NMS SKAITĻU TEORIJA #3: ĶĪNIEŠU ATLIKUMU TEORĒMA

3.1 Ievaduzdevumi

1. Ar $\gcd(\ldots)$ apzīmējam skaitļu kopīgo dalītāju. Vai var atrast tādus naturālus a, b, c, kuri ir savstarpēji pirmskaitļi: $\gcd(a, b, c) = 1$, bet nekādi divi no tiem nav *pa pāriem savstarpēji pirmskaitļi*, t.i. $\gcd(a, b) > 1$, $\gcd(b, c) > 1$ un $\gcd(a, c) > 1$.
2. Atrast kādu veselu skaitli x, kas apmierina šādas sakarības:
$$\begin{cases} x \equiv 5 \pmod 6, \\ x \equiv 3 \pmod 8. \end{cases}$$
3. Naudas lādē glabājas monētas. Ja tās vienādi sadala sešiem draugiem, paliek pāri četras monētas. Ja tās vienādi sadala pieciem draugiem, paliek pāri trīs monētas.

   Pieņemot, ka naudas lādē ir mazākais monētu skaits, kas atbilst šiem nosacījumiem, atrast, cik monētu paliks pāri, ja tās vienādi sadalīs septiņiem draugiem.

3.2 Ķīniešu atlikumu teorēmas jēdzieni

3.2.1 Multiplikatīvi inversie skaitļi

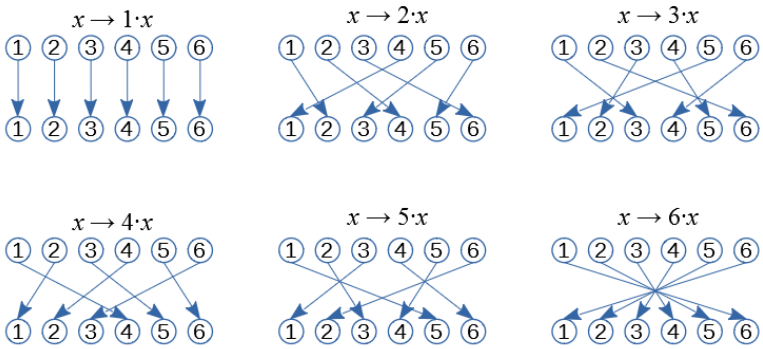
Definīcija: Aplūkojam naturālu skaitli m un veselu skaitli a. Par vesela skaitļa a *multiplikatīvi inverso* pēc m moduļa jeb (mod m) sauc tādu veselu skaitli x, kam izpildās kongruence $a \cdot x \equiv 1 \pmod m$.

Apgalvojums: Lai inversais skaitlis eksistētu ir nepieciešami un pietiekami, ka a un m ir savstarpēji pirmskaitļi. (Gadījumā, ja m ir pirmskaitlis, tas nozīmē, ka a nedrīkst dalīties ar m – tātad inversais eksistē ikvienam skaitlim, izņemot tos, kuri kongruenti ar 0.)

Inverso raksta šādi: $x = a^{-1} \pmod m$. (Nevajadzētu rakstīt $x = 1/a$, jo dalīšana kongruenču klasēm netiek definēta; tās vietā izmanto reizināšanu ar inverso.)

Piemērs: $3 \cdot 5 \equiv 1 \pmod 7$, tāpēc $5 = 3^{-1} \pmod 7$ un arī otrādi: $3 = 5^{-1} \pmod 7$.

Pierādījums: Aplūkosim atsevišķu gadījumu, ja m ir pirmskaitlis. Tad funkcija $f_a(x) = (a \cdot x)\%m$ ir *injektīva funkcija*. Zīmējumā attēlots gadījums $m = 7$.



$a \cdot x_1 \equiv a \cdot x_2$ nozīmētu $a \cdot (x_1 - x_2) \equiv 0 \pmod{m}$.

Tāpēc pēc Dirihlē principa visi nenulles atlikumi $r \not\equiv 0$ saņem kādu $a \cdot x \pmod{m}$ vērtību – katram aplītim iedur kāda bultiņa. Arī atlikumam $r = 1$ iedur bultiņa. Tātad eksistē inversais a^{-1}. □

Šī Python programmiņa rēķina inverso (paplašinātais Eiklīda algoritms):

```
def modInverse(a, m):
    m0 = m
    y = 0
    x = 1
    if m == 1:
        return 0
    while a > 1:
        q = a // m
        t = m
        m = a % m
        a = t
        t = y
        y = x - q * y
        x = t
    if x < 0:
        x = x + m0
    return x
```

Arī tad, ja m nav pirmskaitlis, tad aplūkojot tos atlikumus, kuri ir savstarpēji pirmskaitļi ar m, var atkārtot līdzīgu spriedumu.

