1. IEVADS SKAITĻU TEORIJĀ

Sasniedzamie rezultāti un prasmes:

1. Kopu un funkciju apzīmējumi. Injektīvas, sirjektīvas un bijektīvas funkcijas.
2. Algebriskas identitātes. Pakāpju starpības formula, Sofijas-Žermēnas identitāte.
3. Pirmskaitļu ir bezgalīgi daudz. Faktoriāli un atstarpes pirmskaitļu virknē.
4. Pierādījumi no pretējā. Labās sakārtotības (*Well-ordering*) princips. Multiplikatīvā inversā eksistence ar Dirihlē principu. Nekonstruktīvi pierādījumi.

Kopu un funkciju īpašības	
$f(n) = n^3 \pmod 7$. $3 \not\equiv 5 \not\equiv 6 \pmod 7$, bet $3^3 \equiv 5^3 \equiv 6^3 \equiv 6 \pmod 7$.	Funkcijai f argumentu pāris (a_1, a_2) ir *kolīzija*, ja $a_1 \neq a_2$, bet $f(a_1) = f(a_2)$, t.i. dažādiem argumentiem vērtības "saskrienas".
$f(n) = 3n \pmod 7$. Ja $n_1 \not\equiv n_2 \pmod 7$, tad arī $3n_1 \not\equiv 3n_2 \pmod 7$.	Funkcija f ir *injektīva*, ja no $a_1 \neq a_2$ seko, ka $f(a_1) \neq f(a_2)$, t.i. nav kolīziju.
Rotācijas funkcija, kas virknē pirmo ciparu aiznes uz beigām: rot("`1023`") = "`0231`" ir bijekcija, jo var rotēt atpakaļ.	Funkcija f ir *bijektīva*, ja katram $b \in B$ ir tieši viens $a \in A$, kam $f(a) = b$. Vienāda izmēra kopām katra injektīva funkcija ir arī bijektīva.
Rotācijas funkcijai inversā atgriež pēdējo ciparu skaitļa sākumā: rot^{-1}("`1234`") = "`4123`".	Par f *inverso funkciju* sauc $f^{-1} : B \mapsto A$, kas katram $b \in B$ piekārto to $a \in A$, kam $f(a) = b$. Tikai bijektīvām funkcijām eksistē inversās.
Algebriskas identitātes	
$a^3 - b^3 = (a-b)(a^2+ab+b^2)$.	**Pakāpju starpība (homogēnā forma):** $a^n - b^n =$ $= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.
$a^3 - 1 = (a-1)(a^2+a+1)$.	**Pakāpju starpība (nehomogēnā forma):** $a^n - 1 =$ $= (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$.
$a^3 + b^3 = (a+b)(a^2-ab+b^2)$.	**Nepāru pakāpju summa:** $a^{2n+1} + b^{2n+1} =$ $= (a+b)(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n})$.
$a^4 + 4 =$ $= (a^2 - 2a + 2) \cdot (a^2 + 2a + 2)$	**Sofijas-Žermēnas identitāte (homogēnā forma):** $a^4 + 4b^4 = \left((a+b)^2 + b^2\right) \cdot \left((a-b)^2 + b^2\right)$ jeb $a^4 + 4b^4 = \left(a^2 + 2ab + b^2\right) \cdot \left(a^2 - 2ab + 2b^2\right)$
Pirmskaitļi	
Pirmskaitļu $2, 3, 5, \ldots$ ir bezgalīgi daudz. (No pretējā: ja būtu galīgs skaits, tad $p_1 p_2 \cdots p_k + 1$ nedalītos ne ar vienu no tiem.)	
Eksistē cik patīk garas $\mathbb{N}$ apakšvirknes bez pirmskaitļiem. (Piemēram, $(m+1)! + 2, (m+1)! + 3, (m+1)! + (m+1)$ satur m saliktus skaitļus.)	
$2023 = 7^1 17^2$, $2024 = 2^3 11^1 23^1$, $2025 = 3^4 5^2$.	**Aritmētikas pamatteorēma:** Katru $n \in \mathbb{N}$ var tieši vienā veidā izteikt kā pirmskaitļu pakāpju reizinājumu: $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

1.1 Kopas un funkcijas

Kopas parasti apzīmē ar lielajiem burtiem, piemēram, A, B, X, Y, kopu elementus apzīmējam ar mazajiem burtiem. Pazīstamās skaitļu kopas apzīmējam ar treknajiem burtiem, piemēram, $\mathbb{N} = \{1, 2, 3, \ldots\}$ ir naturālo skaitļu kopa, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ ir veselo skaitļu kopa, $\mathbb{Q}$ ir visu racionālo skaitļu kopa (skaitļi, kas uzrakstāmi kā racionālās daļas), $\mathbb{R}$ ir visu reālo skaitļu kopa (uzrakstāmi kā bezgalīgās decimāldaļas).

