NMS SKAITĻU TEORIJA #1: PIRMSKAITĻI UN DALĀMĪBA

1.1 Ievads

Veselo skaitļu aritmētikas uzdevumi var saturēt jautājumus, kas ar ko dalās vai nedalās vai jautājumus par pirmskaitļiem un saliktiem skaitļiem. Dalāmības attiecību bieži izmanto arī tur, kur dalāmība nav pieminēta, piemēram, risinot vienādojumus veselos skaitļos.

Nodaļas mērķi:

1. Izmantot dalāmības attiecības īpašības.
2. Aprēķināt naturāla skaitļa dalītāju skaitu, dalītāju summu.
3. Aprakstīt skaitļa dalītāju kopas režģveida struktūru.
4. Veidot Eratostēna režģi intervālā.
5. Pierādīt aritmētikas pamatteorēmu, atsaucoties uz 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 attiecība? Veselie skaitļi veido ritmus, šajā kopā var pamatot likumsakarības, kas ļauj citādi paraudzīties uz visdažādākajiem uzdevumiem?

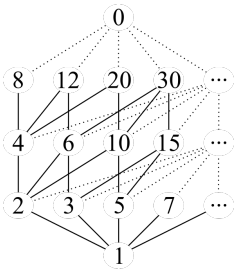
1.2 Skaitļu dalāmība

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* 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*, savukārt m sauc par skaitļa d *daudzkārtni*.

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* 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* 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:

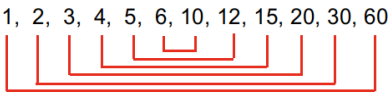
TODO: Ievietot attēlu, kas parāda dalītāju skaitu dažādiem skaitļiem no 1 līdz 30. Vizualizācija zīmē ritmu ar skaitļu $1, 2, 3, 4, \ldots$ daudzkārtņiem horizontālēs. Dalītāju skaitu var saskaitīt vertikāli. Kuriem no skaitļiem ir nepāru skaits dalītāju?

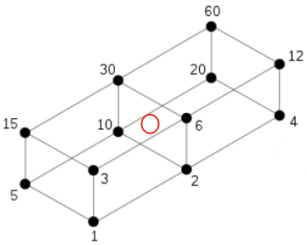
1.3 Naturāla skaitļa dalītāju skaits

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.

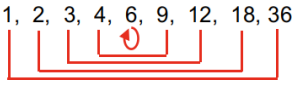
1.3.1 Dalītāju virknes simetrija

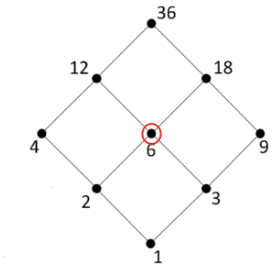
Dalītāji skaitlim 60:





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

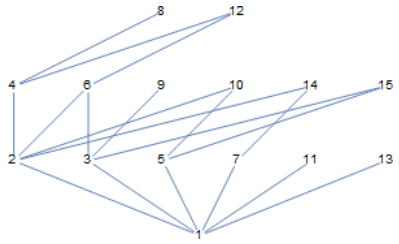


Fig. 1: Hases diagramma skaitļiem $[1; 15]$

1.3.3 Veidotājelementi: 2,3,5

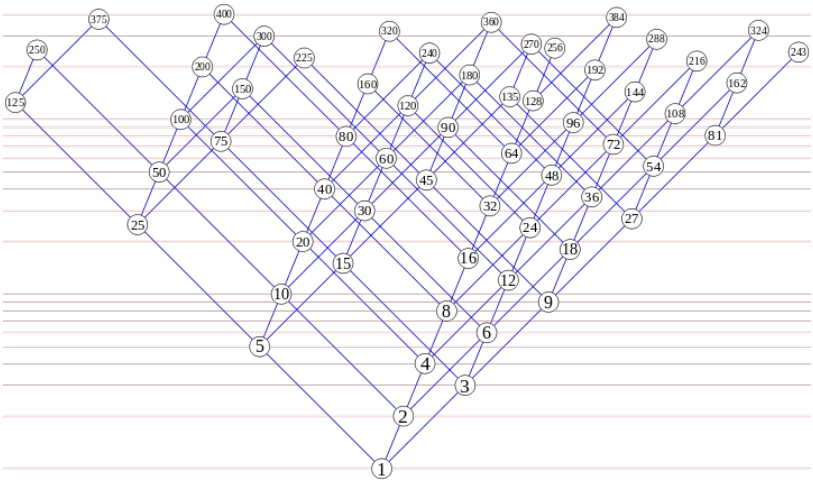


Fig. 2: Hases diagramma skaitļiem līdz 480, https://bit.ly/3qQBntd

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:

