DIRIHLĒ PRINCIPS UN SKAITĻU TEORIJA

Atklātajai matemātikas olimpiādei 24.novembrī izziņota viena uzdevuma tēma – Dirihlē princips. Sk. https://www.nms.lu.lv/olimpiades/atklata-olimpiade/. Aplūkojam dažus ar to saistītus piemērus.

1.1 Funkciju vērtību sadursmes

Dirihlē princips Ja vairāk kā n objekti salikti n kastēs, tad noteikti būs tāda kaste, kurā nonāks vismaz 2 objekti.

Definīcija: Funkciju $f : A \to B$ sauc par *injektīvu*, ja tai nav kolīziju jeb sadursmju: Ja $a_1 \neq a_2$, tad arī $f(a_1) \neq f(a_2)$.

Piemēri:

(A) Funkcija $f(x) = x^2$, kas attēlo nenegatīvos skaitļus $[0; +\infty)$ uz nenegatīviem skaitļiem, ir injektīva: Ja $a < b$, tad arī $a^2 < b^2$. (Tāpēc var uztaisīt inverso funkciju: $g(x) = \sqrt{x}$, kas no kvadrātfunkcijas vērtības atrod argumentu.)

(B) Tā pati funkcija $f(x) = x^2$, kas attēlo $f : \mathbb{R} \to \mathbb{R}$ NAV injektīva, jo piemēram, $2 \neq -2$ bet $f(2) = f(-2)$. Tāpēc vienādojumam $x^2 = 4$ ir divas dažādas saknes.

(C) Funkcija f, kas definēta visiem Latvijas iedzīvotājiem un katram piekārto personas kodu, ir injektīva – neeksistē kolīzijas: divi dažādi cilvēki ar vienādiem personas kodiem.

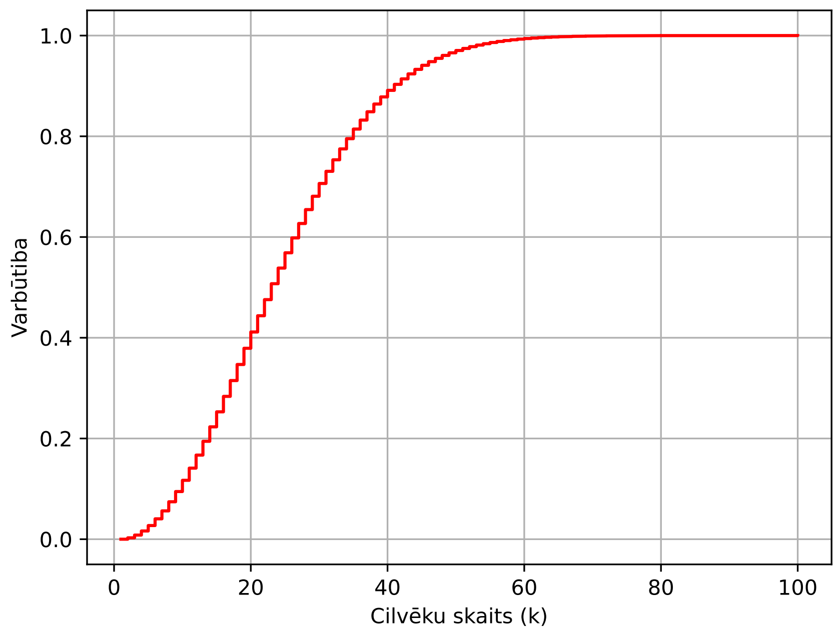
Uzdevums 1: Doti naturāli skaitļi no 1 līdz 8. Pierādīt, ka, izvēloties jebkurus piecus no tiem, varēs atrast tādus divus, kuru summa ir 9.

Uzdevums 2: Pierādīt, ka starp jebkuriem sešiem naturāliem skaitļiem, kas nedalās ar 10, var atrast divus tādus, kuru summa vai starpība dalās ar *10*.

