NMS SKAITĻU TEORIJA #1: PIRMSKAITĻI UN DALĀMĪBA

1.1 Ievads

Daļa skaitļu teorijas uzdevumu tieši izmanto dalāmības attiecību – jautājumi, kas ar ko dalās vai nedalās, uzdevumi par pirmskaitļiem un līdzīgi. Dalāmības attiecība ir svarīga arī citos uzdevumos, piemēram, risinot vienādojumus veselos skaitļos.

Nodaļas mērķi:

1. Formulēt un izmantot dalāmības attiecības īpašības.
2. Aprēķināt naturāla skaitļa dalītāju skaitu, dalītāju summu.
3. Aprakstīt viena skaitļa dalītāju kopu, tās struktūru.
4. Veidot intervālā Eratostēna režģi
5. Pierādīt aritmētikas pamatteorēmu, izmantojot Eiklīda lemmu
6. Izmantot skaitļa dalījumu pirmreizinātājos.
7. Izmantot lielāko kopīgo dalītāju (LKD) un mazāko kopīgo dalāmo (MKD) īpašības.
8. Atrast LKD ar Eiklīda algoritmu.

Kāpēc dalāmības attiecību niansēti jāpārzina? Dalāmības attiecība un arī citi cikli saistībā ar veseliem skaitļiem ļauj bezgalīgajā naturālo (vai veselo) skaitļu kopā saskatīt regularitātes un likumsakarības, ko var izmantot visdažādākajos uzdevumos.

1.2 Skaitļu dalāmība

Datorprogrammas darbojas ar veseliem skaitļiem un arī citiem objektiem (reāliem skaitļiem, attēliem, skaņām), kuri faktiski ir tuvināti vai iekodēti kā veseli skaitļi. Pārveidošanu ciparu formā reizēm sauc par *digitalizāciju*. Veselo skaitļu aritmētika ļauj veikt praktiski vajadzīgas manipulācijas ar pašiem skaitļiem un to pārstāvētiem objektiem.

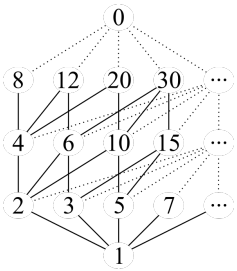
Veselus skaitļus vienmēr var saskaitīt, atņemt, reizināt kā arī kāpināt veselās pozitīvās pakāpēs. Dalīt arī vienmēr var, ja pieļaujam dalīšanu ar atlikumu.

Definīcija: Vesels skaitlis m **dalās ar** (*is divisible by*) veselu skaitli $d \neq 0$, ja eksistē tāds vesels k, kuram $m = d \cdot k$.

To pieraksta $d \mid m$ izrunā šādi: "d dala m" vai arī "m dalās ar d".

Skaitli d, kuram $d \mid m$ sauc par skaitļa m **dalītāju** (*divisor*), savukārt m sauc par skaitļa d **daudzkārtni** (*multiple*).

1.2.1 Dalāmības režģis



- Ja šajā režģī ir augšupejošs ceļš no virsotnes a uz virsotni b, tad b dalās ar a.
- Dalāmības attiecības "minimālais" elements ir 1 (visi skaitļi dalās ar 1). "Maksimālais" elements ir 0 (dalās ar jebkuru citu skaitli). Daži skaitļi šajā attiecībā nav salīdzināmi, piemēram, 5 nedalās ar 3 un arī otrādi.

Apgalvojums: Dalāmības attiecība ir **transitīva** (*transitive*) ja a dala b un b dala c, tad a dala c. (Piemēram, no $15 \mid 60$ un $60 \mid 480$ var secināt, ka $15 \mid 480$.)

"Transitīvais slēgums" - var zīmējumu saraibināt, savienojot arī izsecināmās attiecības (1 ar 4 vai 8 utt.). Izsecināmās attiecības šādos režģos visbiežāk nezīmē.

Dalāmības attiecība ievieš daļēju sakārtojuma attiecību veselo skaitļu kopā līdzīgi kā $\leq$. Pats "mazākais" veselais skaitlis šajā sakārtojumā ir 1; visi pirmskaitļi ir līmeni augstāk, jo tie dalās ar 1, bet 1 ar tiem nē. Vēl līmeni augstāk ir visi iespējamie divu pirmskaitļu reizinājumi, ieskaitot pirmskaitļu kvadrātus. Starp šo līmeni un pirmskaitļu līmeni visur nepastāv sakārtojuma attiecība. Piemēram, 2×3 nav salīdzināms ar 5 (tie savstarpēji cits ar citu nedalās). Sakārtojuma attiecību var turpināt arī augstākiem slāņiem (trīs, četru, utt. pirmskaitļu reizinājumam). Sakārtojuma attiecības pašā augšā atrodas skaitlis 0, jo tas dalās ar jebkuru skaitli.

Dotajā attēlā 1 ir savienots ar 2 un 2 ir savienots ar 4, bet nav novilkta šķautne no 1 uz 4 (kaut arī starp tiem pastāv sakārtojuma attiecība). Tas darīts vienīgi tādēļ, lai nesaraibinātu zīmējumu, jo dalāmības *transitivitātes* dēļ no $1 \mid 2$ un $2 \mid 4$ var secināt, ka $1 \mid 4$.

Sal. **Daļēji sakārtotas kopas** (*Partially ordered sets*) https://bit.ly/3nMRRR6.

1.2.2 Ar dalāmību saistītie operatori

Definīcija: *Dalīšana* (*division*) ir aritmētiska operācija. Dalot divus veselus skaitļus, rezultāts ir vesels vai racionāls.

Dalīšana kā aritmētiska operācija un tās rezultāts var parādīties vairākos veidos:

1. Dalīšana, iegūstot parasto vai jaukto daļskaitli: $17 : 3 = \frac{17}{3} = 5$
2. Dalīšana, iegūstot noapaļotu decimāldaļu: $17 : 3 = 5.6666667$
3. Dalīšana, iegūstot periodisku decimāldaļu: $17 : 3 = 5.(6)$ (lasa "pieci komats periodā seši")
4. Dalīšana, iegūstot dalījumu veselos skaitļos un atlikumu: $17 : 3 = 5$ atl. 2

Definīcija: *Dalāmība* (*divisibility*) ir loģiska attiecība - tās rezultāts ir patiesuma vērtība (`True` vai `False`).

Piemērs: Dalīšanas rezultāts $18/6 = 3$, bet $17/6 = 2\frac{5}{6}$.

Savukārt $18 \mid 6$ rezultāts ir `True`. Bet $17 \mid 6$ rezultāts ir `False`.

Teorēma: Jebkuriem veseliem skaitļiem a, b, c ir spēkā šādas dalāmības īpašības.

1. Ja $a \mid b$ un $a \mid c$, tad $a \mid b + c$ un $a \mid b - c$;
2. Ja $a \mid b$, tad $a \mid b \cdot k$;
3. Ja $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$, tad $a \mid (b_1 k_1 + b_2 k_2 + \ldots + b_n k_n)$;

4. Ja $a \mid b$ un $b \mid c$, tad $a \mid c$;
5. Ja $a \mid x$ un $b \mid y$, tad $ab \mid xy$;
6. Ja $a \mid b$ un $b \mid a$, tad $a = b$.

Definīcija: Dalīt veselu skaitli m ar d ar atlikumu nozīmē izteikt $m = q \cdot d + r$, kur dalījuma veselā daļa q un atlikums r ir veseli skaitļi, turklāt **atlikums** (*remainder*) pieņem kādu no vērtībām: $r \in \{0, 1, \ldots, n-1\}$.

Piemērs: Dalot ar 3 iespējamie atlikumi ir $\{0, 1, 2\}$. Aprēķina paraugs Python.

```
>>> 15 % 3
0
>>> 17 % 3
2
>>> (-17) % 3
1
>>> (-17) // 3
-6
```

$$\begin{cases} 15 = 5 \cdot 3 + 0 \\ 17 = 5 \cdot 3 + 2 \\ -17 = (-6) \cdot 3 + 1 \end{cases}$$

Note: Arī negatīviem skaitļiem iespējama dalīšana ar atlikumu. Jāņem vērā, ka atlikumi nemēdz būt negatīvi. Dažās programmēšanas valodās *atlikuma operators*, ja to izmanto negatīviem skaitļiem, dod negatīvus atlikumus. Pēc matemātiskās definīcijas, atlikums, dalot ar n, vienmēr ir skaitlis starp 0 un $n - 1$.

1.2.3 Jautājumi par dalāmību

1.jautājums Rindā novietoti 30 slēdži ar numuriem no 1 līdz 30. Katrs slēdzis var būt ieslēgts vai izslēgts; sākumā tie visi ir izslēgti. Pirmajā solī pārslēdz pretējā stāvoklī visus slēdžus, kuru numuri dalās ar 1. Otrajā solī pārslēdz visus tos, kuru numuri dalās ar 2. Un tā tālāk - līdz 30.solī pārslēdz pretējā stāvoklī slēdžus, kuru numuri dalās ar 30. Cik daudzi slēdži kļūst ieslēgti pēc visu soļu pabeigšanas?

Ieteikumi: Ko nozīmē "pārslēgt pretējā stāvoklī"? Cik daudzi soļi pārslēdz slēdzi ar konkrētu numuru n? Vai mūs interesē, cik reizes tika pārslēgts tas vai cits slēdzis (vai arī tikai slēdža beigu stāvoklis)?

Atbilde:

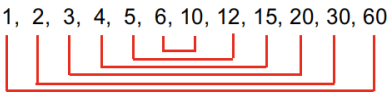
TODO: Ievietot attēlu, kas parāda dalītāju skaitu dažādiem skaitļiem no 1 līdz 30. Vizualizācija zīmē ritmu ar skaitļu $1, 2, 3, 4, \ldots$ daudzkārtņiem horizontālēs. Dalītāju skaitu var saskaitīt vertikāli. Kuriem no skaitļiem ir nepāru skaits dalītāju?

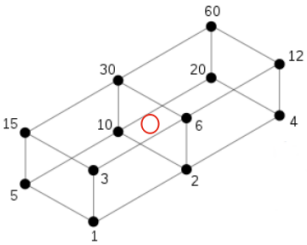
1.3 Naturāla skaitļa dalītāju skaits

Dalītāju izvietojums, skaits, režģis. Fiksēta skaitļa dalītāji veido simetrisku režģveida struktūru. Šī režģa analīze ļauj ātri noskaidrot dalītāju skaitu un citas to kopīgās īpašības. Režģa struktūra noder arī, lai ģeometriski iztēlotos, teiksim, lielāko kopīgo dalītāju diviem skaitļiem.

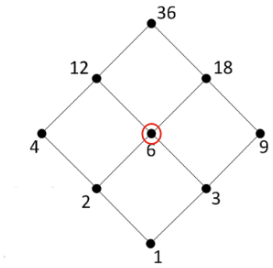
1.3.1 Dalītāju virknes simetrija

Dalītāji skaitlim 60:





Dalītāji skaitlim 36:



- Dalītāji režģī izvietoti centrālsimetriski attiecībā pret sarkano aplīti.
- Visas dalāmības attiecības nav attēlotas ar svītriņām, (bet gan tikai minimāli nepieciešamās.
- Pārējās attiecības ir jāsecina ar "transitīvo slēgumu", kad savelk visas citas bultiņas, ko var izsecināt: Ja $a \mid b$ un $b \mid c$, tad $a \mid c$.

Pilno kvadrātu starp visiem naturālajiem skaitļiem ir salīdzinoši nedaudz. Jebkurā pietiekami garā intervālā to būs krietni mazāk nekā, teiksim, pirmskaitļu. Tādēļ lielajam vairumam naturālo skaitļu ir pāru skaits dalītāju.

1.3.2 Hases diagrammas

H.Hase (*Helmut Hasse*) spriedumos par daļēji sakārtotām kopām ieviesa diagrammas, kas attēlo "transitīvo redukciju":

- Vispirms savieno ar svītriņu visus aplīšus, kas atrodas attiecībā "mazāks".
- Pēc tam izdzēš tās svītriņas, ko var izsecināt no citām, izmantojot transitivitāti.

Hases diagramma skadalītājiem

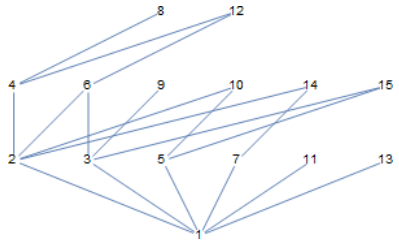


Fig. 1: Hases diagramma skaitļiem $[1; 15]$

1.3.3 Veidotājelementi: 2,3,5

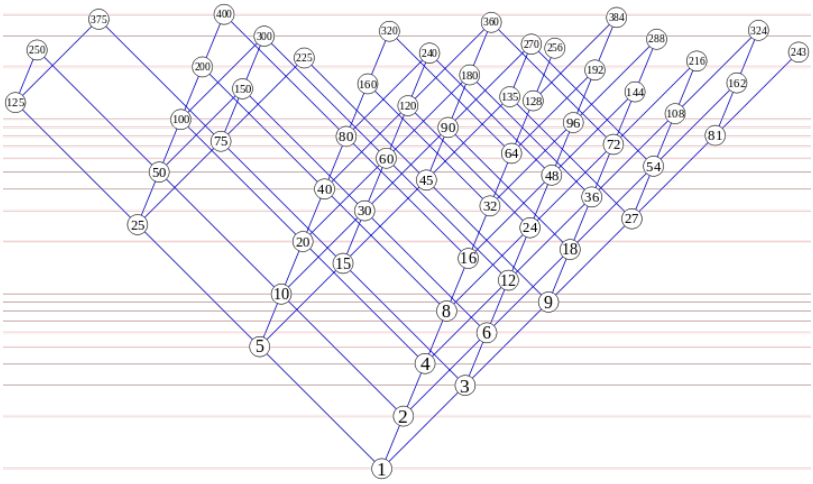


Fig. 2: Hases diagramma skaitļiem līdz 480, https://bit.ly/3qQBntd

1.3.4 Dalītāju summēšanas funkcijas

Fiksēta skaitļa dalītājiem var viegli aprēķināt to skaitu, summu (arī augstāku pakāpju summu).

Definīcija: Naturālam n apzīmējam $\sigma_0(n)$, $\sigma_1(n)$ un $\sigma_2(n)$ šādi:

$$\begin{aligned}\sigma_0(n) &= \sum_{d|n} 1 = \sum_{d|n} d^0,\\ \sigma_1(n) &= \sum_{d|n} d,\\ \sigma_2(n) &= \sum_{d|n} d^2,\end{aligned}$$

Piemērs: $\sigma_0(12) = 6$ (skaitlim 12 ir 6 pozitīvi dalītāji).

$\sigma_1(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

Sk. https://bit.ly/3IrWVCn.

1.3.5 Summēšanas izteiksmes

$\sum_{d|n} f(d)$ summē $f(d)$ visiem n dalītājiem d.

$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1$ – skaitļa n dalītāju skaits.

Līdzīgi apzīmējumi, lai nerakstītu daudzpunkti:

$$\sum_{k=0}^{n} k^2 = 1^2 + 2^2 + \ldots + n^2.$$

$$\prod_{k=0}^{n} k = 1 \cdot 2 \cdot \ldots \cdot n = n!.$$

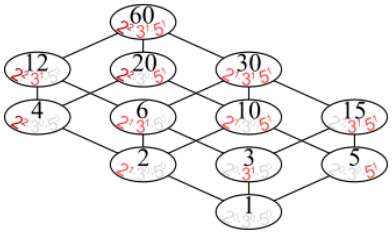
1.3.6 Piemēri ar n=60

$$\sigma_0(60) = |\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}| = 12.$$

$$\sigma_1(60) = 1 + 2 + 3 + 4 + 5 + 6 + 10 + 12 + 15 + 20 + 30 + 60 = 168.$$

$$\sigma_2(60) = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 10^2 + 12^2 + 15^2 + 20^2 + 30^2 + 60^2 = 5460.$$

1.3.7 Dalītāji skaitlim 60



- Dalītāju skaitu var atrast, izmantojot *reizināšanas likumu*.
- Zināms, ka $60 = 2^2 3^1 5^1$.
- Katrs skaitļa 60 dalītājs izsakāms $2^a 3^b 5^c$, kur $a \in \{0, 1, 2\}$, $b \in \{0, 1\}$, $c \in \{0, 1\}$.
- Sareizinām elementu skaitu: $3 \cdot 2 \cdot 2 = 12$.

$$\sigma_0\left(2^2 3^1 5^1\right) =$$

$$= (2 + 1) \cdot (1 + 1)(1 + 1) = 12.$$

1.3.8 Dalītāju un to kvadrātu summas

$\sigma_1(60)$ un $\sigma_2(60)$ arī var ātri aprēķināt, izmantojot algebriskas identitātes:

$$\sigma_1(60) = \left(2^2 + 2^1 + 2^0\right)\left(3^1 + 3^0\right)\left(5^1 + 5^0\right) =$$

$$= (4 + 2 + 1)(3 + 1)(5 + 1) = 7 \cdot 4 \cdot 6 = 168.$$

$$\sigma_2(60) = \left(2^4 + 2^2 + 2^0\right)\left(3^2 + 3^0\right)\left(5^2 + 5^0\right) =$$

$$= (16 + 4 + 1)(9 + 1)(25 + 1) = 5460.$$

Visu šo var iegūt no sadalījuma pirmreizinātājos: $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 3^1 5^1$.

Apgalvojums: Katram naturālam n eksistē bezgalīgi daudzi skaitļi M, kuriem ir tieši n pozitīvi dalītāji.

Pierādījums: Var izvēlēties $M = p^{n-1}$, kur p ir jebkurš pirmskaitlis. ■

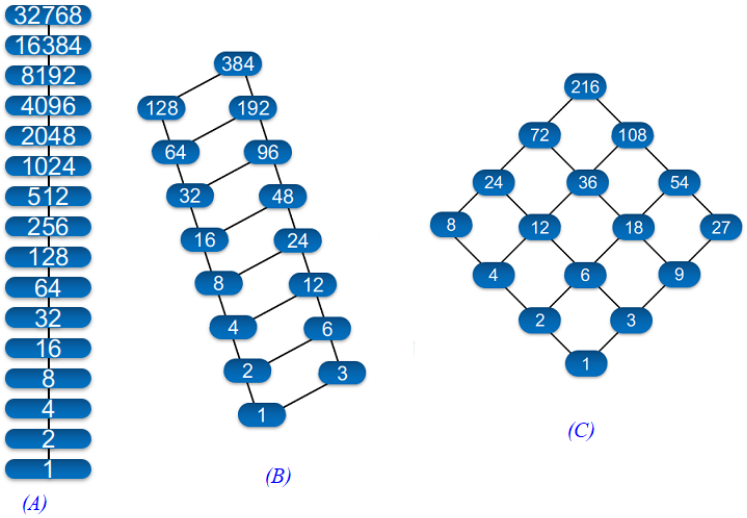
1.3.9 Jautājumi dalītāju skaitam un summai

1.jautājums: Atrast mazāko naturālo skaitli M, kam ir tieši 16 dalītāji.

Atbilde:

Skaitlim M nevar būt vairāk kā četri pirmreizinātāji. Ja $M = p_1^a p_2^b p_3^c p_4^d$, tam ir $(a+1)(b+1)(c+1)(d+1)$ dalītāji. Var iegūt rezultātu 16, ja $a = b = c = d = 1$. Savukārt, ja dažādo M pirmreizinātāju ir vairāk kā četri, tad M būtu vismaz $2^5 = 32$ dalītāji.

Šķirosim dažādus gadījumus, kā 16 var izteikt ne vairāk kā četru dažādu pirmskaitļu (vai to pakāpju) reizinājumu. Dalītāju skaitu nosaka pirmreizinātāju pakāpes, nevis tas, kā izvēlēti paši pirmreizinātāji. Tāpēc sadalījumus pirmreizinātājos šķirosim pēc pirmreizinātāju pakāpēm, veicot pirmreizinātāju izvēli nedaudz vēlāk.

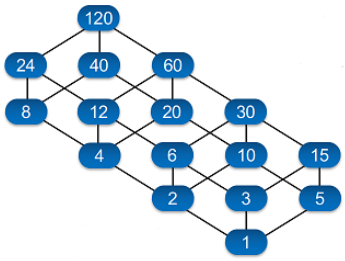


(A) *(B)* *(C)*

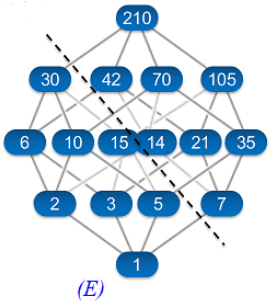
(A) gadījums: $16 = (15 + 1)$ jeb p^{15}, kur p ir pirmskaitlis. Mazākais šāds skaitlis ir $M = 2^{15} = 32768$.

(B) gadījums: $16 = (7 + 1)(1 + 1)$ jeb $p^7 q$, kur p, q ir pirmskaitļi. Mazākais šāds skaitlis ir $2^7 \cdot 3 = 128 \cdot 3 = 384$.

(C) gadījums: $16 = (3+1)(3+1)$ jeb $p^3 q^3$, kur p, q ir pirmskaitļi. Mazākais šāds skaitlis ir $2^3 \cdot 3^3 = 216$.



(D)



(E)

(D) gadījums: $(3+1)(1+1)(1+1)$ jeb p^3qr, kur p, q, r ir pirmskaitļi. Mazākais šāds skaitlis ir $2^3 \cdot 3 \cdot 5 = 120$.

(E) gadījums: $(1+1)(1+1)(1+1)(1+1)$ jeb skaitlis formā $pqrs$, kur p, q, r, s ir pirmskaitļi. Mazākais šāds skaitlis ir $2 \cdot 3 \cdot 5 \cdot 7 = 210$.

Mazākais no apskatītajiem pieciem rezultātiem ir 120 ((D) gadījums). Tā kā ikvienā no gadījumiem izvēlējāmies mazākos iespējamos pirmreizinātājus, tātad šo rezultātu nevar uzlabot.

2.jautājums: Naturālam skaitlim n ir tieši 125 naturāli dalītāji (ieskaitot 1 un pašu n). Kādu visaugstākās pakāpes sakni noteikti var izvilkt no n, iegūstot naturālu rezultātu?

Atbilde:

125 var izteikt kā reizinājumu vairākiem skaitļiem (kas pārsniedz 1) sekojošos veidos:

- $125 = 124 + 1$.
- $125 = 25 \cdot 5 = (24 + 1) \cdot (4 + 1)$.
- $125 = 5 \cdot 5 \cdot 5 = (4 + 1) \cdot (4 + 1) \cdot (4 + 1)$.

Tādēļ skaitli n var sadalīt pirmreizinātājos vienā no sekojošiem veidiem:

$$n = p^{124}, \quad n = p^{24}q^4 \quad \text{vai} \quad n = p^4q^4r^4,$$

kur p, q, r ir pirmskaitļi. Visos gadījumos var izvilkt 4.pakāpes sakni.

1.4 Pirmskaitļu izvietojums

Anotācija: Šajā tēmā pamatojam, ka pirmskaitļu ir bezgalīgi daudz, apsveram iespējas tos algoritmiski atrast (Eratostena režģis, daži mūsdienu algoritmi). Apskatām sacensību uzdevumus, kuri iedvesmojušies no šīs pirmskaitļu teorijas.

Pirmskaitļu izvietojums nelielos intervālos var izskatīties juceklīgs. Tomēr garākos intervālos to blīvums labi tuvināms ar varbūtisku modeli. Vienkāršoti sakot, lieliem naturāliem n, varbūtība, ka n ir pirmskaitlis, ir apgriezti proporcionāla skaitļa n naturālajam logaritmam.

1.4.1 Pirmskaitļu jēdziens

Definīcija: Naturālu skaitli $p > 1$ sauc par **pirmskaitli** (*prime number*), ja vienīgie tā dalītāji ir 1 un p.

Naturālus skaitļus $n > 1$, kas nav pirmskaitļi, sauc par **saliktiem skaitļiem** (*composite number*). Skaitlis 1 nav ne pirmskaitlis, ne salikts skaitlis.

Intervālā $[1; 100]$ ir 25 pirmskaitļi:

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Note: Skaitlis 1 nav ne pirmskaitlis, ne arī salikts skaitlis. Tas ir *vienības elements* naturālu skaitļu reizināšanā. (Veselo skaitļu pasaulē -1 ir otrs vienības elements.)

1.4.2 Eratostena režģis

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130

Eratostena process notiek vairākos soļos.

- Skaitļu tabuliņā atzīmē mazāko skaitli (pirmskaitli 2) un visus tā dalāmos/daudzkārtņus izsvītro.
- Atzīmē mazāko neizsvītroto (pirmskaitli 3) un visus tā daudzkārtņus izsvītro.
- Atzīmē mazāko neizsvītroto (pirmskaitli 5) un visus tā daudzkārtņus izsvītro.

Apgalvojums: Minētais process nekad nebeigsies; pēc katra soļa paliks neizsvītroti skaitļi.

Note: Vai Eratostena režģis ir efektīvs algoritms, ja jāatrod visi pirmskaitļi intervālā $[1, N]$?

Eratostens (276. g. p.m.ē –194. g. p.m.ē.) pazīstams arī ar to, ka diezgan precīzi noteicis Zemeslodes apkārtmēru. Viņa eksperiments balstījās uz novērojumu, ka divās Ēģiptes pilsētās, kas abas atrodas uz tā paša meridiāna (mūsdienās tās sauc Asuāna un Aleksandrija), ir atšķirīgs Saules augstums virs horizonta vasaras saulgriežos. Asuāna atrodas uz Ziemeļu tropiskā loka – Saule tur nonāk tieši zenītā, savukārt Aleksandrijā tā pat saulgriežos atrodas noteiktā leņķī no zenīta – un leņķi var izmērīt, piemēram, kā vertikāla staba ēnas garumu. Attālums no Asuānas līdz Aleksandrijai Eratostenam bija zināms; Zemeslodes apkārtmēru tad noteica ar trigonometrisku sakarību

Eratostena režģis ir dinamiskās programmēšanas piemērs. Šie algoritmi aizpilda apjomīgas datu struktūras (piemēram, masīvus, tabulas). Dinamiskā programmēšana ir efektīva, piemēram, kāpinot skaitļus lielās pakāpēs (atceroties agrāk iegūtus starprezultātus), vai arī, aprēķinot Fibonači skaitļus.

Lai noskaidrotu, vai konkrēts skaitlis n ir pirmskaitlis, Eratostena režģis nav praktisks algoritms (jo tas meklē visus pirmskaitļus, kas par to mazāki).

Piemērs: Kādā no Eratostena režģa veidošanas soļiem tiek izsvītroti visi tie saliktie skaitļi, kuri ir pirmskaitļa 13 daudzkārtņi. Kurš no šajā solī izsvītrotajiem skaitļiem ir pirmais?

Risinājums: Skaitļa 13 daudzkārtņi, kas tiek izsvītroti ir $26, 39, 52, \ldots$. Mazākais no šiem skaitļiem, kas nedalās ar nevienu citu pirmskaitli $p < 13$ ir $13^2 = 169$. Tam seko arī $13 \cdot 17$ un daudzi citi piemēri, kurus šajā solī izsvītro pirmoreiz.

1.4.3 Pirmskaitļu ir bezgalīgi daudz

Teorēma (Eiklīds): Pirmskaitļu ir bezgalīgi daudz.

Pierādījums: No pretējā. Ja pirmskaitļu būtu galīgs skaits, tad eksistētu lielākais pirmskaitlis p_K. Sareizinām visus pirmskaitļus, pieskaitām 1:

$$P = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_K + 1.$$

P nedalās ne ar vienu no pirmskaitļiem, kuri ir galīgajā sarakstā: vienmēr atlikums 1. Vai nu P pats ir pirmskaitlis vai kādu (sarakstā neesošu) pirmskaitļu reizinājums. Pretruna. ■

1.4.4 Pilnās pārlases algoritms

Ir iespējams, pārbaudīt, vai skaitlis n ir pirmskaitlis, to dalot ar $2, 3, \ldots$ – visiem skaitļiem līdz $\sqrt{n}$.

```
import math
def isPrime(n):
    result = True
    ROOT = int(math.sqrt(n))
    for d in range(2,ROOT+1):
        if n % d == 0:
            result = False
            break
    return result

print(isPrime(10000000019))
```

Note: Pilnā pārlase ir ļoti neefektīva (slikti strādā jau pie $n = 10^{30}$). Tam par iemeslu ir nepieciešamība kriptogrāfijā un citos lietojumos pārbaudīt vai ir pirmskaitlis kāds ļoti liels skaitlis, piemēram $p \approx 10^{100}$ (skaitlis ar aptuveni 100 cipariem).

Tad pilnajai pārlasei jāpārbauda aptuveni $\sqrt{p} \approx 10^{50}$ dalīšanās darbības – šis ir jau divreiz īsāks skaitlis, kura pierakstā ir tikai 50 cipari, bet joprojām tik liels, lai visas šīs pārbaudes praksē nevarētu izdarīt. Ja kopš Visuma rašanās (Lielā sprādziena) pagājuši aptuveni 13.8 miljardi gadu, tās ir tikai $4.35 \cdot 10^{23}$ mikrosekundes.

1.4.5 Ātrāki pirmskaitļu testi

Ir algoritmi, kuri darbojas pietiekami efektīvi arī pie $p \approx 10^{100}$ un vēl daudz lielākiem skaitļiem. Pirmais no tiem ir Millera-Rabina tests (ap 1982.g.), kas izmanto nejaušo skaitļu ģeneratoru un var kļūdīties ar kaut kādu varbūtību. Nedaudz palielinot pārbaužu skaitu, šo kļūdīšanās varbūtību var pēc patikas samazināt. Šo algoritmu vēl joprojām visvairāk izmanto praksē. Sk. teoriju https://bit.ly/3qOFLsS un arī algoritma kodu dažās programmēšanas valodās – https://bit.ly/3nNpKBo.

Cits svarīgs algoritms ir https://bit.ly/3FROhLN, AKS algoritms jeb Agrawal-Kayal-Saxena pirmskaitļu tests ap 2002.g.) Tas bija pirmais efektīvais algoritms, kas neizmanto nejaušos skaitļus un arī nepieļauj kļūdīšanās varbūtību.

Piemērs: Vai eksistē 1000 pēc kārtas sekojoši skaitļi, kuri visi ir salikti?

Atstarpēm starp pirmskaitļiem ir tendence pieaugt, ja skaitļi kļūst lielāki; pastāv izvērsta teorija par **pirmskaitļu atstarpēm** (*prime gaps*). Sk. https://bit.ly/3nOnoSG. Enciklopēdijas tabulā atrodam, ka pirmā vieta, kur attālums starp diviem pirmskaitļiem pārsniedz tūkstoti, sākas ar pirmskaitli $p = 1\,693\,182\,318\,746\,371$

```
>>> import sympy
>>> p1 = 1693182318746371
>>> p2 = p1 + 1132
>>> set([sympy.isprime(n) for n in range(p1+1, p2)])
{False}
```

No otras puses, ir arī zināms, ka starpība starp diviem pēc kārtas sekojošiem pirmskaitļiem bezgalīgi daudzas reizes nepārsniedz 246. (T.i. eksistē cik patīk lieli pirmskaitļi p_1 un p_2, kuriem $|p_1 - p_2| \leq 246$.) Jautājums, vai eksistē bezgalīgi daudzi dvīņu pirmskaitļi (starp kuriem attālums ir 2), joprojām ir atklāts.

