāko pirmskaitli, ar ko dalās n. Atrast visus naturālos skaitļus $n \geq 2$, kam

$$P(n) + \lfloor \sqrt{n} \rfloor = P(n+1) + \lfloor \sqrt{n+1} \rfloor.$$

(Piezīme: $\lfloor x \rfloor$ apzīmē lielāko veselo skaitli, kas nepārsniedz x.)
Atrisinājums. Tā kā nav iespējams, ka $P(n)=P(n+1)$, tad $\lfloor \sqrt{n+1} \rfloor > \lfloor \sqrt{n} \rfloor$. Tādēļ $n+1$ ir pilns kvadrāts, ko apzīmējam ar m^2. Aplūkosim gadījumus:

- Ja m ir pirmskaitlis, tad $n = m^2-1 = (m-1)(m+1)$. Šajā gadījumā $P(n+1)=m$ un $P(n)$ ir jābūt $m+1$, lai izpildītos vienādība. Tātad arī $m+1$ ir pirmskaitlis. Vienīgā iespēja ir $m=2$. Tad $n=3$ un $n+1=4$.
- Ja m nav pirmskaitlis, tad $P(n+1)=P(m^2)=p_1<m$. Arī šajā gadījumā $P(n)$ ir jābūt par 1 lielākam, t.i. $P(n)=p_1+1$. Ja p_1 un p_1+1 abi ir pirmskaitļi, tad $p_1=2$ un $p_1+1=3$. Iegūstam, ka $n+1=2^{2k}=4^k$ (nepāra pakāpes nebūtu pilni kvadrāti. Un tad sanāk, ka nepāru skaitlis n ir trijnieka pakāpe.

Pakāpes pacelšanas lemma: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir naturāls skaitlis un p ir nepāru pirmskaitlis tāds, ka $p \mid x-y$, bet ne x ne y nedalās ar p, tad

$$\nu_p\left(x^k - y^k\right) = \nu_p(x-y) + \nu_p(k),$$

kur ar $\nu_p(x)$ apzīmēta augstākā p pakāpe, ar kuru tas ietilpst x sadalījumā pirmreizinātājos.
Pamatojums: Šī apgalvojuma pierādījumu sk. [1]. □
Ievietojam $x=4$, $y=1$, $p=3$. Tad augstākā 3 pakāpe, ar kuru dalās 4^k-1^k, ir $\nu_3(4-1)+\nu_3(k) = 1+\nu_3(k)$. Atskaitot gadījumu $k=1$, nevar gadīties tā, ka 4^k-1 ir kāda vesela trijnieka pakāpe 3^r. Tas ir tādēļ, ka $1+\nu_3(k) \leq k$ (un vienādība ir iespējama tikai kad $k=1$). Tādēļ lielākā 3 pakāpe, ar kuru var dalīties 4^k-1 ir mazāka nekā k-tā pakāpe. Bet tad 4^k-1 ir lielāks par šo trijnieka pakāpi (un tas nozīmē, ka 4^k-1 satur vēl citus pirmreizinātājus kā 3).
Atbilde: Vienīgais atrisinājums ir $n=3$.

Uzdevums 1.7 (Bw2015.17): Atrast visus naturālos skaitļus n, kuriem $n^{n-1}-1$ dalās ar 2^{2015}, bet nedalās ar 2^{2016}.

Atrisinājums: Ar $\nu_2(x)$ apzīmēsim lielāko k, kuram x dalās ar 2^k. Pie $1^0-1=0$ šī funkcija $\nu_2(x)$ nav definēta, jo 0 dalās ar jebkuru divnieka pakāpi. Savukārt, ja $n \geq 2$ ir pāru skaitlis, tad $\nu(n^{n-1}-1)=0$, jo nepāru izteiksmes $n^{n-1}-1$ dalās tikai ar 2^0.
Aplūkosim $n^{n-1}-1$ vērtības, ja $n=3,5,7,9,\ldots$. Apkoposim šīs vērtības tabulā. Ieviesīsim šādus apzīmējumus (trīs jaunas virknes a_n, b_n, c_n, kuru locekļi definēti visiem $n>1$):

$$\begin{cases} a_n &= \nu_2(n^{n-1}-1) \\ b_n &= \nu_2(n-1) \\ c_n &= \nu_2(n+1) \end{cases}$$

Šajā gadījumā visiem pāru n ir spēkā $a_n = b_n = c_n = 0$, bet nepāru $n>1$ virkņu vērtības būs šādas:

n	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
a_n	3	4	4	6	3	4	5	8	3	4	4	6	3	4	6	10
b_n	1	2	1	3	1	2	1	4	1	2	1	3	1	2	1	5
c_n	2	1	3	1	2	1	4	1	2	1	3	1	2	1	5	1
$2b_n+c_n$	4	5	5	7	4	5	6	9	4	5	5	7	4	5	7	11

Ievērosim, ka tabulā redzamajām vērtībām $a_n = 2b_n + c_n - 1$. Šī sakarība izpildās visiem nepāru n. To var pamatot ar sekojošu apgalvojumu.
Apgalvojums (Pakāpes pacelšanas lemma) Ja x un y ir divi nepāru veseli skaitļi un m ir pāru naturāls skaitlis. Tādā gadījumā:

$$\nu_2(x^m - y^m) = \nu_2(x-y) + \nu_2(x+y) + \nu_2(m) - 1.$$

Pamatojums: Šī apgalvojuma pierādījumu sk. [1]. □
Ievietojot $x=n$, $y=1$, $m=n-1$, iegūsim sakarību $a_n = 2b_n + c_n - 1$. Noskaidrosim, kuriem n būs spēkā $a_n = 2015$? Jebkuram nepāru n, vai nu b_n vai nu c_n ir vienāds ar 1, jo no diviem pēc kārtas sekojošiem pāru skaitļiem būs tieši viens, kurš dalās ar 2, bet nedalās ar 4. Tādēļ iegūstam divas iespējas:

- Ja $c_n = 1$, tad $2b_n + 1 - 1 = 2015$ jeb $2b_n = 2015$, kas nav iespējams.
- Ja $b_n = 1$, tad $2 + c_n - 1 = 2015$ jeb $c_n = 2014$.

Atbilde: Pēc c_n definīcijas iegūstam, ka $n+1 = 2^{2014}(2m-1), m \in \mathbb{N}$, jeb $n = 2^{2014}(2m-1)-1$. Šie arī ir visi bezgalīgi daudzie atrisinājumi.

Uzdevums 1.8 (Bw2015.18): Dots n-tās pakāpes polinoms $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ ar pakāpi $n \geq 1$, kuram ir n (ne obligāti dažādas) veselas saknes. Pieņemam, ka eksistē tādi atšķirīgi pirmskaitļi $p_0, p_1, \ldots, p_{n-1}$, ka $a_i > 1$ ir p_i pilna pakāpe visiem $i = 0, \ldots, n-1$. Atrast visas iespējamās n vērtības.

Uzdevums 1.9 (Bw2015.19): Trīs pa pāriem atšķirīgi naturāli skaitļi a, b, c, kam $\gcd(a, b, c) = 1$ apmierina

$$a \mid (b-c)^2, \quad b \mid (c-a)^2, \quad c \mid (a-b)^2.$$

Pierādīt, ka neeksistē trijstūris ar malu garumiem a, b, c (ja nogriežņi savieno trīs punktus uz vienas taisnes, tie neveido trijstūri).