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

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

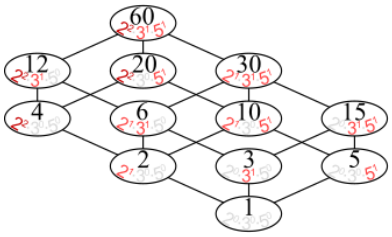
1.3.6 Piemēri ar n=60

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

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

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

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. ■

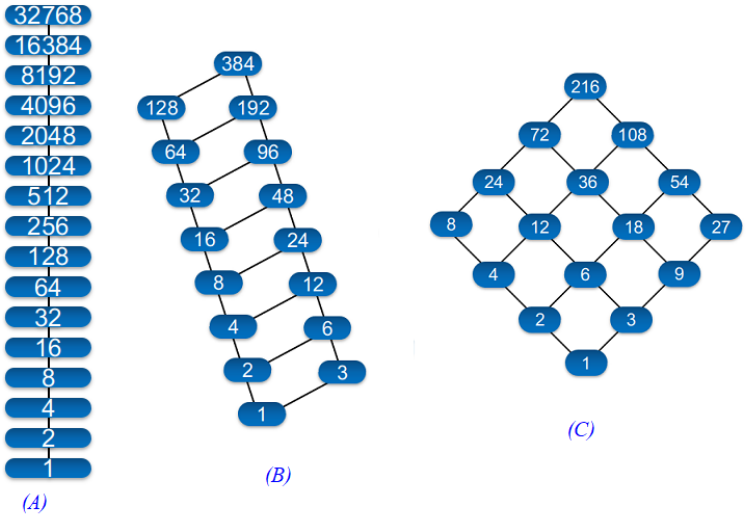
1.3.9 Jautājumi dalītāju skaitam un summai

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.

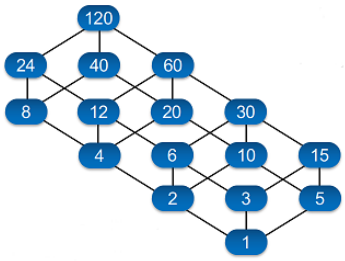


(A) *(B)* *(C)*

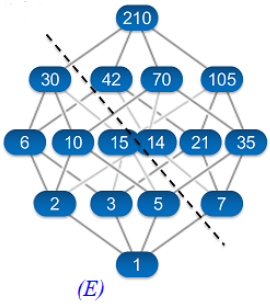
(A) gadījums: $16 = (15 + 1)$ jeb p^{15}, kur p ir pirmskaitlis. Mazākais šāds skaitlis ir $M = 2^{15} = 32768$.

(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 $a \in \{2, \ldots 1001\}$. □

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

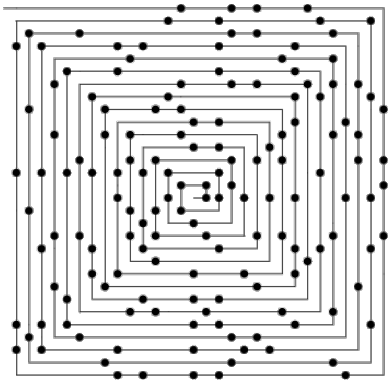
Dirihlē Teorēma (Dirichlet): Ja a un d ir savstarpēji pirmskaitļi, tad bezgalīgā aritmētiskā progresijā

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

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.

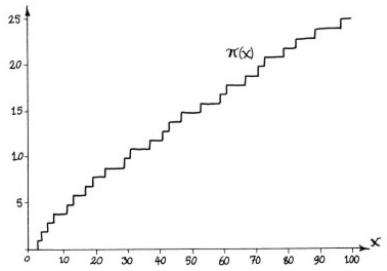
Šī polinoma vērtību vidū arī lielākiem x ir neparasti daudz pirmskaitļu. Ar modulāro aritmētiku iespējams pamatot, ka $x^2 + x + 41$ (kur $x \in \mathbb{N}$) nevar dalīties ne ar vienu pirmskaitli $p < 41$.

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_11. 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 $a^m - b^m$:

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

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

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

Piemēri:

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

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).

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

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

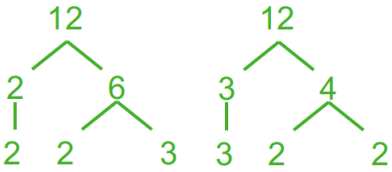
Note: Starp citu, $16^{16} + 1 = 2^{64} + 1 = 2^{2^6} + 1 = F_6$ ir sestais Fermā skaitlis. Tas nav pirmskaitlis: $F_6 = 18\,446\,744\,073\,709\,551\,617$ dalās ar $274177 = 1071 \cdot 2^8 + 1$.