Konstruktīvs pierādījums: Ja mums nav pieejams dators, Internets vai citi palīglīdzekļi, tad 1000 pēc kārtas sekojošus saliktus skaitļus var uzkonstruēt arī ar vienkāršiem algebriskiem spriedumiem.

Izvēlamies $N = 1001! + 2$, tad iegūstam, ka $1000! + a$ dalās ar a katram $a \in \{2, \dots 1001\}$. □

Ievērojam, ka iegūtais $N = 1001! + 2$ (vieta, kur sākas saliktie skaitļi) ir krietni lielāks nekā vērtība $p_1 = 1693182318746371 + 1$, kas norādīta enciklopēdijā.

Uzdevums: Pierādīt, ka ir bezgalīgi daudz nepāru pirmskaitļu, kas izsakāmi formā $4k + 3$ (dod atlikumu 3, dalot ar 4).

TODO: Pamatot līdzīgi kā pierādījumā par bezgalīgo pirmskaitļu skaitu.

1.4.6 Dirihlē teorēma par pirmskaitļiem

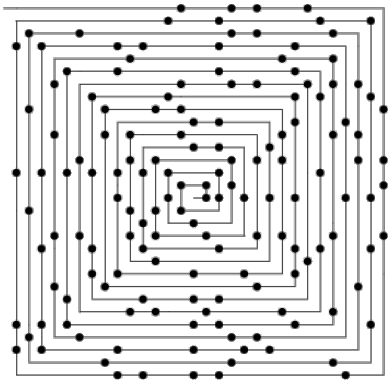
Dirihlē Teorēma (Dirichlet): Ja a un d ir savstarpēji pirmskaitļi, tad bezgalīgā aritmētiskā progresijā

$$a, a + d, a + 2d, a + 3d, \dots$$

ir bezgalīgi daudz pirmskaitļu.

Dažām a un d vērtībām šo teorēmu var pierādīt ar elementārām metodēm (nupat redzējām pie $a = 3$ un $d = 4$). Bet vispārīgajā gadījumā ir piemērotākas matemātiskās analīzes metodes, kas iziet ārpus mūsu kursa.

1.4.7 Ulama spirāle



Ulama spirāli veido, uz rūtiņu papīra zīmējot attinošos spirāli, sākot ar skaitli 1. Pirmskaitļus, atzīmē ar melniem punktiņiem.

Pirmskaitļi neveido viegli paredzamas likumsakarības, bet tie sablīvējas uz dažām taisnēm.

Piemērs: Aplūkojam polinomu $f(x) = x^2 + x + 41$. Visiem argumentiem $x = 0, 1, \ldots, 39$ tas pieņem vērtības, kas ir pirmskaitļi.

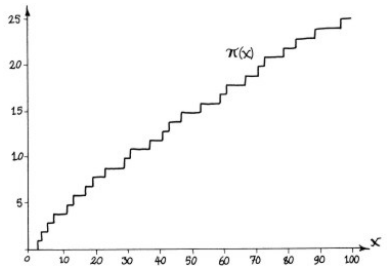
Šī polinoma vērtību vidū arī lielākiem x ir neparasti daudz pirmskaitļu. Ar modulāro aritmētiku iespējams pamatot, ka $x^2 + x + 41$ (kur $x \in \mathbb{N}$) nevar dalīties ne ar vienu pirmskaitli $p < 41$.

Note: Joprojām nepastāv viegli uzrakstāma formula (piemēram, izmantojot elementārās funkcijas, veselās daļas u.c.), kuras vērtību kopa būtu bezgalīga un saturētu tikai pirmskaitļus.

Protams, nav jēgas meklēt tādas starp polinomiem. Tomēr izrādās, ka daži polinomi starp savām vērtībām satur neparasti daudz pirmskaitļu.

TODO: Vizualizācija, kur $x^2 + x + 41$ vērtības atliktas uz Ulama spirāles.

1.4.8 Pirmskaitļu skaitīšanas funkcija



Definīcija: Ar $\pi(x)$ apzīmējam **pirmskaitļu skaitīšanas funkciju** (*prime-counting function*): Katram reālam skaitlim $x \in \mathbb{R}$, $\pi(x)$ izsaka pirmskaitļu p_i skaitu, kuriem $p_i \leq x$.

$\pi(x)$ definīcijas apgabals ir $\mathbb{R}$, vērtību apgabals ir $\mathbb{Z}_{0+}$ – visi veselie nenegatīvie skaitļi.

Piemēri: $\pi(1.99) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(3.14) = \pi(4.99) = 2$, $\pi(100) = 25$.

1.5 Mersena un Fermā skaitļi

Anotācija: Meklējot pirmskaitļus formā $2^n \pm 1$ (vai vispārīgāk - $a^n \pm 1$) saskaramies ar algebriskām likumsakarībām – bieži pastāv identitātes, kas ļauj izteiksmi sadalīt reizinātājos. Toties situācijas, kad tas nav triviāli izdarāms ir pētītas un novedušas pie Fermā un Mersena pirmskaitļu jēdziena. Tās ļauj atrast ļoti lielus pirmskaitļus.

1.5.1 Algebriskas identitātes

- Pakāpju starpības formula (visiem $n \geq 2$):

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b^1 + \ldots + a^1 b^{n-2} + b^{n-1}\right).$$

- Pakāpju summas formula (visiem $n \geq 1$):

$$a^{2n+1} + b^{2n+1} = (a+b)\left(a^{2n} - a^{2n-1}b^1 + a^{2n-2}b^2 - \cdots - a^1 b^{2n-1} + b^{2n}\right).$$

Var pierādīt, atverot iekavas. (Iekavās ar daudzpunktiem ir galīgu ģeometrisku progresiju summas.)

1.5.2 Fermā skaitļu jēdziens

Bijuši vairāki mēģinājumi uzrakstīt kompaktu formulu (bez *for* cikliem vai citiem programmēšanas paņēmieniem), kuras visas vērtības ir pirmskaitļi.

Definīcija: Par n-to Fermā skaitli ($n \geq 0$) sauc $F_n = 2^{2^n} + 1$.

P.Fermā (*Pierre de Fermat*, 1607–1665) izteica hipotēzi, ka visi F_n ir pirmskaitļi.

F_0, F_1, F_2, F_3, F_4 ir vienīgie zināmie pirmskaitļi:

- $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$,
- $F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$,
- $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$,
- $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$,
- $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$.

Jau $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$ nav pirmskaitlis. (Leonards Eilers (Leonhard Euler), 1707-1783).

Note: Izņemot pirmos 5 Fermā skaitļus (no F_0 līdz F_4), nav zināms neviens cits pirmskaitlis. Ir pilnībā sadalīti pirmreizinātājos pirmie 12 šādi skaitļi – no F_0 līdz $F_1 1$. Daudziem citiem ir zināmi daži dalītāji; atklāto/zināmo dalītāju skaits tiek regulāri papildināts.

Skaitļi formā $2^N + 1$ nevar būt pirmskaitļi, ja kāpinātājam N ir kāds nepāru dalītājs, kas lielāks par 1, jo šajā gadījumā var dalīt reizinātājos, izmantojot algebriskas identitātes $a^3 + 1^3$, $a^5 + 1^5$ utml.

Tātad pats kāpinātājs N (lai sanāktu kaut kas interesants, kas nedalās reizinātājos pavisam triviāli) noteikti ir divnieka pakāpe jeb $2^N + 1$ ir faktiski pierakstāms kā $2^{2^k} + 1$. Fermā pirmskaitļi $2^n + 1$ ir iespējami vien tad, ja skaitlim n nav nepāru dalītāju (pretējā gadījumā tos var sadalīt reizinātājos, izmantojot kubu summu, piekto pakāpju summu vai līdzīgu identitāti). Tātad Fermā pirmskaitļi patiesībā izskatās šādi: $2^{2^n} + 1$.

1.5.3 Mersenna skaitļi

Definīcija: Skaitli M_n sauc par **Mersenna skaitli** (*Mersenne number*), ja to var izteikt formā $2^n - 1$. Ja turklāt M_n ir pirmskaitlis, tad to sauc par **Mersenna pirmskaitli** (*Mersenne prime*).

Note: Kāda īpašība noteikti jāizpilda skaitlim n, lai $M_n = 2^n - 1$ būtu izredzes būt pirmskaitlim?

Ja n nav pirmskaitlis un to var sadalīt kā $n = ab$, tad $2^n - 1$ dalās reizinātājos kā divu a-to (vai divu b-to) pakāpju starpība un tātad nav pirmskaitlis. Tātad vienīgie Mersena pirmskaitļi var būt formā $2^p - 1$, kur p ir pirmskaitlis. Šādā formā parasti ir pirmskaitļi-rekordisti (t.i. lielākie starp visiem pirmskaitļiem, kuri ikbrīd zināmi progresīvajai cilvēcei).

Teorēma: Lai Mersena skaitlis $M_n = 2^n - 1$ būtu pirmskaitlis, ir *nepieciešami*, lai pats n būtu pirmskaitlis.

Pierādījums: Ja $n = km$ ir divu naturālu skaitļu reizinājums (turklāt $k > 1$ un $m > 1$), tad var sadalīt reizinātājos kā $a^m - b^m$:

$$M_n = 2^{km} - 1 = \left(2^k\right)^m - 1^m =$$

$$= (2^k - 1)\left((2^k)^{m-1} + \ldots + 1\right) . : math : \text{‘}\blacksquare\text{‘}$$

Nosacījums, ka p ir pirmskaitlis ir *nepieciešams*, bet nav *pietiekams*, lai $2^p - 1$ būtu pirmskaitlis.

Piemēri:

begin{array}{l} $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$,\ $M_{23} = 2^{23} - 1 = 8388607 = 47 \cdot 178481$.\ end{array}

Šādu piemēru ir tik daudz, ka Mersena skaitļi, kuri tiešām ir pirmskaitļi, ir tikai niecīga daļa no visiem $2^p - 1$ (pašlaik zināms tikai 51 Mersena pirmskaitlis; vidēji katru gadu atrod pa vienam jaunam).

Mersena pirmskaitļu piemēri:

n	2	3	5	7	13	17	19	31
$M_n = 2^n - 1$	3	7	31	127	8191	131 071	524 287	2 147 483 647

Lielākais Mersena pirmskaitlis (un vispār - lielākais zināmais pirmskaitlis) ir $2^{82\,589\,933} - 1$. Tas atrasts 2018.g. decembrī.

Pavisam zināmi 51 Mersena pirmskaitļi. Kopš 1996.g. GIMPS (*Great Internet Mersenne Prime Search*) projekta ietvaros 23 gadu laikā atrasti jau 17 pirmskaitļi.

Sk. visu zināmo Mersenna pirmskaitļu sarakstu – https://bit.ly/3nOYhzl.

Note: Šis GIMPS projekts parādījās kā prototips/iedvesma BitCoin un citu līdzīgu kriptovalūtu rēķināšanai. Lielākā zināmā Mersena pirmskaitļa $M_{82,589,933}$ decimālpierakstā ir $24,862,048$ cipari – pilnībā izdrukāts tas aizņemtu vairākus grāmatplauktus.

1.5.4 Perfektie skaitļi

Definīcija: Skaitli sauc par **perfektu** (*perfect number*), ja tas vienāds ar visu savu dalītāju summu (izņemot sevi pašu).

Piemēri: $6 = 1 + 2 + 3$; $28 = 1 + 2 + 4 + 7 + 14$.

Teorēma (Eiklīds): Ja $2^p - 1$ ir pirmskaitlis, tad $2^{p-1}(2^p - 1)$ ir perfekts.

Teorēma (Eilers): Visi pāru perfektie skaitļi izsakāmi formā $2^{p-1}(2^p - 1)$.

Izteiksim dažus perfektos skaitļus binārajā pierakstā:

Pirmskaitlis p	$2^{p-1}(2^p - 1)$ vērtība
$p = 2$	$6_{10} = 110_2$
$p = 3$	$28_{10} = 11100_2$
$p = 5$	$496_{10} = 111110000_2$
$p = 7$	$8128_{10} = 1111111000000_2$
$p = 13$	$33550336_{10} = 1111111111111000000000000_2$

Ar $p = 11$ Mersenna pirmskaitlis nesanāk, jo $2^{11} - 1 = 2047 = 23 \cdot 89$.

1.5.5 Jautājumi par Fermā un Mersena skaitļiem

1.jautājums: Vispārināt Fermā skaitļus, noskaidrojot, kuri no $a^k + 1$ var būt pirmskaitļi naturālām a un k vērtībām (ja $a \neq 2$).

2.jautāums: Pierādīt, ka naturāliem skaitļiem m un n, kam $m > n$, Fermā skaitlis $F_m - 2$ noteikti dalās ar F_n.

Atbilde:

Atkārtoti lietojam kvadrātu starpības formulu dalīšanai reizinātājos:

$$F_m - 2 = 2^{2^m} + 1 - 2 = 2^{2^m} - 1 =$$

$$= \left(2^{2^{m-1}} - 1\right)\left(2^{2^{m-1}} + 1\right) = (F_{m-1} - 2)\, F_{m-1}.$$

Ja arī $m - 1 > n$, tad līdzīgu spriedumu atkārto vēlreiz, dalot reizinātājos $F_{m-1} - 2$ utt. Katrā solī redzam, ka uzrodas reizinātāji F_{m-1}, F_{m-2} utt. Kāds no šiem reizinātājiem būs tieši F_n.

3.jautājums: Dažādiem naturāliem m un n, skaitļi F_m un F_n ir savstarpēji pirmskaitļi. (Piemēram, F_5 dalās ar 641. Tātad neviens cits Fermā skaitlis nevar dalīties ar 641.)

Atbilde:

Pieņemsim, ka $m > n$. Tad $F_m - 2$ dalās ar F_n. Iegūstam:

$$\mathrm{LKD}(F_m, F_n) = \mathrm{LKD}((F_m - 2) + 2, F_n) = \mathrm{LKD}(2, F_n) = 1.$$

4.Jautājums: Atrast visus pirmskaitļus, kas izsakāmi formā $n^n + 1$ un ir mazāki kā 10^{19}.

Atbilde:

Ja n dalās ar kādu nepāru skaitli $c > 1$ (t.i. $n = cd$, kur $c = 2k + 1 \geq 3$), tad pirmskaitlis nesanāk, jo

$$n^n + 1 = \left(n^d\right)^c + 1^c = \left(n^d\right)^{2k+1} + 1^{2k+1},$$

kas dalās reizinātājos pēc formulas $a^{2k+1} + b^{2k+1} = (a + b)(a^{2k} - \ldots + b^{2k})$, kur $a = n^d$ un $b = 1$.

Ja n ir divnieka pakāpe, šķirojam gadījumus:

- Ja $n = 1$, tad $n^n + 1 = 2$ (der)
- Ja $n = 2$, tad $n^n + 1 = 5$ (der)
- Ja $n = 4$, tad $n^n + 1 = 257$ (der)

Ja $n = 8$, tad

$$8^8 + 1 = \left(2^8\right)^3 + 1^3,$$

kas dalās reizinātājos pēc formulas $a^3 + b^3 = (a + b)\left(a^2 - ab + b^2\right)$:

$$8^8 + 1 = \left(2^8 + 1\right)\left(2^{16} - 2^8 + 1\right).$$

Pamatosim, ka pie $n = 16$ skaitlis $n^n + 1 > 10^{19}$, t.i. šāds skaitlis neder (neatkarīgi no tā, vai tas ir pirmskaitlis).

$$16^{16} + 1 = 2^{64} + 1 =$$

$$2^4 \cdot 2^{60} + 1 = 16 \cdot \left(2^{10}\right)^6 + 1 = 16 \cdot 1024^6 + 1 >$$
$$> 16 \cdot 1000^6 = 16 \cdot 10^{18} = 1.6 \cdot 10^{19} > 10^{19}.$$

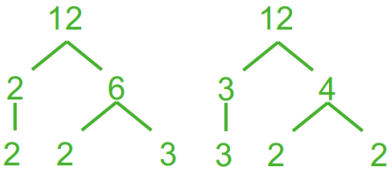
Note: Starp citu, $16^{16} + 1 = 2^{64} + 1 = 2^{2^6} + 1 = F_6$ ir sestais Fermā skaitlis. Tas nav pirmskaitlis: $F_6 = 18\,446\,744\,073\,709\,551\,617$ dalās ar $274177 = 1071 \cdot 2^8 + 1$.

To pamatoja Tomass Klausens (*Thomas Clausen*, 1855.g. Tartu, tag. Igaunija).

1.6 Aritmētikas pamatteorēma

Teorēma: Katrs naturāls skaitlis $n > 1$ ir vai nu pirmskaitlis, vai arī ir izsakāms pirmskaitļu reizinājumā, pie tam šis reizinājums ir viens vienīgs (ja neņem vērā reizinātāju secību).

Eksistence: Pierādām ar indukciju: Ja $n = 2$, tad apgalvojums ir spēkā, jo 2 ir pirmskaitlis. Pieņemam, ka apgalvojums ir spēkā visiem $k < n$. Pamatosim, ka tas izpildās arī skaitlim n. Ja n ir pirmskaitlis, tad tas jau ir šādi izteikts. Savukārt, ja $n = ab$ (kur $a, b > 1$), tad abus a un b jau protam izteikt. □



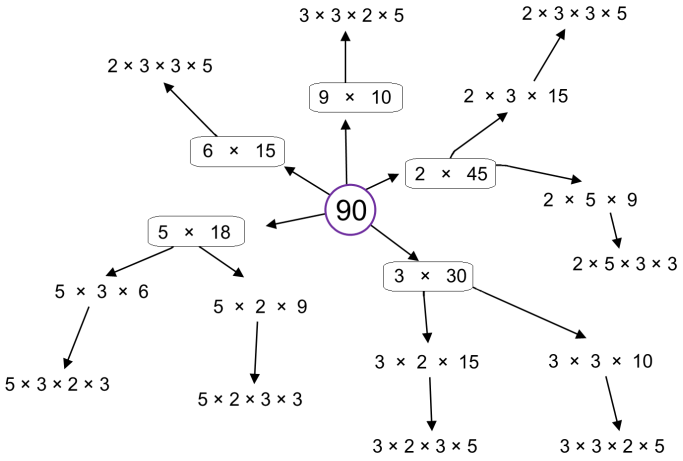
Kāpēc neatkarīgi no **faktorizēšanas** secības, vienmēr sanāk tas pats? (Par faktorizēšanu sauc dalīšanu reizinātājos.)

$$12 = 2 \cdot 6 = 2 \cdot 2 \cdot 3.$$
$$12 = 3 \cdot 4 = 3 \cdot 2 \cdot 2.$$
$$3 \cdot 2 \cdot 2 \cdot 1 \cdot 1 \cdot 1.$$
$$3 \cdot 2 \cdot 2 \cdot (-1) \cdot (-1).$$

Note: Lielu skaitļu (100 un vairāk ciparu) dalīšana reizinātājos ir datoram grūti veicams uzdevums. Pirmskaitļu testi (kā Millera-Rabina tests u.c.) var salīdzinoši ātri dot atbildi, vai skaitlis ir pirmskaitlis vai nē. Bet neeksistē līdzīgs efektīvs algoritms, kas dalītu reizinātājos tos skaitļus, kuri **nav** pirmskaitļi.

Pirmskaitļi te līdzinās atomiem ķīmijā. Ķīmiski tīra viela (neatkarīgi no sadalīšanas veida un soļiem) dod elementu atomus, kuru skaits attiecas kā nelieli veseli skaitļi. Līdzīgi kā ūdens molekulu veido divi ūdeņraža un viens skābekļa atoms, skaitli 12 veido divi pirmskaitļa 2 atomi un viens pirmskaitļa 3 atoms.

Skaitļa 90 faktorizācija



Ļoti dažādi veidi, kā nonākt līdz pirmskaitļu reizinājumam.

Note: Fakts, ka ikvienu naturālu skaitli var tieši vienā veidā izteikt kā (viena vai vairāku) pirmskaitļu reizinājumu, nav triviāls vai pašsaprotams. Tas izriet no vairākām naturālu skaitļu aritmētikā esošām īpašībām (kas tieši **neizriet** no reizināšanas vai dalīšanas attiecības). Pierādījums izmanto naturālu skaitļu sakārtojumu (starp skaitļiem var atrast vismazāko), izmanto iespēju dalīt ar atlikumu. Ir iespējamas tādas īpatnēju "skaitļu" kopas, kurās aritmētikas pamatteorēma neizpildās.

Sk. *Factor trees* – https://bit.ly/3KztiB5.

Viennozīmība: Pieņemsim, ka $s > 1$ izsakāms divos dažādos veidos:

$$s = p_1 p_2 \cdots p_m,$$

$$s = q_1 q_2 \cdots q_n.$$

Jāparāda, ka $m = n$ un q_j ir tie paši, kas p_j (iespējams, citā secībā). Pēc **Eiklīda lemmas** p_1 dala vienu no q_j. Pārnumurējam tā, lai p_1 dalītu q_1.

Tā kā q_1 arī ir pirmskaitlis, tad $p_1 = q_1$. Dalām abas vienādības ar p_1. Iegūstam:

$$s_1 = p_2 \cdots p_m,$$

$$s_1 = q_2 \cdots q_n.$$

Tagad tāpat var pamatot, ka $p_2 = q_2$, utt. ■

Eiklīda lemma: Ja pirmskaitlis p dala divu veselu skaitļu reizinājumu ab, tad p dala vismaz vienu no skaitļiem a vai b.

Pierādījums: Pieņemsim, ka p un a ir savstarpēji pirmskaitļi. (Ja LKD$(p, a) > 1$, tad p dalītu a). Pēc **Eiklīda algoritma** jebkuriem savstarpējiem pirmskaitļiem p, a var atrast tādus veselus x un y, ka $px + ay = 1$ (**Bezū identitāte**).

Tā kā pxb dalās ar p un $ayb = (ab)y$ dalās ar p, tad arī summa $pxb + ayb = (px + ay)b = 1 \cdot b = b$ dalās ar p. ■

Kopsavilkums Kā nupat redzējām: Bezū identitāte ⇒   Eiklīda lemma ⇒   Aritmētikas pamatteorēma.

Aritmētikas pamatteorēma tātad izmanto ne vien pirmskaitļu jēdzienu, bet arī iespēju sakārtot veselus pozitīvus skaitļus (atrast starp bezgalīgi daudzajiem $ax + by = d$ vismazāko pozitīvo), gan arī iespēju dalīt skaitļus ar atlikumu, ka atlikums r ir mazāks par dalītāju d.

Neparasts piemērs: Ieviešam skaitļu kopu $a + b\sqrt{-5}$, kur a, b ir veseli skaitļi. Divu skaitļu $a_1 + b_1\sqrt{-5}$ un $a_2 + b_2\sqrt{-5}$ reizinājums atkal ir skaitlis no šīs kopas. Tātad arī šajā kopā var dalīt skaitļus reizinātājos; definēt "pirmskaitļus" p (kuriem vienīgie dalītāji ir $1, -1, p, -p$).

$$6 = 2 \cdot 3.$$

$$6 = (1 - \sqrt{-5})(1 + \sqrt{-5}) = 1^2 - (\sqrt{5})^2 = 1 - (-5) = 6.$$

Skaitli 6 var sadalīt pirmreizinātājos divos dažādos veidos!

Šajā komplekso skaitļu apakškopā var nodarboties ar skaitļu reizināšanu un pat definēt "pirmskaitļus". Bet tajā nepastāv iespēja skaitļus salīdzināt ar $<$ un $>$, nevar dalīt ar atlikumu, nepastāv arī Eiklīda lemma.

Uzdevums: Pamatot, ka skaitļi $p_1 = 2$, $p_2 = 3$, $p_3 = 1 - \sqrt{-5}$ un $p_4 = 1 + \sqrt{-5}$ ir "pirmskaitļi" skaitļu kopā

$$\left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}.$$

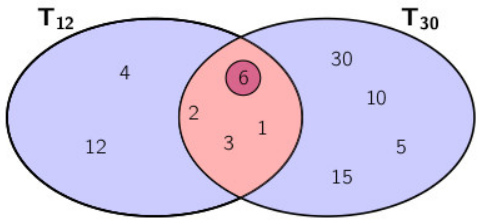
Citiem vārdiem: Ja kādu no šiem p_i ($i = 1, 2, 3, 4$) var izteikt kā reizinājumu:

$$p_i = (a + b\sqrt{-5})(c + d\sqrt{-5}),$$

tad vai nu viens, vai otrs reizinātājs ir $+1$ vai -1.

1.7 LKD un MKD

1.7.1 Intuīcija par LKD



Aplūkojot visus divu skaitļu kopīgos dalītājus (vai dalāmos), izrādās, ka starp tiem vienmēr ir noteiktas sakarības, ko var ļoti kompakti aprakstīt, atrodot lielāko kopīgo dalītāju (attiecīgi mazāko kopīgo dalāmo).

Definīcija: Par veselu skaitļu m un n **lielāko kopīgo dalītāju (LKD)** (*greatest common divisor*, ko reizēm pieraksta arī kā *gcd(m,n)*) sauc lielāko naturālo skaitli, ar kuru dalās gan m, gan n. To apzīmē ar $\mathrm{LKD}(m, n)$.

Piezīme: LKD var definēt arī vairāk nekā diviem skaitļiem, bet tie nedrīkst visi reizē būt 0. Pat ja m, n ir negatīvi, $\mathrm{LKD}(m, n)$ vienmēr ir vesels pozitīvs jeb naturāls skaitlis.

Piemēri:

$$\mathrm{LKD}(8, 12) = 4,$$
$$\mathrm{LKD}(21, 34) = 1,$$
$$\mathrm{LKD}(0, -17) = 17‘.$$

1.7.2 Savstarpēji pirmskaitļi

Definīcija: Skaitļus m un n sauc par **savstarpējiem pirmskaitļiem** (*mutual primes*, *co-primes*), ja $\text{LKD}(m, n) = 1$.

Piemēri:

1. Naturāli skaitļi n un $n + 1$ vienmēr ir savstarpēji pirmskaitļi (piemēram, $\text{LKD}(15, 16) = 1$.
2. Divi dažādi pirmskaitļi vienmēr ir arī savstarpēji pirmskaitļi (piemēram, $\text{LKD}(13, 17) = 1$).

1.7.3 LKD un citi kopīgie dalītāji

Apgalvojums: Ja a un b ir veseli skaitļi, kas nav abi reizē vienādi ar 0, tad to lielākais kopīgais dalītājs $d = \text{LKD}(a, b)$ ir tāds, ka jebkuram citam abu skaitļu kopīgam dalītājam d^* (kur $d^*|a$ un $d^*|b$), šis d^* būs arī d dalītājs.

Neformāli sakot, $d = \text{LKD}(a, b)$ ir nevis vienkārši lielākais skaitlis starp dažādiem a un b kopīgajiem dalītājiem, bet tas ir visu šādu dalītāju režģa augšējais punkts.

1.7.4 LKD, ja dots sadalījums pirmreizinātājos

$\text{LKD}(m, n)$ viegli atrast, ja m, n sadalīti pirmreizinātājos.

Pirmreizinātājs	2	3	5	7
300	2^2	3^1	5^2	7^0
300	2^1	3^2	5^1	7^1

$\text{LKD}(300, 630) = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 30$.

$\text{LKD}(m, n)$ satur tos pašus pirmreizinātājus, ko m un n, bet katra pirmreizinātāja pakāpe ir minimums no pirmreizinātāja pakāpes skaitlī m un šī paša pirmreizinātāja pakāpes skaitlī n.

1.7.5 Dažādas LKD īpašības

- Ja p ir pirmskaitlis, tad $\text{LKD}(p, m)$ ir p vai 1.
- Ja $\text{LKD}(m, n) = d$, tad m/d un n/d ir savstarpēji pirmskaitļi.
- Ja m/d^* un n/d^* abi ir veseli un savstarpēji pirmskaitļi, tad $\text{LKD}(m, n) = d^*$.
- $\text{LKD}(m, n) = \text{LKD}(m - n, n)$. LKD nemainās, ja no viena skaitļa atņem otru skaitli (vai arī divkāršotu, trīskāršotu utt. otru skaitli).
- Ja $m = nq + r$, tad $\text{LKD}(m, n) = \text{LKD}(r, n)$ (skaitli m var aizstāt ar tā atlikumu, dalot ar n).

1.7.6 Kā praktiski atrast LKD?

Varētu sadalīt pirmreizinātājos un atrast minimumus pa visām pirmskaitļu pakāpēm.

Piemērs: Ja $m = 2^{10}3^85^9$ un $n = 2^{17}3^5$, tad $\text{LKD}(m, n) = 2^{10}3^5$.

Faktiski ir ļoti grūti dalīt lielus skaitļus pirmreizinātājos. Piemēram,

$$\text{LKD}(73786976294838206463, 295147905179352825855) = ?$$

1.7.7 Eiklīda algoritms

```
def gcd(a, b):
    while b:
        a, b = b, a % b
    return a
```

Pseidokods:

LIELAKAISKOPIGAISDALITAJS(a, b):
1. **while** $b \neq 0$:
2. $\quad (a, b) := (b, a \bmod b)$
3. **return** a.

Skaitlisks piemērs: Atrast 21 un 30 lielāko kopīgo dalītāju.

Risinājums:

$$\begin{aligned} \text{LKD}(21, 30) &= \text{LKD}(30, 21) = \\ &= \text{LKD}(21, 9) = \\ &= \text{LKD}(9, 3) = \\ &= \text{LKD}(3, 0) = 3. \end{aligned}$$

- Eiklīda algoritmam nepieciešams, lai skaitļi a, b būtu naturāli.
- Lai atrastu LKD(a, b), kur a vai b ir negatīvi, algoritmu izpilda absolūtajām vērtībām:

$$\text{LKD}(a, b) = \text{LKD}\left(|a|, |b|\right).$$

Uzdevums (BW.TST.2016.16): Kāda ir izteiksmes

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

lielākā iespējamā vērtība naturāliem n?

Risinājums: Lietojam Eiklīda algoritmu polinomiem no mainīgā n:

$$\text{LKD}\left(n^2 + 3, (n+1)^2 + 3\right) = \text{LKD}\left(n^2 + 3, n^2 + 2n + 4\right) =$$

no otrā argumenta atņem pirmo:

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

pirmo argumentu var piereizināt ar 2, jo otrais ir nepāru:

$$= \text{LKD}\left(2n^2 + 6, 2n + 1\right) =$$

no pirmā argumenta atņem n-kāršotu otro:

$$= \text{LKD}\left(2n^2 + 6 - n(2n+1), 2n + 1\right) = \text{LKD}(6 - n, 2n + 1) =$$

otrajam argumentam pieskaita divkāršotu pirmo:

$$= \text{LKD}(6 - n, 2n + 1 + 2(6 - n)) = \text{LKD}(n - 6, 13).$$

Secinājums: $\text{LKD}\left(n^2 + 3, (n+1)^2 + 3\right) = \text{LKD}(n - 6, 13)$ var būt vai nu 1 vai 13.

Vērtību 13 (vai kādu daudzkārtni) tas sasniedz, ja $n - 6$ dalās ar 13, piemēram, ja $n-6 = 0$ jeb $n=6$.