Uzdevums 1.10 (Bw2015.20): Katram naturālam $n \geq 2$, definējam A_n kā to naturālo skaitļu m skaitu, kas apmierina šādu īpašību: attālums no n līdz tuvākajam m daudzkārtnim ir vienāds ar attālumu no n^3 līdz tuvākajam m daudzkārtnim. Atrast visus naturālos $n \geq 2$, kam A_n ir nepāru. (Piezīme: Attālums starp diviem veseliem skaitļiem a un b ir definēts kā $|a-b|$.)

2016.g. Atlases Sacensības

Anotācija

2016.gadā BW komandu atlase notika 2 dienas; katru dienu piedāvāja 10 uzdevumus. No 2.dienas desmit uzdevumiem pieci bija par skaitļu teoriju; bez tam arī 1.dienā viens uzdevums bija par skaitļu teoriju (saistībā ar kombinatoriku).

Uzdevums 1.11 (BwTst2016.Day1.6): Dots naturāls skaitlis n, kuram var atrast pirmskaitli, kas ir mazāks nekā $\sqrt{n}$ un kas nav n dalītājs. Virkne $a_1, a_2, \ldots, a_n$ ir skaitļi $1, 2, \ldots, n$ sakārtoti kaut kādā secībā. Šai virknei atradīsim garāko augošo apakšvirkni $a_{i_1} < a_{i_2} < \cdots < a_{i_k}$, $(i_1 < \cdots < i_k)$ un garāko dilstošo apakšvirkni $a_{j_1} > \cdots > a_{j_l}$, $(j_1 < \cdots < j_l)$. Pierādīt, ka vismaz viena no šīm divām apakšvirknēm $a_{i_1}, \ldots, a_{i_k}$ un $a_{j_1}, \ldots, a_{j_l}$ satur skaitli, kas nav n dalītājs.

Atrisinājums. Par monotonām apakšvirknēm ir noderīga sekojoša teorēma.
Erdeša-Sekereša (Erdös–Szekeres) Teorēma: Naturāliem skaitļiem r un s, jebkura dažādu (reālu) skaitļu virkne, kurā ir vismaz $(r-1)(s-1)+1$ locekļi, satur vai nu monotoni augošu apakšvirkni garumā r vai arī monotoni dilstošu apakšvirkni garumā s.
Pamatojums: Ja dota $(r-1)(s-1)+1$ dažādu skaitļu virkne, apzīmējam katru tās locekli n_i ar naturālu skaitļu pārīti (a_i, b_i), kur a_i ir garums garākajai monotoni augošajai apakšvirknei, kas beidzas ar n_i, un b_i ir garums garākajai monotoni dilstošajai apakšvirknei, kas beidzas ar n_i. Ievērosim, ka jebkuri divi skaitļi šajā virknē iegūst atšķirīgus apzīmējumus: Ja $i < j$ un $n_i < n_j$, tad $a_i < a_j$; un, no otras puses, ja $i < j$ un $n_i > n_j$, tad $b_i < b_j$. Bet tā kā ir tikai $(r-1)(s-1)$ dažādi apzīmējumi, ja a_i pieder $[1, r-1]$ un b_i pieder $[1, s-1]$, tad pēc Dirihlē principa, atradīsies vērtība i, kam a_i vai b_i iziet ārpus šiem intervāliem. Ja a_i iziet ārpus intervāla, tad n_i ir skaitlis monotoni augošā virknē ar garumu vismaz r. Ja b_i iziet ārpus intervāla, tad n_i ir skaitlis monotoni dilstošā virknē ar garumu vismaz s.
Pieņemsim no pretējā: augošajā virknē $a_{i_1}, \ldots, a_{i_k}$ un dilstošajā virknē $a_{j_1}, \ldots, a_{j_l}$ visi locekļi ir n dalītāji. Abām šīm virknēm var būt kopīgs ne vairāk kā viens elements; tātad kopā ir vismaz $k+l-1$ dažādi skaitļi, kas ir n dalītāji. No otras puses, skaitlim n var būt ne vairāk kā $\lfloor\sqrt{n}\rfloor - 1$ dalītāji, kas nepārsniedz $\sqrt{n}$ (šeit mēs izmantojam uzdevumā doto – ka eksistē pirmskaitlis mazāks nekā $\sqrt{n}$, kas nav n dalītājs). Vēl var būt tikpat daudz dalītāju, kas pārsniedz $\sqrt{n}$ (šeit mēs izmantojam to, ka uz katru n dalītāju $A < \sqrt{n}$ ir piekārtojams cits n dalītājs $B = n/A > \sqrt{n}$).
Iegūstam, ka $k+l-1 \leq 2(\sqrt{n}-1) = 2\sqrt{n}-2$ jeb $k+l \leq 2\sqrt{n}-1$ jeb $k+l < 2\sqrt{n}$. Vidējais aritmētiskais $(k+l)/2 < \sqrt{n}$, tādēļ vidējais ģeometriskais (kurš nepārsniedz vidējo aritmētisko) būs $\sqrt{kl} \leq (k+l)/2 < \sqrt{n}$ jeb $kl < n$.
Apzīmējam $r-1 = k$ un $s-1 = l$. Tad $(r-1)(s-1) < n$. Mums tātad ir skaitļu virkne garumā vismaz $(r-1)(s-1)+1$. Pēc Erdeša-Sekereša teorēmas, tajā eksistē vai nu monotoni augoša virkne garumā $r = k+1$, vai monotoni dilstoša virkne garumā $s = l+1$. Tā ir pretruna, jo uzdevuma nosacījumā bija apgalvots, ka $a_{i_1} < a_{i_2} < \cdots < a_{i_k}$ ir garākā augošā un $a_{j_1} > a_{j_2} > \cdots > a_{j_l}$ ir garākā dilstošā apakšvirkne, bet sanāca, ka eksistē vēl garākas. Tādēļ pieņēmums, ka visi garāko monotono virkņu locekļi ir skaitļa n dalītāji ir aplams, t.i. kāds no šo virkņu locekļiem **nav** n dalītājs. ■

Uzdevums 1.12 (BwTst2016.Day2.6): Kāda ir izteiksmes

$$\mathrm{LKD}\left(n^2+3,(n+1)^2+3\right)$$

lielākā iespējamā vērtība naturāliem n?

Atrisinājums. Meklējam lielāko kopīgo dalītāju ar Eiklīda algoritmu. Šajos pārveidojumos jāprot dalīt polinomi ar atlikumu. (Viena mainīgā polinomus var dalīt, atrodot reizinātāju, ar kuru piereizinot dalītāju, iegūstam izteiksmi, kuru atņemot no dalāmā, noīsinās vecākais saskaitāmais.)

$$\begin{aligned}
&\mathrm{LKD}\left(n^2+3,(n+1)^2+3\right)=\mathrm{LKD}\left(n^2+3,n^2+2n+4\right)=\\
&=\mathrm{LKD}\left(n^2+3,n^2+2n+4-(n^2+3)\right)=\mathrm{LKD}\left(n^2+3,2n+1\right)=\\
&=\mathrm{LKD}\left(2n^2+6,2n+1\right)= \qquad (6)\\
&=\mathrm{LKD}\left(2n^2+6-n(2n+1),2n+1\right)=\mathrm{LKD}\left(-n+6,2n+1\right)=\\
&=\mathrm{LKD}\left(n-6,2n+1\right)= \qquad (7)\\
&=\mathrm{LKD}\left(n-6,2n+1-2(n-6)\right)=\mathrm{LKD}\left(n-6,13\right)
\end{aligned}$$