Piemērs: Ja $m = 16$, tad inversie elementi ir šādi:

$$
\begin{aligned}
1^{-1} &\equiv 1 \pmod{16} \\
3^{-1} &\equiv 11 \pmod{16} \\
5^{-1} &\equiv 13 \pmod{16} \\
7^{-1} &\equiv 7 \pmod{16} \\
9^{-1} &\equiv 9 \pmod{16} \\
11^{-1} &\equiv 3 \pmod{16} \\
13^{-1} &\equiv 5 \pmod{16} \\
15^{-1} &\equiv 15 \pmod{16}
\end{aligned}
$$

3.2.2 Bezū identitāte

Bezū identitāte: Pieņemsim, ka veseliem skaitļiem a un b lielākais kopīgais dalītājs ir d. Eksistē veseli skaitļi x un y, kas ir atrisinājumi vienādojumam: $ax + by = d$.

Note: Šie atrisinājumi (x, y) nav unikāli, vērtību d var iegūt bezgalīgi daudz veidos.

Note: Visas izteiksmes $ax + by$ (pie dažādiem $x, y \in \mathbb{Z}$) pieņem vērtības, kas ir visi skaitļa d daudzkārtņi.

Piemērs: $a = 18$, $b = 42$, $\gcd(18, 42) = 6$. Der atrisinājumi $(x, y) = (-2, 1)$, $(5, -2)$, $(12, -5)$, ...

$$18 \cdot (-2) + 42 \cdot 1 = 18 \cdot 5 + 42 \cdot (-2) = 18 \cdot (12) + 42 \cdot (-5) = 6.$$

Atrisinājumi $(x_1, y_1), (x_2, y_2), \ldots$ veido aritmētiskas progresijas ar diferencēm $d_x = 7$, $d_y = -3$.

Bezū identitātes pierādījuma ideja: Aplūkojam naturālu skaitļu kopu:

$$S = \{ax + by \mid x, y \in \mathbb{Z} \text{ un } ax + by > 0\}.$$

Šajā kopā eksistē minimālais elements $d^* = ax^* + by^*$ kaut kādām optimālām vērtībām (x^*, y^*).

Jāpamato divas lietas:

1. d^* ir skaitļu a un b kopīgs dalītājs.
2. Ja c ir cits a un b kopīgs dalītājs, tad $c < d^*$.

No abiem šiem punktiem sekotu, ka šādi definētais d^* ir lielākais no visiem kopīgajiem dalītājiem, tātad vienāds ar $d = \gcd(a, b)$.

Pirmā daļa: Tas ir kopīgs dalītājs Ja pieņemam, ka a nedalās ar *d^{ast}*, tad varētu izdalīt, iegūstot pozitīvu atlikumu: $a = d \cdot q + r$, kur q ir kāds vesels skaitlis, bet $0 < r < d^*$.

Bet šādā gadījumā arī $r = a - d^* \cdot q = a - (ax^* + by^*) \cdot q$ varētu izteikt formā $ax + by$, kur r arī ir pozitīvs skaitlis un vēl mazāks par d^*. Bet pēc definīcijas *d^{ast}* ir vismazākais. Pretruna.

Otrā daļa: Tas ir lielākais kopīgais dalītājs: Ja c ir dalītājs skaitļiem a un b, tad izsakām $a = cu$ un $b = cv$, un ievietojam tos d^* izteiksmē:

$$d^* = ax^* + by^* = cux^* + cvy^* = c(ux^* + vy^*).$$

Esam ieguvuši, ka d^* dalās ar c, t.i. $d^* \geq c$. Tātad d^* ir lielākais no kopīgajiem dalītājiem. □

Note: Ievērojam, ka (x^*, y^*), lai iegūtu mazāko $d^* = ax^* + by^*$ noteikti eksistē, bet nav nekāda algoritma, lai šos nezināmos x^*, y^* iegūtu. tas tātad ir *nekonstruktīvs eksistences pierādījums*.

3.2.3 Blankinšipa algoritms

Sk. Blankinship Algorithm.