Pārbaude: Ievietojam $n = 6$:

$$\text{LKD}\left(6^2 + 3, (6+1)^2 + 3\right) = \text{LKD}(39, 52) = 13.$$

1.7.8 MKD jēdziens

Definīcija: Par veselu skaitļu m un n **mazāko kopīgo dalāmo** (*least common multiple*, ko reizēm pieraksta arī kā *lcm(m,n)*) sauc mazāko naturālo skaitli, kurš ir daudzkārtnis gan skaitlim m, gan skaitlim n. To apzīmē ar $\text{MKD}(m, n)$.

Piezīme: MKD definēts tikai tad, ja abi veselie skaitļi $m, n \neq 0$.

MKD sadalījums pirmreizinātājos: Arī $\text{MKD}(m, n)$ (līdzīgi kā $\text{LKD}(m, n)$) var tūlīt uzrakstīt, ja m, n jau sadalīti pirmreizinātājos:

Pirmreizinātājs	2	3	5	7
300	2^2	3^1	5^2	7^0
300	2^1	3^2	5^1	7^1

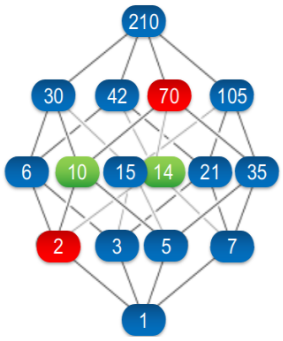
$\text{MKD}(300, 630) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 6300$.

$\text{MKD}(m, n)$ satur tos pašus pirmreizinātājus, ko m un n, bet katra pirmreizinātāja pakāpe ir maksimums no to pakāpēm skaitļos m un n.

1.7.9 LKD un MKD ir savstarpēji izsakāmi

Apgalvojums: Tā kā $\text{LKD}(a, b)$ sareizina a un b pirmreizinātāju pakāpju minimumus, bet $\text{MKD}(a, b)$ - maksimumus, tad

$$ab = \text{LKD}(a, b) \cdot \text{MKD}(a, b).$$

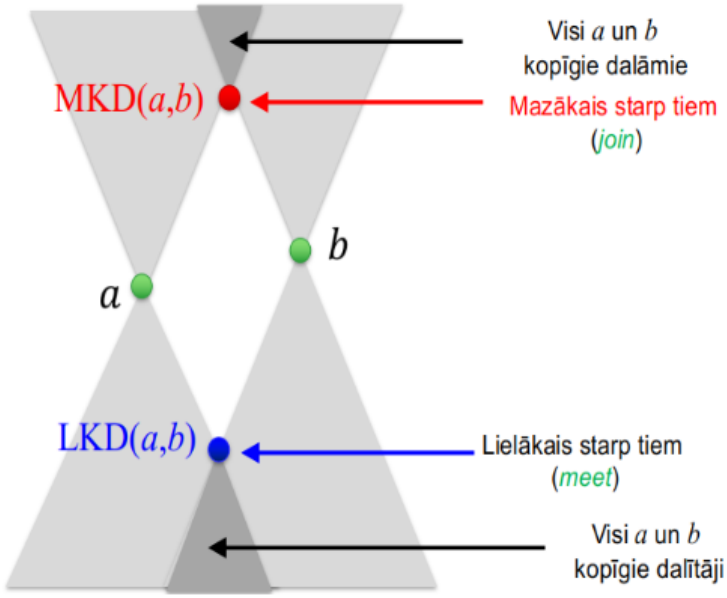


Zaļo un sarkano skaitļu reizinājumi sakrīt: $2 \cdot 70 = 10 \cdot 14$.

- Dalāmības režģī LCD (skaitlis 2 zīmējumā) ir augstākā vieta, no kuras var nonākt gan skaitlī 10, gan skaitlī 14.
- MCD (skaitlis 70) ir zemākā vieta, kur satiekas augšupejošie ceļi no 10 un 14.

$$\text{MKD}(10, 14) = \frac{10 \cdot 14}{\text{LCD}(10, 14)}.$$

1.7.10 Dalāmības attiecības režģis un LKD, MKD



Note: Vidusskolas aritmētikā bieži jānoskaidro gan LKD (lai noīsinātu daļskaitļus), gan arī – MKD (lai atrastu mazāko kopsaucēju). Tomēr nereti skolu kursā koncentrējas vienīgi uz prasmi atrast šos lielumus nelieliem skaitļiem, risinot aritmētikas piemērus, bet maz pievēršas abu lielumu vispārīgajām īpašībām.

Teorēma: Naturāli skaitļi m un n abi ir naturāla skaitļa a dalītāji tad un tikai tad, ja $d = \text{MKD}(m,n)$ ir skaitļa a dalītājs.

$$(\forall m,n,a \in \mathbb{N})\,((m \mid a)\&(n \mid a) \;\Leftrightarrow\; \text{MKD}(m,n) \mid a)\,.$$

To lasa šādi: "Visiem naturā;iem m, n, a, m dala a **UN** n dala a tad un tikai tad (t.t.t.) ja $\text{MKD}(m,n)$ dala a.

Piemēri: Skaitlis a dalās ar 7 un 9 t.t.t. ja a dalās ar 63. Skaitlis a dalās ar 4 un 6 t.t.t. ja a dalās ar 12.

Apzīmējums **t.t.t.** nozīmē "tad un tikai tad" ($\leftrightarrow$). Šajos gadījumos var secināt abos virzienos. (Sal. "Četrstūris ir paralelograms t.t.t. ja tā abas diagonāles krustpunktā dalās uz pusēm.")

1.8 Tipisks piemērs

Uzdevums (BW.TST.2018.14): Par naturālu skaitļu virkni $a_1, a_2, \ldots$ zināms, ka $a_1 = 2$ un visiem $n > 1$ skaitlis a_{n+1} ir lielākais pirmskaitlis, ar ko dalās skaitlis $a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$. Pierādīt, ka neviens no šīs virknes locekļiem nav vienāds ne ar 5, ne ar 11.

Uzdevums ir variācija par Eiklīda pazīstamo pierādījumu, ka pirmskaitļu ir bezgalīgi daudz: tiek konstruēta bezgalīga pirmskaitļu virkne $a_1, a_2, \ldots$.

Ievērojam, ka pirmskaitļi šajā virknē neatkārtojas. No pretējā: Ja pie $m < n$ izpildītos $a_n = a_m$, tad a_n būtu dalītājs gan skaitlim $A_{n-1} = a_1 a_2 \cdots a_{n-1}$ (jo šajā garajā reizinājumā ietilpst $a_m = a_n$), gan arī skaitlim $A_{n-1} + 1$. Tā ir pretruna, jo A_{n-1} un $A_{n-1} + 1$ ir viens otram sekojoši - tātad ir savstarpēji pirmskaitļi.

Lai gan virknē $a_1, a_2, \ldots$ ir bezgalīgi daudz pirmskaitļu (kā jau pamatoja Eiklīds), šī virkne tomēr nesatur **visus** pirmskaitļus. Piemēram, tā nesatur pirmskaitli 5 (un arī 11).

Pierakstām ar kvantoriem pierādāmo apgalvojumu par 5:

$$(\forall n \in \mathbb{N})(a_n \neq 5).$$

(Jebkuram naturālam n, $a_n \neq 5$.)

Ja gribam pierādīt no pretējā, tad pretējais apgalvojums (kas izrādīsies aplams):

$$(\exists n \in \mathbb{N})(a_n = 5).$$

(Eksistē tāds naturāls n, ka $a_n = 5$.)

Mūsu metode ir nepilnā indukcija – vienkārši izrakstām dažus virknes locekļus un meklējam likumsakarības.

$$a_1 = 2,\ a_2 = 3,\ a_3 = 7,\ a_4 = 43,\ a_5 = 139, \ldots$$

jo $a_1a_2a_3a_4 + 1 = 1807 = 139 \cdot 13$.

Pieņemsim no pretējā, ka eksistē virknes loceklis a_n, kurš vienāds ar 5.

Apzīmējam $A_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$. Tas nedalās ar 2 vai 3 (jo dod atlikumu 1). A_n nevar dalīties ar pirmskaitļiem, kas lielāki par 5, jo katrā solī par a_{n+1} izvēlamies lielāko A_n dalītāju.

Tātad, lai virknē (a_n) būtu skaitlis 5, jāizpildās

$$A_n = a_1a_2 \cdots a_n + 1 = 5^m.$$

Apgalvojums: Skaitlis 5^n katram n dod atlikumu 1, dalot ar 4.

Pierādījums: Reizinot divus vai vairāk skaitļus, kuri dod atlikumu 1, dalot ar 5, rodas rezultāts, kurš arī dod atlikumu 1, dalot ar 5. ■

Pēc mūsu pieņēmuma, eksistē $A_n = 5^m$. Tas dod atlikumu 1, dalot ar 4 jeb

$$A_n - 1 = a_1a_2 \cdots a_n$$

dalās ar 4.

Tas nav iespējams, jo $a_1 = 2$, bet visi citi a_i ir pirmskaitļi (tātad nepāru skaitļi). ■

Apgalvojums: Virknē a_n nav locekļa, kas vienāds ar 11.

Ieteikums: Līdzīgi kā iepriekš - var pamatot, ka rodas pretruna no pieņēmuma, ka $A_n = 5^k \cdot 11^\ell$.

Vispirms parāda, ka $\ell = 2\ell_1 + 1$ ir nepāru skaitlis. Tad parāda, ka var izteikt arī $k = 2k_1 + 1$ un arī k ir nepāru. Visbeidzot var parādīt, ka neviens skaitlis formā

$$55 \cdot 5^{2k_1} \cdot 11^{2\ell_1} = 55 \cdot 25^{k_1} \cdot 121^{\ell_1}$$

nevar dot atlikumu 1, dalot ar 7.

No otras puses, $A_n = a_1a_2a_3 \cdots a_n + 1$ noteikti dod atlikumu 1, dalot ar 7, jo $a_3 = 7$. Iegūta pretruna.

1.9 Sacensību uzdevumi

1.Uzdevums Dota kopa $S = \{105, 106, \ldots, 210\}$. Noteikt mazāko naturālo n vērtību, ka, izvēloties jebkuru n skaitļu apakškopu T no kopas S, tajā būs vismaz divi skaitļi, kuri nav savstarpēji pirmskaitļi.

Ieteikumi:

- Kurā kopā meklējam skaitļus, kuri nav savstarpēji pirmskaitļi?
- Kas notiek, ja izraudzītā kopa satur ļoti nedaudzus skaitļus (divus, trīs, četrus)? Ja tā satur gandrīz visus kopas S elementus?
- Ja n ir mazākā vērtība, kas apmierina uzdevuma nosacījumu, ko var apgalvot par vēl mazāku skaitli: $n - 1$? Kādu īpašību tas apmierina?

Monotonas funkcijas starp divām vērtībām. Līdz kādai vietai eksistēs arvien lielākas kopas, kurās savstarpēju pirmskaitļu nav. Sākot ar noteiktu mazāko n (kurš uzdevumā jāatrod) - savstarpēji pirmskaitļi būs neatkarīgi no T izvēles, ja vien $|T| = n$.

2.Uzdevums Visiem veseliem pozitīviem skaitļiem $m > n$ pierādīt, ka

$$\text{MKD}(m, n) + \text{MKD}(m + 1, n + 1) > \frac{2mn}{\sqrt{m - n}}.$$

Ieteikumi:

- Vai prasība $m > n$ ir būtiska? Vai bez tās šāda veida nevienādība pārstāj būt spēkā?
- Kas notiek robežgadījumos: Ja viens no skaitļiem ir 1? Ja n, m un arī $m + 1, n + 1$ ir savstarpēji pirmskaitļi? Ja $m = 2n$?
- Kuras nevienādības mums atgādina nevienādība ar kvadrātsakni?

Sākam zīmēt $\text{MKD}(m, n)$ tabuliņā (m ass pa labi, n ass uz leju). Mums interesē divu MKD summa pa diagonāli. Var tai vietā skatīties

$$\text{MKD}(m, n) + \text{MKD}(m, n + 1), \text{ ja } m >> n.$$

3.Uzdevums Vai eksistē bezgalīga stingri augoša naturālu skaitļu virkne $a_1 < a_2 < a_3 < \ldots$, ka jebkuram fiksētam naturālam skaitlim a virknē $a_1 + a < a_2 + a < a_3 + a, \ldots$ ir tikai galīgs skaits pirmskaitļu?

Ieteikumi: Attēlot neregulāru virkni, kuru nobīda pa a (kur a pieņem dažādas vērtības). Izskaidrot vārdkopu "ne vairāk kā galīgs skaits" - drīkst būt arī 0 pirmskaitļu.

- Vai eksistē bezgalīgi gari gabali bez pirmskaitļiem?
- Vai faktoriālu var lietot tīrā veidā?

4.Uzdevums Pierādīt, ka virkne $1, 11, 111, \ldots$ satur bezgalīgu apakšvirkni, kuras katri divi locekļi ir savstarpēji pirmskaitļi.

Atbilde:

Skaitļi, ko pieraksta ar daudziem vieniniekiem: Virkne $1, 11, 111, \ldots$ jebkuram skaitlim a (kurš nedalās ar 3) ļauj atrast īsāko periodu, ja $1/a$ pieraksta kā bezgalīgu decimāldaļu.

Piemēram, 111111 dalās ar 7. Tātad $1/7$ būs 6-ciparu periods.

$$1/7 = 0.(142857) = 0.142857142857142857\ldots.$$

$111\ldots111$ (tieši 40 vienīnieki) dalās ar 41. (Tas izriet no Mazās Fermā teorēmas, ko skatīsimies nākamreiz.) Bet jau 11111 dalās ar 41. Tātad $1/41$ decimālpierakstā ir daudz īsāks - 5-ciparu periodds.

$$1/41 = 0.(02439) = 0.024390243902439\ldots.$$

1.10 Norādes

1. T.Andreescu, D.Andrica, Z.Feng. 104 Number Theory Problems. Birkhäuser.

Lai attīstītu intuīciju par dalāmību, var pievienot attēlus vai animācijas par sekojošo:

1. Ūdens laistīšanas uzdevums un/vai "atstarošanās uzdevums" (kā ar 8L un 13L krūzēm nomērīt tieši 1L).
2. Skapīšu durvju vai slēdžu pārslēgšanas animācija (sk. NT.JUN01.1).
3. Eratostena režģa animācija.
4. Eiklīda algoritma animācija jebkādiem skaitļiem.
5. Tipiska un vissliktākā Eiklīda algoritma ātrdarbība, rekursīvo izsaukumu skaits šajā algoritmā.
6. Dalītāju režģis 3 vai 4 dimensijās - kā lielam skaitlim, piemēram, formā $p^a q^b r^c$ pamazām (augošā secībā) atklājas visu tā dalītāju kopums.

NMS SKAITĻU TEORIJA #2: MODULĀRĀ ARITMĒTIKA

Skaitļu teorijā daudzi rezultāti ir iegūstami galīgās atlikumu kopās. Tie izmanto kombinatoriskas metodes, jo bezgalīgi daudzo skaitļu vietā šķiro gadījumus. Piemēram, aplūkojot atlikumus, dalot ar 2, iegūstam divus gadījumus – pāra skaitlis un nepāra skaitlis, kur rezultāta paritātei vairs nevajag zināt pašu skaitli, bet tikai atlikumu.

Šādas idejas iespējams vispārināt arī atlikumiem, dalot ar lielākiem skaitļiem. Skaitļu teorijas algoritmus, kas uz skaitļiem raugās "ar atlikumu brillēm" sauc par *modulāro aritmētiku*. Šajā nodaļā aplūkosim sekojošas tēmas:

- Kongruenču klases, modulārā aritmētika.
- Dalāmības pazīmes ar $3, 9, 2^k, 5^k$ kongruenču klašu atrašanai.
- Mazā Fermā teorēma. Periodiskas decimāldaļas.
- Eilera funkcija un Eilera teorēma.
- Cikliski procesi . Periodiskas atlikumu virknes.
- Periodi un priekšperiodi virknēs.

2.1 Ievaduzdevums

Uzdevums (Valsts4Posms-2012.P1): Ar $S(x)$ apzīmēsim skaitļa x ciparu summu. Aprēķināt $S(S(S(2012^{2012})))$.

Risinājuma plāns: Skaitlis 2012^{2012} ir ļoti liels; aprēķināt visus šos ciparus ir praktiski neiespējami. Toties skaitļa ciparu summa apmierina svarīgu invariantu (atlikums, dalot ar 9 saglabājas. Risinājuma pirmajā daļā meklēsim vienīgi skaitļu $S(S(S(2012^{2012})))$, $S(S(2012^{2012}))$, $S(2012^{2012})$ un 2012^{2012} atlikumu, dalot ar 9 (visiem tiem jābūt vienādiem). Risinājuma otrajā daļā noskaidrosim, kurš no skaitļiem ar atrasto atlikumu ir konkrēti $S(S(S(2012^{2012})))$ (novērtējot to ar nevienādībām).

Apgalvojums 1: Ja n ir naturāls skaitlis, tad tā ciparu summa $S(n)$ un pats skaitlis n dod vienādus atlikumus, dalot ar 9. (Šis apgalvojums pazīstams kā vispārināta dalāmības pazīme ar 9.)

Pierādījums: Skaitlis $n = \overline{c_1 c_2 \dots c_{k-1} c_k}$, kur c_i ir decimālcipari, ir pierakstāms kā polinoms, kur mainīgā vietā ir decimālsistēmas bāze $x = 10$:

$$n = c_1 \cdot 10^{k-1} + c_2 \cdot 10^{k-2} + \ldots + c_{k-1} \cdot 10^1 + c_k \cdot 10^0.$$

Ja aprēķinām ciparu summu $S(n) = c_1 + c_2 + \ldots + c_{k-1} + c_k$, tad tā atšķiras no n ar to, ka saskaitāmo $c_i \cdot 10^{k-i}$ vietā ir saskaitāmie c_i. Piemēram, ja ceturtais cipars no skaitļa beigām jeb *tūkstošu cipars* ir $c_{k-3} = 7$, tad vērtības $7 \cdot 1000$ vietā pieskaitām vērtību 7.

Starpība abām vērtībām ir $c_i \cdot 10^{k-i} - c_i = c_i \cdot \overline{99\dots99}$, kur cipars c_i ir pareizināts ar skaitli kas sastāv no daudziem deviņniekiem. Šis skaitlis, acīmredzot dalās ar 9. Tāpēc atlikums, dalot ar 9 nemainās, ja skaitli n aizstāj ar $S(n)$ jeb katru ciparu c_i piesummē vienkārši, nevis reizina ar 10 pakāpi $c_i \cdot 10^{k-i}$. □

Apgalvojums 2: Pamatosim, ka 2012^{2012} dod atlikumu 7, dalot ar 9.

Pierādījums: Aplūkojot pakāpju a^b atlikumus, dalot ar 9, ievērojam, ka tie atkarīgi vienīgi no a atlikuma, dalot ar 9, jo reizinot (un kāpinot) skaitļus ar vienādiem atlikumiem, arī rezultāti dos vienādus atlikumus. Tātad a^b atlikumi dalīšanā ar 9 atkārtojas ar ciklu 9, ja pakāpes bāze a aug. Izsakām $(2012)^{2012} = (223 \cdot 9 + 5)^{2012}$. Tātad jāmeklē atlikums, dalot 5^{2012} ar 9.

Otrs novērojums – pakāpju a^b atlikumi, dalot ar 9, cikliski atkārtojas ik pēc 6, ja kāpinātājs b aug.

n	5^n	Atlikums, dalot ar 9
5^0	1	1
5^1	5	5
5^2	25	7
5^3	125	8
5^4	625	4
5^5	3125	2
5^6	15625	1

Vēl lielākām pakāpēm atlikumi, dalot ar 9 labajā kolonnā sāk atkārtoties: 5^7 dod tādu pašu atlikumu kā 5^1, 5^8 dod tādu pašu atlikumu kā 5^2, utt. Arī šīs tabulas aizpildīšanai var godīgi nekāpināt. Ja, teiksim, $5^2 = 25$ dod atlikumu 7, dalot ar 9, tad nākamā atlikuma iegūšanai pietiek ar 5 pareizināt nevis visu 25, bet gan tikai šo atlikumu 7 – rezultāts jeb atlikums skaitlim 35 būs tas pats, kas atlikums skaitlim 125.

Tā kā 5^6 dod atlikumu 1, dalot ar 9, tad arī $(5^6)^{335} = 5^{2010}$ dod atlikumu 1.

Visbeidzot, $5^{2012} = 5^{2010} \cdot 5^2 = 1 \cdot 25$, kas dod atlikumu 7, dalot ar 9. □

Secinājums: Arī skaitlis $S(S(S(2012^{2012})))$ dod atlikumu 7, dalot ar 9. □. (Apvienojam Apgalvojumu 1 un Apgalvojumu 2.)

Apgalvojums 3: $S(S(S(2012^{2012}))) = 7$.

Pierādījums: Mums jāpārbauda, vai $S(S(S(2012^{2012})))$ nevar būt vienāds ar kādu citu skaitli, kas arī dod atlikumu 7, dalot ar 9. Mazākais šāds skaitlis ir $7 + 9 = 16$. Pamatosim nevienādības:

$$\begin{array}{ll} (1) & S(S(S(2012^{2012}))) < 16, \\ (2) & S(S(2012^{2012})) < 79, \\ (3) & S(2012^{2012}) < 799999999. \end{array}$$

Skaitlis 79 ir mazākais, kurš dod atlikumu 7 dalot ar 9, bet kura ciparu summa ir 16. Skaitlis 799999999 ir mazākais, kurš dod atlikumu 7 dalot ar 9, bet kura ciparu summa ir 79. Tāpēc $(3) \to (2) \to (1)$.

Pierādīsim pašu pēdējo no minētajām nevienādībām, novērtējot pašu skaitli 2012^{2012}.

$$2012^{2012} < 2100^{2100} = ((2.1)^3)^{700} \cdot (1000)^{2100} = (9.261)^{700} \cdot (1000)^{2100} < 10^{700} \cdot 10^{6300} = 10^{7000}.$$

Iegūstam, ka skaitļa 2012^{2012} decimālpierakstā ir ne vairāk kā 7000 cipari. Pat ja tie visi būtu deviņnieki, tad to summa nepārsniedz 63000, kas ir mazāk nekā 799999999. Tātad nevienādība (3) ir pierādīta (un tātad arī nevienādības (2) un (1)). □

Var pārbaudīt iegūto rezultātu (skaitli 7) ar aprēķinu valodā Python:

```
def S(num):
    return sum(int(digit) for digit in str(num))

S(S(S(2012**2012)))
```

2.2 Kongruenču klases

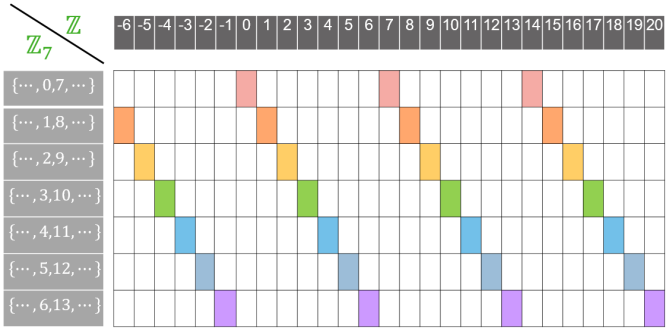
Viena mēneša ietvaros var ievērot, ka datumi $1, 8, 15, 22, 29$ nonāk tanī pašā nedēļas dienā – tādā ziņā tie ir ekvivalenti. Tāpat arī datumi $2, 9, 16, 23, 30$ visi nonāk (citā) nedēļas dienā utml. Vispārīgāk – visus veselos skaitļus (arī tos, kuri nevar būt kalendāra datumi) var sadalīt 7 ekvivalences klasēs.

Apgalvojums: Dots naturāls skaitlis m. Tad katru veselu skaitli n var vienā vienīgā veidā izteikt $n = qm + r$, kur $q \in \mathbb{Z}$, bet $r \in \{0, \dots, m-1\}$. Šajā izteiksmē q ir (veselo skaitļu dalīšanas) dalījums, bet $r \in \{0, 1, \dots, m-1\}$ ir *atlikums*.

Definīcija: Ja divi veseli skaitļi $n_1, n_2 \in \mathbb{Z}$ dod vienādus atlikumus, dalot ar m, tad sauksim tos par *kongruentiem* pēc m moduļa. Pieraksts: $n_1 \equiv n_2 \pmod{m}$.

Piemērs: Kongruence pēc moduļa 7 sadala visus veselos skaitļus $n = 7$ klasēs. Katrā klasē ietilpst skaitļi, kas dod vienādus atlikumus pēc moduļa 7. Katru šādu klasi var aprakstīt šādi:

$$\{qk + r \mid q \in \mathbb{Z},\, r \in \{0, 1, \dots, 6\}\}.$$



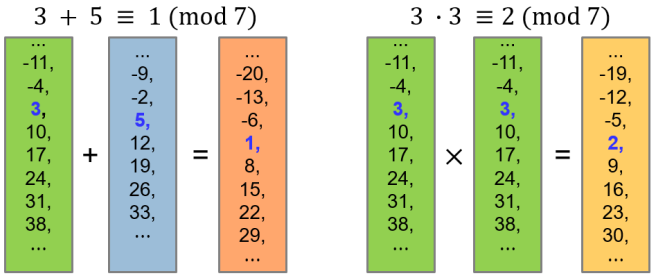
Definīcija: Dots vesels skaitlis $m > 1$. Ar $\mathbb{Z}_m$ apzīmēsim skaitļu kopu ar m elementiem $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$, kurā var veikt saskaitīšanas, atņemšanas, reizināšanas un kāpināšanas darbības, kuru rezultāti ir atlikumi, dalot ar m.

Piemērs: $a + b$ šajā kopā dod rezultātu c, ja $c = (a + b) \bmod m$, kas ir atlikums, dalot $(a + b)$ ar m.

Apgalvojums: Veicot aritmētiskas darbības kopā $\mathbb{Z}_m$, skaitļu $a, b \in \mathbb{Z}_m$ vietā var izvēlēties jebkurus veselus skaitļus a' un b', kuri dod atlikumus attiecīgi a un b, dalot ar m.

Šis apgalvojums ir spēkā, jo saskaitīšanas, atņemšanas un reizināšanas darbību atlikumu, dalot ar m, nosaka vienīgi operandu atlikumi, dalot ar m. Šajā zīmējumā parādīts, kā var saskaitīt un sareizināt kopā $\mathbb{Z}_7$. Saskaitāmo un reizinātāju 3 un 5 vietā var izvēlēties jebkuru pārstāvi no attiecīgās kongruenču klases.

Citiem vārdiem, modulārā aritmētika kongruences klašu kopā $\mathbb{Z}_7$ izkrāso visus skaitļus 7 krāsās. Un balstās uz faktu, ka saskaitot divus skaitļus ar noteiktu krāsu, rezultāta krāsa arī būs viennozīmīgi noteikta.



	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Fig. 1: Saskaitīšanas un reizināšanas tabulas 7 kongruenču klasēm no $\mathbb{Z}_7$.

2.2.1 Paritāte

Apakšgadījums kongruencēm pēc moduļa ir *paritāte*, kas visus veselos skaitļus iedala pāra skaitļos ($\equiv 0 \pmod 2$) un nepāra skaitļos ($\equiv 1 \pmod 2$).

```
p + p = p          p * p = p
p + n = n          p * n = p
n + p = n          n * p = p
n + n = p          n * n = n
```

Šajos apzīmējumos $\mathtt{p} = [0]_2$ and $\mathtt{n} = [1]_2$ ir abas ekvivalences klases pēc 2 moduļa.

2.2.2 Lietojums mūzikas teorijā

Modulāro aritmētiku var viegli iztēloties kā aritmētiku uz pulksteņa ciparnīcas. Piemēram, $14 \equiv 2 \pmod{12}$ (pulksten `2:00` un `14:00` uz ciparnīcas izskatās vienādi). Savukārt, pieskaitot 9 pie 22 (pēc 12 moduļa) iegūstam 7, jo $22 + 9 \equiv 7 \pmod{12}$. Ja kopš laika momenta `22:00` paiet 9 stundas, tad parasti saka, ka pulkstenis ir `7:00`, nevis `31:00`. Kaut arī `31:00` pauž to pašu informāciju.

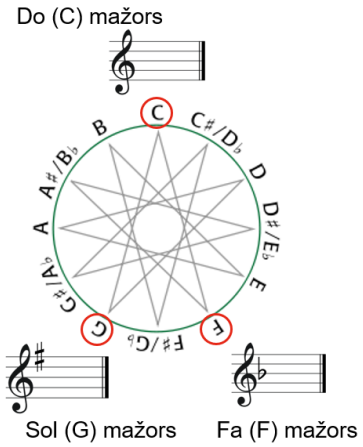


Fig. 2: "Kvintu aplis" zvaigznītes formā savieno "radniecīgus" nošu augstumus.

Līdzīgi "pulksteņa ciparnīcas aritmētikai" ir arī riņķošana pa nošu augstumiem, pārejot no vienas toņkārtas uz citu. Zīmējumā dots mūzikas teorijā pazīstamais *kvintu aplis*. Apļa augšā atrodas skaņa DO (jeb C), kuras mažora gammā nav nevienas alterācijas zīmes (diēza vai bemola). Pārlecot par kvintu (jeb 7 pustoņiem) uz priekšu, nonākam pie SOL (jeb G), kuras mažora gammā ir viens diēzs. Pēc sešiem pārlēcieniem par kvintu būsim nonākuši līdz FA diēzam

(vienu pustoni uz augšu, salīdzinot ar C). Virzoties pretējā virzienā, gammai nāk klāt pa vienam bemolam. Pašu FA diēza mažoru var uzrakstīt divos veidos – vai nu kā FA diēza mažoru (kur sešas skaņas gammā ir paaugstinātas), vai arī kā SOL bemol minoru (kur sešas skaņas gammā ir pazemінātas).

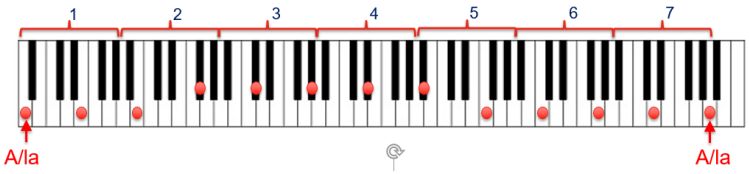


Fig. 3: Kvintu aplis uz klavierēm, aptver 7 oktāvas.

Kvintu aplis faktiski ir aritmētiska progresija ar diferenci 7 pustoņi pēc moduļa 12. Šajā progresijā apzīmējam skaņas augstumu A(la) ar 9, jo tas ir 9 pustoņus augstāk par C(do). Pēc divpadsmit soļiem virkne atgriežas sākumpunktā.

$$9,\ 4,\ 11,\ 6,\ 1,\ 8,\ 3,\ 10,\ 5,\ 0,\ 7,\ 2,\ 9 \pmod{12}$$

Mūzikā skaitlim 12 ir īpaša loma, jo oktāvu dala divpadsmit pustoņos. Savukārt skaitļu teorijas lietojumos modulārā aritmētika pēc 12 moduļa ir iespējama, bet bieži vien neērta, jo skaitļi, kuriem ir kopīgi dalītāji ar 12 (pāru skaitļi, 3 un 9) pēc šī moduļa uzvedas atšķirīgi no citiem skaitļiem. Minēto iemeslu dēļ matemātikā populārākā modulārā aritmētika ir $\pmod{p}$, kur p ir jebkurš pirmskaitlis. Dažos gadījumos arī $\pmod{p^k}$ – kongruences pēc pirmskaitļu pakāpju moduļiem.