Uzdevums 3: Uz tāfeles uzrakstīti četru naturālu skaitļu kubi: a^3, b^3, c^3, d^3. Pierādīt, ka no tiem atradīsies divi tādi, kuru summa vai starpība dalās ar 13.

```
[n**3 % 13 for n in range(0, 13)]
```

Uzdevums 4: Dota funkcija, kas katram cilvēkam atrod dzimšanas datumu neatkarīgi no gada (pieņemam, ka ir tieši 365 datumi, 29.februāri neizmantojam). Uzrakstīt izteiksmi varbūtībai, ka starp n cilvēkiem būs cilvēki ar vienādām dzimšanas dienām.



1.2 Reizināšana pēc pirmskaitļa moduļa

Definīcija: Divus skaitļus saucam par *kongruentiem* pēc m moduļa, ja $a - b$ dalās ar m (jeb abi skaitļi dod vienādus atlikumus, dalot ar m). Pieraksts:

$$a \equiv b \pmod{m}.$$

Aplūkojam nepāra pirmskaitli, piemēram $p = 11$. Izveidojam nenulles atlikumu kopu pēc moduļa 11:

$$\mathbb{Z}_{11}^{\times} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Šiem atlikumiem var izveidot reizināšanas tabulu – katru divu atlikumu reizinājums arī ir skaitlis, kas dod noteiktu atlikumu, dalot ar 11:

$a \cdot b$	$b = 1$	$b = 2$	$b = 3$	$b = 4$	$b = 5$	$b = 6$	$b = 7$	$b = 8$	$b = 9$	$b = 10$
$a = 1$	1	2	3	4	5	6	7	8	9	10
$a = 2$	2	4	6	8	10	1	3	5	7	9
$a = 3$	3	6	9	1	4	7	10	2	5	8
$a = 4$	4	8	1	5	9	2	6	10	3	7
$a = 5$	5	10	4	9	3	8	2	7	1	6
$a = 6$	6	1	7	2	8	3	9	4	10	5
$a = 7$	7	3	10	6	2	9	5	1	8	4
$a = 8$	8	5	2	10	7	4	1	9	6	3
$a = 9$	9	7	5	3	1	10	8	6	4	2
$a = 10$	10	9	8	7	6	5	4	3	2	1

Definīcija: Par skaitļa a multiplikatīvi inverso pēc moduļa m sauc tādu skaitli a^{-1}, kam izpildās $a^{-1}a \equiv 1 \pmod{p}$.

Apgalvojums: Katram skaitlim a, kas ir savstarpējs pirmskaitlis ar m eksistē multiplikatīvi inversais.

Pierādījums: Pieņemsim no pretējā, ka neeksistē tāds skaitlis x, kuram ax dod atlikumu 1 dalot ar p.

Aplūkosim visus atlikumus $a \cdot 1, \ldots, a \cdot (p-1)$. Ir pavisam $p-1$ dažādi atlikumi un neviens no tiem nevar būt 1 (pēc mūsu pieņēmuma).

Tāpēc pēc Dirihlē principa, atradīsies divi tādi skaitļi $i > j$, kuriem reizinājumi $a \cdot i$ un $a \cdot j$ dod vienādus atlikumus:

$$a \cdot i \equiv a \cdot j \pmod{p} \quad \text{jeb} \quad a \cdot (i-j) \pmod{0} \pmod{p}.$$

Bet skaitlis $a \cdot (i-j)$ nevar dalīties ar p, jo $0 < i - j < p$. □

Uzdevums 5:

(A) Atrast skaitļa 20 multiplikatīvi inverso pēc 23 moduļa jeb atrisināt kongruenču vienādojumu: $20x \equiv 1 \pmod{2}3$.

(B) Kādā valstī apgrozībā ir 20 centu un 23 centu monētas. Iedomāsimies, ka pircējam ir tikai 20 centu monētas, bet pārdevējs var izdot tikai 23 centu monētas. Kā pircējs var samaksāt tieši 1 centu?

Uzdevums 6: Skaitlis a nedalās ar 23. Pierādīt, ka kongruenču vienādojumam

$$x^2 \equiv a \pmod{2}3$$

ir vai nu divi atrisinājumi, vai arī nav neviena atrisinājuma.