Sāk ar *matricu* (taisnstūrveida tabuliņu ar skaitļiem):

$$A = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}.$$

No vienas rindiņas skaitļiem var atņemt otras rindiņas skaitļus (un arī otrādi). Cenšamies panākt, lai matrica pārveidotos kādā no formām:

$$\begin{pmatrix} d & x & y \\ 0 & x' & y' \end{pmatrix} \text{ vai } \begin{pmatrix} 0 & x' & y' \\ d & x & y \end{pmatrix}$$

Piemērs: Pircējam un pārdevējam ir neierobežots skaits monētu ar vērtībām 21 un 34 centi. Tā kā tie ir savstarpēji pirmskaitļi, tad Bezū identitātē var iegūt $21x + 34y = 1$. Kā pircējs var nomaksāt pārdevējam 1 centu?

Risinājums ar Blankinšipa algoritmu:

$$\left(\begin{array}{cc|cc} 21 & & 1 & 0 \\ 34 & & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 21 & & 1 & 0 \\ 13 & & -1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 8 & & 2 & -1 \\ 13 & & -1 & 1 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{cc|cc} 8 & & 2 & -1 \\ 5 & & -3 & 2 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 3 & & 5 & -3 \\ 5 & & -3 & 2 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 3 & & 5 & -3 \\ 2 & & -8 & 5 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{cc|cc} 1 & & 13 & -8 \\ 2 & & -8 & 5 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & & 13 & -8 \\ 0 & & -34 & 21 \end{array}\right).$$

$$\begin{cases} 21 = 1 \cdot \{21\} + 0 \cdot \{34\} \\ 34 = 0 \cdot \{21\} + 1 \cdot \{34\} \end{cases} \Rightarrow \quad 1 = 13 \cdot \{21\} + (-8) \cdot \{34\}.$$

Sekas: Lineārai kongruencei $ax \equiv c \pmod{b}$ (kur a, b ir veseli skaitļi un c dalās ar $d = \text{LKD}(a, b)$) eksistē atrisinājums.

Pierādījums: No Bezū identitātes: Var atrisināt *$ax+by=d$*, kam $ax - d$ dalās ar b (tātad ax un d ir kongruenti pēc b moduļa).

Pēc tam šādi atrastu x reizina ar c/d, ja c ir kāds lielāks skaitlis par LKD.

Lineāru kongruenču piemēri:

1. Atrisināt kongruenci $16x \equiv 14 \pmod{4}0$.
2. Atrisināt kongruenci $26x \equiv 14 \pmod{4}2$.
3. Dots, ka $x \equiv 7 \pmod{1}1$ un *x equiv 2 pmod 7*. Atrast, ar ko kongruents *x* (mod 77).
4. Atrisināt kongruenci $x^2 \equiv 7 \pmod{27}$.

3.2.4 Ķīniešu atlikumu teorēma

Ķīniešu atlikumu teorēma: Ja doti naturāli skaitļi $n_1, n_2, \ldots, n_k$ kuri ir pa pāriem savstarpēji pirmskaitļi un arī jebkādi veseli skaitļi $a_1, a_2, \ldots, a_k$, tad sistēmai

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

eksistē atrisinājums un šis atrisinājums ir viens vienīgs pēc moduļa $N = n_1 n_2 \cdots n_k$.

3.3 Skaitliski piemēri

1.Jautājums: Atrisināt kongruenču sistēmu:

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 4 \pmod 5, \\ x \equiv 6 \pmod 7. \end{cases}$$

Procedūra, kā atrisināt šādas sistēmas:

Aplūkojam kongruenču sistēmu, kurai visi moduļi ir pa pāriem savstarpēji pirmskaitļi.

1. Sākam ar kongruenci, kurā modulis ir vislielākais: $x \equiv a_k \pmod{n_k}$. Pārrakstām to ar izteiksmi, kurā ir mainīgais: $x = n_k j_k + a_k$, kur j_k ir kāds naturāls skaitlis.
2. Ievietojam šo izteiksmi mainīgā x vietā – kongruencē ar nākamo lielāko moduli: $n_k j_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}$. Atrodam kādu j_k, kuram tas izpildās. Ievietojam to mainīgā x izteiksmē un iegūstam jaunu formulu mainīgajam x. Piemēram, $x = n_k n_{k-1} j_{k-1} + a_{k-1}$, kur j_{k-1} ir kāds naturāls skaitlis.
3. Ievietojam šo x izteiksmi trešajā lielākajā kongruencē un risinām to, utt.