2.3 Kongruenču īpašības

Apgalvojums: Saskaitīšanas, atņemšanas un reizināšanas izteiksmēs veseliem skaitļiem rezultāta pēdējo ciparu nosaka izteiksmē ietilpstošo skaitļu pēdējie cipari.

Piemērs: Ar kādu ciparu beidzas 2022^{2022}?

Risinājums: Saskaņā ar apgalvojumu, pietiek atrast izteiksmes 2^{2022} pēdējo ciparu. Izrakstot skaitļa 2 pakāpes $(1, 2, 4, 8, 16, 32, 64, \ldots)$ secinām, ka pakāpe vienmēr beidzas ar ciparu 4 tad, ja kāpinātājs dod atlikumu 2, dalot ar 4. (Piemēram, $2^2 = 4$, $2^6 = 64$, utt.) Tāpēc arī 2^{2022} beigsies ar ciparu 4.

2.3.1 Modulārā kāpināšana

Ja pakāpes bāze a un kāpinātājs k ir nelieli skaitļi tad pakāpes a^k atlikumu dalot ar nelielu skaitli m, aprēķinus bieži var veikt uz papīra – pat ja skaitlis a^k ir tik liels, lai to tieši izrēķināt nevarētu.

Piemērs 1: Atrast atlikumu, dalot 2^{1000} ar 17.

Risinājums: Ievērojam, ka $2^4 = 16 \equiv -1 \pmod{17}$. Tad $2^{1000} = (2^4)^{250} \equiv (-1)^{250} \equiv 1 \pmod{17}$.

Piemērs 2: Atrast atlikumu, dalot $10^6 = 1000000$ ar 7.

Risinājums: Pārveidojam šo pakāpi:

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \equiv (3 \cdot 3) \cdot (3 \cdot 3) \cdot (3 \cdot 3) \equiv 2 \cdot 2 \cdot 2 \equiv 1 \pmod{7}.$$

Piemērs 3: Atrast atlikumu, dalot 8^{1834} ar 7.

Piemērs 4: Atrast atlikumu, dalot 6^{2022} ar 7.

Piemērs 5: Zināms, ka skaitlis 1001 dalās ar 13. Atrast atlikumu, dalot 10^{100} ar 13.

Visos šajos piemēros pakāpes var pārveidot, izmantojot kāpināšanas identitātes, izrēķināt dažas apakšizteiksmes, aizstāt lielākus skaitļus ar kongruentiem, bet mazākiem skaitļiem.

Augstāk aprakstītās metodes noder, risinot nelielus piemērus uz papīra. Tomēr izrādās, ka arī visai lieliem skaitļiem kāpināšanu pēc moduļa var veikt efektīvi uz datora – un nepieciešamais darbību skaits ir nesalīdzināmi mazāks par to, kas būtu aprēķinot pašu pakāpi (nevis tās atlikumu) un arī nesalīdzināmi mazāks par to, kāds būtu, ja ar "godīgu ciklu" veiktu kāpināšanu – pat ar modulāro aritmētiku.

Piemērs 6: Aprēķināt $511889566403493410 03^{480374535209418723 61}$ pēc moduļa 15522299127691416427.

```
>>> a = 51188956640349341003
>>> k = 48037453520941872361
>>> m = 15522299127691416427
>>> pow(a,k,m)
1288083363532019064
>>> bin(k)
'0b1010011010101001110101000101110110110001100001001111110100111010 01'
```

Rezultātu 1288083363532019064 Python programma izrēķina acumirklī – tur nenotiek reizināšana $k = 48037453520941872361$ reizes (pat pēc m moduļa). Tai vietā kāpinātāju k pieraksta bināri - izsaka kā divnieka pakāpju summu; pēc tam skaitli a atkārtoti kāpina kvadrātā, iegūstot $a^0, a^1, a^2, a^4, a^8, a^{16}, \ldots$. Un pēc tam sareizina tās pakāpes, kuras nepieciešamas, lai saliktu skaitli k.

Ja, piemēram, k binārajā pierakstā ir 66 cipari (un 35 no tiem ir vienīnieki), tad šādai kāpināšanai $a^k \pmod m$ vajag veikt tikai $66 - 1 + 35 = 100$ reizināšanas pēc moduļa m. Ievērosim, ka 100 reizināšanas darbības (pēc m moduļa) ir liels uzlabojums, salīdzinot ar $\approx 48 \cdot 10^{18}$ jeb 48 kvintiljoniem reizināšanas darbību, kas prasītu ievērojamu laiku arī uz ļoti ātra datora.

2.3.2 Atņemšana kongruenču klasēs

Katram elementam no $\mathbb{Z}_m$ eksistē pretējais (saskaitot elementu ar tam pretējo, iegūstam 0).

$$\begin{aligned} -1 &\equiv 6 \pmod 7 \\ -2 &\equiv 5 \pmod 7 \\ -3 &\equiv 4 \pmod 7 \\ -4 &\equiv 3 \pmod 7 \\ -5 &\equiv 2 \pmod 7 \\ -6 &\equiv 1 \pmod 7 \end{aligned}$$

Pretējā elementa eksistēšana nozīmē, ka kongruencei var abām pusēm pieskaitīt un atņemt tādu pašu kongruences klasi:

$$\text{Ja } x + a \equiv y + a \pmod m, \text{ tad } x \equiv y \pmod m.$$

No abām kongruences pusēm var atņemt to pašu skaitli, noīsinot abus saskaitāmos. Jebkuram naturālam modulim $m \in \mathbb{N}$ var šādi īsināt.

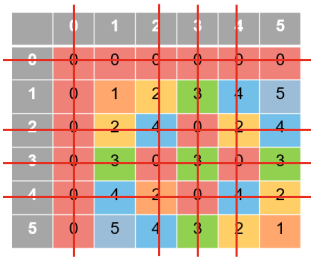
	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Saskaitīšanas tabula rāda, ka ikvienā rindiņā parādās visas iespējamās vērtības (tāpēc jebkura skaitļa pieskaitīšana pēc moduļa m ir injektīva darbība – tā saglabā informāciju un tātad var atņemt to pašu konstanti no abām pusēm).

2.3.3 Dalīšana kongruenču klasēs

Vai no $ka \equiv kb \pmod{m}$ seko, ka $a \equiv b \pmod{m}$? Atbilde atkarīga no tā, vai reizināšana ar k ir injektīva (t.i. "nesalipina" divus skaitļus) vai nē. Tikai injektīvām funkcijām eksistē inversās. Reizināšanas tabulai pēc pirmskaitļa moduļa reizināšana ir injektīva (reizināšanai eksistē inversā darbība). Vienīgais izņēmums ir reizināšana ar kongruenču klasi 0.

Savukārt reizināšanas tabula pēc salikta skaitļa satur tādas kongruenču klases (tostarp atšķirīgas no 0)), kuras reizinot var iegūt atkārtotas vērtības. Reizināšanas tabula (mod 6) ar izsvītrotiem n, kam $\gcd(n, 6) > 1$.



Piemēram kongruenču klasēm (pēc moduļa 6) ir dažas klases $(2, 3, 4)$, kuras atšķiras no 0, bet reizināšanas tabula satur atkārtotas rindas.

$$2 \cdot 3 \equiv 6 \equiv 0 \pmod{6}$$

Arī pēdējie cipari (atlikumi pēc 10) neveido injektīvu reizināšanas darbību. Piemēram, nevar viennozīmīgi atrisināt šādu kongruenču vienādojumu:

$$4x \equiv 2 \pmod{10}.$$

Eksistē divas saknes $x \equiv 3 \pmod{10}$ un $x \equiv 8 \pmod{10}$.

2.4 Mazā Fermā teorēma

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, kur a nedalās ar p un arī $(i-j) < p$. Tātad p nebūtu pirmskaitlis – pretruna.

Tādēļ kopa $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$ satur visas tās pašas kongruenču klases, ko $\{1, 2, \ldots, p-1\}$ (tikai, iespējams, citā secībā). Sareizinot visas šīs kongruenču klases, iegūsim

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

Saīsinām abas kongruences puses ar faktoriālu (kurš nav kongruents ar 0, jo nevar dalīties ar p) un iegūstam teorēmas apgalvojumu:

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

Sekas: Jebkuram pirmskaitlim $p > 5$, skaitlis, kura decimālpieraksts sastāv no $p-1$ deviņniekiem dalās ar p.

Piemērs: Skaitlis no 40 deviņniekiem 9999999999999999999999999999999999999999 dalās ar 41. (Faktiski, jau daudz īsāks skaitlis 99999 dalās ar 41, bet arī, uzrakstot šo piecu deviņnieku grupu astoņas reizes, iegūstam četrdesmit deviņniekus un arī tas dalās ar 41.)

Piemērs: Pirmskaitlim $p = 7$ skaitlis 999999 (skaitlis no $p - 1 = 6$ deviņniekiem) dalās ar 7. (Un ar mazāku deviņnieku skaitu nepietiek.)

Teorēma: Ja p ir nepāra pirmskaitlis un a ir jebkurš skaitlis, kas nedalās ar p, tad

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Pierādījums. Zināms (M.Fermā teorēma), ka $a^p - 1$ dalās ar p, jeb

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

Ja reizinājums dalās ar p, tad viens no reizinātājiem dalās ar p. Tātad izteiksme $a^{\frac{p-1}{2}}$ ir kongruenta vai nu ar $+1$ vai ar -1 pēc p moduļa.

Piemērs: Aplūkojam $p = 11$ un visas kongruenču klases pēc šī moduļa:

a	1	2	3	4	5	6	7	8	9	10
a^5	1	32	243	1024	3125	7776	16807	32768	59049	100000
a^5 mod 11	1	10	1	1	1	10	10	10	1	10

2.4.1 M.Fermā teorēma un periodiskas decimāldaļas

Mazā Fermā teorēma nav tikai gari formulēts matemātikas rezultāts, kas lietojams īpašās situācijās. Tās izpausmes ir redzamas, piemēram, ikreiz, kad ar kalkulatoru dala divus veselus skaitļus.

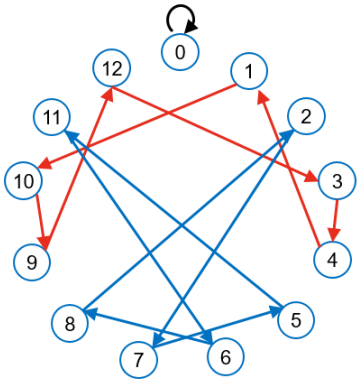
Vienkāršības dēļ aplūkosim daļas $1/p$, kur skaitli 1 dala ar pirmskaitli p, bet atrastie daļu periodi der arī citām racionālām daļām ar to pašu saucēju.

Tabulā attēlots novērojums, ka $1/p$ bezgalīgās decimāldaļas perioda garums sakrīt ar mazāko k, kuram $10^k - 1$ (skaitlis, ko veido k deviņnieki) dalās ar p. Un pēc Mazās Fermā teorēmas – vai nu $k = p - 1$, vai arī k ir skaitļa $p - 1$ dalītājs.

p	Min.dalāmais formā $10^k - 1$	$1/p$ kā decimāldaļa
3	$10^1 - 1 = 9$	$1/3 = 0.(3) = 0.33\ldots$
7	$10^6 - 1 = 999999$	$1/7 = 0.(142857) = 0.142857142857\ldots$
11	$10^2 - 1 = 99$	$1/11 = 0.(09) = 0.0909\ldots$
13	$10^6 - 1 = 999999$	$1/13 = 0.(076923)$
17	$10^{16} - 1$	$1/17 = 0.(0588235294117647)$
19	$10^{18} - 1$	$1/19 = 0.(052631578947368421)$
23	$10^{22} - 1$	$1/23 = 0.(0434782608695652173913)$
29	$10^{28} - 1$	$1/29 = 0.(0344827586206896551724137931)$
31	$10^{15} - 1$	$1/31 = 0.(032258064516129)$
37	$10^3 - 1 = 999$	$1/37 = 0.(027) = 0.027027\ldots$
41	$10^5 - 1 = 99999$	$1/41 = 0.(02439)$
43	$10^{21} - 1$	$1/43 = 0.(023255813953488372093)$

Varam ar konkrētu piemēru aplūkot detalizēti, kā veidojas periodiski decimāldaļskaitļi.

Piemērs: Aprēķinām $1/13$, dalot stabiņā.




```
1:13=0.076923...
10
00
100
 91
  90
  78
  120
  117
    30
    26
     40
     39
      10
```

Aplūkojot šo dalīšanas algoritmu kā veselu skaitļu aritmētikas problēmu, rēķinām virkni ar atlikumiem:

$$x_n = \begin{cases} 1, & \text{if } n = 0, \\ (10 \cdot x_{n-1}) \bmod 13, & \text{if } n > 0. \end{cases}$$

Pirmie šīs virknes locekļi:

$$1, 10, 9, 12, 3, 4, 1, \ldots$$

Tā kā ikviens no šīs virknes locekļiem viennozīmīgi atkarīgs no iepriekšējā (un iespējamo atlikumu ir tikai 12, jo dalīšanas rezultātā nevar rasties atlikums 0, bet var rasties citi atlikumi $\{1, \ldots, 12\}$).

Redzot, ka šīs virknes periods ir tieši seši locekļi, iegūstam, ka $x_{n+6} \equiv \left(10^6 \cdot x_n\right) \pmod{13}$. No šejienes iegūstam, ka $10^6 \equiv 1 \pmod{13}$.

Lai no periodiskas decimāldaļas atgrieztos pie racionālas daļas, aplūkojam sekojošu piemēru (kas ļaus konstruēt jebkuru periodisku daļskaitli ar periodu 6):

$$1 : 999999 = 0.000001000001000001000001\ldots = 0.(000001)$$

Par šo vienādību pārliecinās vai nu dalot stabiņā, vai arī summējot bezgalīgi dilstošu ģeometrisku progresiju, izmantojot formulu $b_1/(1-q)$, kur b_1 ir progresijas pirmais loceklis, bet q ir tās kvocients.

$$0.(000001) = \frac{1}{10^6} + \frac{1}{10^12} + \frac{1}{10^18} + \frac{1}{10^24} + \ldots$$
$$S = \frac{b_1}{1-q} = \frac{\frac{1}{10^6}}{1-\frac{1}{10^6}} = \frac{1}{10^6-1} = \frac{1}{999999}$$

Aplūkosim kādu citu periodisku daļskaitli ar periodu 6:

$$0.076923076923076923076923\ldots = 76923 \cdot 0.000001000001000001\ldots = \frac{76923}{999999}$$

Pēc noīsināšanās iegūstam, ka

$$\frac{76923}{999999} = \frac{1}{13}.$$

Apgalvojums (Pazīme, ka n/p periodā ir k cipari): Dots pirmskaitlis p un n nedalās ar p. Skaitlis n/p ir periodiska daļa ar periodu k tad un tikai tad, ja k ir mazākais naturālais skaitlis, kam $10^k - 1$ dalās ar p.

2.4.2 Jautājumi par Mazo Fermā teorēmu

1.jautājums: Pārveidot sekojošu periodisku decimāldaļskaitli par racionālu daļu: $0.(20221115)$.

2.jautājums: Uzrakstīt tādu $1/p$ (p ir pirmskaitlis), kura decimālpierakstā ir periods tieši no 4 cipariem.

3.jautājums: Kāds ir mazākais naturālu skaitļu kopas izmērs, lai no šīs kopas noteikti varētu izvēlēties tādus a, b kuru piekto pakāpju starpība $a^5 - b^5$ dalītos ar 11?

2.5 Pretrunas moduļa metode

Pretrunas moduļa metode parāda, ka vienādojumam nav atrisinājumu veselos skaitļos (jo vienādojuma kreisā puse ir kongruenta ar citiem atlikumiem nekā labā puse, tātad tās nevar būt vienādas). Lietojot pretrunas moduli, svarīgi ievērot šādas vadlīnijas:

- Izvēlamies tikai pirmskaitļus vai to pakāpes.
- Ja vesela izteiksme satur mainīgos arī kāpinātājos, tad var iznākt, ka pretruna parādās tikai moduļiem m, kas satur dažādus pirmreizinātājus. Tomēr šo pretrunu var iegūt arī aplūkojot tikai pirmskaitļa pakāpes.
- Sākam ar maziem moduļiem $2, 3, 4, 5, 7, 8, 9, 11, \ldots$.
- Izvēlamies moduļus, kas ir vienādojuma koeficientu dalītāji, samazinot vienādojuma locekļu skaitu.
- Vienādojumos, kuros figurē skaitļu k-tās pakāpes, aplūkojam moduļus k^2 un visus pirmskaitļus, kas izsakāmi formā $mk + 1$.

Piemēri: Pierādīt, ka sekojošiem vienādojumiem nav atrisinājumu veselos skaitļos:

(A) $y^2 - 5x^2 = 6$,

(B) $15x^2 - 7y^2 = 9$,

(C) $x^2 - 2y^2 + 8z = 9$,

(D) $x^3 + y^3 + z^3 = 1969^2$.

2.6 Eilera teorēma

Ja n nav pirmskaitlis, tad arī iespējama Mazajai Fermā teorēmai līdzīga analīze, ko drīz aplūkosim. Vispirms definējam jaunu funkciju.

Definīcija: Funkciju $\varphi(n)$ no naturāliem skaitļiem uz naturālām vērtībām saucam par *Eilera funkciju*, ja tā saskaita, cik ir tādu naturālu skaitļu j intervālā $[1; n]$, kas ir savstarpēji pirmskaitļi ar n.

Ja zināms skaitļa sadalījums pirmreizinātājos, Eilera funkcijas aprēķināšana ir vienkārša.

Apgalvojums: Ja $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ ir skaitļa n sadalījums pirmskaitļa pakāpju reizinājumā (sadalījums pirmreizinātājos), tad Eilera funkcija:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Šo apgalvojumu pamatosim nodaļā *Multiplikatīvas funkcijas*. Pagaidām pieņemsim bez pierādījuma šo formulu, kas $\varphi(n)$ atrod, izmantojot n pirmreizinātājus.

Apgalvojums: Par Eilera funkciju ir spēkā šādi apgalvojumi:

- Ja p ir pirmskaitlis, tad $\varphi(p) = p - 1$.

- Ja p^k ir pirmskaitļa pakāpe, tad $\varphi(p^k) = p^k - p^{k-1}$.

Piemērs: Ja $m = 70 = 2 \cdot 5 \cdot 7$, tad $\varphi(70) = 70 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$.

Piemērs: Ja $m = 144 = 2^4 \cdot 3^2$. Iegūstam, ka $\varphi(144) = 144 \cdot \frac{1}{2} \cdot \frac{2}{3} = 48$.

Piemērs: Ja $m = 2022 = 2^1 \cdot 3^1 \cdot 337^1$. Iegūstam, ka $\varphi(2022) = 2022 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{336}{337} = (2-1)(3-1)(337-1) = 672$.

Teorēma: Ja a un n ir savstarpēji pirmskaitļi, tad

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

Pierādījums: Līdzīgi kā Mazajai Fermā teorēmai – izraksta visas kongruenču klases:

$$S = \{b_1, \ldots, b_{\varphi(n)}\}, \text{kam } \gcd(b_i, n) = 1.$$

Pēc tam reizina tās visas ar kongruenču klasi a. Pārliecinās, ka šī reizināšana ir injektīva, tātad tas ir kopas S bijektīvs attēlojums pašai par sevi. Sareizinot visas kongruenču klases abās vienādībās, iegūsim

$$\prod_{i=1}^{\varphi(n)} b_i \equiv \prod_{i=1}^{\varphi(n)} (a \cdot b_i) \pmod{n}.$$

Pēc noīsināšanas ar visu kongruenču klašu reizinājumu, iegūstam Eilera teorēmas identitāti. □

Piemērs. $\varphi(10) = 4$, tādēļ katram no skaitļiem $1, 3, 7, 9$ ir spēkā sakarība $a^4 \equiv 1 \pmod{10}$. Teiksim, skaitļa 3 pakāpes ir $1, 3, 9, 27, 81, \ldots$. Iegūstam, ka 3^4 beidzas ar to pašu ciparu, ar ko $3^0 = 1$.

Protams, cikls var iestāties arī ātrāk. Piemēram, kāpinot skaitļus, kuri beidzas ar ciparu 1, periods (pēdējā cipara atkārtošanās) vienāds ar 1. Bet tas nemaina faktu, ka $a^4 \equiv 1 \pmod{10}$. Pēdējā cipara periods var būt 1, 2 vai 4 (jo Eilera teorēma neapgalvo, ka $\varphi(n)$ būs **mazākais** kāpinātājs k, kuram a^k ir kontruents ar 1. Toties Eilera teorēma apgalvo, ka mazākajam periodam ir jābūt $\varphi(n)$ dalītājam.

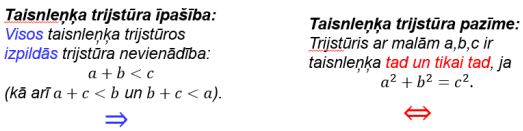
Piemērs: Zināms, ka $\varphi(100) = \varphi(25) \cdot \varphi(4) = (25-5)(4-2) = 40$. Iedomāsimies, ka a ir skaitlis, kas nedalās ne ar 2, ne ar 5, turklāt k ir mazākais naturālais skaitlis, kuram a^k beidzas ar cipariem "01" . Kāda noteikti nevar būt k vērtība?

Atbilžu varianti: **(A)** 5, **(B)** 10, **(C)** 15, **(D)** 20.

2.7 Dalāmības pazīmes

2.7.1 Kas ir pazīmes?

Matemātikā, medicīnā un citās jomās par *pazīmēm* sauc nosacījumus, kas ir nepieciešami un pietiekami kādam apgalvojumam (*necessary and sufficient conditions*). Tās atšķiramas no *īpašībām* (*necessary conditions*), kas ir nepieciešamas, bet var nebūt pietiekamas.



Pazīmes darbojas abos virzienos, tādēļ tās viegli lietot, lai "pārtulkotu" kādu apgalvojumu citā formā. Ģeometrijā sakarības starp malām vai leņķiem var norādīt uz kādas figūras speciālu īpašību. Arī skaitļu teorijā šāda tulkošana ir noderīga.

Aprakstošs/kvalitatīvs apgalvojums	Ekvivalents/kvantitatīvs apgalvojums
Skaitlis n ir pāra skaitlis	Var izteikt $n = 2k$
Skaitlis n ir nepāra skaitlis	Var izteikt $n = 2k + 1$
Skaitlis n nedalās ar 3	$n \equiv \pm 1 \pmod 3$
n pieraksts beidzas ar 37	$n \equiv 37 \pmod{100}$
n pieraksts ir $\overline{abcabc}$	$n = 1001 \cdot \overline{abc}$
a un b nav savstarpēji pirmskaitļi	LKD$(a, b) > 1$
Skaitlis n ir pilns kvadrāts	Var izteikt $n = k^2$
Skaitlis x ir racionāls	$x = \frac{p}{q}$
Skaitlis x ir galīga decimāldaļa	$x = \frac{p}{2^m \cdot 5^n}$
Skaitlis n dalās ar 9	n ciparu summa dalās ar 9

2.7.2 Dalāmības pazīmes ar 2 un 5 pakāpēm

Dalāmības pazīme (*divisibility rule*) ir kāds paņēmiens, kas ļauj noskaidrot skaitļa n dalāmību ar kādu nelielu skaitli m. Parasti dalāmības pazīme dod atbildi par dalāmību ātrāk nekā pilnvērtīga n dalīšana ar m, piemēram, stabiņā.

Aplūkosim tās dalāmības pazīmes, kuras pārveido n par kādu daudz mazāku skaitli $f(n)$, kas dod tādu pašu atlikumu, dalot ar m kā sākotnējais skaitlis n. Tādēļ dalāmības pazīmes ne tikai paātrina aprēķinus, bet ļauj labāk saprast skaitļa decimālpierakstu.

Teorēma (dalāmība ar 2 pakāpēm): Jebkuram naturālam skaitlim n ir spēkā sekojoši apgalvojumi:

- n dalās ar 2 tad un tikai tad, ja n pēdējais cipars dalās ar 2 .
- n dalās ar 2 tad un tikai tad, ja n pēdējie divi cipari (kā skaitlis) dalās ar 4 (n beidzas ar $00, 04, 08, 12, \ldots, 96$).
- n dalās ar 8 tad un tikai tad, ja n pēdējie trīs cipari (kā skaitlis) dalās ar 8 (n beidzas ar $000, 008, 016, \ldots, 992$).

Teorēma (dalāmība ar 5 pakāpēm): Jebkuram naturālam skaitlim n ir spēkā sekojoši apgalvojumi:

- Skaitlis dalās ar 5 tad un tikai tad, ja tā pēdējais cipars dalās ar 5 (beidzas ar ciparu 0 vai 5).
- Skaitlis dalās ar 25 tad un tikai tad, ja tā pēdējo divu ciparu veidotais skaitlis dalās ar 25 (beidzas ar $00, 25, 50, 75$).
- Skaitlis dalās ar 125 tad un tikai tad, ja tā pēdējo trīs ciparu veidotais skaitlis dalās ar 125 (beidzas ar $000, 125, 250, 375, 500, 625, 750, 875$).

Visas šīs dalāmības pazīmes var vispārināt arī tiem gadījumiem, ja skaitlis n nedalās ar pārbaudāmo skaitli. Piemēram, var iegūt šādu apgalvojumu:

Sekas: Jebkuram naturālam skaitlim n ir spēkā sekojošs apgalvojums: n dod tādu pašu atlikumu dalot ar 4 (vai ar 25) kādu dod tā pēdējie divi cipari. Citiem vārdiem, ja $n = \overline{d_k d_{k-1} \ldots d_1 d_0}$, kur d_i ir skaitļa n decimālpieraksta cipari, tad

$$\begin{aligned} n &\equiv \overline{d_1 d_0} \pmod 4 \\ n &\equiv \overline{d_1 d_0} \pmod{25} \end{aligned}$$

Iemesls, kādēļ drīkst atmest visus pārējos ciparus ir tas, ka pilni simti (arī tūkstoši, desmittūkstoši utt.) dalās ar 4 un ar 25 bez atlikuma. Tie neizmaina n kongruences klasi.

Minētos rezultātus var vispārināt arī dažiem citiem skaitļiem (piemēram, atrodot dalāmības pazīmi ar $10, 20, 40, 50$ utt.).

Tabulā redzamas visas iespējamās kombinācijas ar skaitļu 2 un 5 pakāpēm un to reizinājumiem. Izceltajās tabulas šūnās ierakstīti skaitļi $(16, 80, 400, 2000, 10000, 5000, 2500, 1250, 625)$, kuru dalāmības noskaidrošanai pietiek aplūkot skaitļa n pēdējos 4 ciparus. Visus desmittūkstošu (un vēl vecākus) ciparus var atmest, jo 10000 dalās ar visiem nosauktajiem skaitļiem.

1	2	4	8	16	32
5	10	20	40	80	160
25	50	100	200	400	800
125	250	500	1000	2000	4000
625	1250	2500	5000	10000	20000
3125	6250	12500	25000	50000	100000

Runājot par dalāmības pazīmēm, skaitļi $k = 2^m 5^n$ ieņem īpašu vietu. Katram no tiem eksistē mazākā desmitnieka pakāpe, kas dalās ar k. Dalāmības pazīme var atmest ciparus, kuru pozīcija (vieta decimālpierakstā no labās puses) ir lielāka par $\max(m, n)$.

2.7.3 Dalāmības pazīmes ar 3, 9

Teorēma: Ar $S(n)$ apzīmējam skaitļa n ciparu summu. Tad $S(n) \equiv n \pmod 9$.

Pierādījums: Sākotnējais skaitlis ir

$$n = \overline{d_k d_{k-1} d_{k-2} \dots d_2 d_1 d_0} == d_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

Šeit d_i apzīmē ciparus. Ja šo skaitli aizstāj ar $S(n) = d_k + d_{k-1} + \ldots + d_1 + d_0$, tad reizinātājs pie jebkura cipara d_j bija 10^j, bet kļuva 1. No viena decimālpieraksta ir samazinājums par šādu lielumu:

$$\left(10^j d_j - d_j\right) = \underbrace{\overline{9999 \dots 9999}}_{j \text{ deviņnieki}}$$

Skaitlim samazinoties par $(10^j - 1)d_j$, atlikums, dalot ar 9, nemainās.

Sekas: Katram naturālam skaitlim ir spēkā kongruence $n \equiv S(n) \pmod 3$.

Sekas: Skaitlis n dalās ar 9 (vai ar 3) tad un tikai tad, ja ciparu summa $S(n)$ dalās ar 9 (vai ar 3).

Note: Citu skaitļu, izņemot 3 un 9) ar līdzīgu dalāmības pazīmi nav. Šeit izmantojam faktu, ka veselie skaitļi $9, 99, 999, ldots$ visi dalītos ar 3 vai ar 9.

2.7.4 Dalāmības pazīmes ar 11 kā arī 7 un 13

Naturāla skaitļa decimālpieraksts ir $n = \overline{d_{2k-1} d_{2k-1} d_{2k-2} \dots d_2 d_1 d_0}$. (Ja skaitlī ir nepāra skaits ciparu, tad tam priekšā pieraksta nulli tā, lai ciparu skaits būtu tieši $2k$.) Apzīmējam atsevišķi pāru un nepāru ciparu summas šajā skaitlī.

$$S_0(n) = \sum_{j=0}^{k-1} d_{2j} = d_0 + d_2 + d_4 + \ldots + d_{2k-2}$$

$$S_1(n) = \sum_{j=0}^{k-1} d_{2j+1} = d_1 + d_3 + d_5 + \ldots + d_{2k-1}$$

Tātad $S_0(n)$ apzīmē skaitļa n vienu ciparu plus simtu ciparu plus desmittūkstošu ciparu, utt. Savukārt $S_1(n)$ apzīmē skaitļa n desmitu ciparu plus tūkstošu ciparu plus simttūkstošu ciparu, utt.

Teorēma: Katram naturālam n, $S_0(n) - S_1(n) \equiv n \pmod{11}$.

Pierādījums: Sākotnējais skaitlis ir

$$n = \overline{d_{2k-1}d_{2k-1}d_{2k-2}\dots d_2d_1d_0} = \\ = d_{2k-1}10^{2k-1}a_{2k-2}10^{2k-2} + \dots + d_2 10^2 + d_1 10^1 + d_0.$$

Visas pāra pakāpes 10^{2j} dod atlikumu 1, dalot ar 11, bet visas nepāra pakāpes 10^{2j+1} dod atlikumu -1, dalot ar 11. Tas seko no fakta, ka $10 \equiv (-1) \pmod{11}$.