Izteiksmē (6) pirmais LKD(...) arguments tika pareizināts ar 2 (lielākais kopīgais dalītājs no tā nemainījās, jo otrs arguments joprojām ir nepāru skaitlis, kas ar 2 nedalās). Līdzīgi izteiksmē (7) pirmajam argumentam zīme tika nomainīta uz pretējo. Abas manipulācijas neiespaido rezultātu, bet atvieglo polinomu dalīšanu.
Esam ieguvuši, ka abu izteiksmju lielākais kopīgais dalītājs vienāds ar LKD$(n-6,13)$, t.i. tas nevar pārsniegt skaitli 13. Skaitli 13 var sasniegt, ja izvēlas, piemēram, $n=6$. Šajā gadījumā

$$\mathrm{LKD}\left(n^2+3,(n+1)^2+3\right)=\mathrm{LKD}(36+3,49+3)=\mathrm{LKD}(39,52)=13$$

Atbilde. Lielākā iespējamā $\mathrm{LKD}\left(n^2+3,(n+1)^2+3\right)$ vērtība ir 13.

Uzdevums 1.13 (BwTst2016.Day2.7): Vai var atrast piecus tādus pirmskaitļus p,q,r,s,t, ka

$$p^3+q^3+r^3+s^3=t^3?$$

Atrisinājums. Pamatosim, ka viens no pirmskaitļiem, piemēram, p ir 2. No pretējā: Ja visi 5 pirmskaitļi būtu nepāru, tad mēs iegūtu, ka 4 nepāru skaitļu summa ir nepāru skaitlis. Pretruna.
Aplūkosim atlikumus, kādus veido veselu skaitļu kubi, dalot ar 7. Pārlasot visas 7 kongruenču klases (t.i. skaitļus a, kas dod visus iespējamos atlikumus $0,1,2,3,4,5,6$, tos dalot ar 7), iegūstam, ka

$$\begin{cases}
a^3\equiv 1 \pmod 7, & \text{ja } a\equiv 1 \text{ vai } a\equiv 2 \text{ vai } a\equiv 4 \pmod 7\\
a^3\equiv 6 \pmod 7, & \text{ja } a\equiv 3 \text{ vai } a\equiv 5 \text{ vai } a\equiv 6 \pmod 7\\
a^3\equiv 0 \pmod 7, & \text{ja } a\equiv 0 \pmod 7
\end{cases}$$

Tā kā viens no kreisās puses saskaitāmajiem ir 2^3 (atlikums 1, dalot ar 7), tad ir tikai nedaudzi veidi, kā tam pieskaitot vēl 3 kongruenču klases, izvēloties no 0, 1, 6 pēc (mod 7) varam iegūt summu 0, 1 vai 6, kas varētu atbilst kāda vesela skaitļa kubam:

$$\begin{cases}
1+(0+0+0) &\equiv 1 \pmod 7\\
1+(0+0+6) &\equiv 0 \pmod 7\\
1+(0+1+6) &\equiv 1 \pmod 7\\
1+(0+6+6) &\equiv 6 \pmod 7\\
1+(1+6+6) &\equiv 0 \pmod 7
\end{cases}$$

Faktiski, $1+(1+6+6)\equiv 0$ nav iespējams panākt, jo tad sanāktu, ka saskaitot četru pirmskaitļu kubus, var iegūt 7^3. Bet, pat izvēloties pašus lielākos pirmskaitļus, kuru kubi dotu attiecīgi atlikumus 1, 6 un 6, mēs dabūtu $2^3+(3^3+5^3+5^3)=285<343=7^3$. Tādēļ ekvivalences kreisajā pusē noteikti viens no

četriem saskaitāmajiem ir kongruenču klase 0, kuru dod vienīgi pirmskaitlis, kas vienāds ar 7 (jebkurš cits skaitlis, kurš dalās ar 7 nav pirmskaitlis). Apzīmējumus izvēlamies tā, lai $q = 7$.
Esam ieguvuši vienādojumu $2^3 + 7^3 + r^3 + s^3 = t^3$. Tālāk aplūkojam kongruenču klases pēc (mod 13). Kongruenču klases no 0 līdz 12, ja tās kāpina kubā, dod šādus 13 rezultātus:

$$\{0, 1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12\}.$$

Ņemot vērā to, ka divi no pirmskaitļiem kreisajā pusē ir 2 un 7, un $2^3 \equiv 8 \pmod{13}$, bet $7^3 \equiv 5 \pmod{13}$, tad šo abu kongruenču klašu summa ir 0. Piemeklēt r^3, s^3 un t^3 starp kongruenču klasēm $\{0, 1, 5, 8, 12\}$ tā, lai $2^3 + 7^3 + r^3 + s^3$ un t^3 piederētu tai pašai klasei (mod 13) var tikai divos veidos, ja neņem vērā abu iekavās esošo saskaitāmo secību: $8 + 5 + (1 + 12) \equiv 0$ vai arī $8 + 5 + (5 + 8) \equiv 0$. Jebkurā gadījumā sanāk, ka t^3 un arī t ir kongruents 0 jeb dalās ar 13. Tādēļ $t = 13$, jo tas ir vienīgais pirmskaitlis, kurš dalās ar 13.
Iegūstam, ka jārisina vienādojums $2^3 + 7^3 + r^3 + s^3 = 13^3$. Turklāt, kongruences pēc (mod 7) parāda, ka vienīgā iespēja ir $1 + 0 + 6 + 6 \equiv 6 \pmod{7}$, jo 13^3 labajā pusē ir kongruents skaitlim 6. Bet šajā situācijā r^3 un s^3 atrast vairs nav iespējams, jo vienīgais pirmskaitlis, kurš nepārsniedz 13 un dod atlikumu 6, dalot ar 7 ir skaitlis 13. Bet, acīmredzot, $2^3 + 7^3 + 13^3 + 13^3 \neq 13^3$. Iegūta pretruna. Tādēļ pirmskaitļi p, q, r, s, t, kas apmierinātu uzdevuma vienādību, neeksistē. ■

Uzdevums 1.14 (BwTst2016.Day2.8): Atrisināt veselos skaitļos vienādojumu sistēmu:

$$\begin{cases} a^3 &= abc + 2a + 2c \\ b^3 &= abc - c \\ c^3 &= abc - a + b \end{cases}$$

Uzdevums 1.15 (BwTst2016.Day2.9): Pierādīt, ka vienādojumam

$$x^{2015} + y^{2015} = z^{2016}$$

ir bezgalīgi daudz atrisinājumu, kur x, y un z ir dažādi naturāli skaitļi.
Atrisinājums. Ja kāpinātājs 2015 šķiet pārāk liels, varam sākt ar vienādojumu $x^2 + y^2 = z^3$. Var uzminēt dažus atrisinājumus (tiesa, ar sakrītošām saknēm): $(x, y, z) = (10, 5, 5)$ un $(x, y, z) = (30, 10, 10)$. Varam noskaidrot, kā ģenerēt arvien jaunas saknes z: $5 = 2^2 + 1^2$, $10 = 3^2 + 1^2$, $13 = 3^2 + 2^2$.
Atgriežamies pie sākotnējā vienādojuma...
Izvēlamies divus naturālus skaitļus $a > b > 1$. Apzīmējam $N = a^{2015} + b^{2015}$. Tad $(x, y, z) = (aN, bN, N)$ ir vienādojuma atrisinājums. Pārbaude:

$$\begin{aligned} (aN)^{2015} + (bN)^{2015} &= a^{2015}N^{2015} + b^{2015}N^{2015} = \\ &= \left(a^{2015} + b^{2015}\right) N^{2015} = \\ &= N \cdot N^{2015} = N^{2016}. \end{aligned}$$

Tā kā skaitļus a un b var izvēlēties bezgalīgi daudzos veidos un arī izteiksmei N var būt bezgalīgi daudz vērtību, tad vienādojumam ir bezgalīgi daudz atrisinājumu. ■

Uzdevums 1.16 (BwTst2016.Day2.10): Kādiem naturālu skaitļu pāriem (a, b) izteiksmes

$$\left(a^6 + 21a^4b^2 + 35a^2b^4 + 7b^6\right)\left(b^6 + 21b^4a^2 + 35b^2a^4 + 7a^6\right)$$

vērtība ir pirmskaitļa pakāpe?