Definīcija: Par *funkciju* no kopas A kopā B sauc attiecību starp šo kopu elementiem, kas katram $a \in A$ piekārto tieši vienu elementu $b \in B$. Šādu funkciju pieraksta $f : A \mapsto B$.

Piemēri: Ja katram Latvijas pastāvīgajam iedzīvotājam (cilvēku kopā A) ir piešķirts personas kods (11-ciparu ciparu virknīšu kopā B), tad attēlojums f, kas katram cilvēkam piekārto personas kodu, ir funkcija. Savukārt, tāds attēlojums, kas katram cilvēkam piekārto viņa vārdu, nav funkcija, ja pieļaujam, ka cilvēkam var būt vairāki vārdi. (Toties funkcija ir tāds attēlojums, kas katram cilvēkam piekārto visus viņa vārdus.)

Definīcija: Par *injektīvu funkciju* $f : A \mapsto B$ sauc tādu funkciju, kas uz katru $b \in B$ attēlo ne vairāk kā vienu elementu $a \in A$. Tātad, ja $a_1 \neq a_2$, tad $f(a_1) \neq f(a_2)$.

Definīcija: Par *kolīziju* funkcijai $f : A \mapsto B$ sauc tādus divus elementus $a_1, a_2 \in A$, kam $a_1 \neq a_2$, bet $f(a_1) = f(a_2)$. (Injektīvām funkcijām atbilstoši definīcijai kolīziju nevar būt.)

Piemērs: Ja Latvijas iedzīvotājam piešķirtais personas kods ir unikāls, tad funkcija, kas piekārto personas kodus ir injektīva. Kolīzija šajā funkcijā rastos vienīgi tad, ja diviem dažādiem cilvēkiem izsniegtu vienādus personas kodus – cilvēku pēc viņa koda nevarētu viennozīmīgi noteikt.

Definīcija: Par *bijektīvu funkciju* $f : A \mapsto B$ sauc tādu funkciju, kas uz katru $b \in B$ attēlo tieši vienu elementu $a \in A$.

Piemērs: Personas koda piešķiršanas funkcija nav bijektīva, ja aplūko visus 11-ciparu skaitļus kā iespējamos kodus – eksistē neizmantoti kodi. No 11 cipariem varētu izveidot 100 miljardus dažādu kodu – daudz vairāk nekā ir iedzīvotāju. Šo funkciju varētu padarīt par bijektīvu vienīgi tad, ja kopa B ir faktiski izsniegtie personas kodi nevis visas ciparu virknes vajadzīgajā garumā.

Definīcija: Par bijektīvas funkcijas $f : A \mapsto B$ *inverso funkciju* $f^{-1} : B \mapsto A$ sauc tādu funkciju, kas attēlo kopu B atpakaļ kopā A un katram $b \in A$ atrod to $a \in A$, kuram $f(a) = b$.

Piemēri:

(A) Kvadrātfunkcija, $f : \mathbb{R} \mapsto \mathbb{R}$, kas definēta ar formulu $f(x) = x^2$ katru reālu skaitli kāpina kvadrātā. Šī funkcija nav injektīva, jo tai eksistē kolīzijas: $f(-2) = f(2) = 4$.

(B) Ja kvadrātfunkciju definē tikai nenegatīviem argumentiem $\mathbb{R}_{0+} = [0; +\infty)$, tad tā ir injektīva, jo nenegatīvu skaitļu kvadrāti visi atšķiras (parabolas labais zars). Tomēr kvadrātfunkcija $f : \mathbb{R}_{0+} \mapsto \mathbb{R}$ nav bijektīva: ne katrs reāls skaitlis ir kāda skaitļa kvadrāts: kolīziju šai funkcijai nav (katram reālam skaitlim iedur ne vairāk kā viena bultiņa), bet uz negatīviem reāliem skaitļiem nekas neattēlojas – tiem neiedur neviena bultiņa.

(C) Visbeidzot, ja kvadrātfunkciju definē kā attēlojumu no reāliem nenegatīviem uz reāliem nenegatīviem skaitļiem $f : \mathbb{R}_{0+} \mapsto \mathbb{R}_{0+}$, tad tā ir bijektīva. Šīs funkcijas inversā funkcija ir kvadrātsakne: $f^{-1}(x) = \sqrt{x}$. Tādēļ kvadrātsakne ir definēta tikai nenegatīviem skaitļiem un pieņem nenegatīvas vērtības.

(D) Ir iespējama bijektīva funkcija no vaļēja intervāla $(-\pi/2; \pi/2)$ uz visu reālo skaitļu taisni: $\mathbb{R} = (-\infty; \infty)$. Šāda funkcija ir, piemēram, tangenss: $f : (-\pi/2; \pi/2) \mapsto (\mathbb{R})$, kas definēts ar formulu $f(x) = \tan x = \dfrac{\sin x}{\cos x}$. (Tangenss ir definēts arī citām reālām x vērtībām, ja tās nav vienādas ar $\pi/2 + \pi \cdot k$ veseliem k, kur saucējā esošais kosinuss ir 0.)