Tāpēc skaitlim n spēkā šāda kongruence:

$$\begin{aligned} d_{2k-1}10^{2k-1} + a_{2k-2}10^{2k-2} + \dots + d_2 10^2 + d_1 10^1 + d_0 \equiv \\ \equiv d_{2k-1} \cdot (-1) + d_{2k-2} \cdot 1 + \dots + d_2 \cdot 1 + d_1 \cdot (-1) + d_0 \cdot 1 \equiv \\ \equiv (d_{2k-2} + d_{2k-4} + \dots + d_2 + d_0) + (d_{2k-1} + d_{2k-3} + \dots + d_3 + d_1) \equiv \\ \equiv S_0(n) - S_1(n) \pmod{11}. \end{aligned}$$

Sekas: Skaitlis dalās ar 11 tad un tikai tad, ja tā ciparu summa, kas atrodas pāra pozīcijās, mīnus ciparu summa, kas atrodas nepāra pozīcijās, dalās ar 11.

Teorēma: Dots naturāls skaitlis $n \in \mathbb{N}$; $n = \overline{d_{3k-1}d_{3k-2}d_{3k-3}\dots d_2d_1d_0}$. Grupējam tā ciparus pa trīs, skaitot no labās puses, un izveidojam summu ar mainītām zīmēm $1, -1, 1, -1, \dots$.

$$S_3(n) = \overline{d_2d_1d_0} - \overline{d_5d_4d_3} + \overline{d_8d_7d_6} - \dots + (-1)^k\overline{d_{3k-1}d_{3k-2}d_{3k-3}}.$$

Skaitlis $S_3(n)$ apmierina kongruences $S_3(n) \equiv n \pmod{m}$, kur $m = 7, 11, 13$ vai $m = 1001$.

Piemērs: $n = 62510448$. Papildinām to līdz deviņiem cipariem: $n = (062)(510)(448)$. Iegūstam $S_3(62510448) = 448 - 510 + 062 = 0$. Tā kā 0 dalās ar jebko, tad $n = 62510448$ dalās ar 7, 11, 13 un arī 1001.

Piemērs: $n = 729183$. Iegūstam $S_3(n) = 183 - 729 = -546$. Tā kā $S_3(n) = -546$ dalās ar 7 un 13, tad arī 729183 dalās ar 7 un 13 (bet ne ar 11).

2.7.5 Citas dalāmības pazīmes

Ir virkne tādu dalāmības pazīmju, kas ļauj pārbaudīt dalāmību ar kādu skaitli m, bet lieto tādus pārveidojumus, kas nesaglabā kongruenci pēc m moduļa. Sk. apkopojumu http://www.savory.de/maths1.htm.

Teorēma: Naturāls skaitlis n dalās ar 7 tad un tikai tad, ja nosvītrojot pēdējo ciparu, divkāršojot to un atņemot no "saīsinātā" skaitļa, rezultāts dalās ar 7. Citiem vārdiem, ja $n = 10a + b$, kur b ir skaitļa pēdējais cipars, tad

$$7 \mid 10a + b \;\leftrightarrow\; 7 \mid a - 2b.$$

Attēlā redzama dalāmības pazīmes ar 7 lietošana lielam skaitlim:

1940372 → 194037 – 4 →
→ 194033 → 19403 – 6 →
→ 19397 → 1939 – 14 →
→ 1925 → 192 – 10 →
→ 182 → 18 – 4 →
→ 14 → 1 – 8 →
→ −7

2.7.6 Jautājumi par dalāmības pazīmēm

1.jautājums: Atrast $S_0(n)$ un $S_1(n)$ dotajiem skaitļiem; pārbaudīt to dalāmību ar 11.

- $n = 1331$.
- $n = 14641$.
- $n = 1001$.
- $n = 979$.
- $n = 16808$.

Definīcija: Skaitļa decimālpierakstu sauc par *palindromu*, ja ciparu virkne ir identiska, to lasot no abiem galiem. Piemēram, 44 un 131 ir palindromi, bet 1431 nav, jo, lasot no otra gala, veidojas cits skaitlis 1341.

2.jautājums: Vai piecciparu palindroms var būt pirmskaitlis? Vai sešciparu palindroms var būt pirmskaitlis?

Atbilde:

Tā kā palindromā pastāv simetrija starp cipariem, kuri ir vienādi tālu no sākuma un beigām, tad (izņemot skaitli 11) nebūs palindromu-pirmskaitļu, kuros ir pāru skaits ciparu. Tas seko no dalāmības pazīmes ar 11. Savukārt piecciparu palindromus atras nav grūti –- jau 10001, 10101, 10201 ir salikti skaitļi. Bet jau 10301 ir pirmskaitlis.

3.jautājums: Autobusa biļetei ir sešciparu numurs no 000000 līdz 999999. Kādu biļešu ir vairāk: tādu, kuru numuru pirmo trīs ciparu summa ir vienāda ar pēdējo trīs ciparu summu, vai tādu, kuru numurs dalās ar 11?

4.jautājums: Pēc kārtas izrakstīti visu naturālo skaitļu (no 1 līdz 2016) kubu decimālpierakstu cipari:

$$1827641252163435127291000 \ldots 8193540096$$

(Pēdējie cipari apzīmē to, ka $2016^3 = 8193540096$.) Atrast atlikumu, šo garo skaitli dalot ar 9.

5.jautājums: Pamatot sekojošu dalāmības pazīmi ar 13: "Skaitlis dalās ar 13 tad un tikai tad, ja šim skaitlim nosvītrojot pēdējo ciparu, četrkāršojot to un pieskaitot "saīsinātajam" skaitlim, iegūtais rezultāts dalās ar 13. Citiem vārdiem, ja $n = 10a + b$, kur b ir skaitļa pēdējais cipars, tad

$$13 \mid 10a + b \;\leftrightarrow\; 13 \mid a + 4b.$$

Vai skaitļa $n = 10a+b$ aizstāšana ar $n' = a+4b$ saglabā skaitļa kongruences klasi? Citiem vārdiem, vai $n \equiv n' \pmod{13}$?

2.8 Periodiski procesi

Ja kādā sistēmā ir galīgs skaits stāvokļu un katru nākamo stāvokli viennozīmīgi nosaka viens vai daži iepriekšējie stāvokļi. tad sistēmas stāvokļi pēc kāda laika sāk periodiski atkārtoties.

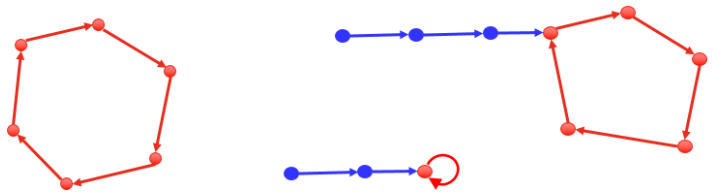
Piemēri:

- Naturālu skaitļu aritmētisku progresiju atlikumi (mod m).
- Naturālu skaitļu ģeometrisku progresiju atlikumi (mod m).
- Fibonači virknes locekļu atlikumi (piemēram, pēdējie 2 cipari Fibonači virknes locekļiem).
- Ciparu virkne aiz komata skaitļa $\frac{P}{Q}$ decimālpierakstā.

Visi šie procesi ir periodiski. Dažreiz virkne ir *tīri periodiska* (periods sākas jau no paša sākuma), citreiz virknei ir priekšperiods (*prefix*) un tā kļūst periodiska sākot ar kādu vietu, bezgalīgi atkārtojot vienu un to pašu periodu (*repetend*). Sk. https://bit.ly/3tHRQBv

2.8.1 Kādos gadījumos rodas priekšperiods

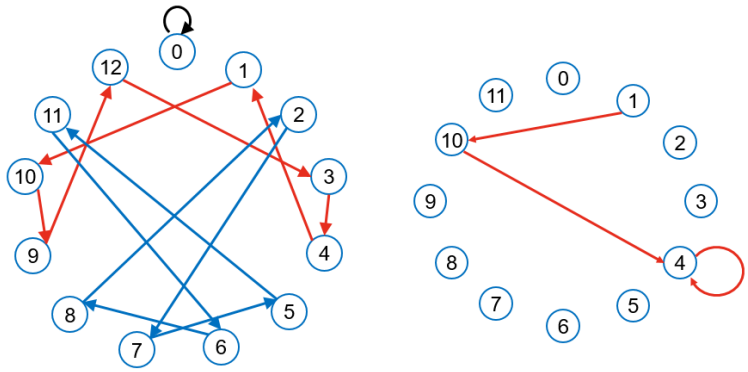
Attēlā redzami trīs grafi ar stāvokļu pārejas bultiņām. Pirmajam no tiem nav priekšperioda (visas bultiņas ir sarkanas), pārējiem diviem ir priekšperiods (aiz zilajām bultiņām seko sarkanā bultiņa - stabils/bezgalīgs periods).



Šie attēli ilustrē racionālu skaitļu izteikšanu bezgalīgu decimāldaļu veidā:

$$\frac{7}{13} = 0.(538461) = 0.538461538461538461\ldots$$
$$\frac{7}{12} = 0.58(3)\ldots = 0.58333\ldots$$
$$\frac{2020}{5125} = 0.3941463414634\ldots$$

Dalot ar 13 nav priekšperioda (skaitlis ir tīri periodisks ar sešu ciparu periodu). Dalot ar 12 ir divu ciparu priekšperiods un tad periods no viena cipara. Dalot ar $5125 = 125 \cdot 41$ ir trīs ciparu priekšperiods un tad piecu ciparu periods.



Kāpēc veselu skaitļu dalīšana var noved pie šiem atšķirīgajiem gadījumiem? Aplūkojam dalīšanu stabiņā kā stāvokļu pārejas starp atlikumiem.

Dalot ar 13 stāvokļu pārejas veido parastu, "tīru" ciklu. Savukārt, dalot ar 12, atlikumam 4 "iedur" divas bultiņas. Ja $10a \equiv 4 \pmod{12}$, tad iespējamas divas situācijas: vai nu $a = 4$, vai arī $a = 10$.

Jautājumi par periodiskām virknēm Katrai no virknēm noteikt, vai tā ir tīri periodiska vai arī periodiska no kādas vietas (un ja ir, tad atrast tās periodu un arī priekšperiodu).

(A) Virknes $1; 1+2; 1+2+3; 1+2+3+4; \ldots$ pēdējais cipars?

(B) Katram naturālam n definējam b_n, kas ir virknes $n!$ pēdējais nenulles cipars.

(C) Fibonači skaitļu virknes $F(n)$ pēdējie divi cipari (Fibonači skaitļa atlikums, dalot ar 100).

(D) Virkne, kas satur locekli $+1$, ja $\sin\left(\frac{13\pi n}{7}\right) > 1$, bet -1 pretējā gadījumā. Šeit $n \in \mathbb{N}$ ir patvaļīgs naturāls skaitlis.

(E) Atlikums, dalot a^n ar b, kur a, b ir abi naturāli.

(F) Pēdējie 4 cipari 5^n pierakstā?

(G) Skaitļa $\sin\left(\frac{n}{10}\right)$, $n \in \mathbb{N}$ zīme?

(H) n-tais cipars aiz komata skaitļa $7/13$ decimālpierakstā?

Risinājumi:

(A) Virkne ir periodiska – periods ir 20.

(B) Faktoriālam katru nākamo elementu viennozīmīgi nosaka iepriekšējais, Tomēr pēdējais nenulles cipars viennozīmīgi neizriet no iepriekšējā faktoriāla pēdējā nenulles cipara. (Tas gan **nav** pierādījums, ka virkne nav periodiska, bet tajā neizpildās nepieciešamais periodiskuma nosacījums).

(C) Fibonači skaitļa pēdējie divi cipari viennozīmīgi nenosaka nākamā locekļa pēdējos divus ciparus. Bet Fibonači skaitļu pārītis nosaka. Tādēļ ir periodiska.

(D) Ja n pārlec 14 vienības uz priekšu, tad sinusa zīme (un arī vērtība) nemainās.

Piemērs: Vai eksistē Fibonači skaitlis, kura decimālpieraksts beidzas ar divām nullēm?

Piemērs: Cik ir tādu n, kam $5^n \equiv 25 \pmod{10000}$?

Piemērs: Cik ir tādu n, kam $17^n \equiv 1 \pmod{100000}$? (T.i. 17^n decimālpieraksts beidzas ar `00001`.)

Ieteikumi: Visos gadījumos jānoskaidro, vai process, kurš ieciklojas, ir viennozīmīgi apvēršams. Salīdzinām, teiksim $\frac{7}{41}$ decimālpierakstu ar $\frac{7}{12}$ decimālpierakstu. Pirmajam no skaitļiem nav pusperioda, tas uzreiz aiz komata sāk 5 ciparu periodu. Savukārt, dalot ar 12, rodas pusperiods.

2.9 Sacensību Uzdevumi

1.Uzdevums (BW.2018.18): Dots tāds naturāls skaitlis $n \geq 3$, ka $4n+1$ ir pirmskaitlis. Pierādiet, ka $n^{2n}-1$ dalās ar $4n+1$.

Atbilde:

No Fermā teorēmas tieši seko, ka $n^{4n}-1$ dalās ar $4n+1$. Jo $n^{p-1} \equiv 1 \pmod{p}$.

Bet par kongruenču klasi n^{2n} ir divas iespējas. Ja šīs klases kvadrāts ir 1, tad pati klase varētu būt gan $+1$, gan arī -1.

2.Uzdevums (BW.2016.1): Atrast visus pirmskaitļu pārus (p,q), kuriem

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

Atbilde:

Izrakstām iespējamās starpības $p^3 - q^5$ un meklēsim tajā pilnus kvadrātus. Šai izteiksmei jābūt nenegatīvai, lai tā būtu vienāda ar $(p+q)^2$.

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

Aplūkojam atlikumu pārīšus (pēc 3 moduļa). Dažādām izteiksmēm izrakstām, ar ko tās kongruentas.

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`

Pārliecināmies, ka skaitlim p vai q ir jādalās ar 3; tātad kāds no tiem ir vienāds ar 3 (jo ir pirmskaitlis). Pārskatot nedaudzos gadījumus ar pirmskaitli 3, iegūsim, ka $(p, q) = (7, 3)$ ir vienīgais atrisinājums.

3.Uzdevums (BWTST.2018.13): Vai eksistē tāds pirmskaitlis q, ka nevienam pirmskaitlim p skaitlis

$$\sqrt[3]{p^2 + q}$$

nav naturāls?

Atbilde:

Ja $q = 2$, tad nesanāk, jo $5^2 + 2 = 3^3$ ir pilns kubs.

Ja $q = 3$, tad sanāk. Pierādījuma shēma – "pretrunas modulis" Atrodam tādu m, ka p^2 dod nelielu atlikumu skaitu, dalot ar m. Tad arī $p^2 + 3$ dod nedaudzus, paredzamus atlikumus. Vienlaikus var panākt, ka šādi atlikumi ir neiespējami naturāla skaitļa kubam a^3.

Nepāru skaitļu pilniem kvadrātiem ir izdevīgi aplūkot atlikumus, dalot ar 8 — tas arī būs mūsu pretrunas modulis.

Ievērojam, ka jebkurš nepāru skaitļu kvadrāts n^2 dod atlikumu 1, dalot ar 8. (Lai par to pārliecinātos, apzīmējam $n = 2k + 1$. Tad $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Tieši viens no $k, k + 1$ ir pāru skaitlis, tātad reizinājums $4k(k + 1)$ dalās ar 8.)

Esam pārbaudījuši, ka $\sqrt[3]{p^2 + 3}$ nav vesels skaitlis, jo vai nu $p^2 + 3 = 7$ (ja $p = 2$), vai arī $p^2 + 3$ dod atlikumu 4, dalot ar 8 Tas nav iespējams, jo visu pāru skaitļu kubi dalās ar 8.

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

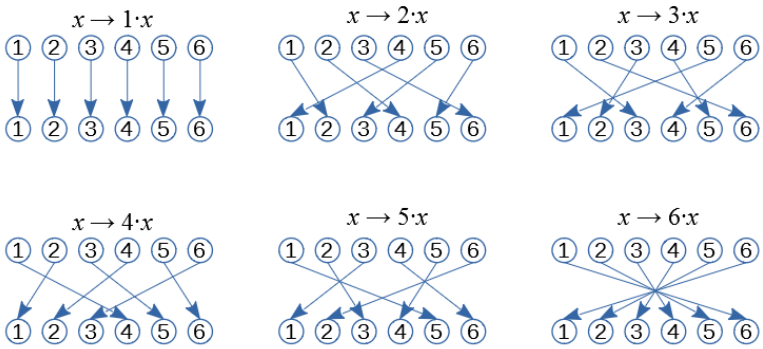
Definīcija: Aplūkojam naturālu skaitli m un veselu skaitli a. Par vesela skaitļa a *multiplikatīvi inverso* pēc m moduļa jeb (mod m) sauc tādu veselu skaitli x, kam izpildās kongruence $a \cdot x \equiv 1 \pmod m$.

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:

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

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

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

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

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).

NMS SKAITĻU TEORIJA #4: MULTIPLIKATĪVAS FUNKCIJAS

Vidusskolas matemātikas kursā parasti runā par funkcijām, kas vienam reālam skaitlim piekārto citu reālu skaitli. Piemēram, attēlo skaitli x par $x^2 + px + q$ (kvadrātfunkcija), vai par $\sqrt{x}$ (kvadrātsakne, kas definēta, ja $x \geq 0$), vai kāda no trigonometriskajām funkcijām.

Vispārīgākā nozīmē funkcija ir jebkurš attēlojums, kas kopas A elementam $x \in A$ piekārto elementu no kopas B, ko pieraksta kā $f(x) \in B$.

Šajā nodaļā aplūkosim funkcijas, kurām vai nu definīcijas apgabals vai vērtību apgabals ir veselie (vai naturālie) skaitļi, ja šīs funkcijas izmantojamas skaitļu teorijā.

4.1 Ievaduzdevumi

Definīcija: Apzīmēsim ar $\lfloor x \rfloor$ skaitļa x apakšējo veselo daļu – lielāko veselo skaitli, kas nepārsniedz x.

1. Pieņemsim, ka reāls skaitlis $x \in \mathbb{R}$ ir nevesels. Atrast $\lfloor -x \rfloor + \lfloor x \rfloor$.
2. Izteikt skaitļa n dalāmo skaitu starp naturāliem skaitļiem intervālā $(0; x)$, kur x ir reāls pozitīvs skaitlis. (Var uzrakstīt formulu, kurā ietilpst veselā daļa.)
3. Dota augoša aritmētiska progresija ar pirmo locekli a un diferenci d. Cik daudzi šīs progresijas locekļi būs intervālā $[b; c)$. (Var pieņemt, ka visi a, b, c, d ir naturāli skaitļi un $a < b < c$.)
4. Katriem diviem reāliem x, y pierādīt nevienādības:
$$\lfloor x \rfloor + \lfloor x \rfloor \ \leq \ \lfloor x + y \rfloor \ \leq \ \lfloor x \rfloor + \lfloor x \rfloor + 1$$
5. Pierādīt, ka jebkuram reālam $x \in \mathbb{R}$ un jebkuram naturālam $n \in \mathbb{N}$ ir spēkā vienādība
$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor .$$
6. Pierādīt, ka jebkuram reālam $x \in \mathbb{R}$ ir spēkā vienādības:
$$\begin{cases} \lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor . \\ \lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor . \end{cases}$$
7. Kādā skolā ir $n = 600$ skolēni. No viņiem $n_a = 300$ mācās angļu valodu, $n_v = 200$ mācās vācu valodu, bet $n_{av} = 100$ mācās angļu **un** vācu valodas (šīs kopas var pārklāties). Cik ir tādu skolēnu, kuri nemācās nevienu no šīm valodām?

4.2 Mazā Fermā un Eilera Teorēma

Mazā Fermā teorēma: Doti naturāli skaitļi a un p, kur p ir pirmskaitlis. Ja a nedalās ar p, tad ir spēkā sakarība

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

Sekas: Jebkuram naturālam skaitlim a izteiksme $a^p - a$ dalās ar a. (Iznesam a pirms iekavām: $a^p - a = a \cdot (a^{p-1} - 1)$. Ja pats a dalās ar p, tad pirmais reizinātājs dalīsies ar p. Ja a nedalās ar p, tad pēc Fermā teorēmas otrais reizinātājs $a^{p-1} - a$ dalās ar p.

Piemēri:

- Ja $a = 2$, bet $p = 7$, tad $2^6 = 64 \equiv 1 \pmod{7}$, jo 63 dalās ar 7 bez atlikuma.
- Cik deviņnieki pēc kārtas jāuzraksta, lai iegūtais skaitlis dalītos ar 7?
- Cik deviņnieki pēc kārtas jāuzraksta, lai skaitlis dalītos ar 41? Kāds ir mazākais deviņnieku skaits, lai skaitlis dalītos ar 41?

Šo teorēmu nelieliem pirmskaitļiem var skaitliski pārbaudīt ar Python:

```
[x**2 for x in range(0,7)]
[x**2 % 7 for x in range(0,7)]
[x**3 % 7 for x in range(0,7)]
[x**6 % 7 for x in range(0,7)]
```

Pēdējā no rindiņām parāda, ka visi iespējamie atlikumi jeb kongruenču klases $(0, \ldots, 6)$, kāpinot 6.pakāpē dod atlikumu 1, dalot ar 7. (Vienīgais izņēmums ir atlikums 0, kurš pats dalās ar 7.)

Definīcija: Ar $\varphi(n)$ apzīmējam *Eilera funkciju* – to veselo skaitļu skaitu intervālā $[1; n]$, kas ir savstarpēji pirmskaitļi ar n.

Piemēri:

- Ja p ir pirmskaitlis, tad $\varphi(p) = p - 1$.
- Ja p^k ir pirmskaitļa pakāpe, tad $\varphi(p^k) = p^k - p^{k-1} = p^k \cdot \left(1 = \frac{1}{p}\right)$.

Eilera teorēma: Ja a un n ir savstarpēji pirmskaitļi, tad

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

Piemēri:

- Kuram n skaitlis $2^n - 1$ noteikti dalīsies ar 9?
- $\varphi(10) = 4$, tādēļ katram no skaitļiem $1, 3, 7, 9$ ir spēkā sakarība $a^4 \equiv 1 \pmod{10}$. Teiksim, skaitļa \$3\$ pakāpes ir $1, 3, 9, 27, 81, \ldots$. Iegūstam, ka 3^4 beidzas ar to pašu ciparu, ar ko $3^0 = 1$.

Note: Protams, cikls var iestāties arī ātrāk. Piemēram, kāpinot skaitļus, kuri beidzas ar ciparu 1, periods (pēdējā cipara atkārtošanās) notiek uzreiz. Ja skaitlis beidzas ar ciparu 9, tad pēdējā cipara atkārtošanās notiek katrā otrajā solī. Bet tas nemaina faktu, ka $a^4 \equiv 1 \pmod{10}$. Pēdējā cipara periods tātad var būt $1, 2, 4$, jo Eilera teorēma neapgalvo, ka $\varphi(n)$ būs *mazākais* kāpinātājs k, kuram a^k ir kontruents ar 1. Toties no Eilera teorēmas seko, ka arī mazākais periods ir skaitļa $\varphi(n)$ dalītājs.

4.2.1 Skaitliski piemēri

1.Jautājums Ar kādiem pēdējiem diviem cipariem var beigties naturāla skaitļa n pakāpe n^{20}?

2.Jautājums Aplūkojam naturālu skaitli $n = 561$. Tas nav pirmskaitlis, jo $n = 561 = 3 \cdot 11 \cdot 17$. Pierādīt, ka jebkuram naturālam a skaitlis $a^n - a$ dalās ar n.

Note: Šī pati īpašība piemīt arī visiem pirmskaitļiem – tiešas sekas no Fermā teorēmas. Nepirmskaitļus, kam arī tā izpildās, sauc par Kārmaikla (*Carmichael*) skaitļiem. $n = 561$ ir mazākais no Kārmaikla skaitļiem.

4.2.2 Sacensību uzdevumi

1.Jautājums Aplūkojam virkni $a_n = 2^n + 3^n + 6^n - 1$, kur $n = 1, 2, \ldots$. Pierādīt, ka jebkuram pirmskaitlim p atradīsies tāds a_n, ka a_n dalās ar p.

2.Jautājums Atrast tādu bezgalīgi augošu aritmētisku progresiju no naturāliem skaitļiem, ka neviens no tās locekļiem nav divu pilnu kubu summa.

3.Jautājums Naturālam skaitlim n atrodam visus tos naturālos skaitļus $a_i \in [1; n]$, kuri ir savstarpēji pirmskaitļi ar n. Pamatot, ka visu šo a_i summa

$$a_1 + \ldots + a_k = \frac{n \cdot \varphi(n)}{2}.$$

4.Jautājums Katram naturālam skaitlim n pierādīt vienādību:

$$\sum_{d|n} \varphi(d) = n.$$

4.3 Multiplikatīvas funkcijas

Eilera funkcija $\varphi(n)$ ir tipisks piemērs vispārīgākai veselo skaitļu funkciju kopai, ko sauc par *multiplikatīvām funkcijām*.

Definīcija Funkciju $f : \mathbb{N} \to \mathbb{R}$ sauc par multiplikatīvu, ja katriem diviem naturāliem $a, b \in \mathbb{N}$, kuri ir savstarpēji pirmskaitļi, ir spēkā sakarība:

$$f(ab) = f(a) \cdot f(b).$$

Īpašības:

- Multiplikatīvām funkcijām jābūt spēkā: $f(1) = 1$.
- Multiplikatīvai funkcijai pietiek zināt vērtības $f(p^k)$ pirmskaitļu pakāpēm. Citas vērtības var iegūt ar reizināšanu.

Piemēri:

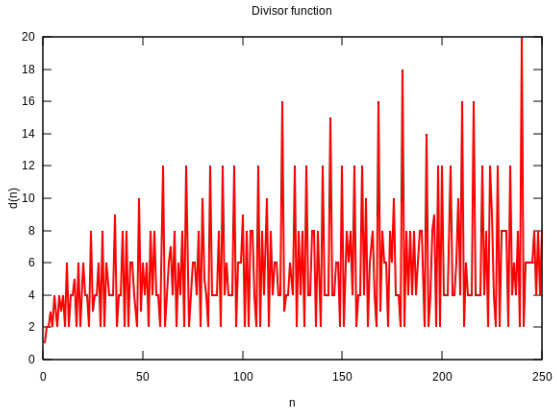
- $\gcd(n, k)$: divu skaitļu lielākais kopīgais dalītājs, kur n ir arguments, bet k ir konstante.
- $\varphi(n)$: Eilera funkcija –- cik ir naturālu $k \in [0; n]$, kas ir savstarpēji pirmskaitļi ar n.
- $\sigma_0(n) = d(n)$ – skaitļa n dalītāju skaits.
- $\sigma_1(n) = \sigma(n)$ - skaitļa n dalītāju summa.

4.3.1 Dalītāju skaita funkcija

Definīcija: Naturālam skaitlim n visu pozitīvo dalītāju skaitu apzīmējam ar

$$d(n) = \sum_{d|n} 1.$$

Attēlā parādīta dalītāju skaita funkcija $\sigma_0(n) = d(n)$ skaitļiem intervālā $[1; 250]$:



Šajā grafikā redzama virkne ar naturāliem skaitļiem, kuri pirmo reizi sasniedz noteiktas dalītāju skaita vērtības:

n	1	2	4	6	12	16	24	36	48	60	64	120	144	180	240
$d(n)$	1	2	3	4	6	5	8	9	10	12	7	16	15	18	20

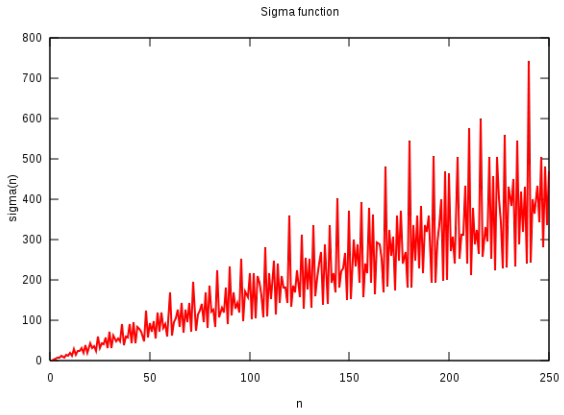
Teorēma: Ja zināms skaitļa sadalījums pirmreizinātājos: $n = p_1^{k_1} \cdots p_m^{k_m}$, tad dalītāju skaita funkciju nosaka ar formulu:

$$d(n) = \prod_{i=1}^{m} (k_i + 1) = (1 + k_1)\,(1 + k_2) \cdot \ldots \cdot (1 + k_m)\,.$$

Pierādījums: Šī formula iegūstama no fakta, ka visi skaitļa n dalītāji ir iekodējami ar veselu skaitļu vektoriņiem: $(x_1, x_2, \cdots, x_m)$, kur $0 \leq x_i \leq k_i$, t.i. skaitļa n dalītājam d var uzrakstīt līdzīgu sadalījumu pirmreizinātājos: $d = p_1^{x_1} \cdots p_m^{x_m}$, kur katru no kāpinātājiem x_i var izvēlēties $(k_i + 1)$ dažādos veidos. □

4.3.2 Dalītāju summas funkcija

Piemērs: Attēlā parādīta dalītāju summas funkcija $\sigma_1(n) = \sigma(n)$ skaitļiem intervālā $[1; 250]$:



Teorēma: Ja zināms skaitļa sadalījums pirmreizinātājos: $n = p_1^{k_1} \cdots p_m^{k_m}$, tad dalītāju skaita funkciju nosaka ar formulu:

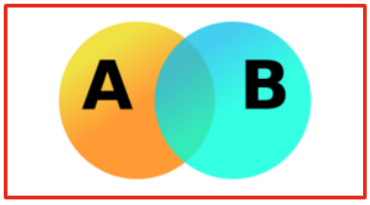
$$\sigma(n) = \prod_{i=1}^{m} \left(1 + p_i^1 + p_i^2 + \ldots + p_i^{k_1}\right) = \left(1 + p_1 + \ldots p_1^{k_1}\right) \left(1 + p_2^1 + \ldots + p_2^{k_2}\right) \cdot \ldots \cdot \left(1 + p_m^1 + \ldots + p_m^{k_m}\right).$$

Pierādījums: Atverot iekavas pēdējā izteiksmē, iegūsim $d(n)$ saskaitāmos – katrs izrādīsies kāds no n dalītājiem. □

4.3.3 Ieslēgšanas-Izslēgšanas princips

Piemērs: Skolā pavisam ir ap 1000 bērni. 300 mācās vācu valodu, 250 mācās franču valodu, 150 mācās abas. Cik daudzi nemācās nevienu?

Pierādījums: Divām kopām var izmantot ieslēgšanas izslēgšanas principu:



Divām kopām ieslēgšanas-izslēgšanas metode izskatītos sekojoši:

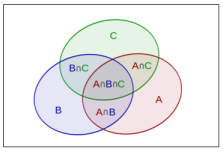
$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Ievietojam uzdevumā dotos skaitļus, lai atrastu, cik ir skolēnu, kuri mācās vismaz vienu svešvalodu (vācu vai franču):

$$|A \cup B| = 300 + 250 - 150 = 400.$$

Tātad to, kuri nemācās nevienu no šīm svešvalodām ir $1000 - 400 = 600$. ■

Piemērs: Zīmējumā attēlota kopa U (universs) un trīs tā apakškopas A, B, C. Zināms elementu skaits katrā no kopām (un arī to šķēlumos pa divām vai trim). Atrast elementu skaitu visu trīs kopu apvienojumā.