Uzdevums 1.17 (Bw2016.1): Atrast visus pirmskaitļu pārus (p, q), kuriem

$$p^3 - q^5 = (p+q)^2.$$

Atrisinājums: Lai saprastu, kādas var būt starpības $p^3 - q^5$, izrakstīsim tās dažādiem pirmskaitļu pāriem, aplūkojot pirmās astoņas pirmskaitļa p vērtības no 2 līdz 19; un katrai no tām – pirmskaitļa q vērtības, kam starpība $p^3 - q^5$ sanāk pozitīva. Meklēsim, kuras no šīm starpībām ir pilni kvadrāti, vai pat apmierina sakarību $(p+q)^2$. Pirmskaitļa p vērtība mainīsies pa tabulas kolonnām, pirmskaitļa q vērtība – pa rindiņām.

$p=$	2	3	5	7	11	13	17	19
$q=2$	–	–	93	311	1299	2165	4881	6827
$q=3$	–	–	–	100	1088	1954	4670	6616
$q=5$	–	–	–	–	–	–	1788	3734

Vienīgais skaitlis šajā tabulā, kurš ir pilns kvadrāts ir $7^3 - 3^5 = 343 - 243 = 100$. Tas arī vienāds ar $(7+3)^2$. Pamatosim, ka vienādojumam citu atrisinājumu nav.

Ņemot vērā, ka p un q ir pirmskaitļi, aplūkosim kongruenču klases pēc kāda pirmskaitļa r moduļa. Lai kādu pirmskaitli mēs izvēlētos, būs tikai galīgs skaits potenciālo atrisinājumu, kuriem p vai q ir kongruenti ar 0 pēc attiecīgā pirmskaitļa moduļa (jo vienīgais pirmskaitlis, kurš dalās ar r bez atlikuma, ir viņš pats).

Izvēloties $r = 2$, pretruna nesanāk, jo abi p un q var būt nepāru skaitļi un tad vienādojuma abās pusēs ir pāru skaitļi.

Izvēlēsimies $r = 3$ un aprakstīsim visus $3 \cdot 3 = 9$ gadījumus, kā p un q pieder kongruenču klasēm 0, 1 un 2. Visas kongruences šajā tabulā ir (mod 3):

p	q	p^3	q^5	$(p+q)^2$	$p^3 - q^5 \equiv (p+q)^2$
$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	`true`
$\equiv 0$	$\equiv 1$	$\equiv 0$	$\equiv 1$	$\equiv 1$	`false`
$\equiv 0$	$\equiv 2$	$\equiv 0$	$\equiv 2$	$\equiv 1$	`true`
$\equiv 1$	$\equiv 0$	$\equiv 1$	$\equiv 0$	$\equiv 1$	`true`
$\equiv 1$	$\equiv 1$	$\equiv 1$	$\equiv 1$	$\equiv 1$	`false`
$\equiv 1$	$\equiv 2$	$\equiv 1$	$\equiv 2$	$\equiv 0$	`false`
$\equiv 2$	$\equiv 0$	$\equiv 2$	$\equiv 0$	$\equiv 1$	`false`
$\equiv 2$	$\equiv 1$	$\equiv 2$	$\equiv 1$	$\equiv 0$	`false`
$\equiv 2$	$\equiv 2$	$\equiv 2$	$\equiv 2$	$\equiv 1$	`false`

Vienīgie (p, q) kongruenču klašu pāri (mod 3), kuriem vienādojuma kreisā un labā puse pieder tai pašai kongruenču klasei ir sekojoši: $(0,0)$, $(0,2)$, $(1,0)$. Tas nozīmē, ka vai nu p vai q, vai tie abi ir vienādi ar pirmskaitli 3. Viegli redzēt, ka p vispār nevar būt vienāds ar 3, jo atņemot no tā jebkura pirmskaitļa piekto pakāpi, rezultāts ir negatīvs.

Tādēļ vienīgā iespēja, kas paliek: $q = 3$. Pamatosim, ka p nevar būt lielāks par 7. Tā kā pie $p = 7$ izpildās vienādība $p^3 - 3^5 = (p+3)^2$, tad aplūkojam, par kādu skaitli palielinās abas puses šajā vienādībā, ja p aizstāj ar $p+1$. Iegūstam, ka kreisās un labās puses izmaiņas ir atšķirīgas:

$$\begin{aligned} ((p+1)^3 - 3^5) - (p^3 - 3^3) &= (p+1)^3 - p^3 = 3p^2 + 3p + 1 \\ ((p+1)+3)^2 - (p+3)^2 &= (p^2 + 8p + 16) - (p^2 + 6p + 9) = 2p + 7 \end{aligned} \tag{8}$$

Ja $p > 7$, tad acīmredzot $3p^2 + 3p + 1$ ir lielāks pieaugums nekā $2p + 7$, jo $3p > 2p$ un $3p^2 + 1 > 7$. Tādēļ nevienai vērtībai $p > 7$ nevar būt $p^3 - 3^5 = (p+3)^2$, jo šī vienādojuma kreisā puse aug straujāk nekā labā.

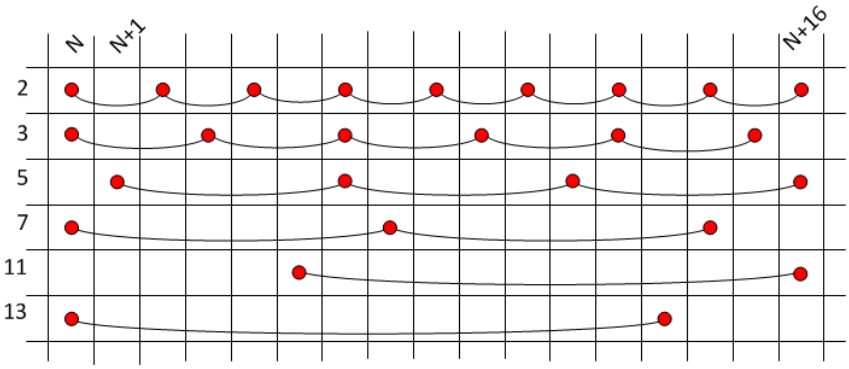
Atbilde: Vienīgais vienādojuma atrisinājums ir $(p, q) = (7, 3)$.

Uzdevums 1.18 (Bw2016.2): Pierādīt vai atspēkot sekojošus apgalvojumus.