Inversajai funkcijai, ko sauc par *arktangensu* izmanto tikai vienu no šīs funkcijas zariem. Tā ir bijektīva funkcija, kas attēlo taisni $\mathbb{R}$ par galīgu intervālu $(-\pi/2; \pi/2)$. Katrs reāls skaitlis ar arktangensa funkciju attēlojas par unikālu skaitli šajā galīgajā intervālā.

(E) Funkcija, kas reizina ar nenulles atlikumu pēc pirmskaitļa moduļa ir bijektīva. Piemēram, reizināšana ar $a \neq 0$ pēc pirmskaitļa $p = 7$ moduļa ir bijektīva:

n	0	1	2	3	4	5	6
$f(n) = 3n$	0	3	6	2	5	1	4
$f(n) = 4n$	0	4	1	5	2	6	3

Ievērojiet, ka vienalga, vai reizina ar 3 vai ar 4 (vai jebkuru citu atlikumu, kas nedalās ar 7) reizināšanas tabulas rindiņā visi atlikumi ir dažādi.

(F) Funkcija, kas reizina ar nenulles atlikumu $a \neq 0$ pēc salikta skaitļa moduļa ir bijektīva tad un tikai tad, ja a un modulis ir savstarpēji pirmskaitļi. Piemēram, reizināšana pēc $p = 9$ moduļa var būt un var nebūt bijektīva:

n	0	1	2	3	4	5	6	7	8
$f(n) = 3n$	0	3	6	0	3	6	0	3	6
$f(n) = 4n$	0	4	8	3	7	2	6	1	5

Reizinot ar 3 pēc moduļa 9, iegūstam nevis deviņus, bet tikai trīs atlikumus $(0, 3, 6)$ un daudzas kolīzijas. Savukārt, reizinot ar 4 iegūstam bijektīvu attēlojumu, kas ir

Apgalvojums: Dotas divas galīgas kopas A un B, kurās ir vienāds skaits elementu ($|A| = |B|$). Ja funkcija $f : A \mapsto B$ ir injektīva, tad šī funkcija ir arī bijektīva.

Pierādijums: Ja eksistētu tāds $b \in B$, par kuru neattēlojas neviens $a \in A$, tad kopā B būtu mazāk nekā $|B| = |A|$ elementu, par kuriem attēlojas kopas A elementi. Pēc Dirihlē principa būs divi tādi elementi $a_1, a_2 \in A$, kuri attēlosies par vienu un to pašu elementu no B, jo kopas A elementu ir vairāk nekā iespējamo attēlu. Tā ir kolīzija un tāpēc šāda funkcija f nevar būt arī injektīva. Iegūta pretruna. ■

Definīcija: Par skaitļa a *multiplikatīvi inverso* pēc moduļa m saucam tādu skaitli a^{-1}, kas apmierina sakarību $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Multiplikatīvi inversie eksistē tikai tad, ja m un a ir savstarpēji pirmskaitļi. (Ja m ir pirmskaitlis, tad multiplikatīvi inversais eksistē katram $a \neq 0$).

Piemēri:

(A) Pēc pirmskaitļa moduļa $m = 7$ ir seši multiplikatīvi inversie:

$$1^{-1} \equiv 1,\ \ 2^{-1} \equiv 4,\ \ 3^{-1} \equiv 5,\ \ 4^{-1} \equiv 2,\ \ 5^{-1} \equiv 3,\ \ 6^{-1} \equiv 6 \pmod{7}.$$

Multiplikatīvi inversais 0^{-1} pēc moduļa 7 nav definēts, jo 0 reizinot ar jebko, nevar iegūt atlikumu 1.

(B) Pēc moduļa $m = 10$ ir četri multiplikatīvi inversie:

$$1^{-1} \equiv 1,\ \ 3^{-1} \equiv 7,\ \ 7^{-1} \equiv 3,\ \ 9^{-1} \equiv 9 \pmod{10}.$$

Apgalvojums: Katram pirmskaitlim p un katram $a \not\equiv 0 \pmod{p}$ eksistē inversais a^{-1}.

Pierādījums: Pamatosim, ka funkcija $f(n) = an$, kas katram atlikumam pēc moduļa p ($n \in \{0, \ldots, p-1\}$) piekārto citu atlikumu no tās pašas kopas $\{0, \ldots, p-1\}$, ir bijektīva.