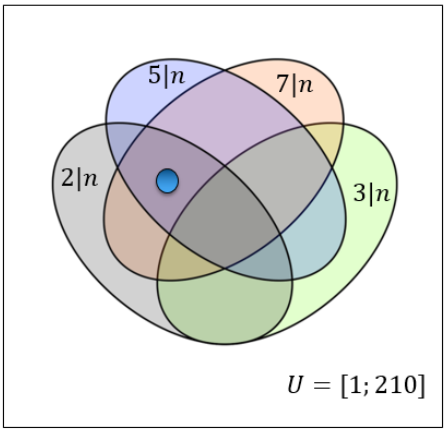
Risinājums:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

4.3.4 Eilera funkcija

Skaitļu teorijā bieži ir vieglāk noteikt dažādu skaitļu kopu šķēlumu nevis apvienojumu. Apvienojuma elementu saskaitīšanai var noderēt ieslēgšanas-izslēgšanas princips.

Piemērs: Zīmējumā attēloti veselie skaitļi $\{1, 2, \ldots, 210\}$. Krāsaino ovālu iekšpusē ir skaitļi, kuri dalās attiecīgi ar $2, 3, 5, 7$. Skaitlis $210 = 2 \cdot 3 \cdot 5 \cdot 7$ ir pirmo četru pirmskaitļu reizinājums.



- Atrast skaitļu piemērus apgabalā ar zilo bumbulīti.
- Cik ir pelēkā un zaļā ovāla šķēlumā?
- Cik ir ārpus visiem ovāliem? Cik no veselajiem skaitļiem intervālā $[1; 100]$ ir tādi, kas nedalās ne ar 2, ne ar 3, ne ar 5, ne ar 7?

Risinājums:

$$\begin{aligned} & 210 - \tfrac{210}{2} - \tfrac{210}{3} - \tfrac{210}{5} - \tfrac{210}{7} + \tfrac{210}{2\cdot3} + \tfrac{210}{2\cdot5} + \tfrac{210}{2\cdot7} + \tfrac{210}{3\cdot5} + \tfrac{210}{3\cdot7} + \tfrac{210}{5\cdot7} - \tfrac{210}{2\cdot3\cdot5} - \tfrac{210}{2\cdot3\cdot7} - \tfrac{210}{2\cdot5\cdot7} - \tfrac{210}{3\cdot5\cdot7} + \tfrac{210}{2\cdot3\cdot5\cdot7} = \\ = \; & 210 \cdot \left(1 - \tfrac{1}{2}\right) \cdot \left(1 - \tfrac{1}{2}\right) \cdot \left(1 - \tfrac{1}{5}\right) \cdot \left(1 - \tfrac{1}{7}\right). \end{aligned}$$

Piemērs: Pieņemsim, ka skaitlim n ir tikai 3 pirmskaitļu dalītāji p, q, r. Ar M_a apzīmēsim, cik intervālā $[1; n]$ ir skaitļa a daudzkārtņu.

Iegūsim, šādu sakarību:

$$\begin{aligned} \varphi(n) = \; & n - (M_p + M_q + M_r) + (M_{pq} + M_{pr} + M_{qr}) - M_{pqr} = \\ = \; & n - \left(\tfrac{n}{p} + \tfrac{n}{q} + \tfrac{n}{r}\right) + \left(\tfrac{n}{pq} + \tfrac{n}{pr} + \tfrac{n}{qr}\right) - \tfrac{n}{pqr} = n\left(1 - \tfrac{1}{p}\right)\left(1 - \tfrac{1}{q}\right)\left(1 - \tfrac{1}{r}\right). \end{aligned}$$

Teorēma: Eilera funkcija $\varphi(n)$ ir multiplikatīva.

Piemēri: Eilera funkcijas multiplikativitāti var izmantot, lai to praktiski aprēķinātu tad, ja zināms skaitļa n sadalījums pirmreizinātājos:

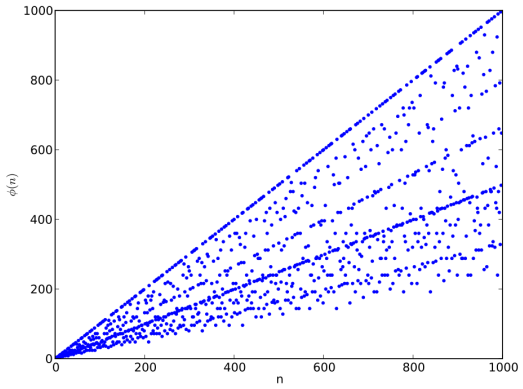
$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}.$$

Tad Eilera funkciju aprēķina katra pirmskaitļa pakāpei atsevišķi un rezultātus sareizina:

$$\varphi(n) = p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot p_m^{k_m}\left(1-\frac{1}{p_m}\right) = n\cdot\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_m}\right).$$

$$\begin{aligned}
&\varphi(10) = \varphi(5)\cdot\varphi(2) = (5-1)(2-1) = 4.\\
&\varphi(70) = \varphi(2)\cdot\varphi(5)\cdot\varphi(7) = (2-1)(5-1)(7-1) = 24.\\
&\varphi(100) = \varphi(25)\cdot\varphi(4) = (25-5)(4-2) = 40.\\
&\varphi(2012) = \varphi(4)\cdot\varphi(503) = (2^2-2^1)(503-1) = 2\cdot 502 = 1004.
\end{aligned}$$

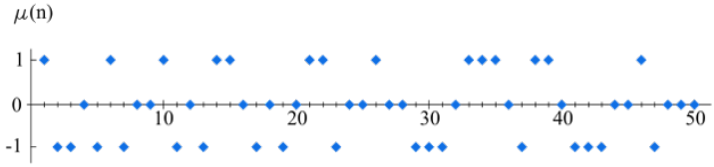
Piemērs: Attēlā dots Eilera funkcijas grafiks. Tās īpašības analizētas arī https://mathworld.wolfram.com/TotientFunction.html.



4.3.5 Mēbiusa funkcija

Definīcija: Mēbiusa (Möbius) funkciju definē šādi:

- -1, ja n ir nepāra skaita pirmskaitļu reizinājums,
- $+1$, ja n ir pāra skaita pirmskaitļu reizinājums,
- 0, ja n sadalījums pirmreizinātājos satur kāda pirmskaitļa pakāpi, kas augstāka par pirmo.



Teorēma: Mēbiusa funkcija ir multiplikatīva.

Apgalvojums: Katram naturālam n ir spēkā sekojoša formula:

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & \text{ja n=1} \\ 0, & \text{ja n>1} \end{cases}$$

Ieteikums: Ja $n > 1$, to izsaka kā pirmskaitļu reizinājumu (daži no pirmskaitļiem var arī sakrist):

$$n = p_1 p_2 \cdots p_k.$$

Jāpamato, ka šī izteiksme vienāda ar 0:

$$\begin{array}{ll} & \mu(1)+ \\ + & (\mu(p_1)+\mu(p_2)+\ldots+(p_k))+ \\ + & (\mu(p_1p_2)+\ldots+\mu(p_{k-1}p_k))+ \\ + & \ldots+ \\ + & \mu(p_1p_2\cdots p_k). \end{array}$$

Apgalvojums: Ir spēkā izteiksme

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}.$$

Pierādījums: Šajā izteiksmē paliek pāri tikai nedaudzi reizinātāji – kur n dala ar dažādiem pirmskaitļiem (vai atšķirīgu pirmskaitļu reizinājumiem), šo to pieskaita, šo to atņem.

4.3.6 Perfekti skaitļi

Ar dalītāju summas funkciju saistīta neparasta skaitļu kategorija – *perfekti skaitļi*.

Definīcija: Skaitļus n, kas vienādi ar visu savu dalītāju summu (atskaitot pašu n):

$$n=\sum_{d|n\wedge d<n} d$$

sauc par *perfektiem skaitļiem*

Piemēri: Perfekti skaitļi ir: $6=1+2+3$, $28=1+2+4+7+14$, utt.

Eiklīda teorēma: Ja 2^p-1 ir pirmskaitlis, tad $2^{p-1}(2^p-1)$ ir perfekts.

Piemēri:

- Ja $p=2$, tad $p^2-1=3$ ir Mersenna pirmskaitlis.
- 2^p-1 var būt pirmskaitlis tikai tad, ja p ir pirmskaitlis. Pirmskaitļus šādā formā 2^p-1 sauc par Mersenna skaitļiem. (Zināmi 50 šādi pirmskaitļi.) Nav zināms, vai Mersenna pirmskaitļu ir bezgalīgi daudz. Un arī nav zināms, vai neeksistē perfekti skaitļi kādā citā formā (tsk.vai ir iespējami nepāra perfekti skaitļi).

4.3.7 Skaitliski piemēri

1.jautājums: Pierādīt, ka neeksistē tāds n, kuram Eilera funkcijas vērtība $\varphi(n)=14$.

2.jautājums: Atrisināt vienādojumu naturālos skaitļos:

$$\varphi(2x)=\varphi(3x).$$

3.jautājums: Zināms, ka naturālam skaitlim A ir tieši 62 naturāli dalītāji. Pierādīt, ka A nedalās ar 36.

4.jautājums: Atrast tādu naturālu n, kuram visu dalītāju apgriezto lielumu summa ir 2. Citiem vārdiem, atrast skaitli n, kuram

$$\sum_{d|n}\frac{1}{d}=2.$$

5.jautājums: Atrast tādu n, kuram

$$\mu(n)+\mu(n+1)+\mu(n+2)=3.$$

4.4 Sacensību uzdevumi

1.Uzdevums: Parādīt, ka

$$d(1) + d(2) + \ldots + d(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \ldots + \left\lfloor \frac{n}{n} \right\rfloor .$$

2.Uzdevums: Parādīt, ka

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) = 1 \cdot \left\lfloor \frac{n}{1} \right\rfloor + 2 \cdot \left\lfloor \frac{n}{2} \right\rfloor + \ldots + n \cdot \left\lfloor \frac{n}{n} \right\rfloor .$$

3.Uzdevums: Dots naturāls skaitlis n. Noteikt atkarībā no n, cik ir skaitļu $x \in \{1, 2, \ldots, n\}$, kuriem $x^2 \equiv x \pmod{n}$.

Ieteikumi: Meklēto atrisinājumu skaitu var vispirms atrast vienkāršākajiem gadījumiem. Apzīmējam meklēto atrisinājumu skaitu vienādojumam $x^2 \equiv x \pmod{n}$ (no kopas $\{1, \ldots, n\}$ ar $f(n)$. Atradīsim to sekojošiem n:

- $n = 1$.
- $n = p$, kur p ir pirmskaitlis.
- $n = p^k$, kur p^k ir pirmskaitļa pakāpe.
- $n = pq$, kas ir divu pirmskaitļu reizinājums.

Hipotēze: $f(n) = 2^{\omega(n)}$, kur ar $\omega(n)$ apzīmē skaitļa n dažādo pirmskaitļu dalītāju skaitu, neņemot vērā to, kādā pakāpē tie ietilpst skaitlī n.

Atbilde:

Divi atrisinājumi acīmredzami der arī ja n ir pirmskaitlis:

$$\begin{cases} 1^2 \equiv 1 \pmod{n} \\ n^2 \equiv n \pmod{n} \end{cases}$$

Ja $n = 10$, tad ir četri atrisinājumi:

$$\begin{cases} 1^2 \equiv 1 \pmod{10} \\ 5^2 \equiv 5 \pmod{10} \\ 6^2 \equiv 6 \pmod{10} \\ 10^2 \equiv 10 \pmod{10} \end{cases}$$

NMS SKAITĻU TEORIJA #5: VALUĀCIJAS

5.1 Valuāciju jēdziens

Valuācijas apraksta augstāko pirmskaitļa pakāpi, ar kuru dalās dotais skaitlis.

- Skaitļu teorijā dažreiz pietiek analizēt situāciju terminos "dalās" vai "nedalās" (no šejienes ir termini *pirmskaitlis*, *savstarpēji pirmskaitļi*, *LKD*, *MKD*).
- Dažreiz jāaplūko arī moduļi jeb kongruenču klases pēc kāda pirmskaitļa vai pirmskaitļa pakāpes moduļa (par to ir modulārā aritmētika)
- Vēl detalizētāk var aplūkot atlikumus, dalot ar dažādiem pirmskaitļiem (vai dažādu pirmskaitļu pakāpēm) – ķīniešu atlikumu teorēma.
- Visbeidzot, valuācijas ir vēl precīzāks instruments – aplūko "cik laba ir dalāmība" ar kādu pirmskaitli.

Definīcija: Ar n apzīmējam jebkuru naturālu skaitli un ar p – kādu pirmskaitli. Par skaitļa n p-valuāciju sauc tādu skaitli k, ka n dalās ar p^k, bet nedalās ar p^{k+1}. Šo faktu pieraksta, izmantojot grieķu burtu "nī":

$$\nu_p(n) = k.$$

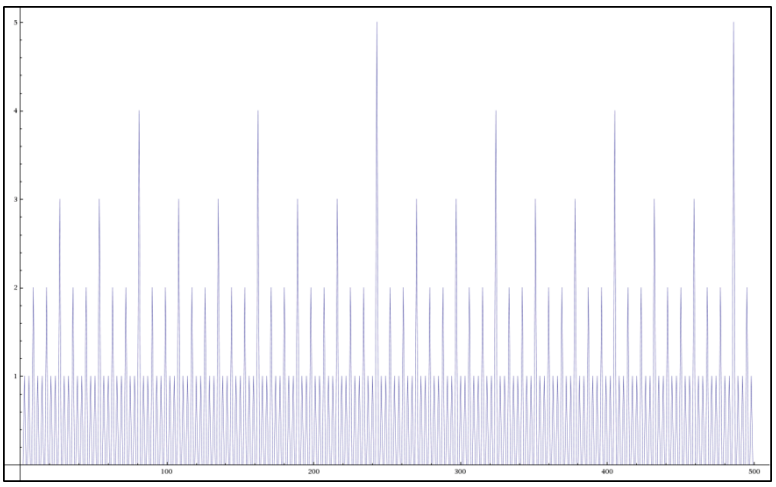
Α α	Β β	Γ γ	Δ δ	Ε ε	Ζ ζ
Η η	Θ θ	Ι ι	Κ κ	Λ λ	Μ μ
Ν ν	Ξ ξ	Ο ο	Π π	Ρ ρ	Σ σ
Τ τ	Υ υ	Φ φ	Χ χ	Ψ ψ	Ω ω

Fig. 1: Grieķu alfabēts

Piemēri: Ja pirmskaitlis $p = 3$, tad

$$\begin{cases} \nu_3(1) = \nu_3(2) = \nu_3(4) = \nu_3(5) = \ldots = 0 \\ \nu_3(3) = \nu_3(6) = \nu_3(12) = \nu_3(15) = \ldots = 1 \\ \nu_3(9) = \nu_3(18) = \nu_3(36) = \nu_3(45) = \ldots = 2 \\ \nu_3(27) = \nu_3(54) = \ldots = 3 \\ \nu_3 81 = \ldots = 4 \\ \ldots \end{cases}$$

Funkcijas $f(n) = \nu_3(n)$ grafiks redzams zīmējumā – tā ir zāģveidīga trepīte, kurā ar regulārām atstarpēm rodas arvien garāki "zāģa zobi".



Valuāciju īpašības: Iedomāsimies, ka p ir jebkurš fiksēts pirmskaitlis.

- $\nu_p(a) = \infty$ tad un tikai tad, ja $a = 0$. (Visiem citiem veseliem skaitļiem atrodas tik augsta pirmskaitļa p pakāpe p^{k+1}, ka a vairs nedalās ar p^{k+1}.)
- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$. (Augstākās pakāpes saskaitās, ja abus skaitļus a un b reizina.)
- $\nu_p(a + b) \geq \min(\nu_p(a), \nu_p(b))$. Šajā izteiksmē pastāv vienādība, ja $\nu_p(a) \neq \nu_p(b)$.

Valuāciju funkcijas $\nu_2(n)$, $\nu_3(n)$ un citas nevar būt periodiskas, jo laiku pa laikam parādās arvien lielākas vērtības, piemēram, $\nu_2(2^k) = k$. No otras puses, to grafikiem piemīt savdabīga simetrija. Arī katrai konstantei $C > 0$ funkcija $f(n) = \min(C, \nu_2(n))$ ir periodiska (periodiskumu var panākt, ja lielās vērtības "apgriež" tā, lai tās nepārsniegtu C).

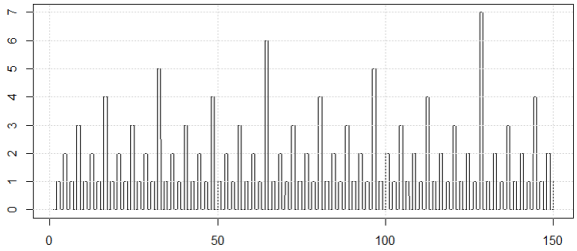


Fig. 2: Funkcijas $\nu_2(n)$ grafiks (lokālie maksimumi pie $n = 64$ un $n = 128$).

5.2 Valuācijas kombinatorikā

5.2.1 Ležandra teorēma

Teorēma (Adrien-Marie Legendre): Katram pirmskaitlim p un katram naturālam n p-valuācija ir aprēķināma pēc formulas

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

kur $\lfloor x \rfloor$ apzīmē apakšējo veselo daļu. (Izskatās, ka šajā vienādībā ir bezgalīga summa, bet jebkurām n un p vērtībām šajā summā ir tikai galīgs skaits nenulles saskaitāmo.)

Apgalvojums: Lielākā 2 pakāpe, ar ko dalās $n!$ ir $n - S_2(n)$, kur ar $S_2(n)$ apzīmēta n ciparu summa divnieku pierakstā.

N_{10}	N_2	$N!$	$\nu_2(N!)$
1	1	1	0
2	10	2	1
3	11	6	1
4	100	24	3
5	101	120	3
6	110	720	4
7	111	5040	4
8	1000	40320	7
9	1001	362880	7
10	1010	3628800	8
11	1011	39916800	8
12	1100	479001600	10

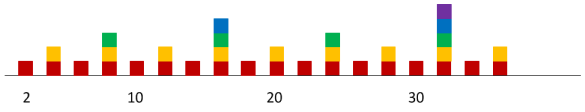
Fig. 3: Funkcijas $\nu_2(n!)$ tabula.

Piemērs: Skaitļa 100 divnieku pieraksts ir 1100100_2, tādēļ ciparu summa ir $S_2(100) = S_2(1100100_2) = 3$. Iegūstam, ka $\nu_2(100!) = 100 - 3 = 97$.

Lemma: Starp pirmajiem m naturālajiem skaitļiem ir tieši $\lfloor m/n \rfloor$ skaitļa n daudzkārtņu.

(Ar $\lfloor x \rfloor$ apzīmē skaitļa apakšējo veselo daļu – vislielāko veselo skaitli, kas nepārsniedz x.)

Piemērs: Ar kādu lielāko 2 pakāpi dalās skaitlis 36!?



Pārformulēsim šo citādi: Iztēlosimies, ka 36! sadalīts pirmreizinātājos:

$$36! = 2^{k_2} \cdot 3^{k_3} \cdot 5^{k_5} \cdot 7^{k_7} \cdot \ldots \cdot 31^{k_{31}}.$$

Atradīsim k_2 jeb kāpinātāju pie pirmskaitļa 2 šajā izteiksmē. (Kāpēc 36! dalās tikai ar pirmajiem 11 pirmskaitļiem no 2 līdz 31?)

Zīmējumā redzami visi reizinātāji, kuri veido 36!. Tie, kuri dalās ar 2, attēloti ar klucīšu stabiņu, kas rāda, cik divniekus (kā pirmreizinātājus) šis skaitlis pievienojis faktoriālam.

$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \left\lfloor \frac{n}{16} \right\rfloor + \left\lfloor \frac{n}{32} \right\rfloor + \left\lfloor \frac{n}{64} \right\rfloor + \cdots = \mathbf{18} + \mathbf{9} + \mathbf{4} + \mathbf{2} + \mathbf{1}.$

Rēķinot faktoriālu, klucīši summējas pa kolonnām. Ležandra formula tos saskaita pa rindiņām (vispirms sarkanos, tad oranžos, utt.)

Šī diagramma ilustrē svarīgu metodi: Ja ir jānovērtē veselu skaitļu summa, ko var saskaitīt divos dažādos veidos (piemēram, krāsaino klucīšu zīmējumā gan pa kolonnām, gan pa rindiņām), to bieži ir vērts mēģināt darīt, lai iegūtu ērtāku izteiksmi. Šoreiz ietaupījums ir acīmredzams – tai vietā lai saskaitītu 18 stabiņos esošos klucīšus, pietiek (rindiņās) summēt tikai piecus skaitļus, kurus turklāt vieglāk izrēķināt precīzi. Lielākiem n Ležandra formulas ietaupījums ir vēl lielāks: Ja $n = 1000$, tad saskaitāmo skaits samazinās no 500 līdz 10, jo jau $1000/2^{10} < 1$.

Lietojot Ležandra formulu arī citiem pirmskaitļiem, $p > 2$, iegūstam šādu sadalījumu pirmreizinātājos:

$$36! = 2^{34} \cdot 3^{17} \cdot 5^{8} \cdot 7^{5} \cdot 11^{3} \cdot 13^{2} \cdot 17^{2} \cdot 19^{1} \cdot 23^{1} \cdot 29^{1} \cdot 31^{1}.$$

Šis skaitlis beidzas ar $\min(\nu_2(36!), \nu_5(36!)) = \min(34, 8) = 8$ nullēm – katra nulle decimālpierakstā rodas, sareizinoties pirmreizinātājam 2 ar pirmreizinātāju 5. Skaitļa 36! tiešs aprēķins, sareizinot pirmos 36 naturālos skaitļus, rāda to pašu:

```
>>> from functools import reduce
>>> reduce(lambda a, b: a*b, range(1,37))
371993326789901217467999448150835200000000
```

Piemērs: Atrast robežas (skaitļus, kuriem neierobežoti tuvojas izteiksme zem robežas tad, ja n kļūst ļoti liels):

- $\lim\limits_{n\to\infty} \dfrac{\nu_2(n!)}{n}$.
- $\lim\limits_{n\to\infty} \dfrac{\nu_3(n!)}{n}$.
- $\lim\limits_{n\to\infty} \dfrac{\nu_5(n!)}{n}$.

5.2.2 Kummera teorēma

Teorēma (Ernst Kummer) Doti skaitļi n un m, kas apmierina nevienādības $n \geq m \geq 0$ un arī pirmskaitlis p. Tad binomiālajam koeficientam C_n^m p-valuācija sakrīt ar pārnesumu skaitu, ja m saskaita ar $n - m$ skaitīšanas sistēmā ar bāzi p.

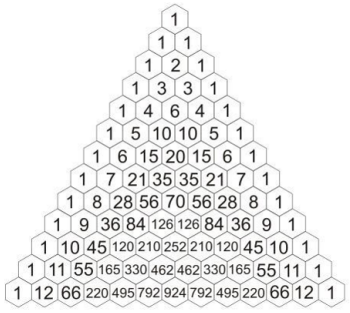
Šo teorēmu var pierādīt, izsakot binomiālo koeficientu:

$$C_n^m = \frac{n!}{m!(n-m)!}$$

un izmantojot Ležandra teorēmu.

Note: Par kombināciju jeb bionmiālo koeficientu skaitļu teorijas īpašībām ir vēl arī citi derīgi rezultāti (sal. Lūkas teorēmu https://bit.ly/3Frc1pT), bet tie neattiecas uz veselo skaitļu funkciju tēmu.

Piemērs: Zīmējumā attēlots Paskāla trijstūris, kurā iepelēkotas visas nepāru šūnas. Pēc Kummera teorēmas tās ir visas tās kombinācijas pa m no n, kam m var saskaitīt $n - m$ binārajā pierakstā pilnīgi bez pārnesumiem.



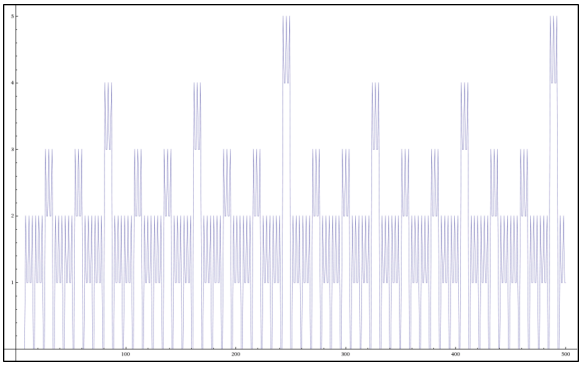
Apgalvojums: Dots naturāls skaitlis n. Pierādīt, ka jebkuru n pēc kārtas ņemtu naturālu skaitļu reizinājums dalās ar $n!$.

Pierādījums: Apzīmēsim lielāko no reizinātajiem skaitļiem ar m. Tad jāpierāda, ka

$$\frac{m(m-1)(m-2)\cdots(m-n+1)}{n!} \in \mathbb{N}.$$

Pierakstītā izteiksme sakrīt ar $C_m^n = \frac{m!}{n!(m-n)!}$. Tā kā kombinācijas (pie $n \leq m$) apzīmē, cik veidos no m elementiem var izvēlēties nesakārtotu izlasi ar n elementiem, kombinācijas vienmēr ir naturāli skaitļi.

Piemērs: Zīmējumā attēlots funkcijas $f(n) = \nu_3(C_n^7)$ grafiks. Vairumam skaitļu kombinācija pa 7 no n dalās ar nelielām 3 pakāpēm.



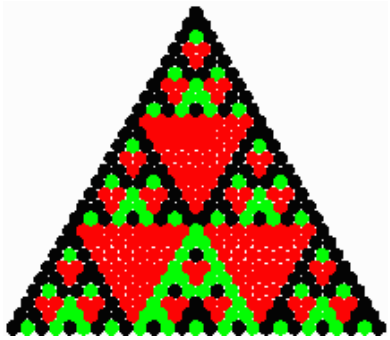
5.2.3 Lūkas teorēma

Teorēma (Lucas): Visiem nenegatīviem m un n, un jebkuram pirmskaitlim p, ir spēkā šāda sakarība:

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p},$$

kur $n = n_k p^k + n_{k-1} p^{k-1} + \ldots + n_1 p + n_0$, bet $m = m_k p^k + m_{k-1} p^{k-1} + \ldots + m_1 p + m_0$.

Piemērs: Attēlā dots Paskāla trijstūris (k-tais elements šī trijstūra n-tajā rindiņā attēlo, cik dažādos veidos var izvēlēties k elementus no n elementu kopas). Šis Paskāla trijstūris izkrāsots 3 krāsās (aplītis ir sarkans, ja tajā vietā ierakstītais skaitlis dalās ar 3; aplītis ir melns, ja dod atlikumu 1, dalot ar 3, aplītis ir zaļš, ja dod atlikumu 2, dalot ar 3). Atrast, cik ir melno aplīšu šī Paskāla trijstūra 1000 rindiņā: Cik daudzi no visiem 1001 skaitļiem šajā rindiņā dod atlikumu 1, dalot ar 3.



Risinājums: 16.

Pierakstām skaitli $1000 = 729 + 243 + 27 + 1 = 3^6 + 3^5 + 3^3 + 1 = 1101001_3$ trijnieku skaitīšanas sistēmā.

Aplūkosim vispirms kombinācijas C_{999}^k. Pamatosim, ka ir tieši 8 vērtības, kurām $C_{999}^k \equiv 1 \pmod 3$ jeb rodas melni aplīši (visām pārējām C_{999}^k dalās ar 3: šie aplīši ir sarkani).

$$C_{999}^0 \equiv C_{999}^{27} \equiv C_{999}^{243} \equiv C_{999}^{270} \equiv C_{999}^{729} \equiv C_{999}^{756} \equiv C_{999}^{972} \equiv C_{999}^{999} \equiv 1 \pmod 3.$$

Izmantojot Kummera teorēmu var pamatot, ka visiem citiem k, $C_{999}^k \equiv 0 \pmod 3$. Tas ir tāpēc, ka visos citos gadījumos iegūt skaitli, kura decimālpieraksts ir 999 ($999_{10} = 1101000_3$) var tikai saskaitot k un $999 - k$ tā, ka rodas pārnesums (saskaitot stabiņā trijnieku skaitīšanas sistēmā). Ir tikai 8 veidi kā sadalīt trīs vieniniekus no 1101000_3 pa abiem saskaitāmajiem tā, lai nerastos neviens pārnesums.

Savukārt visas astoņas vērtības, kas minētas kongruencē (sk. vienādojumu augstāk) ir vienādas ar 1 (nevis ar 2) saskaņā ar Lūkas teorēmu.

Zem Paskāla trijstūra rindiņas, kurā ir visi C_{999}^k, ir nākamā rindiņa, kurā ir visi C_{1000}^k. Šajā rindiņā melno elementu būs divreiz vairāk, jo katrs no astoņiem melnajiem, kas minēti (augšējā vienādojumā) saskaitīsies ar sarkano kaimiņu kreisajā un arī labajā pusē. Kopā būs 16 melni elementi (bet zaļo - tādu C_{1000}^k, kas kongruenti ar 2 pēc moduļa 3) nebūs. To secina vai nu no iepriekšējās rindiņas, vai arī tieši izmantojot Lūkas teorēmu.

5.3 Kāpinātāja pacelšanas lemmas

Kāpinātāja pacelšanas lemmas (Lifting the Exponent Lemmas) ir vairāki savstarpēji saistīti rezultāti, kuri ļauj atrast p-valuācijas divu skaitļu pakāpju starpībai vai summai.

5.3.1 Valuācijas nepāra pirmskaitļiem

Šajā nodaļā aplūkosim vienkāršāko gadījumu, ja p ir nepāra skaitlis.

Piemērs (UKMO2013): Skaitlis pierakstīts decimālās sistēmas bāzē satur 3^{2013} ciparus 3; citu ciparu skaitļa pierakstā nav. Atrast augstāko skaitļa 3 pakāpi, kas dala šo skaitli.

Ieteikums: Var aplūkot iesākumā mazāku skaitli, kura decimālpierakstā ir 27 trijnieki (jeb 3^3):

$$N = 333\,333\,333\ \ 333\,333\,333\ \ 333\,333\,333$$

Šo skaitli var sadalīt vairākos reizinātājos (katrs reizinātājs dalās ar 3, bet nedalās ar 9 (var pārbaudīt ar ciparu summām). Tas ļauj droši noskaidrot, ar kādu 3 pakāpi dalās N.

Piemērs: Zīmējam grafiku veselu skaitļu funkcijai $f(k) = \nu_3(10^k - 1)$, kur $k \in \mathbb{N}$.

$$\begin{array}{ll}
9 = 3 \cdot 3, & f(1) = 2, \\
99 = 9 \cdot 11, & f(2) = 2, \\
999 = 9 \cdot 111, & f(3) = 3, \\
9999 = 9 \cdot 1111, & f(4) = 2, \\
99999 = 9 \cdot 11111, & f(5) = 2, \\
999999 = 9 \cdot 1001 \cdot 111, & f(6) = 3, \\
9999999 = 9 \cdot 1111111, & f(7) = 2, \\
99999999 = 9 \cdot 11111111, & f(8) = 2, \\
999999999 = 9 \cdot 1001001 \cdot 111, & f(9) = 4.
\end{array}$$

Katru no skaitļiem, kas uzrakstīti ar visiem deviņniekiem, mēģinām dalīt reizinātājos tā, lai katram reizinātājam (111 utml.) būtu viegli atrodama 3-valuācija.