(a) Visiem $k \geq 2$, jebkura k pēc kārtas sekojošu naturālu skaitļu virkne satur skaitli, kas nedalās ne ar vienu pirmskaitli, kas ir mazāks par k.

(b) Visiem $k \geq 2$, jebkura k pēc kārtas sekojošu naturālu skaitļu virkne satur skaitli, kas ir savstarpējs pirmskaitlis ar visiem pārējiem šīs virknes locekļiem.

Atrisinājums. Ja jebkura k pēc kārtas sekojošu naturālu skaitļu virkne saturētu skaitli $x \in \{a, \ldots, a + (k-1)\}$, kas nedalās ar pirmskaitļiem mazākiem par k, tad šis skaitlis x būtu savstarpējs pirmskaitlis ar jebkuru citu skaitli starp a un $a + (k-1)$, jo mazākais skaitļa x dalītājs, kas atšķirīgs no 1 būtu lielāks vai vienāds ar k, t.i. tas pārsniegtu attālumu no x līdz nogriežņa $[a, a + (k-1)]$ galapunktiem (un arī visiem punktiem, kuri ir starp tiem). Tātad no pirmā apgalvojuma seko otrais.
Tomēr abi šie apgalvojumi ir aplami, jo ir iespējams atrast $k = 17$ pēc kārtas sekojošus naturālus skaitļus no N līdz $N + 16$, no kuriem ikviens dalās ar kādu pirmskaitli no 2 līdz 13. Un arī ikvienam no šiem 17 skaitļiem ir kāds kopīgs dalītājs (lielāks par 1) ar kādu citu skaitli no šīs virknes. Konstrukciju veicam, atzīmējot atsevišķās rindās ar bumbulīšiem skaitļus, kuri dalās attiecīgi ar 2, 3, 5, 7, 11 un 13. Bumbulīšu rindās "sākumfāzes" nesakrīt (nav tādas kolonnas, kurā bumbulīši ir katrā rindā) - jo citādi nākamajā kolonnā nebūtu neviena bumbulīša (šāds skaitlis nedalītos ne ar vienu pirmskaitli no 2 līdz 13). Tai vietā "sākumfāzes" ir nobīdītas tā, lai vismaz viens bumbulītis atrastos katrā kolonnā; un vienlaikus - katrā rindā būtu vismaz divi bumbulīši, t.i. būtu redzami skaitļi, kuri nav savstarpēji pirmskaitļi, jo tiem ir kopīgs dalītājs, kas lielāks par 1.



Vēl jānoskaidro jautājums, vai N var atrast tā, lai rastos visi zīmējumā redzamie atlikumi ar pirmskaitļiem no 2 līdz 13 jeb mums vajadzīgās "sākumfāzes". Citiem vārdiem, vai eksistē tāds naturāls N, kam vienlaicīgi izpildās 6 kongruences:

$$\begin{cases} N \equiv 0 \pmod 2 \\ N \equiv 0 \pmod 3 \\ N \equiv 4 \pmod 5 \\ N \equiv 0 \pmod 7 \\ N \equiv 6 \pmod{11} \\ N \equiv 0 \pmod{13} \end{cases}$$

Tā kā moduļi ir pēc skaitļiem $2, 3, 5, 7, 11, 13$ (t.i. pēc skaitļiem, kam nav kopīgu dalītāju), visas sešas kongruences nevar nonākt savstarpējā pretrunā; vienmēr eksistē atrisinājums (Ķīniešu atlikumu teorēma). Pirmā, otrā, ceturtā un sestā kongruence izpildās, ja vien $N = 2 \cdot 3 \cdot 7 \cdot 13 \cdot k$ kādam naturālam k. Izvēloties $k = 4$, izpildās arī atlikušās divas kongruences. Tātad $N = 2184$ un 17 pēc kārtas sekojošie skaitļi ir šādi:

$$\{2184, 2185, 2186, \ldots, 2198, 2199, 2200\}.$$

Uzdevums 1.19 (Bw2016.3): Kuriem naturāliem $n = 1, \ldots, 6$ vienādojumam

$$a^n + b^n = c^n + n$$

eksistē atrisinājums veselos skaitļos?

Atrisinājums.

- Ja $n = 1$, tad eksistē atrisinājums veselos skaitļos, piemēram, $(a, b, c) = (0, 0, -1)$ un $0+0 = -1+1$. Ir, protams, arī daudzi citi atrisinājumi, kur divu skaitļu summa ir par 1 lielāka nekā trešais skaitlis.
- Ja $n = 2$, tad pietiek aplūkot nenegatīvus a, b, c, jo $(-a)^2 = a^2$. Der, piemēram, $(a, b, c) = (1, 1, 0)$, jo $1^2 + 1^2 = 0 + 2$. Ir arī vairāki citi atrisinājumi, piemēram, $3^2 + 3^2 = 4^2 + 2$ un $5^2 + 11^2 = 12^2 + 2$.
- Ja $n = 3$, tad var uzminēt dažus atrisinājumus. Piemēram, $(a, b, c) = (1, 1, -1)$, jo $1^3 + 1^3 = (-1)^3 + 3$. Un arī $(a, b, c) = (4, 4, 5)$, jo $4^3 + 4^3 = 5^3 + 3$. Pēdējo var pārkombinēt ar citām zīmēm: $(a, b, c) = (-5, 4, -4)$, jo $(-5)^3 + 4^3 = (-4)^3 + 3$.
- Ja $n = 4$, tad aplūkojam vienādību $a^4 + b^4 = c^4 + 4$ pēc 8 moduļa. Kāpinot ceturtajā pakāpē visas kongruenču klases $(0, 1, \ldots, 7)$, iegūsim, ka vesela skaitļa ceturtā pakāpe a^4 var dot atlikumu 0 vai 1, dalot ar 8. Tātad labajā pusē $c^4 + 4$ dos atlikumu 4 vai 5, dalot ar 8. Nevienu no šiem diviem atlikumiem nav iespējams iegūt, saskaitot skaitļus $a^4 + b^4$ no kongruenču klasēm 0 un 1 (varam aplūkot visus 4 iespējamos pārus). Tātad $a^4 + b^4 \neq c^4 + 4$ jebkādiem veseliem a, b, c.
- Ja $n = 5$, tad aplūkojam vienādību $a^5 + b^5 = c^5 + 5$ pēc 11 moduļa. Kāpinot piektajā pakāpē visas kongruenču klases $(0, 1, \ldots, 10)$, iegūsim, ka vesela skaitļa piektā pakāpe a^5 var dot kādu no atlikumiem $0, 1, 10$, dalot ar 11. Tātad labajā pusē $c^5 + 5$ dos atlikumu 4, 5 vai 6, dalot ar 11. Nevienu no šiem trim atlikumiem nav iespējams iegūt, saskaitot skaitļus $a^5 + b^5$ no kongruenču klasēm $0, 1, 10$ (varam aplūkot visus 9 iespējamos pārus). Tātad $a^5 + b^5 \neq c^5 + 5$ jebkādiem veseliem a, b, c.
- Ja $n = 6$, tad aplūkojam vienādību $a^6 + b^6 = c^6 + 6$ pēc 13 moduļa. Kāpinot sestajā pakāpē visas kongruenču klases $(0, 1, \ldots, 12)$, iegūsim, ka vesela skaitļa sestā pakāpe a^6 var dot kādu no atlikumiem $0, 1, 12$, dalot ar 13. Tātad labajā pusē $c^6 + 6$ dos atlikumu 5, 6 vai 7, dalot ar 13. Nevienu no šiem trim atlikumiem nav iespējams iegūt, saskaitot skaitļus $a^6 + b^6$ no kongruenču klasēm $0, 1, 10$ (varam aplūkot visus 9 iespējamos pārus). Tātad $a^6 + b^6 \neq c^6 + 6$ jebkādiem veseliem a, b, c.