Šī funkcija ir injektīva, jo pieņemot, ka $an_1 \equiv an_2 \pmod{p}$ iegūsim, ka $an_1 - an_2 \equiv 0 \pmod{p}$ jeb $a(n_1 - n_2)$ dalās ar p. Tā kā $a \not\equiv 0 \pmod{p}$, tad vienīgi $(n_1 - n_2) \equiv 0 \pmod{p}$, jeb iegūstam, ka n_1 un n_2 ir viens un tas pats atlikums.

Pēc agrāka apgalvojuma šī funkcija $f(n) = an$ ir arī bijektīva. Tātad katram skaitlim (tai skaitā arī $1 \in \{0, \ldots, p-1\}$) eksistē kāds skaitlis n', kurš par viņu attēlojas: $f(n') \equiv 1 \pmod{p}$. Šis arī ir multiplikatīvi inversais skaitlim a pēc moduļa p. ■

1.2 Pirmskaitļi

Definīcija: Naturālu skaitli $p > 1$ sauc par *pirmskaitli*, ja vienīgie tā dalītāji ir 1 un p. Naturālus skaitļus $n > 1$, kas nav pirmskaitļi, sauc par *saliktiem skaitļiem*.

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

Piemērs: 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

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. ■

Apgalvojums: Katram naturālam N eksistē N pēc kārtas sekojoši skaitļi, kuri visi ir salikti.

Pierādījums: N pēc kārtas sekojošus saliktus skaitļus var atrast šādi: Aprēķinām $(N+1)!$ un izrakstām šādus skaitļus:

$$(N+1)! + 2,\ (N+1)! + 3,\ \ldots,\ (N+1)! + (N+1).$$

Šie ir N pēc kārtas sekojoši skaitļi, no kuriem pirmais dalās ar 2 (jo $(N+1)!$ un 2 dalās ar 2), otrais dalās ar 3 utt. Pēdējais no skaitļiem dalās ar $(N+1)$. Tātad neviens no tiem nav pirmskaitlis. ■

Piemērs: Pietiekami lielas atstarpes starp pirmskaitļiem novērojamas arī daudz mazākiem skaitļiem. Piemēram, 113 un 127 abi ir pirmskaitļi, bet starp tiem ir 13 salikti skaitļi intervālā $[114; 126]$.

Var izmantot $14! = 87178291200$ kā apgalvojuma pierādījumā, un tad intervālā $[87178291202; 87178291214]$ arī būs 13 pēc kārtas sekojoši salikti skaitļi.

1.3 Pierādījumi no pretējā

Definīcija: Skaitļu kopa A ir *labi sakārtota* (*well-ordered*) ja katrai tās netukšai apakškopai $S \subseteq A$ ir mazākais elements.

Piemēri:

(A) Naturālo skaitļu kopa $\mathbb{N}$ ir labi sakārtota. Jebkurā netukšā naturālu skaitļu apakškopā $S \subseteq \mathbb{N}$ atradīsies mazākais skaitlis. (To var pārbaudīt, izvēloties jebkuru $n_1 \in S$. Vai nu n_1 jau ir mazākais kopas S elements, vai arī eksistē kāds $n_2 \in S$, kas ir par to vēl mazāks: $n_2 < n_1$. Atkārto to pašu spriedumu skaitlim n_2 un tā tālāk. Pēc kāda laika būsim atraduši mazāko kopas S skaitli, jo nevar eksistēt bezgalīgi dilstoša virkne $n_1 > n_2 > n_3 > \ldots$ tikai no naturāliem skaitļiem).

(B) Veselo skaitļu kopa $\mathbb{Z}$ nav labi sakārtota. Ja izvēlas netukšu $\mathbb{Z}$ apakškopu, kurā ir bezgalīgi daudz negatīvu skaitļu, tad starp tiem nevarēs atrast pašu mazāko. Par katru negatīvu skaitli eksistēs vēl mazāks.

(C) Reālo skaitļu nogrieznis $[0;1]$ nav labi sakārtots. Pašā nogrieznī $[0;1]$ eksistē mazākais elements 0. Bet izvēloties vaļēju intervālu kā apakškopu, piemēram, $(0;1) \subseteq [0;1]$, vairs nevarēs izvēlēties mazāko pozitīvo skaitli. Ja izvēlamies $\varepsilon \in (0;1)$, tad izdalot ar 2, iegūsim $\varepsilon/2 \in (0;1)$, kas arī ir pozitīvs skaitlis un $\varepsilon/2 < \varepsilon$. Var konstruēt bezgalīgu virkni ar skaitļiem, kuri kļūst arvien mazāki un tuvojas nullei – neviens starp tiem nebūs vismazākais.

Labās sakārtotības īpašība naturālajiem skaitļiem ļauj veidot pierādījumus, kuri līdzīgi matemātiskās indukcijas metodei, bet atklātas indukcijas vietā izmanto pierādījumu no pretējā.

Apgalvojums: Katram naturālam skaitlim $n > 1$ eksistē kāds pirmreizinātājs p, t.i. pirmskaitlis kurš dala skaitli n bez atlikuma.