Apgalvojums 1: Doti divi veseli skaitļi x un y un arī naturāls skaitlis $n \in \mathbb{N}$. Dots arī pirmskaitlis p (var būt arī $p = 2$). Izpildās šādi nosacījumi:

- n nedalās ar p.
- x, y nedalās ar p.
- $x - y$ dalās ar p.

Tad izpildās vienādība:

$$\nu_p(x^n - y^n) = \nu_p(x - y).$$

Piemērs 1: $x = 10$, $y = 1$, $n = 7$, bet $p = 3$. Tad skaitlis $x^7 - y^7 = 10^7 - 1^7 = 9999999$ dalās ar $3^2 = 9$, bet nedalās ar $3^3 = 27$. (Tāpat kā skaitlis $x - y = 10 - 1 = 9$.)

Pierādījums: Apgalvojumu 1 pierāda, sadalot $x^n - y^n$ reizinātājos. Un tad pamatojot, ka summa

$$x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} \equiv nx^{n-1}$$

nedalās ar p. □

Apgalvojums 2: Doti divi veseli skaitļi x un y un arī naturāls skaitlis $n \in \mathbb{N}$. Dots arī pirmskaitlis p (var būt arī $p = 2$). Izpildās šādi nosacījumi:

- n ir nepāra skaitlis.
- n nedalās ar p.
- x, y nedalās ar p.
- $x - y$ dalās ar p.

Tad izpildās vienādība:

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

Piemērs 2: $x = 10$, $y = 1$, $n = 7$, bet $p = 11$. Tad skaitlis $x^7 + y^7 = 10^7 + 1^7 = 10000001$ dalās ar $11^1 = 11$, bet nedalās ar $11^2 = 121$. (Tāpat kā skaitlis $x + y = 11$.)

Turpmākajos piemēros nometam prasību, ka n nedalās ar p. Toties papildus prasām, lai pirmskaitlis p būtu nepāra skaitlis. Ir spēkā vairākas kāpinātāja pacelšanas lemmas:

Pierādījums: Apgalvojumu 2 pierāda, ievietojot y vietā $-y$ un lietojot iepriekšējo Apgalvojumu 1. □

Lemma 1 (Lifting the Exponent, LTE): Doti divi veseli skaitļi x un y un arī naturāls skaitlis $n \in \mathbb{N}$. Dots arī **nepāra** pirmskaitlis p. Izpildās šādi nosacījumi:

- x, y nedalās ar p.
- $x - y$ dalās ar p.

Tad izpildās vienādība:

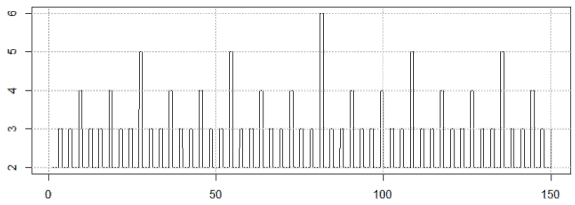
$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$

Piemērs 3: $x = 10$, $y = 1$, $n = 27$, bet $p = 3$. Tad skaitlis

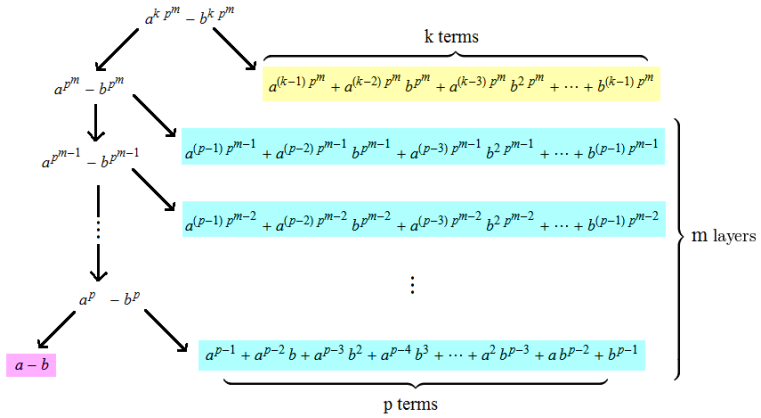
$$x^{27} - y^{27} = 10^7 - 1^7 = 999999999\,999999999\,999999999$$

dalās ar 3^k pie $k = \nu_3(10 - 1) + \nu_3(27) = 2 + 3 = 5$ (t.i. dalās ar $3^6 = 243$). Bet šis skaitlis nedalās ar 3^{k+1} (t.i. ar $3^6 = 729$).

Aplūkojot jebkādas n vērtības, iegūstam grafiku funkcijai $f(n) = \nu_3(10^n - 1)$, t.i. ar kādu augstāko trijnieka pakāpi dalās skaitlis "n deviņnieki":



Pierādījums: Lemmu 1 pierāda, atkārtoti dalot reizinātājos izteiksmi $x^n - y^n$, kur var izteikt $n = k \cdot p^m$ (kur k nedalās ar p):



Piemērs: Ar kādu lielāko skaitļa 41 pakāpi dalās šāds skaitlis:

$$\underbrace{9999\ldots9999}_{8405 \text{ deviņnieki}}.$$

Risinājums: Citiem vārdiem, mums jāatrod $\nu_{41}(10^{8405}-1)$. Dalām reizinātājos $8405 = 5 \cdot 41^2$.

Lemmu 1 nevar pielietot uzreiz izteiksmei $10^{5\cdot 41^2} - 1^{5\cdot 41^2}$, jo $10-1$ nedalās ar 41. Par laimi, jau $99999 = 10^5 - 1$ dalās ar 41. Pārveidojam izteiksmi:

$$\nu_{41}(10^{5\cdot 41^2} - 1^{5\cdot 41^2}) = (100000^{41^2} - 1^{5\cdot 41^2}) = \nu_{41}(10000-1) + \nu_{41}(41^2) = 3.$$

Tātad minētais skaitlis dalās ar 41^3 (bet nedalās ar lielāku 41 pakāpi).

Piemērs: Katram dotajam naturālam skaitlim $k > 0$ atrast iespējami mazu n vērtību, kurai $10^n - 1$ dalās ar 3^k, izmantojot divas dažādas metodes:

- Eilera teorēmu
- LTE Lemmu 1

Risinājums: Ievērosim, ka dotajam 3^k Eilera funkcijas vērtība ir $\varphi(3^k) = 3^k - 3^{k-1}$. Pēc Eilera teorēmas, skaitlis $10^{\varphi(3^k)} - 1$ garantēti dalīsies ar 3^k. Savukārt pēc kāpinātāja pacelšanas lemmas mums vajag lai $\nu_3(10-1) + \nu_3(n)$.

Apkoposim iegūtās vērtības tabulā (skaitļus formā $10^n - 1$, kas dalās ar vajadzīgo 3 pakāpi):

k	1	2	3	4	5	5
Eilera teorēma	10^1-1	10^6-1	$10^{18}-1$	$10^{54}-1$	$10^{162}-1$	$10^{486}-1$
LTE Lemma	10^1-1	10^1-1	10^3-1	10^9-1	$10^{27}-1$	$10^{81}-1$

Kā redzam tabulā, LTE Lemma dod daudz precīzāku novērtējumu; atrastās n vērtības tiešām ir minimālās, kam $10^n - 1$. Savukārt Eilera teorēma piedāvā sešreiz lielāku skaitli, kurš arī der un $10^n - 1$ dalās ar 3^k, bet tas var nebūt mazākais. Šajā piemērā tas pat vienmēr ir sešreiz lielāks nekā LTE dotais novērtējums.

Lemma 2 (Lifting the Exponent, LTE): Doti divi veseli skaitļi x un y un arī naturāls skaitlis $n \in \mathbb{N}$. Dots arī **nepāra** pirmskaitlis p. Izpildās šādi nosacījumi:

- n ir nepāra skaitlis.
- x, y nedalās ar p.
- $x + y$ dalās ar p.

Tad izpildās vienādība:

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

Piemērs 4: $x = 10$, $y = 1$, $n = 121$, bet $p = 11$. Tad skaitlis

$$x^{121} + y^{27} = 10^{121} + 1^{121} = 1\underbrace{00\ldots00}_{120\text{ nulles}}1$$

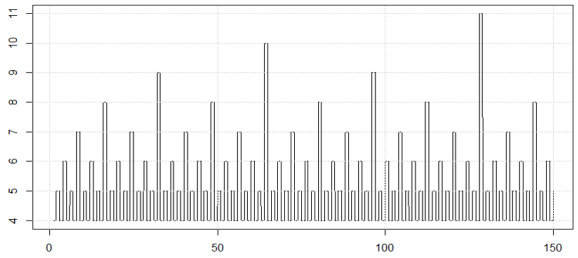
dalās ar 11^k pie $k = \nu_{11}(10 + 1) + \nu_{11}(121) = 1 + 2 = 3$ (t.i. dalās ar $11^3 = 1331$). Bet šis skaitlis nedalās ar 11^{k+1} (t.i. ar $11^4 = 14641$).

Pierādījums: Lemmu 2 pierāda, aizstājot y ar $(-y)$ un izmantojot iepriekšējo Lemmu 1. (Šeit ir būtiski, lai n ir nepāra; lai gan pats y, gan arī $(-y)^n$ maina zīmi. □

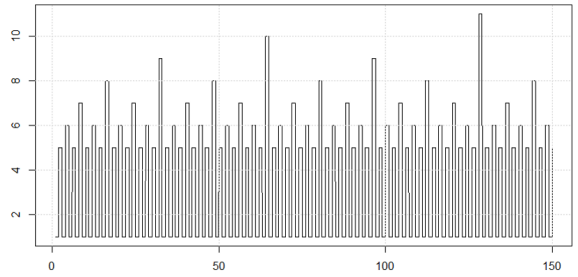
5.3.2 Valuācijas pirmskaitlim 2

Uzdevums (Valsts4Posms-1993.9-12.2): Dots naturāls skaitlis $a > 2$. Pierādīt, ka eksistē tikai galīgs skaits tādu naturālu n, ka $a^n - 1$ dalās ar 2^n.

Izvēlamies "patvaļīgu" naturālu skaitli $a = 17$. Apskatīsim $17^n - 1$ dalāmību ar 2 pakāpēm – ieviešam funkciju $f(n) = \nu_2\left(17^n - 1\right)$.



Salīdzināsim šo ar citu naturālu skaitli $a = 15$. Līdzīgi kā iepriekš apskatām funkciju $f(n) = \nu_2\left(15^n - 1\right)$.



Ievērosim, ka abi grafiki izturas līdzīgi nepāra vērtībām n. Tie sakrīt ar $\nu_2(n)$ grafiku, kas pabīdīts 4 vienības uz augšu. Toties pie nepāra n uzvedības atšķiras: $\nu_2\left(17^n - 1\right) = 4$ un $\nu_2\left(15^n - 1\right) = 1$.

Lemma 3 (Lifting the Exponent, LTE): Skaitļi x un y ir divi veseli nepāra skaitļi un n ir pozitīvs **pāra** skaitlis. Tad

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

Ja savukārt n ir pozitīvs **nepāra** skaitlis, tad

$$\nu_2(x^n - y^n) = \nu_2(x - y).$$

5.3.3 Skaitliski piemēri

1.jautājums: Ar cik nullēm beidzas skaitlis 2022! (2022 faktoriāls, t.i. visu skaitļu no 1 līdz 2022 reizinājums)?

2.jautājums: Ar kādu lielāko skaitļa 2 pakāpi dalās kombinācija C_{2022}^{415}?

3.jautājums: Atrast mazāko k vērtību, kurai $11^k - 1$ beidzas ar 4 nullēm.

4.jautājums: Atrast 5-valuāciju reizinājumam

$$(2-1)\cdot(2^2-1)\cdot(2^3-1)\cdot\ldots\cdot(2^{1000}-1).$$

5.jautājums: Atrast 7-valuāciju reizinājumam

$$(2-1)\cdot(2^2-1)\cdot(2^3-1)\cdot\ldots\cdot(2^{1000}-1).$$

6.jautājums: Neizmantojot Kummera teorēmu (bet izmantojot interpretāciju) pamatot, ka C_{2012}^{17}: dalās ar 2012. (**Ieteikums:** Izmantot faktu, ka 17 un 2012 ir savstarpēji pirmskaitļi un tādēļ kombinācijām C_{2012}^{17}, ko iztēlojas kā pa apli izvietotas 2012 krellītes, no kurām tieši 17 ir nokrāsotas - būs simetriskas attiecībā pret 2012 pagriezieniem ap apļa centru.)

Diemžēl, šo nevar izspriest otrādi. No tā, ka k un 2012 ir kopīgi dalītāji vēl neseko, ka C_{2012}^{17} nedalās ar 2012.

```
>>> bin(2022)
'0b11111100110'
>>> bin(415)
'0b110011111'
>>>
```

5.4 Sacensību uzdevumi

1.Uzdevums: Pamatot, ka harmoniskas rindas pirmo n locekļu summa:

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{n}$$

nevar būt vesels skaitlis, ja $n > 1$.

2.Uzdevums (CGMO2012.8) Cik kopā $\{0, 1, 2, \ldots, 2012\}$ ir elementu k, kam C_{2012}^{k}: dalās ar 2012? Ar C_n^k apzīmējam kombinācijas no n pa k jeb

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Ieteikumi:

- Sadalām reizinātājos: $2012 = 2^2 \cdot 503$
- Ievērojam, ka $503 \mid C_{2012}^{k}$ tad un tikai tad, ja 503 nedala k.
- Ievērojam, ka $4 \mid C_{2012}^{k}$ tad un tikai tad, ja saskaitot binārajā pierakstā k un $2012-k$ rodas vismaz divi pārnesumi (Kummera teorēma).

3.Uzdevums (IMO2019.P4) Atrast visus naturālo skaitļu (k, n) pārus, kuriem izpildās

$$k! = (2^n-1)(2^n-2)(2^n-4)\cdots(2^n-2^{n-1}).$$

4.Uzdevums (IMO2000.5): Vai eksistē naturāls n, ka skaitlim n ir tieši 2000 dalītāji, kuri ir pirmskaitļi, un $2^n + 1$ dalās ar n. (Skaitlis n drīkst dalīties arī ar pirmskaitļu pakāpēm.)

5.Uzdevums (APMO1997.2): Atrast veselu skaitli n, kam $100 \leq n \leq 1997$, ka n dala $2^n + 2$.

6.Uzdevums (Sierpinski): Pierādīt, ka nevienam $n > 1$ neizpildās

$$n \mid 2^{n-1} + 1.$$

7.Uzdevums (IMO1990.3): Noteikt visus veselos skaitļus $n > 1$, kam $\frac{2^n+1}{n^2}$ ir vesels skaitlis.

8.Uzdevums (BW2015.16): Ar $P(n)$ apzīmējam lielāko pirmskaitli, ar ko dalās n. Atrast visus naturālos skaitļus $n \geq 2$, kam

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

9.Uzdevums (BW2015.17): Atrast visus naturālos skaitļus n, kuriem $n^{n-1} - 1$ dalās ar 2^{2015}, bet nedalās ar 2^{2016}.

Ieteikumi: Apzīmēsim virkni $a_n = \nu_2(n^{n-1} - 1)$. Pamatot, ka $a_n = 2\nu_2(n-1) + \nu_2(n+1) - 1$.

10.Uzdevums (Valsts4Posms-1992.12.1): Pierādīt, ka eksistē bezgalīgi daudz naturālu skaitļu kvadrātu, kurus var iegūt, divas reizes pēc kārtas uzrakstot kādu naturālu skaitli.

Ieteikumi: Divreiz uzrakstāmos skaitļus var mērķtiecīgāk meklēt, ja mēģina dalīt reizinātājos izteiksmi $10^n + 1$. Dalītāji 101, 1001, 10001 utt. parādās tad, ja aplūko divreiz pēc kārtas uzrakstītus skaitļus, piemēram, 1212, 123123, 12341234. Savukārt, $10^n + 1$ labi dalās reizinātājos, ja aplūko, teiksim, $\nu_{11}(10^n + 1)$. Atkārtojamo ciparu skaitu n var pielāgot tā, lai $10^n + 1$ dalītos ar to, ko mums vajag.

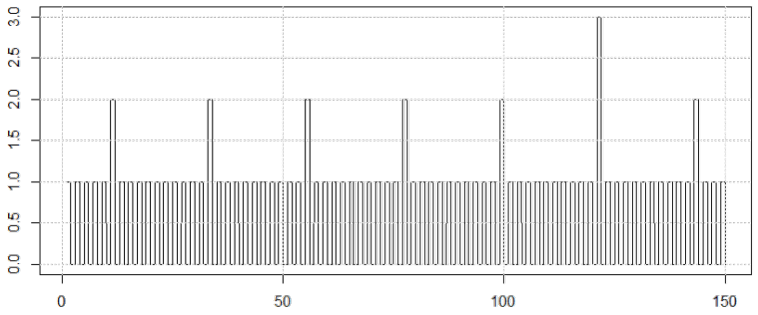


Fig. 4: Grafiks funkcijai $f(n) = \nu_{11}(10^n + 1)$ (Kāpinātāja Pacelšanas Lemma 2)

5.5 Atsauces

1. https://cp4space.hatsya.com/2014/04/13/lifting-the-exponent/.
2. https://bit.ly/3KdtxBH.
3. http://artofproblemsolving.com/articles/files/SatoNT.pdf.
4. http://www.aquatutoring.org/KummerTheoremLucasTheorem.pdf.
5. http://reu.dimacs.rutgers.edu/~mslusky/.

NMS SKAITĻU TEORIJA #6: RACIONĀLI UN IRACIONĀLI SKAITĻI

Veselā daļa: Apakšējās veselās daļas funkcija $f(x) = \lfloor x \rfloor$, tās īpašības.

Iracionalitātes pierādījumi: Sakņu un logaritmu iracionalitāte, skaitļa e iracionalitāte, skaitļa decimālpieraksta aplūkošana, algebriskas metodes. Tuī-Morzes virkne.

Iracionāli skaitļi kā robežas: Piemēri, kad racionālas izteiksmes robežpārejā dod iracionālus rezultātus. Permutāciju skaitīšanas uzdevums; rekurentu virkņu attiecības. Ķēžu daļas.

Iracionālu izteiksmju vienkāršošanās: Kad iracionalitāte ļauj atrast racionālus rezultātus.

Fareja virknes un tuvinājumi: Konstruēt Fareja virknes; racionālu skaitļu mediānas. Iracionālu skaitļu tuvināšana.

6.1 Veselā daļa

Kā ievadmateriālu pirms racionālajiem/iracionālajiem skaitļiem aplūkojam skaitļu teorijā svarīgu funkciju: apakšējo veselo daļu un tai radniecīgas funkcijas.

Definīcija: Katram $x \in \mathbb{R}$ *apakšējā veselā daļa* (floor function) ir lielākais veselais skaitlis, kas nepārsniedz x. To apzīmē $\lfloor x \rfloor$.

Note: Dažreiz literatūrā izmanto arī apzīmējumu $[x]$; to dažreiz izmanto, jo kvadrātiekavas ir ērtāk ievadīt datorā nekā speciālos simbolus $\lfloor \ldots \rfloor$, bet šajā tekstā to neizmantojam, jo kvadrātiekavas bieži lietojamas citiem apzīmējumiem.

Definīcija: Par skaitļa $x \in \mathbb{R}$ *daļveida daļu* (*fractional part*) sauc vērtību, par kuru skaitlis x pārsniedz savu veselo daļu:

$$\{x\} = x - \lfloor x \rfloor.$$

Definīcija: Par skaitļa *augšējo veselo daļu* (*ceiling function*) sauc mazāko veselo skaitli, kas nav mazāks par x. To apzīmē ar $\lceil x \rceil$.

Piemēri:

$$\begin{aligned} \lceil 3.5 \rceil = 4, \quad \lfloor 3.5 \rfloor = 4, \\ \lceil -1.5 \rceil = -1, \quad \lfloor 3.5 \rfloor = -2, \\ \lceil 17 \rceil = 17, \quad \lfloor 17 \rfloor = 17, \\ \{3.14\} = 0.14, \quad \{-3.14\} = 0.86, \quad \{17\} = 0, \\ \lceil 0.9999\ldots \rceil = 1, \quad \lfloor 0.9999\ldots \rfloor = 1, \end{aligned}$$

Pēdējā piemērā skaitlis $0.9999\ldots = 0.(9) = 1$ ir vesels, tāpēc tā veselā un daļveida daļa sakrīt.

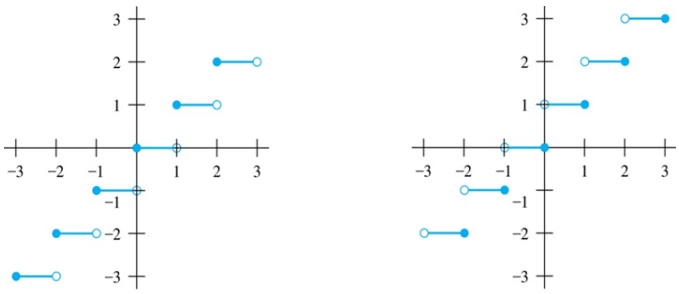


Fig. 1: Grafikos attēlotās funkcijas $y = \lfloor x \rfloor$ un $y = \lceil x \rceil$ un

Teorēma: Patvaļīgam reālam skaitlim $x \in \mathbb{R}$ un veselam skaitlim $n \in \mathbb{Z}$ ir spēkā šādi apgalvojumi:

1. Ir spēkā loģiskas ekvivalences (var secināt abos virzienos):

- $\lfloor x \rfloor = n$ tad un tikai tad, ja $n \leq x < n + 1$.
- $\lceil x \rceil = n$ tad un tikai tad, ja $n - 1 < x \leq n$.
- $\lfloor x \rfloor = n$ tad un tikai tad, ja $x - 1 < n \leq x$.
- $\lceil x \rceil = n$ tad un tikai tad, ja $x \leq n < x + 1$.

2. $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.
3. $\lfloor -x \rfloor = -\lceil x \rceil$ un $\lceil -x \rceil = -\lfloor x \rfloor$.
4. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ un $\lceil x + n \rceil = \lceil x \rceil + n$.
5. Ja $a = qb + r$ ir veselu skaitļu a un b dalījums ar atlikumu un $b > 0$, tad šo skaitļu dalījums $q = \left\lfloor \frac{a}{b} \right\rfloor$ un atlikums $r = \left\{ \frac{a}{b} \right\} \cdot b$.
6. Funkcija $f(x) = \left\lfloor x + \frac{1}{2} \right\rfloor$ izsaka reāla skaitļa $x \in \mathbb{R}$ noapaļošanu pēc skolas algoritma – noapaļo līdz tuvākajam veselajam skaitlim (un tad, ja daļveida daļa ir precīzi puse, tad apaļo uz augšu).
7. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
8. Skaitļa n pozitīvo daudzkārtņu skaits, kas nepārsniedz x, ir $\left\lfloor \frac{x}{n} \right\rfloor$.
9. $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$.

Piemērs: Dots reāls skaitlis x. Pierādīt, ka $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Pierādījums: Apzīmējam $x = n + \varepsilon$, kur n ir vesels skaitlis un $0 \leq \varepsilon < 1$.

1.gadījums: $\varepsilon < \frac{1}{2}$. Tad $2x = 2n + 2\varepsilon$ un $\lfloor 2x \rfloor = 2n$, jo $0 \leq 2\varepsilon < 1$.

Savukārt $\lfloor x \rfloor = \lfloor x + \frac{1}{2} \rfloor = n$, jo $x + \frac{1}{2} = n + (\frac{1}{2} + \varepsilon)$ un $0 \leq \frac{1}{2} + \varepsilon < 1$.

Tātad, $\lfloor 2x \rfloor = 2n$ un $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + n = 2n$.

2.gadījums: $\varepsilon \geq \frac{1}{2}$.

Tad $2x = 2n + 2\varepsilon = (2n + 1) + (2\varepsilon - 1)$ un $\lfloor 2x \rfloor = 2n + 1$, jo $0 \leq 2\varepsilon - 1 < 1$.

Savukārt $\lfloor x \rfloor = n$, bet $\lfloor x + \frac{1}{2} \rfloor = \lfloor n + (1/2 + \varepsilon) \rfloor = \lfloor n + 1 + (\varepsilon \breve{} \frac{1}{2}) \rfloor = n + 1$. Tātad, $\lfloor 2x \rfloor = 2n + 1$ and $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + (n + 1) = 2n + 1$.

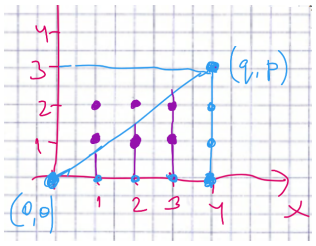
Piemērs (Ermīta identitāte, Hermite identity): Pierādīt, ka ikvienam reālam skaitlim $x \in \mathbb{R}$ ir spēkā vienādība

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{3} \right\rfloor + \left\lfloor x + \frac{2}{3} \right\rfloor = \lfloor 3x \rfloor.$$

Piemērs (Gauss): Divi naturāli skaitļi p un q ir savstarpēji pirmskaitļi. Pierādīt sekojošu sakarību:

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \ldots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

Risinājums: Varam novilkt taisni $y = \frac{p}{q} \cdot x$. Šī taisne iet caur diviem punktiem $(0;0)$ un $(q;p)$, bet tā kā p, q ir savstarpēji pirmskaitļi, uz tās nav citu punktu ar abām veselām koordinātēm.



Tad katrs saskaitāmais $\left\lfloor \frac{k \cdot p}{q} \right\rfloor$ izsaka veselo punktu skaitu zem šīs taisnes, bet virs x ass. Visu šādu punktu skaitu var noteikt vai nu izmantojot Pīka formulu, sk. https://bit.ly/3JL3scm, vai arī uzliekot trijstūra formas režģim virsū otrādi apgrieztu identisku trijstūri un saskaitot punktus abos trijstūros kopā.

Note: Šo identitāti var vispārināt arī citām vērtībām;

Piemērs: Atrast mazāko naturālo skaitli k, pie kura vienādojumam

$$\left\lfloor \frac{2021}{n} \right\rfloor = k$$

nav atrisinājuma veselos skaitļos.

Piemērs: Reāls skaitlis r apmierina attēlā doto vienādību.

$$\left\lfloor r + \frac{19}{100} \right\rfloor + \left\lfloor r + \frac{20}{100} \right\rfloor + \left\lfloor r + \frac{21}{100} \right\rfloor + \ldots + \left\lfloor r + \frac{91}{100} \right\rfloor = 546.$$

Atrast $\lfloor 100r \rfloor$.

Piemērs: Definējam augošu virkni $a_1, a_2, \ldots$, kas satur visus tos naturālos skaitļus, kas nav pilni kvadrāti:

$$a_1 = 2,\ a_2 = 3,\ a_3 = 5,\ a_4 = 6,\ a_5 = 7,\ a_6 = 8,\ a_7 = 10, \ldots$$

Pierādīt, ka šīs virknes locekļus var aprēķināt ar formulu

$$a_n = n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor.$$

Piemērs: Definējam virkni $b_1, b_2, \ldots$:

$$b_1 = 1,\ b_2 = 2,\ b_3 = 2,\ b_4 = 3,\ b_5 = 3,\ b_6 = 3,\ b_7 = 4, \ldots$$

Šo virkni konstruē, iekļaujot tajā naturālu skaitli $k = 1, 2, 3, \ldots$ precīzi k reizes $(1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, \ldots)$. Pierādīt, ka šīs virknes locekļus var aprēķināt ar formulu:

$$b_n = \left\lfloor \sqrt{2n} + \frac{1}{2} \right\rfloor.$$

Virknes sākuma aprēķina paraugs:

```
>>> import math
>>> [math.floor(math.sqrt(2*n) + 1/2) for n in range(1,29)]
[1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 7, 7]
```

6.2 Iracionāli skaitļi

6.2.1 Atkārtojums par skaitļu kopām

Definīcija: Aprakstām šādas skaitļu kopas: $\mathbb{Z}^{0+}$ (veselie nenegatīvie skaitļi); $\mathbb{N}$ (naturālie skaitļi); $\mathbb{Z}$ (veselie skaitļi); $\mathbb{Q}$ (racionālie skaitļi).

- Veselie nenegatīvie skaitļi $\mathbb{Z}^{0+} = \{0, 1, 2, \ldots\}$ satur skaitļus 0, 1, šajā kopā vienmēr var veikt saskaitīšanu un reizināšanu. Naturālie skaitļi $\mathbb{N} = \mathbb{Z}^{+}$ nesatur nulli.
- Veselie skaitļi $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ var veikt saskaitīšanu, reizināšanu un atņemšanu.
- Racionālie skaitļi $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z} \wedge q \in \mathbb{N}\}$. Tā ir mazākā skaitļu kopa, kas satur skaitļus 0 un 1, kurā var veikt visas četras aritmētiskās darbības (izņēmums: nevar dalīt ar 0, jo reizināšana ar nulli zaudē informāciju – šī darbība nav injektīva.).

Racionālie skaitļi ir praktiska un ērta skaitļu kopa:

- Ar efektīviem algoritmiem racionālus skaitļus var saskaitīt, atņemt, reizināt, dalīt, salīdzināt.
- Racionāliem skaitļiem eksistē ērts galīgs pieraksts, tos viegli glabāt datora atmiņā (jāvar saīsināt daļas; nereti glabājas tuvinājumi)

6.2.2 Reālie skaitļi

Vēl viena svarīga skaitļu kopa ir $\mathbb{R}$ – reālie skaitļi. To parsti saista ar ģeometriskiem objektiem. piemēram, atzīmējot uz taisnes divus punktus – sākumpunktu un vienības nogriezni – jebkurš punkts uz šīs taisnes ir reāls skaitlis.

Bez visiem racionālajiem skaitļiem reālo skaitļu taisne satur arī iracionālus skaitļus. Kādēļ vajadzīgi arī iracionālie skaitļi?

- Ģeometrijā daudzi svarīgi attālumi nav racionāli, bet izsakāmi, piemēram, ar kvadrātsaknēm.
- Arī algebrā saknes, eksponentfunkcijas, logaritmi, trigonometriskās funkcijas visbiežāk pieņem iracionālas vērtības.
- Racionālu skaitļu virkņu robežas mēdz būt iracionālas.

Piemērs: Veidosim virkni, ko veido skaitļa π decimālpieraksta sākumgabali:

$$3,\ 3.1,\ \ 3.14,\ \ 3.141,\ \ 3.1415,\ \ 3.14159,$$

Katrs loceklis šajā virknē ir racionals skaitlis: $\frac{3}{1}, \frac{31}{10}, \frac{314}{100}, \ldots$, bet pati virknes robeža ir iracionāls skaitlis.

Racionālu skaitli parasti attēlo kā racionālu daļu $\frac{p}{q}$. Dažreiz ir vairāki pieraksti, bet var pārveidot saīsinātā formā un veikt visas darbības.

Savukārt iracionāla skaitļa attēlošana ir krietni sarežģītāks jautājums. Ko nozīmē, ka mūsdienu matemātikā pazīstamas iracionālas konstantes $\pi = 3.1415926535\ldots$, $\sqrt{2} = 1.4142135\ldots$ vai $e = 2.7182818284\ldots$? Vai šīs konstantes kāds ir precīzi izrēķinājis? Vai tās vispār var izrēķināt?