Mazā Fermā teorēma: Ja p ir pirmskaitlis, tad katram a, kurš nedalās ar p ir spēkā sakarība:

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

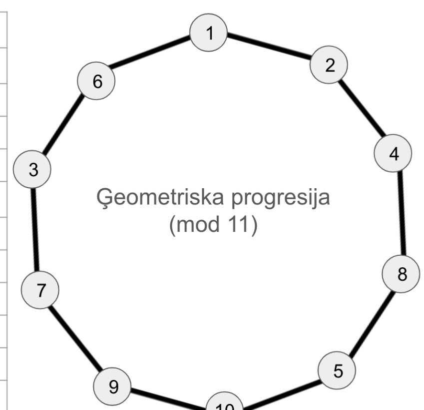
Pierādījums: Aplūkojam visus skaitļus $\{1, 2, \ldots, p-1\}$. Piereizinām tos visus ar a. Iegūsim $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$.

Nav iespējams, ka diviem dažādiem $i, j \in \{1, 2, \ldots, p-1\}$ izpildās $i \cdot a \equiv j \cdot a \pmod{p}$. Citādi sanāktu, ka reizinājums $a(i-j)$ dalās ar p. □

Fermā teorēma parāda, cik ilgi skaitli var reizināt pašu ar sevi (veidot ģeometrisku progresiju pēc moduļa p), lai atlikums kļūtu vienāds ar 1.

Ne visiem skaitļiem būs visi 10 nenulles atlikumi pēc moduļa 11. Apskatām modulārās kāpināšanas tabulu:

n^0	n	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^{10}
0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
1	2	4	8	5	10	9	7	3	6	1
1	3	9	5	4	1	3	9	5	4	1
1	4	5	9	3	1	4	5	9	3	1
1	5	3	4	9	1	5	3	4	9	1
1	6	3	7	9	10	5	8	4	2	1
1	7	5	2	3	10	4	6	9	8	1
1	8	9	6	4	10	3	2	5	7	1
1	9	4	3	5	1	9	4	3	5	1
1	10	1	10	1	10	1	10	1	10	1



Uzdevums 7: Pierādīt, ka vienādojumam nav atrisinājuma: $x^3 + y^3 + z^3 = 1969^2$.

Uzdevums 8: Doti pieci naturāli skaitļi. Šo skaitļu reizinājums apzīmēts ar R, bet to piekto pakāpju summa ar S. Zināms, ka S dalās ar 1001. Vai ir iespējams, ka R un S ir savstarpēji pirmskaitļi?

Sk. 1.piemēru no 8.darba lapas: https://www.nms.lu.lv/arhivs-un-materiali/materiali/nnv-materiali/.

1.3 Ķīniešu atlikumu teorēma

Ķīniešu atlikumu teorēma: Doti naturāli skaitļi $m_1, m_2, \ldots, m_k$ kuri ir pa pāriem savstarpēji pirmskaitļi un arī jebkādi veseli skaitļi $a_1, a_2, \ldots, a_k$, tad sistēmai

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

eksistē atrisinājums un šis atrisinājums ir viens vienīgs pēc moduļa $N = m_1 m_2 \cdots m_k$.

Uzdevums 9: Izveidot tabulu ar $m_1 = 8$ rindām un $m_2 = 13$ kolonnām. Katram atlikumu pārim $a_1 \in [0;8)$ un $a_2 \in [0;13)$ ierakstīt rūtiņā skaitli - Ķīniešu atlikumu teorēmas atrisinājumu pēc moduļa $N = 8 \cdot 13 = 104$.

Uzdevums 10: Atrisināt kongruenču sistēmu:

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

Uzdevums 11: Kādi ir pēdējie divi cipari skaitlī 7^{2021}?

Uzdevums 12: Pierādīt, ka eksistē 99 pēc kārtas sekojoši naturāli skaitļi $a_1, a_2, \ldots, a_{99}$, kur a_i dalās ar kāda naturāla skaitļa kubu, kas lielāks par 1.

1.4 Diskrētie logaritmi un FFDH atslēgu apmaiņa

Kāpināšana a^b ļauj ieviest divu dažādu veidu funkcijas:

Pakāpes funkcijas: $f(x) = x^n$. Šīs funkcijas ir injektīvas, ja $x \geq 0$ un $n > 0$. Pakāpes funkcijai inerso funkciju sauc par n-tās pakāpes sakni: $g(x) = \sqrt[n]{x}$.