Pierādījums: No pretējā. Iedomāsimies, ka eksistē tāda netukša kopa $S \in \mathbb{N}$, kas satur tādus skaitļus $n > 1$, kuriem nav neviena pirmreizinātāja. No kopas $\mathbb{N}$ labās sakārtotības secinām, ka netukšajā kopā S eksistē mazākais elements $n \in S$.

Skaitlis n nevar būt pirmskaitlis, jo citādi tas būtu pats sev pirmreizinātājs. Tāpēc tas ir salikts skaitlis $n = ab$. Bet tādā gadījumā arī skaitļiem a un b nevar būt pirmreizinātāji (citādi ar tiem dalītos arī skaitlis n). Tāpēc arī $a, b \in S$. Bet šie abi skaitļi ir mazāki nekā n, kas ir pretruna ar to, ka n bija izraudzīts kā kopas S mazākais elements. ■

1.4 Uzdevumi

1.1.uzdevums: (*Multiplikatīvi inversie*)

(A) Aplūkot rēbusu `XX`??? $\cdot$ 13 = `XXX001`, kur "X" un "?" vietā var būt jebkādi cipari. Kuri cipari jāliek jautājumzīmju vietā, lai vienādība būtu pareiza?

(B) Izmantojot punktā (A) atrastos ciparus, atrisināt arī citus līdzīgus rēbusus, piemēram, `XX`???$\cdot$13 = `XXX123`.

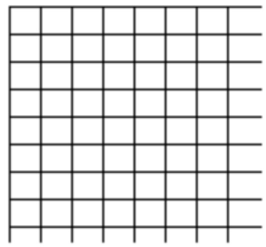
1.2.uzdevums: (*Labā sakārtojuma princips.*) Katrā netukšā naturālu skaitļu kopā ir mazākais elements. (Kopa var būt galīga vai bezgalīga; tajā var neeksistēt lielākais elements, bet mazākais vienmēr eksistē.)

(A) Kurš ir lielākais naturālais skaitlis S, ko nevar izteikt formā $S = 3n + 5m$, kur n, m ir veseli nenegatīvi skaitļi.

(B) Kādā valstī ir trīs veidu monētas: 6, 9 un 20 centu vērtībā. Kāda ir lielākā naudas summa S, ko nevar samaksāt tikai ar šādām monētām? Ar monētām maksā tikai pircējs, atlikumu izdot nedrīkst.

(C) Izmantot labā sakārtojuma principu, lai pamatotu, ka S tiešām ir mazākā summa, ko nevar samaksāt ar norādīto vērtību monētām.

1.3.uzdevums: (*Bezgalīga 2D tabula ar neparastu īpašību*)



(A) Bezgalīgajā rūtiņu kvadrantā iekrāsot daļu no rūtiņām zilas tā, lai katrā kolonnā visas, izņemot galīgu skaitu, rūtiņas nebūtu iekrāsotas zilas, bet katrā rindiņā visas, izņemot galīgu skaitu, rūtiņas būtu zilas.

(B) 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?

1.4.uzdevums (AMO1987.10.5): (*Stratēģijas nozagšana un nekonstruktīvi pierādījumi.*) Divi spēlētāji pēc kārtas raksta uz tāfeles naturālus skaitļus, kas nepārsniedz 10. Aizliegts rakstīt tādus skaitļus, kas ir jau uzrakstīto skaitļu dalītāji. Zaudē tas, kas nevar izdarīt gājienu.

(A) Vai uz tāfeles var rakstīt skaitli 1? Kurš spēlētājs to var rakstīt? Vai šis skaitlis ir kāds no gājieniem uzvarošajā stratēģijā? Pamatot, kurš no abiem spēlētājiem, pareizi spēlējot, uzvar. Stratēģija **nav** jānorāda.

(B) Noskaidrot, kuram spēlētājam ir uzvaroša stratēģija, un atrast to.

1.5.uzdevums (Mersenna skaitļi): Apzīmējam $M_n = 2^n - 1$. Pierādīt, ka M_n var būt pirmskaitlis tikai tad, ja arī n ir pirmskaitlis. (Tas ir *nepieciešamais*, bet ne *pietiekamais* nosacījums. Piemēram, $M_{11} = 2047 = 23 \cdot 89$ nav pirmskaitlis.)

Atbilde:

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

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

1.6.uzdevums (A.Engel 6.E1): Ja $n > 1$, tad $n^4 + 4^n$ nevar būt pirmskaitlis.

2. MODULĀRĀ ARITMĒTIKA

Sasniedzamie rezultāti un prasmes:

1. Vienkāršu lineāru kongruenču risināšana, piereizināšana ar multiplikatīvi inverso.
2. Modulārās aritmētikas funkciju apraksts ar tabulām.
3. Multiplikatīvi inversā atrašana ar uzminēšanu vai gadījumu pārlasi.
4. Vienādojumu risināšana veselos skaitļos ar pretrunas moduli.
5. Dalāmības pazīme ar 9 modulārās aritmētikas pierakstā.