Pie $n = 1, 2, 3$ vienādojumam eksistē atrisinājumi (pie $n = 1, 2$ tie ir pat diezgan daudzi). Savukārt pie $n = 4, 5, 6$ vienādojumam atrisinājuma veselos skaitļos nav.

Piezīme: Kā var uzzināt, ka skaitļu piektās pakāpes ir interesanti aplūkot pēc 11 moduļa, bet sestās pakāpes pēc 13 moduļa? Atbilde ir - mazā Fermā teorēma. Kā zināms, ja p ir pirmskaitlis un a nedalās ar p, tad $a^{p-1} \equiv 1 \pmod{p}$. Tādēļ, jebkuru skaitli (izņemot tos, kuri dalās ar 11) kāpinot 10 pakāpē, iegūsim atlikumu 1, dalot ar 11. Kāpinot divreiz mazākā pakāpē, t.i. a^5, iegūsim nedaudz vairāk iespēju: jo šajā gadījumā mums der arī $a^5 \equiv 10 \equiv -1$, jo arī tad $a^10 = (a^5)^2 \equiv (-1)^2 = 1$.
Līdzīgi var izspriest arī par a^6 pēc 13 moduļa. Mazā Fermā teorēma mums pasaka, kādi moduļi var būt interesanti. Pēc tam jau varam pārlasīt dažādus gadījumus un iegūt pretrunu, ja nu izrādās, ka vienādojumā abas puses dod dažādus atlikumus dalot ar to pašu skaitli (attiecīgi 11 un 13). Tā ir pretruna, kas pamato, ka vienādojumam atrisinājuma nav.

Uzdevums 1.20 (Bw2016.4): Dots naturāls skaitlis n un tādi veseli skaitļi a, b, c, d, ka gan $a + b + c + d$, gan $a^2 + b^2 + c^2 + d^2$ dalās ar n. Pierādīt, ka arī $a^4 + b^4 + c^4 + d^4 + 4abcd$ dalās ar n.

Atrisinājums: No abām izteiksmēm, kuras dalās ar n, ar saskaitīšanu, atņemšanu un reizināšanu centīsimies iegūt pēdējo izteiksmi, lai pamatotu, ka arī tā dalās ar n. Kāpinot un savstarpēji reizinot skaitļu a, b, c, d summu un kvadrātu summu, ievērojam, ka rezultāts ir bieži izsakāms ar mainīgo burtu a, b, c, d *simetriskiem polinomiem*. Par simetriskiem polinomiem uzskatīsim tos, kuru vērtība nemainās, ja burtu apzīmējumus a, b, c, d kaut kādā veidā samaina vietām. Ieviesīsim apzīmējumus sekojošiem 5 simetriskiem polinomiem:

$$\begin{cases} v &= a^4+b^4+c^4+d^4 \\ w &= a^3b+a^3c+a^3d+b^3a+b^3c+b^3d+c^3a+c^3b+c^3d+d^3a+d^3b+d^3c \\ x &= a^2b^2+a^2c^2+a^2d^2+b^2c^2+b^2d^2+c^2d^2 \\ y &= a^2bc+a^2bd+a^2cd+b^2ac+b^2ad+b^2cd+c^2ab+c^2ad+c^2bd+d^2ab+d^2ac+d^2bc \\ z &= abcd \end{cases}$$

Ar jaunajiem apzīmējumiem v, w, x, y, z varam izteikt dažas izteiksmes, kuras iegūtas no a, b, c, d summas un kvadrātu summas – un kuras tātad arī dalās ar n:

$$\begin{cases} (a+b+c+d)^4 &= v &+4w &+6x &+12y &+24z &\equiv 0 \pmod n \\ (a+b+c+d)^2(a^2+b^2+c^2+d^2) &= v &+2w &+2x &+2y &&\equiv 0 \pmod n \\ (a^2+b^2+c^2+d^2)^2 &= v &&+2x &&&\equiv 0 \pmod n \\ \hline & v &&&&+4z &\equiv 0 \pmod n \end{cases}$$

Augšējās trīs vienādības var pamatot "ar rupju spēku" – ievietojot v, w, x, y, z izteiksmes un atverot iekavas. Bet var pamatot arī ātrāk; piemēram fakts, ka $(a+b+c+d)^4$ atverot iekavas pie saskaitāmā a^3b (un jebkura cita saskaitāmā, kur kubs reizināts ar pirmo pakāpi) būs koeficients 4 izriet no kombinatoriska apsvēruma: Ir četras vienādas iekavas; tās iekavas, no kurām ņemt burtu b, var izvēlēties 4 dažādos veidos. Tādēļ koeficients ir 4, un varam rakstīt "$4w$" mūsu izteiksmē. Līdzīgi pamatojam, ka jāraksta arī "$6x$", "$12y$" un "$24z$". Ir spēkā "polinomiālā koeficienta formula": koeficients pie a^3b ir $\frac{4!}{3!1!}$; koeficients pie a^2b^2 ir $\frac{4!}{2!2!}$ utml.
Zem svītras rakstītā kongruence pagaidām nav pamatota (tā mums ir jāpierāda). Bet tā ir šeit pierakstīta klāt kā pieņēmums. Mēģināsim izsecināt, kādu kongruenci tagad varam izsecināt no visām četrām rindiņām (trim dotajām kongruencēm un viena pieņēmuma). Tad mums būs skaidrs, kas mums būtu vēl jāpamato, lai iegūtu pierādāmo apgalvojumu.
Izslēgsim no kongruenču sistēmas mainīgo v un pēc tam arī mainīgo w. To darām tādēļ, ka ar augstiem kāpinātājiem uzrakstītas izteiksmes (a^4 vai a^3b) varētu būt grūtāk dalīt reizinātājos. Mēs to nepamatojam, bet gan izmantojam kā intuīciju, lai saprastu, kādā virzienā taisīt algebriskos pārveidojumus. Lai izslēgtu v, no 1.,2.,3. kongruencēm atņemsim 4. kongruenci (to, kura ir zem svītras). Pēc atņemšanas paliks pāri trīs kongruences, kurās vairs nav burta v:

$$\begin{cases} 4w &+6x &+12y &+20z &\equiv 0 \pmod n \\ 2w &+2x &+2y &-4z &\equiv 0 \pmod n \\ &2x &&-4z &\equiv 0 \pmod n \end{cases}$$

Lai izslēgtu burtu w, pareizināsim vidējo kongruenci ar 2 un atņemsim to no augšējās. Paliks divas kongruences, kurās vairs nav burta w:

$$\begin{cases} +2x &+8y &+28z &\equiv 0 \pmod n \\ 2x &&-4z &\equiv 0 \pmod n \end{cases}$$