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. □



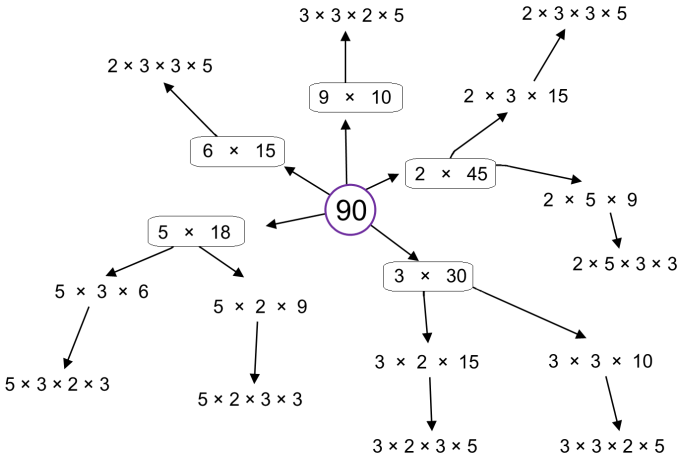
Kāpēc neatkarīgi no **faktorizēšanas** secības, vienmēr sanāk tas pats? (Par faktorizēšanu sauc dalīšanu reizinātājos.)

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

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

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

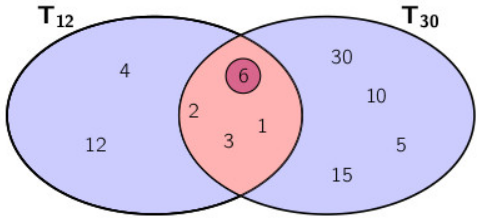
Citiem vārdiem: Ja kādu no šiem p_i ($i = 1, 2, 3, 4$) var izteikt kā reizinājumu:

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

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 $m=2^{10}3^8 5^9$ un $n=2^{17}3^5$, tad $\text{LKD}(m,n)=2^{10}3^5$.

Faktiski ir ļoti grūti dalīt lielus skaitļus pirmreizinātājos. Piemēram,

$$\text{LKD}(737869762948382064 63, 295147905179352825855)=?$$

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: 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

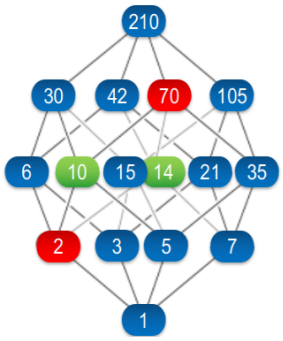
$\text{MKD}(300, 630) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 6300$.

$\text{MKD}(m, n)$ 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

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

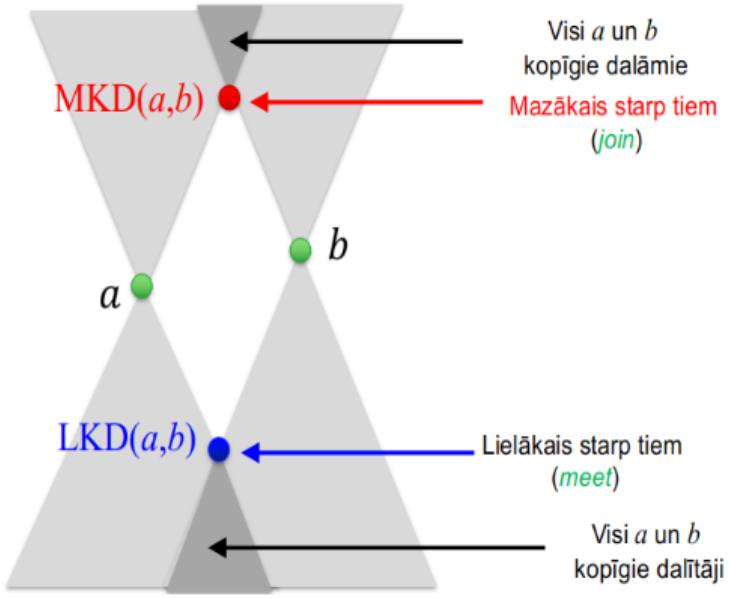


Zaļo un sarkano skaitļu reizinājumi sakrīt: $2 \cdot 70 = 10 \cdot 14$.

- 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 Terminu vārdnīca

Termins	Tulkojums
a is divisible by b	a dalās ar b
divisor	dalītājs
multiple	daudzkārtnis
partially ordered set	daļēji sakārtota kopa
transitive	transitīvs

1.11 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.