Pretrunas moduļi	
$a^2 = 8b + 5$ nav atrisinājumu, jo $a^2 \equiv 0, 1, 4 \pmod 8$, bet $8b + 5 \equiv 5 \pmod 8$.	Vienādojumam $f(a, b, c) = g(a, b, c)$ nav atrisinājumu veselos skaitļos, ja var atrast moduli m, kuram $f(a, b, c)$ jebkurām a, b, c vērtībām dod citu atlikumu $(\bmod\ m)$ nekā $g(a, b, c)$.
$a^2 \equiv 0, 1 \pmod 3$ $a^2 \equiv 0, 1, 4 \pmod 5$ $a^2 \equiv 0, 1 \pmod 4$ $a^2 \equiv 0, 1, 4 \pmod 8$.	Pilniem kvadrātiem a^2 piemēroti pretrunas moduļi – visi nepāra pirmskaitļi vai $m = 4$ un $m = 8$.
$a^3 \equiv 0, 1, 6 \pmod 7$ $a^3 \equiv 0, 1, 8 \pmod 9$.	Pilniem kubiem a^3 piemēroti pretrunas moduļi – $m = 7$ un $m = 9$.

2.1 Uzdevumi

2.1.uzdevums: Atrast moduli, pie kura dotajam vienādojumam veselos skaitļos nav atrisinājuma. Atrisinājumā minēt moduli m kas ļauj atrast pretrunu. Norādīt, kuriem atlikumiem (pēc m moduļa) var būt kongruenta kreisā puse, kuriem atlikumiem var būt kongruenta labā puse un kāpēc tās nevar būt vienādas.

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

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

(C) $x^2 - 2y^2 + 8z = 19$,

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

(E) $x^2 + y^2 = 8z + 6$,

(F) $x^2 + 8z = 2y^2 + 3$,

(G) $x^4 - 12y^4 = 24$,

(H) $11^x - 8^y = 1$.

2.2.uzdevums: Vai pilna kvadrāta ciparu summa var būt (A) 3, (B) 7, (C) 2024?

2.3.uzdevums: Dots polinoms $P(n)$ ar veseliem koeficientiem un pirmskaitlis p. Pierādīt, ka jebkuram naturālam n skaitlis $P(n) + P(n+1) + \ldots + P(n+p-1)$ dalās ar p.

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

2.5.uzdevums (BW.2016.1): Atrast visus pirmskaitļu pārus (p, q), kuriem $p^3 - q^5 = (p+q)^2$.

2.6.uzdevums (BWTST.2018.13): Vai eksistē tāds pirmskaitlis q, ka nevienam pirmskaitlim p skaitlis $\sqrt[3]{p^2+q}$ nav naturāls?

3. POZICIONĀLĀS SKAITĪŠANAS SISTĒMAS

1. Veidot intuīciju, kā mainās skaitļu cipari un to pieraksta garums, veicot aritmētiskas operācijas.
2. Skaitļa garuma saistība ar logaritmu, garuma izmaiņa nomainot sistēmas bāzi.
3. Izmantot skaitļa pieraksta kopsakaru ar polinomu (ar mainīgo vienādu ar sistēmas bāzi). Izteikt skaitļa pieraksta ciparus, izmantojot kongruences, atlikumus un veselās daļas.

3.1 Ievaduzdevumi

3.2 Spriedumu un aprēķinu piemēri

1. Pozicionālais pieraksts kā polinoms ar fiksētu bāzi.
2. Kā cipari skaitļa pierakstā izsakāmi ar algebru vai kongruencēm.
3. Logaritms ar bāzi 2 vai 10; skaitļa ciparu skaits.
4. Dalāmības pazīmes; Kongruenču klases atrašana, izmantojot dalāmības pazīmi.
5. Pārveidošana no viena pieraksta otrā. Arī pārveidojumi no binārās uz oktālo vai heksadecimālo utml. Aritmētiskas darbības citos pierakstos.
6. Skaitļa pieraksta īpašību "iztulkošana" algebriski. Dalāmības pazīmju vispārinājumi.

3.3 Uzdevumi

3.1. Uzdevums (IMO1960.1): Atrast visus trīsciparu skaitļus N ar īpašību, ka N dalās ar 11 un $N/11$ ir vienāds ar N ciparu kvadrātu summu.

3.2. Uzdevums (IMO1962.1): Atrast mazāko naturālo n ar šādām īpašībām:

a. Tā decimālpieraksts beidzas ar ciparu "6";

b. Ja pēdējo ciparu "6" nodzēš un pieraksta priekšā pārējiem cipariem, tad iegūtais skaitlis ir četrreiz lielāks nekā sākotnējais n.