Visbeidzot izslēgsim burtu x, atņemot otro kongruenci no pirmās:

$$8y+32z \equiv 0 \pmod n.$$

Šī pēdējā kongruence mums būtu jāpamato. Tad ir cerība, to sakombinējot ar trim jau pierādītajām kongruencēm, iegūt $v+4z \equiv 0 \pmod n$, kuru mums šinī uzdevumā vajag. Pārrakstām y un z, ievietojot burtus a, b, c, d un aizstājot $32z = 32abcd$ ar $8abcd+8abcd+8abcd+8abcd$:

$$
\begin{aligned}
&8a^2bc + 8a^2bd + 8a^2cd + 8b^2ac + 8b^2ad + 8b^2cd + \\
&+8c^2ab + 8c^2ad + 8c^2bd + 8d^2ab + 8d^2ac + 8d^2bc + \\
&+8abcd + 8abcd + 8abcd + 8abcd = \\
&= 8(a^2bc + a^2bd + a^2cd + abcd) + 8(b^2ac + b^2ad + b^2cd + abcd) + \\
&+8(c^2ab + c^2ad + c^2bd + abcd) + 8(d^2ab + d^2ac + d^2bc + abcd) = \\
&= 8a(abc + abd + acd + bcd) + 8b(bac + bad + bcd + acd) + \\
&+8c(cab + cad + cbd + abd) + 8d(dab + dac + dbc + abc) = \\
&= (8a + 8b + 8c + 8d)(abc + abd + acd + bcd).
\end{aligned}
$$

Pēdējā izteiksme dalās ar $a+b+c+d$, tātad tā dalās ar n. Esam pamatojuši, ka $8y + 32z \equiv 0 \pmod{n}$. Visbeidzot kombinēsim šo sakarību ar trim sākotnējām kongruencēm, lai pārliecinātos, ka var iegūt arī, ka $v + 4z$ dalās ar n.
Rakstām jaunu kongruenču sistēmu (šoreiz tajā nebūs zemsvītras pieņēmumu):

$$
\begin{cases}
v & +4w & +6x & +12y & +24z & \equiv & 0 & (\mathrm{mod}\ n) & \mid \cdot 1 \\
v & +2w & +2x & +2y & & \equiv & 0 & (\mathrm{mod}\ n) & \mid \cdot(-2) \\
v & & +2x & & & \equiv & 0 & (\mathrm{mod}\ n) & \mid \cdot(-1) \\
& & & 8y & +32z & \equiv & 0 & (\mathrm{mod}\ n) & \mid \cdot(-1)
\end{cases}
$$

Reizinot visas kongruences ar skaitļiem, kas norādīti labajā pusē aiz svītras un saskaitot tās kopā, iegūsim:

$$-2v - 8z \equiv 0 \pmod{n} \text{ jeb } 2v + 8z \equiv 0 \pmod{n}.$$

Iespējami divi gadījumi.

- Ja n ir nepāru skaitlis, tad kongruenci var izdalīt ar 2 un no šī uzreiz seko, ka arī $v + 4z = (a^4 + b^4 + c^4 + d^4) + 4abcd$ dalās ar n.
- Ja n ir pāru skaitlis, tad četru kongruenču sistēmu var pārrakstīt kā kongruences (mod $2n$). Tas ir tāpēc, ka visas izteiksmes $(a+b+c+d)^4$, $(a+b+c+d)^2(a^2+b^2+c^2+d^2)$ un $(a^2+b^2+c^2+d^2)^2$ dalās ne vien ar n, bet arī ar n^2 (tātad arī ar $2n$, ja n ir pāru). Un arī $8y + 32z$ dalās ar $2n$, jo var pamatot, ka $4y + 16z$ dalās ar n (atkārtojot līdzīgu spriedumu ar garas izteiksmes dalīšanu reizinātājos). Tātad, varam pamatot, ka $2v + 8z$ dalās ar $2n$ un tādēļ $v + 4z$ dalās ar n.

■

Uzdevums 1.21 (Bw2016.5): Dots pirmskaitlis $p > 3$, kuram $p \equiv 3 \pmod{4}$. Dotam naturālam skaitlim a_0 virkni $a_0, a_1, \ldots$ definē kā $a_n = a_{n-1}^{2^n}$ visiem $n = 1, 2, \ldots$. Pierādīt, ka a_0 var izvēlēties tā, ka apakšvirkne $a_N, a_{N+1}, a_{N+2}, \ldots$ nav konstanta pēc moduļa p nevienam naturālam N.

Atrisinājums: Ievietojot rekurentajās izteiksmēs, izteiksim visus virknes a_n locekļus ar a_0. Ir spēkā sekojošas vienādības:

$$
\begin{aligned}
a_1 &= (a_0)^{2^1} \\
a_2 &= (a_1)^{2^2} = (a_0)^{2^1 \cdot 2^2} = (a_0)^{2^{1+2}} \\
a_3 &= (a_2)^{2^3} = (a_0)^{2^{1+2} \cdot 2^3} = (a_0)^{2^{1+2+3}} \\
&\ldots \\
a_n &= (a_0)^{2^{1+2+\ldots+n}}
\end{aligned}
$$

Apgalvojums A (Mazā Fermā teorēma): Katram pirmskaitlim p un katram a, kas nedalās ar šo pirmskaitli, ir spēkā sakarība $a^{p-1} \equiv 1 \pmod{p}$.
Pamatojums: Teorēmas pierādījumu sk. [3]. □
No šīs teorēmas izriet, ka a_n vērtības pēc moduļa var noteikt arī tad, ja mums zināms $2^{1+2+\ldots+n}$ atlikumi, dalot ar $p-1$. Tas tādēļ, ka

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

t.i. kāpinātājus, kas ir $(p-1)k$ drīkst atmest katram veselam k un paliek pāri 2^r, kur r ir atlikums, dalot $1+2+\ldots+n$ ar $p-1$.

Apgalvojums B: Dots naturāls skaitlis k. Tādā gadījumā starp atlikumiem, kurus dod $2^{1+2+\ldots+n}$, dalot ar $4k+2$ (kur n pieņem pēc kārtas visas naturālās vērtības $1, 2, \ldots$) ne vairāk kā divi blakusesoši atlikumi var būt vienādi.
Pamatojums: Apzīmēsim r_n: atlikums, dalot $2^{1+2+\ldots+n}$, dalot ar $4k+2$. Pieņemsim no pretējā, ka ir 3 pēc kārtas sekojoši vienādi atlikumi: r_N, r_{N+1} un r_{N+2} ir vienādi. Apzīmēsim $2^{1+2+\ldots+N}$ ar L. Šajā gadījumā vienlaikus izpildīsies divas sakarības:

$$r_N \cdot 2^{N+1} \equiv r_{N+1} = r_N \pmod{4k+2}$$
$$r_{N+1} \cdot 2^{N+2} \equiv r_{N+2} = r_N \pmod{4k+2}$$

Pielīdzinām abu kongruenču kreisās puses:

$$r_N \cdot 2^{N+1} \equiv r_{N+1} \cdot 2^{N+2} \pmod{4k+2}.$$

Tā kā bijām pieņēmuši, ka $r_n = r_{N+1}$, tad apzīmējam kongruenču klasi $x \equiv r_N \cdot 2^{N+1} \equiv 2^{1+2+\ldots+N} \cdot 2^{N+1}$ un iegūstam:

$$x \equiv 2x \pmod{4k+2}.$$

Tātad eksistē tāda kongruenču klase x, kurai x ir kongruents ar $2x$ jeb $x \equiv 0$. Bet x ir izsakāms kā divnieka pakāpe un tā nevar bez atlikuma dalīties ar $4k+2$, tādēļ iegūta pretruna. Līdz ar to, nevar eksistēt 3 pēc kārtas sekojoši vienādi atlikumi, ja dala pakāpes $2^{1+2+\ldots+n}$ (kur $n = 1, 2, \ldots$) ar $4k+2$. □