Eksponentfunkcijas: $f(x) = a^x$. Šīs funkcijas ir injektīvas, ja $x > 0$ un $a > 0$ (turklāt $a \neq 1$). Eksponentfunkcijai inverso funkciju sauc par *logaritmu* ar bāzi a.

Piemēri: $\log_{10} 1 = 0$, $\log_{10} 10 = 1$, $\log_{10} 1000000 = 6$, $\log_{10} 0.01 = -2$.

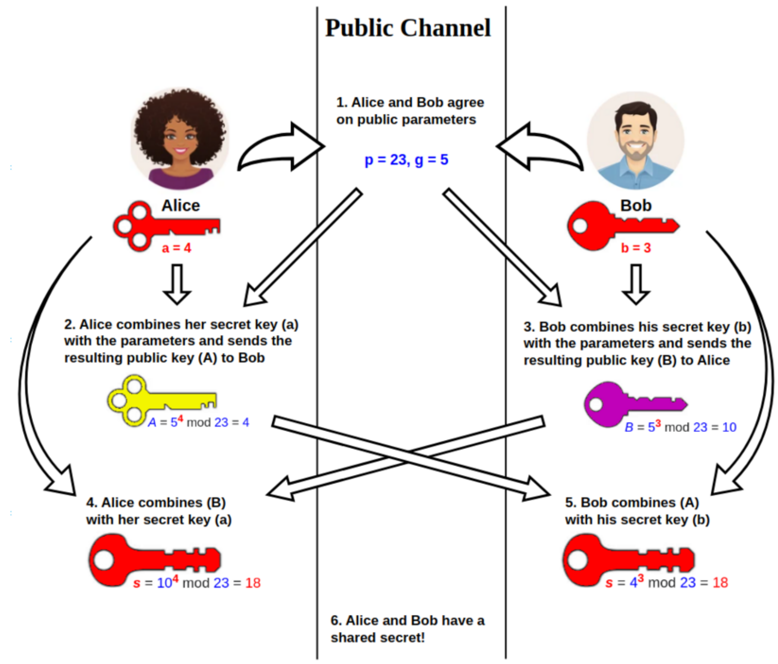
$\log_4 2 = 0.5$, $\log_4 4 = 1$, $\log_4 8 = 1.5$.

Kādiem kāpinātājiem k skaitlī 2^k būs vismaz 30 cipari?

$2^k > 10^{29}$ jeb $k > \log_2 10^{29} = 29 \log_2 10$

```
>>> import math
>>> 29* math.log2(10)
96.3359147517335
>>> [2**k for k in [97, 98, 99]]
[158456325028528675187087900672, 316912650057057350374175801344, ... ]
```

- Alise un Bobs publiski apsola izmantot moduli $p = 23$ un bāzi $g = 5$, kas ir primitīvā sakne mod 23.
- Alise izvēlas noslēpumu $a = 4$, tad nosūta Bobam $A = g^a \bmod p$. Šoreiz $A = 5^4 \bmod 23 = 4$.
- Bobs izvēlas noslēpumu $b = 3$, tad nosūta Alisei $B = g^b \bmod p$. Šoreiz $B = 5^3 \bmod 23 = 10$.
- Alice aprēķina $s = B^a \bmod p$. Jeb $s = 10^4 \bmod 23 = 18$.



- Bobs aprēķina $s = A^b \bmod p$. Jeb $s = 4^3 \bmod 23 = 18$.
- Alises un Boba kopīgais noslēpums ir skaitlis 18.

Definīcija: Atlikumu g sauc par primitīvo sakni pēc p moduļa, ja starp pakāpēm $g^0, g^1, g^2, \ldots, g^{p-2}$ ir atrodami visi nenulles atlikumi pēc p moduļa.

Primitīvās saknes eksistē katram pirmskaitlim p. Tās var izmantot kā diskrēto logaritmu bāzes.

Uzdevums 13: Atrast visas primitīvās saknes pēc 23 moduļa. Citiem vārdiem – cik ir tādu ģeneratoru elementu (līdzīgi $g = 5$ iepriekšējā piemērā), ja izmanto moduli 23. Atrast visus un atrast to kopskaitu.