Konstruējami reālie skaitļi: Reālus skaitļus α reizēm var definēt, norādot algoritmu, kas saņemot ciparu skaitu n, izrēķina racionālu tuvinājumu: $a_n \in \mathbb{Q}$, kuram $|a_n - \alpha| < 10^{-n}$.

Matemātikā pazīstamās konstantes (e, $\sqrt{2}$ utml.) ir šādi konstruējamas. No otras puses, var pamatot, ka lielais vairums iracionālo skaitļu nav konstruējami (bezgalīgi tuvināmi ar kaut kādu algoritmu).

Ir iespējamas arī "nekonstruktīvas" definīcijas, kas definē reālus skaitļus kā bezgalīgas decimālas vai racionālu skaitļu Košī virknes. (Ir pazīstami arī reālu skaitļu apraksti, izmantojot ts. Dedekinda šķēlumus, bet tos šajā kursā neaplūkojam).

Ja reālus skaitļus pieraksta kā decimāldaļas, ir vienkāršs un praktisks kritērijs, kā atšķirt racionālos no iracionālajiem.

Teorēma: Skaitlis $\alpha \in [0; 1)$ ir racionāls tad un tikai tad, ja tā decimālpieraksts bezgalīgas daļas veidā ir periodisks, sākot no kaut kādas vietas. Formāli runājot, skaitli pierakstot kā bezgalīgu decimāldaļu

$$\alpha = 0.d_1d_2d_3d_4d_5d_6\ldots$$

eksistē priekšperioda garums $k \in \mathbb{Z}^{0+}$ un eksistē periods $T \in \mathbb{N}$, ka visiem $n > k$ ir spēkā $d_{n+T} = d_n$.

Note: Priekšperioda garums var būt arī 0. Tad bezgalīgo decimāldaļu sauc par *tīri periodisku*: Tūlīt aiz decimālpunkta sākas pirmais periods.

Note: Dažus racionālus skaitļus var pierakstīt kā galīgas decimāldaļas. Bet arī uz tām attiecas augšminētā teorēma. Piemēram, galīgu decimāldaļu 0.5 var pārveidot par bezgalīgu decimāldaļu – turklāt pat divos dažādos veidos:

$$0.5 = 0.50000000000\ldots = 0.49999999999\ldots$$

Abām šīm daļām priekšperioda garums $k = 1$ un arī perioda garums ir $T = 1$. Vidusskolas matemātikas kursā deviņniekus periodā parasti neraksta, jo šāds pieraksts var radīt pārpratumus. Piemēram, apraujot bezgalīgo ciparu virkni, var rasties aplams priekšstats, ka $0.4999999\ldots < \frac{1}{2}$, pat ja patiesībā abas daļas ir skaitliski vienādas.

Apgalvojums: Racionālam skaitlim $\frac{p}{q}$ bezgalīgajā decimālpierakstā nav priekšperioda tad un tikai tad, ja daļas saucējs q nesatur pirmreizinātājus 2 vai 5.

Apgalvojums: Racionālu skaitli $\frac{p}{q}$ pieraksta kā galīgu decimāldaļu (citiem vārdiem, kā bezgalīgu decimāldaļu ar periodu, kas sastāv tikai no nullēm vai tikai no deviņniekiem) tad un tikai tad, ja daļas saucējs $q = 2^a5^b$, t.i. saucējs satur tikai pirmreizinātājus 2 vai 5.

6.2.3 Iracionalitātes pierādījumi

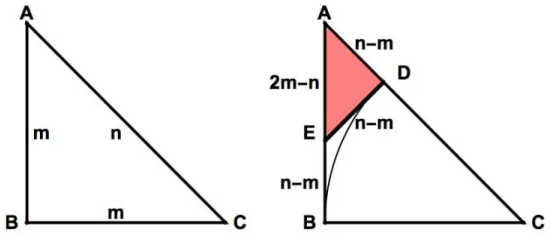
6.2.4 Saknes

Apgalvojums: Jebkuriem naturāliem skaitļiem a un n vai nu $\sqrt[n]{a}$ ir naturāls skaitlis, vai arī tas ir iracionāls skaitlis.

Pierādījums: Pietiek pārbaudīt, ka neviena sakne nevar būt racionāla daļa, kas nav vesela. No pretējā: Pieņemam, ka $\sqrt[n]{a} = \frac{P}{Q}$. Ja daļa $\frac{P}{Q}$ ir nesaīsināma, tad kāpinot katru skaitli n-tajā pakāpē, arī daļa $a = \frac{P^n}{Q^n}$ būs nesaīsināma, turklāt $Q^n \neq 1$, jo arī $Q \neq 1$. Pretruna, jo ir dots, ka a ir vesels.

Secinājums: Kvadrātsaknes $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \ldots$ (no skaitļiem, kuri nav pilni kvadrāti) visas ir iracionāli skaitļi.

Kvadrātsakņu iracionalitātei iespējami arī ģeometriski pierādījumi (pagaidām nav zināms labs piemērs, kad iracionalitāti vieglāk pierādīt, izmantojot ģeometrisku konstrukciju nevis algebras vai skaitļu teorijas metodes par pirmreizinātājiem utml.)



Apgalvojums: Skaitlis $\sqrt{2}$ ir iracionāls.

Pierādījums: Pieņemsim, ka $\sqrt{2} = \frac{n}{m}$. Tādā gadījumā $m^2 + m^2 = n^2$ un pēc Pitagora teorēmas eksistē vienādsānu taisnleņķa trijstūris ar katešu garumiem m un hipotenūzu $|AC| = n$. Pieņemsim, ka skaitļi m un n ir mazākie veselie skaitļi, kuriem var izveidot šādu trijstūri.

Ap punktu C ar rādiusu m velkam riņķa līniju, kas krusto hipotenūzu AC punktā D. Šajā punktā velkam pieskari riņķa līnijai - tā ir perpendikulāra nogrieznim AC (riņķa rādiusam), un krusto kateti AB punktā E.

Nogriežņu garumi $|AD| = n - m$ (jo no hipotenūzas n atšķelts nogrieznis CD garumā m). Sarkanais trijstūrītis arī ir vienādsānu taisnleņķa, tāpēc arī $|ED| = n - m$. Arī $EB = n - m$, jo EB, ED ir divas pieskares tai pašai riņķa līnijai.

Visbeidzot $|AE| = m - (n - m) = 2m - n$. Esam ieguvuši sarkano trijstūrīti $\triangle ADE$ ar veseliem malu garumiem, kam arī hipotenūzas attiecība pret kateti ir $\sqrt{2}$, bet malu garumi ir mazāki nekā sākotnējā trijstūrī ABC. Pretruna ar pieņēmumu, ka n un m ir mazākās veselās katetes, kuru attiecība ir $\sqrt{2}$. □.

Sk. pierādījuma publikāciju *American Mathematical Monthly* https://bit.ly/3ug0Uwp (Tom M. Apostol. Vol. 107, No. 9 (Nov., 2000), pp. 841-842)

6.2.5 Logaritmi

Apgalvojums: $\log_2 3$ ir iracionāls skaitlis.

Piemērs: Pamatot, ka $\log_2 10 \approx 3.321928\ldots$ ir iracionāls.

```
>>> import math
>>> math.log2(10)
3.321928094887362
```

Pierādījums: Pieņemsim no pretējā, ka $\log_2 10 = \frac{P}{Q}$, kur P, Q ir naturāli skaitļi un daļa ir nesaīsināma. Pēc logaritma definīcijas:

$$2^{P/Q} = 10 \text{ jeb } 2^P = 10^Q.$$

Pēdējā vienādība nevar izpildīties, ja $P, Q > 0$, jo skaitļa 10 pozitīvas pakāpes dalās ar 5, bet skaitļa 2 pakāpes ar 5 nedalās.

Piemērs: Vērtība $\log_2 10$ rāda, par cik jāpalielina kāpinātājs, lai pakāpe 2^n palielinātos 10 reizes.

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1024$
$2^{11} = 2048$
$2^{12} = 4096$
$2^{13} = 8192$
$2^{14} = 16384$
$2^{15} = 32768$
$2^{16} = 65536$
$2^{17} = 131072$
$2^{18} = 262144$
$2^{19} = 524288$
$2^{20} = 1048576$
$2^{21} = 2097152$
$2^{22} = 4194304$
$2^{23} = 8388608$
$2^{24} = 16777216$
$2^{25} = 33554432$
$2^{26} = 67108864$
$2^{27} = 134217728$
$2^{28} = 268435456$
$2^{29} = 536870912$

Šī logaritma $\log_2 10 \in (3; 4)$ iracionalitāte parāda, ka reizēm trīs, reizēm četras divnieka pakāpes ir ar vienu un to pašu ciparu skaitu, bet ciparu skaita pieaugums neveido "prognozējamu ritmu".

Apgalvojums: Naturālā skaitļa n decimālpierakstā ciparu skaits ir tieši $\lfloor \log_{10} n \rfloor + 1$.

Piemērs: Atrast skaitļa 2 pakāpes, kuru decimālpierakstā ir tieši 300 cipari.

Atrisinājums: Šīs pakāpes ir 2^{994}, 2^{995} un 2^{996}.

```
>>> import math
>>> math.floor(math.log10(2**994))
300
>>> math.floor(math.log10(2**995))
300
>>> math.floor(math.log10(2**996))
300
```

Piemērs: Pamatot, ka logaritms $\log_{32} 8$ ir racionāls skaitlis.

Apgalvojums: Jebkuriem naturāliem a, b $(a > 1)$ logaritms $\log_a b$ ir iracionāls, ja vien a un b nav tā paša skaitļa divas veselas pakāpes.

Piemērs: Uzrakstīt attēlā redzamās izteiksmes vērtību kā racionālu skaitli $\frac{p}{q}$.

$$\frac{2}{\log_4 2000^6} + \frac{3}{\log_5 2000^6}.$$

6.2.6 Iracionalitātes pierādījumi no pretējā

Piemērs: Skaitļa a decimālpierakstu veido, izrakstot aiz komata visu naturālo skaitļu ciparus:

$$\alpha = 0.12345678910111213141516171819\ldots$$

Pierādīt, ka α ir iracionāls.

Definīcija: Skaitlis e (saukts arī *eksponente* vai *naturālo logaritmu bāze*) apzīmē šādas rindas summu:

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots = \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \ldots = 2.71828\,18284\,59045\,23536\ldots$$

Apgalvojums: Skaitlis e ir iracionāls.

Pierādījums: No pretējā. Pieņemam, ka $e = \frac{a}{b}$. Aplūkojam izteiksmi:

$$E = b!\left(e - \left(1 + 1 + \frac{1}{2!} + \ldots + \frac{1}{b!}\right)\right).$$

Pēc pieņēmuma šis skaitlis ir vesels, jo skaitlis e ir pareizināts ar b daudzkārtni; un arī visi faktoriāli, kas ir mazāki par $b!$ ir noīsinājušies.

No otras puses, šī starpība ir visa atlikusī rinda, kas ir e definīcijā:

$$\begin{aligned}
&\frac{b!}{(b+1)!} + \frac{b!}{(b+2)!} + \frac{b!}{(b+3)!} + \ldots = \\
&= \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \ldots < \\
&< \frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \ldots = \frac{1}{b}.
\end{aligned}$$

Pēdējā rindiņā lietojām bezgalīgas ģeometriskas progresijas summas formulu. Šis skaitlis ir pozitīvs, bet mazāks par 1, tātad tas ir daļskaitlis un izteiksme E (agrāk minētajā formulā) nevar būt vesela. Iegūta pretruna.

6.2.7 Algebriski pārveidojumi

Uzdevums: Vai sekojošs skaitlis ir racionāls vai iracionāls?

$$\left(\sqrt{5}+\sqrt{6}+\sqrt{7}\right)\left(-\sqrt{5}+\sqrt{6}+\sqrt{7}\right)\left(\sqrt{5}-\sqrt{6}+\sqrt{7}\right)\left(\sqrt{5}+\sqrt{6}-\sqrt{7}\right)$$

Atrisinājums: Vienkāršojam reizinājumu ar kvadrātsaknēm. Algebriskās identitātes labākas lasāmības dēļ skaitļus aizstājam ar burtiem:

$$\begin{aligned}
&\left(\sqrt{a}+\sqrt{b}+\sqrt{c}\right)\left(-\sqrt{a}+\sqrt{b}+\sqrt{c}\right)\left(\sqrt{a}-\sqrt{b}+\sqrt{c}\right)\left(\sqrt{a}+\sqrt{b}-\sqrt{c}\right) = \\
&= \left(\sqrt{a}+(\sqrt{b}+\sqrt{c})\right)\left(-\sqrt{a}+(\sqrt{b}+\sqrt{c})\right)\left(\sqrt{a}-(\sqrt{b}-\sqrt{c})\right)\left(\sqrt{a}+(\sqrt{b}-\sqrt{c})\right) = \\
&= \left((\sqrt{b}+\sqrt{c})^2-(\sqrt{a})^2\right)\left((\sqrt{a})^2-(\sqrt{b}-\sqrt{c})^2\right) = \left((\sqrt{b}+\sqrt{c})^2-a\right)\left(a-(\sqrt{b}-\sqrt{c})^2\right) = \\
&= a(\sqrt{b}+\sqrt{c})^2 + a(\sqrt{b}-\sqrt{c})^2 - a^2 - (\sqrt{b}+\sqrt{c})^2(\sqrt{b}-\sqrt{c})^2 = \\
&= a\left((\sqrt{b}+\sqrt{c})^2+(\sqrt{b}-\sqrt{c})^2\right) - a^2 - \left((\sqrt{b}+\sqrt{c})(\sqrt{b}-\sqrt{c})\right)^2 = \\
&= a\left(b+2\sqrt{b}\sqrt{c}+c+b-2\sqrt{b}\sqrt{c}+c\right) - a^2 - (b-c)^2 = \\
&= a(2b+2c) - a^2 - (b^2-2bc+c^2) = 2ab+2ac+2bc-a^2-b^2-c^2.
\end{aligned}$$

Ievietojot vērtības $a = 5$, $b = 6$, $c = 7$, iegūstam, ka izteiksmes vērtība ir

$$2 \cdot 5 \cdot 6 + 2 \cdot 5 \cdot 7 + 2 \cdot 6 \cdot 7 - 5^2 - 6^2 - 7^2 = 60 + 70 + 84 - 25 - 36 - 49 = 104.$$

Uzdevums: Visos sekojošajos piemēros pierādīt vai apgāzt apgalvojumus par racionāliem un iracionāliem skaitļiem.

(A) Vai eksistē pozitīvi iracionāli skaitļi α, β, kuriem $\alpha + \beta \in \mathbb{Q}$ un $\alpha \cdot \beta \in \mathbb{Q}$?

(B) Vai eksistē pozitīvs reāls $a \in \mathbb{R}$, kuram $a^2 \notin \mathbb{Q}$, bet $a^3 \in \mathbb{Q}$?

(C) Vai eksistē pozitīvi iracionāli skaitļi α, β, kuriem $\alpha - \beta \in \mathbb{Q}$ un $\alpha^2 - \beta^2 \in \mathbb{Q}$?

(D) Vai eksistē pozitīvi iracionāli skaitļi α, β, kuriem $\alpha + \beta \in \mathbb{Q}$ un $\alpha^3 + \beta^3 \in \mathbb{Q}$?

6.3 Dažas iracionālu skaitļu īpašības

6.3.1 Ķēžu daļas

Uzrakstām algebrisku pārveidojumu skaitlim $\sqrt{2}$:

$$\sqrt{2} = 1 + \left(\sqrt{2} - 1\right) = 1 + \frac{1}{1 + \sqrt{2}}.$$

Varam lietot šo identitāti atkārtoti un iegūt arvien garāku virkni:

$$\begin{aligned}
\sqrt{2} &= 1 + \frac{1}{1 + \sqrt{2}} = \\
&= 1 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}} = \\
&= 1 + \frac{1}{1 + 1 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}}} = \\
&= 1 + \frac{1}{1 + 1 + \frac{1}{1 + 1 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}}}} = \dots
\end{aligned}$$

Savelkot kopā vieniniekus un turpinot neierobežoti ilgi, iegūstam izteiksmi:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}}.$$

Jebkuru pozitīvu reālu skaitli $x \in \mathbb{R}^+$ var pārveidot kā šādu bezgalīgu *ķēžu daļu*. Atkārto sekojošus soļus:

1. Atrod x veselo daļu $\lfloor x \rfloor$.
2. Atņem no x šo veselo daļu: $x - \lfloor x \rfloor$.
3. Atrod skaitlim $x - \lfloor x \rfloor$ apgriezto $\frac{1}{x - \lfloor x \rfloor}$.

Ja skaitlis x ir racionāls, tad šie pārveidojumi reiz beidzas, jo pēc kāda laika izrādās, ka viens no apgrieztajiem lielumiem (kas iegūts solī #3) ir vesels skaitlis. Ja savukārt skaitlis x ir iracionāls, tad izveidojas bezgalīga ķēžu daļa.

Šeit ir piemērs, kā pārveidojas divu blakusesošu Fibonači skaitļu dalījums:

$$\frac{13}{8} = 1 + \frac{5}{8} = 1 + \frac{1}{\frac{8}{5}} = 1 + \frac{1}{1 + \frac{3}{5}} = 1 + \frac{1}{1 + \frac{1}{\frac{5}{3}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}.$$

Savukārt divu blakusesošu Fibonači skaitļu F_n un F_{n-1} attiecības robeža, ja $n \to \infty$ ir zelta attiecība, kurai ir šāda viegli iegaumējama ķēžu daļa:

$$\phi = \frac{1 + \sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}.$$

Kompaktā ķēžu daļu pierakstā nelieto daļsvītras, bet tikai pieskaitāmos skaitļus. Daži piemēri:

- $\sqrt{19} = [4; 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, ...]$. Pēc pirmā skaitļa 4 bezgalīgi atkārtojas sešu ciparu periods $2, 1, 3, 1, 2, 8$.
- $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, ...]$. Skaitļi nav periodiski, bet ik pēc trim skaitļiem tur ir pāra skaitlis, kas ir par divi lielāks nekā iepriekšējais pāra skaitlis.
- $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, ...]$. Skaitļi šajā virknē ir tikuši padziļināti pētīti, bet nekāda viegli aprakstāma likumsakarība nav konstatēta.
- $\phi = [1; 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...]$. Zelta attiecībai, kā jau redzējām, ķēžu daļa sastāv tikai no vieniniekiem.
- $\frac{13}{8} = [1; 1, 1, 1, 2]$. Visiem racionāliem skaitļiem atbilst galīgas ķēžu daļas.

Var pamatot, ka ikviena periodiska ķēžu daļa ir izteiksme ar kvadrātsaknēm (kāda kvadrātvienādojuma ar racionāliem koeficientiem atrisinājums). Augstākas pakāpes saknēm un citiem iracionāliem skaitļiem dažas ķēžu daļas ir izpētītas, bet vispārīgu likumsakarību ir maz.

6.3.2 Tuī-Morzes virkne

Definīcija: Tuī-Morzes virkni apraksta, definējot pa soļiem sekojošā veidā. Sākotnējais gabals T_0 sastāv tikai no viena cipara "0". Katru nākamo gabalu iegūst, pierakstot galā iepriekšējam kopiju, kurā visas nulles pārvērstas par vieniniekiem, bet visi vienīnieki pārvērsti par nullēm. Tiek iegūti sekojoši gabali:

$$\begin{aligned}
T_0 &= 0, \\
T_1 &= 01. \\
T_2 &= 0110. \\
T_3 &= 01101001. \\
T_4 &= 0110100110010110. \\
T_5 &= 01101001100101101001011001101001.
\end{aligned}$$

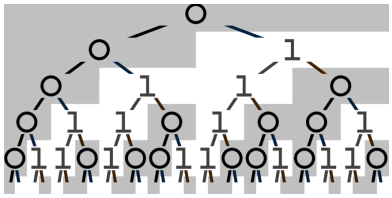
Virknes gabalam T_n ir 2^n cipari. Pati Tuī-Morzes virkne ir bezgalīga – to turpina, pierakstot arvien garākus gabalus augstākminētajā veidā.

Piemērs: Tuī-Morzes virknei ir saistīta ar ciparu summām skaitļu binārajā pierakstā.

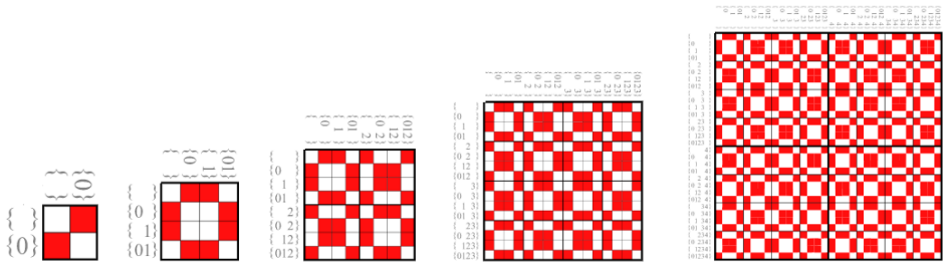
n	Binārī	Vienīnieki	T.M.virkne
0	0000	0	0
1	0001	1	1
2	0010	1	1
3	0011	2	0
4	0100	1	1
5	0101	2	0
6	0110	2	0
7	0111	3	1
8	1000	1	1
9	1001	2	0
10	1010	2	0
11	1011	3	1
12	1100	2	0
13	1101	3	1
14	1110	3	1
13	1111	4	0

Virknes n-tais loceklis t_n sakrīt ar skaitļa n binārā pieraksta ciparu summas atlikumu, dalot ar 2.

Piemērs: Tuī-Morzes virkni var ģenerēt, pārveidojot ciparus par ciparu pāriem.



Piemērs: Izrakstām kopai $\{0, 1, 2, \ldots, n-1\}$ visas iespējamās apakškopas (leksikogrāfiski sakārtotas no beigām). Iekrāsojam rūtiņu t.t.t. ja kopu A un B simetriskā starpība satur nepāru skaitu elementu: $|A \oplus B| \equiv 1 \pmod 2$.



Uzdevums: Pamatot, ka augšminētajā veidā iegūtajos 2D attēlos iegūstam Tuī-Morzes virkni T_{2n}, ja kvadrāta attēlu izraksta pa rindiņām.

Uzdevums: Pamatot, ka Tuī-Morzes virkne nevar būt periodiska (tsk. periodiska, sākot no kādas vietas). Citiem vārdiem, skaitlis, kura binārais pieraksts ir $0.0110100110010110\ldots_2$ ir iracionāls.

6.4 Racionāli tuvinājumi

6.4.1 Tuvinājumi un Dirihlē princips

Zināms, ka $\sqrt{2} \approx 1.4142135623731$. Iracionālajam skaitlim $\sqrt{2}$ viegli iedomāties racionālus tuvinājumus. Piemēram,

- $\sqrt{2} \approx 1$ ar kļūdu $0.41421\ldots$;
- $\sqrt{2} \approx 1.4$ ar kļūdu $0.01421\ldots$;
- 1.41 ar kļūdu $0.00421\ldots$; utt.

Bet $141/100$ nav optimāls racionālais tuvinājums, jo citām daļām kļūda ir vēl mazāka. Piemēram,

$$\left|\sqrt{2} - \frac{17}{12}\right| \approx 0.00245$$

Nākmajā nodaļā aplūkosim, kā labus tuvinājumus var atrast un cik labi vispār var tuvināt.

6.4.2 Labākie racionālie tuvinājumi

Teorēma: Katram pozitīvam reālam skaitlim x var atrast bezgalīgi daudzus racionālus tuvinājumus $\frac{p}{q}$ (visas tās ir nesaīsināmas daļas), kam visām izpildās nevienādība:

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Note: Šie tuvinājumi ir daudz labāki nekā, piemēram, noapaļotas decimāldaļas, jo 1.414 jeb $\frac{1414}{1000}$ tuvina $\sqrt{2}$ ar kļūdu, kas var sasniegt $\frac{1}{2000} = 0.0005$ (puse no pēdējā zīmīgā cipara vērtības). Savukārt minētā teorēma, ja pareizi izvēlas daļu saucējus, ļauj atrast daudz labākus tuvinājumus, kam precizitāte ir nevis $\frac{1}{2q}$, bet gan $\frac{1}{q^2}$; ja saucējā ir skaitlis 1000, tad labs tuvinājums atšķiras no paša skaitļa ne vairāk kā par $\frac{1}{q^2}$ jeb par $\frac{1}{1000^2} = \frac{1}{1000000}$.

Definīcija: Par n-to Fareja virkni intervālā $[0;1]$ saucam visu to racionālo skaitļu virkni $r_0, r_1, \ldots, r_N \in [0;1]$ kas uzrakstāmas nesaīsinātu daļu veidā $\frac{p}{q}$, kam saucējs $q \leq n$. Fareja virknes locekļus attēlo sakārtotus augošā secībā.

Dažas pirmās Fareja virknes:

F_1 : $\frac{0}{1}$ $\frac{1}{1}$

F_2 : $\frac{0}{1}$ $\frac{1}{2}$ $\frac{1}{1}$

F_3 : $\frac{0}{1}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{1}{1}$

F_4 : $\frac{0}{1}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{1}{1}$

F_5 : $\frac{0}{1}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{1}{2}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{1}{1}$

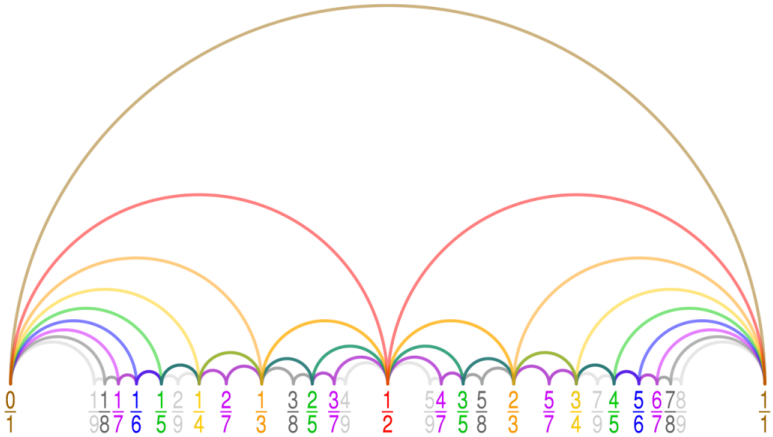
F_6 : $\frac{0}{1}$ $\frac{1}{6}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{1}{2}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{5}{6}$ $\frac{1}{1}$

F_7 : $\frac{0}{1}$ $\frac{1}{7}$ $\frac{1}{6}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{2}{7}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{3}{7}$ $\frac{1}{2}$ $\frac{4}{7}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{5}{7}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{5}{6}$ $\frac{6}{7}$ $\frac{1}{1}$

F_8 : $\frac{0}{1}$ $\frac{1}{8}$ $\frac{1}{7}$ $\frac{1}{6}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{2}{7}$ $\frac{1}{3}$ $\frac{3}{8}$ $\frac{2}{5}$ $\frac{3}{7}$ $\frac{1}{2}$ $\frac{4}{7}$ $\frac{3}{5}$ $\frac{5}{8}$ $\frac{2}{3}$ $\frac{5}{7}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{5}{6}$ $\frac{6}{7}$ $\frac{7}{8}$ $\frac{1}{1}$

Teorēma: Dotam naturālam n un Fareja virknei F_n aplūkosim divas racionālas daļas $\frac{a}{b}, \frac{c}{d} \in [0;1]$, kuras ir kaimiņi virknē F_n un pieņemsim ka $\frac{a}{b} < \frac{c}{d}$. Tad izpildās sekojoši apgalvojumi:

1. Izpildās vienādības $\frac{c}{d} - \frac{a}{b} = \frac{1}{bd}$ un $bc - ad = 1$.
2. Pirmais skaitlis (skaitlis ar vismazāko saucēju m), kuru kādā vēlākā Fareja virknē F_m iesprauž starp abām "kaimiņu" daļām $\frac{a}{b}, \frac{c}{d}$ ir abu šo daļu *mediāna*: $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.



Jautājums: Kā iegūt vislabākos (ar mazāko saucēju) racionālos tuvinājumus skaitļiem $\sqrt{2}$ un $\sqrt{5}$? Skaitļiem π un e. Kādi ir labi optimāli tuvinājumi no augšas un no apakšas?

Uzdevums: Pierādīt, ka eksistē tāds naturāls skaitlis n, ka 2^n decimālais pieraksts sākas ar ciparem $2022\ldots$.

Risinājums: Aplūkosim šādu risinājuma plānu: Uzrakstīsim nevienādības, kas izsaka uzdevuma nosacījumu, ko apmierina skaitļi, kas sākas ar vajadzīgajiem ciparem. Skaitļa 2 piereizināšanu pakāpei 2^n, lai iegūtu nākamo pakāpi 2^{n+1} var uztvert kā (iracionāla) skaitļa pieskaitīšanu decimāllogaritma daļveida daļai.

(Risinājums nav pabeigts.)

6.5 Sacensību uzdevumi

1.Uzdevums: Atrast naturālu skaitli n, kuram izpildās attēlā dotā vienādība. (Formulā ar $\lfloor x \rfloor$ apzīmēta skaitļa x veselā daļa.)

$$\lfloor \log_2 1 \rfloor + \lfloor \log_2 2 \rfloor + \lfloor \log_2 3 \rfloor + \ldots \lfloor \log_2 n \rfloor = 1898.$$

2.Uzdevums: Cik daudzi no pirmajiem 100 naturālajiem skaitļiem $(1, \ldots, 100)$ ir izsakāmi ar attēlā redzamo izteiksmi, kur x ir reāls skaitlis.

$$\lfloor 2x \rfloor + \lfloor 4x \rfloor + \lfloor 6x \rfloor + \lfloor 8x \rfloor.$$

3.Uzdevums: Dots pozitīvs skaitlis a, kam $\{a^{-1}\} = \{a^2\}$ un $2 < a^2 < 3$. Atrast izteiksmes $a^{12} - 144a^{-1}$ vērtību.

4.Uzdevums: Pierādīt, ka eksistē tāds naturāls skaitlis n, ka vienlaicīgi 2^n sākas ar ciparem $1995\ldots$, bet 3^n sākas ar ciparem $5991\ldots$.

5.Uzdevums: Pierādīt, ka funkcija $y = \sin x + \sin \sqrt{3}x$ nav periodiska.

6.Uzdevums: Pierādīt, ka $\sqrt[3]{2}$ nevar izteikt formā $a + b\sqrt{r}$, kur a, b, r ir racionāli skaitļi.

7.Uzdevums: Definējam sekojošu virkni:

$$1000, x, 1000 - x, \ldots$$

Tajā pirmie divi locekļi ir 1000 un x, bet katru nākamo a_n iegūst atņemot iepriekšējo no tam iepriekšējā: $a_n = a_{n-2} - a_{n-1}$. Virknes pēdējais loceklis ir pirmais negatīvais skaitlis, kas parādās šajā procesā. Kura naturāla x vērtība rada visgarāko virkni?

8.Uzdevums: Dots reāls skaitlis $x \in \mathbb{R}$. Pierādīt identitāti:

$$\sum_{k=0}^{\infty} \left\lfloor \frac{x + 2^k}{2^{k+1}} \right\rfloor = \lfloor x \rfloor.$$