Apgalvojums C (Teorēma par primitīvo sakni): Katram pirmskaitlim p eksistē primitīva sakne pēc p moduļa, t.i. tāds skaitlis a, kuram kongruenču klases $a^1, a^2, \ldots, a^{p-1}$ pieņem visas vērtības $1, 2, \ldots, p-1$ kaut kādā secībā.
Pamatojums: Pierādījumu sk. [2]. □.
Ja mēs izvēlamies a_0 kā vienu no primitīvajām saknēm pēc p moduļa, tad $a_0^{r_N}$, $a_0^{r_{N+1}}$ un $a_0^{r_{N+2}}$ nevarēs visi 3 būt kongruenti pēc p moduļa, jo arī atlikumi r_N, r_{N+1} un r_{N+2} nav visi kongruenti pēc $p-1 = 4k+2$ moduļa un neviens no tiem nav 0. Primitīvo sakni kāpinot dažādās pakāpēs no kopas $\{1, 2, \ldots, p-1\}$ iegūsim nekongruentus rezultātus.
Pēc Mazās Fermā teorēmas seko, ka tad arī attiecīgi virknes (a_n) locekļi: $a_N, a_{N+1}, aN+2$ nav visi vienādi, jo $a_N \equiv a_0^{r_N}$, $a_{N+1} \equiv a_0^{r_{N+1}}$, $a_{N+2} \equiv a_0^{r_{N+2}}$ pēc p moduļa. ■
Piezīme: Šajā uzdevumā p nevar izvēlēties kā Fermā pirmskaitli, piemēram $5, 17, 257$ utt. No otras puses, nedaudz pamainot spriedumu, var pamatot, ka virkne a_n nav konstanta pēc moduļa p arī tad, ja $p = 13$ vai kāds cits skaitlis, kam $p-1$ satur nepāru pirmreizinātājus. Tādēļ nav obligāti, lai p dotu atlikumu 3, dalot ar 4.

Uzdevums 1.22 (Bw2016.11): Kopa A sastāv no 2016 dažādiem skaitļiem, visi šo skaitļu pirmreizinātāji ir mazāki par 30. Pierādīt, ka kopā A var atrast tādus 4 dažādus skaitļus a, b, c un d, ka $abcd$ ir naturāla skaitļa kvadrāts.

Atrisinājums. Par 30 mazāki ir tieši 10 pirmskaitļi - $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Skaitlis $abcd$ ir naturāla skaitļa kvadrāts tikai tad, ja tas satur ikvienu no šiem pirmskaitļiem pāru pakāpē. Tādēļ mūsu uzdevums ir atrast tādus a, b, c, d, kam kāpinātāji pie katra no desmit pirmskaitļiem summēsies par pāru skaitļiem.

Definīcija: Ar $\nu_p(n)$ (grieķu burtu ν lasa "nī" latviski vai "nu" `['nju:]` angliski) apzīmējam pirmskaitļa p augstāko pakāpi, kas atrodama skaitļa n sadalījumā pirmreizinātājos. T.i. ja $n = p_1^{a_1} \cdots p_k^{a_k}$ ir sadalījums pirmreizinātājos, tad $\nu_{p_i}(n) = a_i$ (vai arī $\nu_{p_i}(n) = 0$, ja pirmskaitlis p_i vispār neietilpst skaitļa n sadalījumā pirmreizinātājos). (Piemēram, $\nu_3(1) = 0$, $\nu_3(2) = 0$, $\nu_3(3) = 1$, $\nu_3(6) = 1$, $\nu_3(9) = 2$, $\nu_3(81) = \nu_3(162) = 4$, utt.)
Aplūkosim vispirms divu skaitļu reizinājumu, jo tad jāanalizē mazāks variantu skaits.
Apgalvojums: Reizinājums ab satur kādu pirmskaitli p pāru pakāpē divos gadījumos:

- Vai nu $\nu_p(a) \equiv \nu_p(b) \equiv 0 \pmod 2$
- Vai arī $\nu_p(a) \equiv \nu_p(b) \equiv 1 \pmod 2$

To var pamatot tā, ka reizinot divas p pakāpes ar pāru kāpinātājiem vai arī reizinot divas p pakāpes ar nepāru kāpinātājiem, rezultātā sanāks p pakāpe ar pāru kāpinātāju.
Šis apgalvojums norāda, ka reizinājumā ab kāpinātāja paritāte pie p (t.i. vai kāpinātājs ir pāru vai nepāru) ir atkarīga no p kāpinātāja paritātes abos reizinātājos a un b. Sadalīsim visus 2016 dažādos skaitļus $2^{10} = 1024$ apakškopās. Divi skaitļi a un b nonāk vienā apakškopā tikai tad, ja tiem sakrīt $\nu_p(a)$ un $\nu_p(b)$ paritātes visiem pirmskaitļiem, kas mazāki par 30. Citiem vārdiem, a un b atrodas vienā apakškopā tad un tikai tad, ja

$$\begin{cases} \nu_2(a) & \equiv & \nu_2(b) & \pmod 2 \\ \nu_3(a) & \equiv & \nu_3(b) & \pmod 2 \\ \nu_5(a) & \equiv & \nu_5(b) & \pmod 2 \\ \quad \dots & & & \\ \nu_{29}(a) & \equiv & \nu_{29}(b) & \pmod 2 \end{cases}$$

Tā kā ir pavisam 10 dažādi pirmskaitļi, tad katram no tiem paritāte var būt vai nu pāris ($\equiv 0 \pmod 2$) vai arī nepāris ($\equiv 1 \pmod 2$). Izvēloties šīs paritātes neatkarīgi vienu no otras visiem 10 pirmskaitļiem, iegūsim 1024 dažādus variantus. Dažas no atbilstošajām 1024 apakškopām var būt tukšas, citas var saturēt vairākus elementus.
Ja starp 1024 apakškopām sadala 2016 dažādus skaitļus, tad vismaz divās no apakškopām būs vismaz divi elementi, vai arī vismaz vienā no apakškopām – četri elementi. (No pretējā: Ja visās apakškopās ir ne vairāk kā trīs elementi, un neatrodas divas, kurās ir katrā pa diviem, tad iegūstam 1023 apakškopas ar ne vairāk kā vienu elementu un 1 apakškopu ar ne vairāk kā trim elementiem. Tas atbilstu $1023 + 3 = 1026$ elementiem, bet mums ir 2016.)
Tātad varam izvēlēties a, b, c, d tā, lai a, b un arī c, d būtu vienā apakškopā. Līdz ar to ab un arī cd ir pilni kvadrāti (jo kāpinātāji pie visiem pirmskaitļiem ir pāru skaitļi – pāris plus pāris vai nepāris plus nepāris). Tādēļ arī to reizinājums $abcd$ būs pilns kvadrāts. ■

Atsauces

[1] Amir Hossein Parvardi. Lifting The Exponent Lemma (LTE). 2011-04-07. `http://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/lifting-the-exponent.pdf`

[2] Stackexchange. Proof of existence of primitive roots. 2017-07-04 (nesenākais skatījums). `https://math.stackexchange.com/questions/807290/proof-of-existence-of-primitive-roots`.

[3] Chris K. Caldwell. Proof of Fermat's Little Theorem. 2017-07-04 (nesenākais skatījums). `https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html`