2.Jautājums: Atrisināt kongruenču sistēmu:

$$\begin{cases} x \equiv 2 \pmod 6, \\ x \equiv 5 \pmod 9, \\ x \equiv 7 \pmod 1)5. \end{cases}$$

3.Jautājums: Trīs komētas riņķo pa eliptiskām orbītām ap Sauli ar periodiem attiecīgi 3, 8 un 13 gadi. To perihēliji (moments, kad komēta ir vistuvāk Saulei) pēdējo reizi iestājās 2020.gadā, 2014.gadā un 2021.gadā.

Noskaidrot, kurš būs tuvākais gads, kad visām trim komētām perihēlijs iestāsies tanī pašā gadā. (Pieņemt, ka apriņķošanas periodi izteikti gados ir veseli skaitļi un komētas neiespaido citu debess ķermeņu gravitācija, izņemot Sauli.)

4.Jautājums: Kādi ir pēdējie divi cipari skaitlī 7^{2021}?

5.Jautājums: Atrast mazāko naturālo skaitli, kuru dalot ar 5, ar 7, ar 9 un ar 11, iegūtie atlikumi ir attiecīgi 1, 2, 3 un 4.

6.Jautājums: Kādam virsniekam bija ne vairāk kā 1200 karavīri.

- Ja tie nostājas rindās pa 5 karavīriem rindā, 3 paliek pāri;
- Ja tie nostājas rindās pa 6 karavīriem rindā, 3 paliek pāri;
- Ja tie nostājas rindās pa 7 karavīriem rindā, 1 paliek pāri;
- Ja tie nostājas rindās pa 11 karavīriem rindā, 0 paliek pāri.

Cik karavīru bija pavisam?

7.Jautājums: Tenisa spēlētājai ir pilns grozs ar bumbiņām. Ja tās izņem no groza pa 2, tad 1 paliek pāri. Ja tās izņem no groza pa 3, tad 2 paliek pāri. Ja tās izņem no groza pa 4, 5 vai 6, tad paliek pāri attiecīgi 3, 4 vai 5. Toties, ja tās izņem no groza pa 7, tad nepaliek pāri neviena. Kāds mazākais bumbiņu skaits var būt grozā?

8.Jautājums: Trim draugiem A, B, C, D visiem kopā ir mazāk nekā 200 EUR. Zināms, ka katram no viņiem ir vesels daudzums eiru un izpildās sakarības:

- Ja B aizņemtos 1 EUR no A, tad B naudas daudzums būtu $\frac{2}{3}$ no A naudas daudzuma.
- Ja C aizņemtos 2 EUR no B, tad C naudas daudzums būtu $\frac{3}{5}$ no B naudas daudzuma.
- Ja D aizņemtos 3 EUR no C, tad D naudas daudzums būtu $\frac{5}{7}$ no C naudas daudzuma.

Kāds ir mazākais naudas daudzums, kas viņiem visiem kopā var piederēt?

9.Jautājums: Kāds ir atlikums, ja skaitli $12^{34^{56^{78}}}$ dala ar 90?

10.Jautājums: Atrast pēdējos divus nenulles ciparus skaitļa 2021! decimālpierakstā.

3.4 Sacensību uzdevumi

1.Uzdevums Pierādīt, ka eksistē 99 pēc kārtas sekojoši naturāli skaitļi $a_1, a_2, \ldots, a_{99}$, kuriem a_i dalās ar kāda naturāla skaitļa kubu, kas lielāks par 1.

Ieteikumi: Lai pamatotu, ka eksistē skaitļi ar noteikta veida neparastu īpašību, sadalām šo īpašību daudzās lineārās kongruencēs (pēc moduļiem, kuri ir savstarpēji pirmskaitļi) un risinām šo sistēmu.

2.Uzdevums (LV.VO.2001.9.1): Sienāža lēciena garums ir 5. Viņš sākotnēji atrodas punktā ar koordinātām $(0; 0)$ un var pārvietoties tikai pa punktiem, kam abas koordinātas ir veseli skaitļi.

1. Pierādīt, ka sienāzis var nokļūt punktā ar koordinātām $(1; 0)$,
2. Vai sienāzis var nokļūt jebkurā punktā ar veselām koordinātām?