4. PROGRESIJAS, EIKLĪDA ALGORITMS

Aritmētiskas progresijas	
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.	**Binomiālie koeficienti:** $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$, kur $\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$.
$(a+b+c+d)^4 = \ldots + 12a^2bc + \ldots$, jo $\frac{4!}{2!1!1!} = 12$.	**Polinomiālie koeficienti:** $(a_1 + a_2 + \cdots + a_m)^n$ izvirzījums satur $a_1^{k_1}a_2^{k_2}\cdots a_m^{k_m}$ ar koeficientu $\frac{n!}{k_1!k_2!\cdots k_m!}$, ja $k_1 + k_2 + \cdots + k_m = n$.
$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$.	**Nepāru pakāpju summa:** $a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n})$.
$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$.	**Pakāpju starpība:** $a^n - b^n =$ $= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.
$ax^2 + bx + c = 0$ ir 3 saknes $\Rightarrow a = b = c = 0$	**Identiski polinomi:** Ja $P(x)$ un $Q(x)$ ir n-tās pakāpes polinomi un to vērtības sakrīt $n+1$ dažādiem x_i, tad $P(x) = Q(x)$.
$P(x) = 4x^3 - 3x^2 - 25x - 6$ dalās ar $(x-3)$.	Polinoms $P(x)$ dalās ar $(x-a)$ tad un tikai tad, ja a ir $P(x)$ sakne.
$x^4 + 4 =$ $= (x^2 - 2x + 2)\cdot$ $\cdot(x^2 + 2x + 2)$	**Sofijas-Žermēnas identitāte:** $a^4 + 4b^4 = \left((a+b)^2 + b^2\right) \cdot \left((a-b)^2 + b^2\right)$
Ja $a + b + c = 0$, tad $a^3 + b^3 + c^3 = 3abc$.	**3 kubu identitāte:** $a^3 + b^3 + c^3 - 3abc = (a+b+c)\left(a^2 + b^2 + c^2 - ab - bc - ca\right)$. **Sekas:** $(x-y)^3 + (y-z)^3 + (z-x)^3 = 3(x-y)(y-z)(z-x)$.

1. Novērtēt aritmētisko, ģeometrisko progresiju un progresiju summu augšanas ātrumu un attiecīgo formulu izvedumus.
2. Pildīt Eiklīda algoritmu $\mathrm{LKD}(a, b)$ atrašanai, pamanīt atšķirības, ja a, b ir/nav savstarpēji pirmskaitļi.

4.1 Ievaduzdevumi

4.1. Uzdevums (IMO1959.1): Pierādīt, ka daļa $\dfrac{21n+4}{14n+3}$ ir nesaīsināma katram naturālam n. (Vispārinājums: kādus nosacījumus jāizpilda (a, b, c, d), lai daļas $\dfrac{an+b}{cn+d}$ būtu nesaīsināmas.)

4.2. Uzdevums (IMO1964.1):

a. Atrast visus naturālos n, kuriem $2^n - 1$ dalās ar 7.

b. Pierādīt, ka neeksistē tāds naturāls n, kuram $2^n + 1$ dalās ar 7.

4.2 Spriedumu un aprēķinu piemēri

1. Aritmētiskas progresijas atlikumi pēc fiksēta moduļa.
2. Bezū identitāte.
3. LKD un savstarpēju pirmskaitļu jēdziens.
4. MKD un LKD sakarību formulas.
5. Eiklīda algoritms efektīvai LKD atrašanai, tā ātrdarbība.
6. Eksponentfunkcijas veidotie atlikumi.
7. Skaitļa a multiplikatīvā kārta pēc moduļa m.
8. Eiklīda algoritms LKD atrašanai. Bezū identitātes atrisināšana.
9. Uzdevuma pārveidošana, reducējot uz citu uzdevumu.

4.3 Uzdevumi

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

4.4. Uzdevums (AT_PL1980.1): Dotas trīs bezgalīgas aritmētiskas progresijas no naturāliem skaitļiem, kurām katrs skaitlis $1, 2, 3, 4, 5, 6, 7$ un 8 pieder vismaz vienai no tām. Pierādīt, ka arī skaitlis 1980 pieder vismaz vienai no tām.

4.5. Uzdevums (IMO1996.1): Dots naturāls skaitlis r un taisnstūrveida laukums $ABCD$ ar izmēriem $AB = 20$, $BC = 12$. Taisnstūris sadalīts ar režģa līnijām 20×12 vienības kvadrātos. Atļauti sekojoši gājieni - var pārvietoties no viena kvadrāta uz citu tikai tad, ja šo kvadrātu centru attālums ir sqrt{r}. Uzdevums ir atrast gājienu virkni, kas aizved no kvadrāta, kas satur virsotni "A" uz kvadrātu, kas satur virsotni "B".

a. Pierādīt, ka uzdevums nav izpildāms, ja r dalās ar 2 vai ar 3.
b. Pierādīt, ka uzdevums ir izpildāms, ja $r = 73$.
c. Vai uzdevums ir izpildāms, ja $r = 97$?

4.6. Uzdevums: Aplūkojam naturālu skaitļu kopu:

$$S = \{ax + by \mid x, y \text{ ir veseli un } ax + by > 0\}.$$

Pamatot, ka šajā kopā eksistē minimālais elements $d^* = ax^* + by^*$ un (x^*, y^*) ir viens no Bezū identitātes atrisinājumiem.

4.7. Uzdevums (IMO1979.1): Pieņemsim, ka p un q ir naturāli skaitļi, kuriem izpildās $\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots - \frac{1}{1318} + \frac{1}{1319}$. Pierādīt, ka p dalās ar 1979.

4.8. Uzdevums (IMO1981.4):

a. **Kuriem $n > 2$ eksistē n pēc kārtas sekojoši naturāli skaitļi,** kuriem lielākais skaitlis ir dalītājs mazākajam kopīgajam dalāmajam no pārējiem $n - 1$ skaitļiem?
b. Kurai $n > 2$ vērtībai ir tieši viena kopa ar šo īpašību?

4.9. Uzdevums (IMO1991.4): Pieņemsim, ka G ir sakarīgs grafs ar k šķautnēm. Pierādīt, ka šķautnes var sanumurēt ar skaitļliem $1, 2, \ldots, k$ tā, ka jebkurā virsotnē, kas pieder vismaz divām šķautnēm, visu tajā ienākošo šķautņu lielākais kopīgais dalītājs ir 1.

4.10. Uzdevums: Visiem veseliem pozitīviem skaitļiem m>n pierādīt, ka $MKD(m, n) + MKD(m + 1, n + 1) > \dfrac{2mn}{\sqrt{m - n}}$.

5. DALĪŠANA PIRMREIZINĀTĀJOS

Kaut kas.

6. KOMBINATORISKAS METODES

Something.

7. FERMĀ UN EILERA TEORĒMAS

Kaut kas

8. ĶĪNIEŠU ATLIKUMU TEORĒMA

Etc.

9. MULTIPLIKATĪVAS FUNKCIJAS

ABC.

10. RACIONĀLI UN IRACIONĀLI SKAITĻI

Vēl šis tas.

11. VESELU SKAITĻU POLINOMI

Whatever…

12. ALGEBRISKI PĀRVEIDOJUMI

Pārveidojumi	
Polinomu identitātes	
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.	**Binomiālie koeficienti:** $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$, kur $\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$.
$(a+b+c+d)^4 = \ldots + 12a^2bc + \ldots$, jo $\frac{4!}{2!1!1!} = 12$.	**Polinomiālie koeficienti:** $(a_1 + a_2 + \cdots + a_m)^n$ izvirzījums satur $a_1^{k_1}a_2^{k_2}\cdots a_m^{k_m}$ ar koeficientu $\frac{n!}{k_1!k_2!\cdots k_m!}$, ja $k_1 + k_2 + \cdots + k_m = n$.
$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$.	**Nepāru pakāpju summa:** $a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n})$.
$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$.	**Pakāpju starpība:** $a^n - b^n =$ $= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.
$ax^2 + bx + c = 0$ ir 3 saknes $\Rightarrow a = b = c = 0$	**Identiski polinomi:** Ja $P(x)$ un $Q(x)$ ir n-tās pakāpes polinomi un to vērtības sakrīt $n+1$ dažādiem x_i, tad $P(x) = Q(x)$.
$P(x) = 4x^3 - 3x^2 - 25x - 6$ dalās ar $(x-3)$.	Polinoms $P(x)$ dalās ar $(x-a)$ tad un tikai tad, ja a ir $P(x)$ sakne.
$x^4 + 4 =$ $= (x^2 - 2x + 2)\cdot$ $\cdot(x^2 + 2x + 2)$	**Sofijas-Žermēnas identitāte:** $a^4 + 4b^4 = \left((a+b)^2 + b^2\right)\cdot\left((a-b)^2 + b^2\right)$
Ja $a + b + c = 0$, tad $a^3 + b^3 + c^3 = 3abc$.	**3 kubu identitāte:** $a^3 + b^3 + c^3 - 3abc = (a+b+c)\left(a^2 + b^2 + c^2 - ab - bc - ca\right)$. **Sekas:** $(x-y)^3 + (y-z)^3 + (z-x)^3 = 3(x-y)(y-z)(z-x)$.

13. NEVIENĀDĪBAS SKAITĻU TEORIJĀ

Sth.

14. EKSTREMĀLIE ELEMENTI

Kautkas.

15. MATEMĀTISKĀS INDUKCIJAS METODE

DEF

16. VALUĀCIJAS

Abc.