3.Uzdevums (LT.VUMIF.2016.10.3):

Atrodiet mazāko naturālo skaitli n, kuram skaitļi $\sqrt[5]{5n}$, $\sqrt[6]{6n}$, $\sqrt[7]{7n}$ ir naturāli.

Sk. Viļņas universitātes Matemātikas un informātikas fakultātes rīkotā olimpiāde skolēniem: http://mif.vu.lt/matematikos-olimpiados/mif/.

4.Uzdevums (USAMO.2008.1): Pierādīt, ka jebkuram naturālam n, eksistē $n + 1$ savstarpēji pirmskaitļi $k_0, k_1, \ldots, k_n$, kas visi lielāki par 1, kuriem $k_0 \cdot k_1 \cdot \ldots \cdot k_n - 1$ ir divu pēc kārtas sekojošu naturālu skaitļu reizinājums.

Lemma 1: Ja $t_i^2 + t_i + 1$ dalās ar pirmskaitli p_i $(i = 0, \ldots, n)$, tad eksistēs arī tāds t^*, kuram $(t^*)^2 + t^* + 1$ dalās ar visu šo pirmskaitļu reizinājumu?

Lemma 2: Vai eksistē bezgalīgi daudz pirmskaitļu p_i, kuriem var atrisināt $t^2 + t + 1 \equiv 0$ pēc p_i moduļa? (T.i. polinoma $P(t) = t^2 + t + 1$ vērtība kaut kādam t dalās ar p_i)?

5.Uzdevums (US.MPGO.2010.2): Pierādīt, ka jebkuram naturālam n, eksistē veseli skaitļi a un b, kuriem $4a^2 + 9b^2 - 1$ dalās ar n.

6.Uzdevums (BW.2016.2): Pierādīt vai apgāzt sekojošus apgalvojumus:

(a) Jebkuram $k \geq 2$, un jebkuriem k pēc kārtas sekojošiem naturāliem skaitļiem atradīsies skaitlis, kurš nedalās ne ar vienu pirmskaitli, kas mazāks par k.

(b) Jebkuram $k \geq 2$, un jebkurai k pēc kārtas sekojošu naturālu skaitļu virknei atradīsies skaitlis, kas ir savstarpējs pirmskaitlis ar visiem citiem virknes locekļiem.

7.Uzdevums: Sauksim režģa punktu X rūtiņu plaknē par *redzamu* no koordinātu sākumpunkta O, ja nogrieznis O nesatur citus režģa punktus, izņemot O un X. Pierādīt, ka jebkuram naturālam n eksistē kvadrāts ar izmēru $n \times n$ (kur kvadrāta malas ir paralēlas koordinātu asīm), ka neviens no kvadrātā ietilpstošajiem režģa punktiem nav redzams no koordinātu sākumpunkta.

8.Uzdevums:

Vai eksistē bezgalīgi daudzi Fibonači skaitļi, kuri: Dalās ar 1001 bez atlikuma (atlikums 0),

Vai eksistē bezgalīgi daudzi Fibonači skaitļi, kuri: dod atlikumu 900, dalot ar 1001.

Vai eksistē bezgalīgi daudzi Fibonači skaitļi, kuri: dod atlikumu 1000, dalot ar 1001.

Note: Fibonači virkni $(0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots)$ definē šādi: $F_0 = 0$, $F_1 = 1$ un $F_{k+1} = F_{k-1} + F_k$ visiem $k \geq 1$. (Katrs nākamais loceklis ir divu iepriekšējo locekļu summa.)

9.Uzdevums (BW.2016.2) Pierādīt vai apgāzt sekojošus apgalvojumus:

1. Jebkuram $k \geq 2$, un jebkuriem k pēc kārtas sekojošiem naturāliem skaitļiem atradīsies skaitlis, kurš nedalās ne ar vienu pirmskaitli, kas mazāks par k.
2. Jebkuram $k \geq 2$, un jebkurai k pēc kārtas sekojošu naturālu skaitļu virknei atradīsies skaitlis, kas ir savstarpējs pirmskaitlis ar visiem citiem virknes locekļiem.

Ieteikumi: Otrajā apgalvojumā ar mēģinājumu/kļūdu metodi atrod, ka atbilde ir 17: Var atrast 17 skaitļu intervālu $[n; n + 16]$; kuru var pārklāt ar aritmētiskām progresijām ar diferencēm $d = 2, 3, 5, 7, 11, 13$ (un no katras progresijas virknē ir vismaz divi locekļi).