DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

16.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Pirmskaitļi **4**

1.1. Pirmskaitļu īpašības, hipotēzes un neatrisinātas problēmas 4

1.1.1. Fakti 4

1.1.2. Speciāla veida pirmskaitļi 6

1.1.3. "Pirmskaitļu teorēma" 7

1.1.4. Pirmskaitļu virknes 9

1.1.5. Goldbaha hipotēze 10

1.2. Rīmana ζ-funkcija 10

1.2.1. Definīcija 10

1.2.2. Vienkāršākās īpašības 11

2. Skaitļu teorija un ģeometrija **14**

2.1. Vienkārši rezultāti 14

2.1.1. Režģi 14

2.1.2. Veselo punktu skaitīšana 17

2.1.3. Gausa un Eizenšteina skaitļi 19

2.2. Klasiski rezultāti 23
2.2.1. Gausa riņķa problēma 23
2.2.2. Dirihlē dalītāju problēma 25

3. 16.mājasdarbs **27**

1. Pirmskaitļi

Pirmskaitļi dabā - dažiem dzīvniekiem dzīves (attīstības) cikla ilgums (gados) ir pirmskaitlis, tas ir izveidojies evolūcijas rezultātā, lai labāk izvairītos no plēsējiem.

Ja kukaiņa dzīves cikla garums n ir salikts skaitlis, tad evolūcijas rezultātā lielāka iespēja ir parādīties vairākiem plēsējiem, kuru dzīves ciklu garumu ir n dalītāji, tādējādi dotās sugas kukaiņi būs vairāk apdraudēti. Evolūcijas rezultātā kukaiņu dzīves cikla ilgums konverģē uz pirmskaitli. Ir zināmi konkrēti piemēri.

1.1. Pirmskaitļu īpašības, hipotēzes un neatrisinātas problēmas

1.1.1. Fakti

Visi pirmskaitļi $p > 3$ apmierina nosacījumu

$$p \equiv \pm 1 (\mathrm{mod}\ 6).$$

1.1. teorēma. Eksistē patvaļīgi gari "pirmskaitļu tuksneši".

1.2. teorēma. (*Bertrana postulāts, Čebiševa teorēma*)

$$\forall n > 1 \; \exists p : n < p < 2n.$$

1.3. teorēma. Rinda $\sum_p \frac{1}{p}$ diverģē.

1.4. teorēma. (*Dirihlē teorēma par pirmskaitļiem aritmētiskās progresijās*) Ja $LKD(a, b) = 1$, tad aritmētiskā progresija

$$a, a + b, a + 2b+, ...$$

satur bezgalīgi daudz pirmskaitļu. Ekvivalents formulējums: eksistē bezgalīgi daudz pirmskaitļu p, kas apmierina nosacījumu

$$p \equiv a (\text{mod } b).$$

1.1. piezīme. Diezgan viegli ir pierādīt Dirihlē teorēmu speciālgadījumos, piemēram $p \equiv 1(\text{mod } 2)$ vai $p \equiv 3(\text{mod } 4)$.

1.1.2. Speciāla veida pirmskaitļi

Tiek pētītas vairākas pirmskaitļu sērijas. Pirmskaitļi ir vajadzīgi kriptogrāfijā.

Populārākā pirmskaitļu sērijas:

- *Fermā pirmskaitļi* $2^{2^n}+1$ - $3, 5, 17, 257, 65537$;
- *Mersenna pirmskaitļi* 2^n-1 - 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, ..., pašlaik ir zināmi ap 26 pirmskaitļi;
- *Vagstafa pirmskaitļi* $\frac{2^n+1}{3}$ - 3, 11, 43, 683, 2731, 43691, 174763, 2796203,...;

1.1.3. "Pirmskaitļu teorēma"

Definēsim ar $\pi(x)$ pirmskaitļu skaitu, kas nepārsniedz x:

$$\pi(x) = \sum_{p \leq x} 1.$$

Definēsim

$$li(x) = \int_0^x \frac{dt}{\ln(t)}.$$

K.Gauss ap 1792.gadu izteica hipotēzi, kas tika pierādīta tikai 1896.gadā.

1.5. teorēma. (*pirmskaitļu teorēma*)

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

vai

$$\lim_{x\to\infty} \frac{\pi(x)}{li(x)} = 1.$$

PIERĀDĪJUMS Ļoti grūts. Vienādība seko no Lopitāla teorēmas. ■

1.2. piezīme. Īstenībā tika pierādīts vairāk:

$$|\pi(x) - li(x)| < C_1 x e^{-C_2\sqrt{ln(x)}}.$$

Vēlāk tika pierādīts, ka $\pi(x) - li(x)$ bezgalīgi bieži maina zīmi. Nav zināms neviens x, kuram $\pi(x) - li(x) > 0$.

1.3. piezīme. Hipotēze:

$$\pi(x) = li(x) + O(\sqrt{x}ln(x)).$$

1.1.4. Pirmskaitļu virknes

Pirmskaitļu pāri $(p, p+2)$ sauc par *dvīņu pirmskaitļiem.*

Hipotēze: dvīņu pirmskaitļu ir bezgalīgi daudz.

Hipotēzes: pirmskaitļu virkņu

- $(p, p+4)$,
- $(p, p+6)$,
- $(p, p+2, p+6)$,
- $(p, p+4, p+6)$,
- $(p, p+2, p+6, p+8)$,
- $(p, p+2, p+6, p+8, p+12)$,

ir bezgalīgi daudz.

1.1.5. Goldbaha hipotēze

Hipotēze (*stiprā Goldbaha hipotēze*): katrs pāra skaitlis $n > 2$ ir izsakāms divu pirmskaitļu summas veidā (1742.gads). (Pārbaudīta līdz 10^{18}).

Hipotēze (*vājā Goldbaha hipotēze*): katrs nepāra skaitlis $n > 7$ ir izsakāms trīs pirmskaitļu summas veidā (1742.gads). (Ir pierādīta pietiekoši lieliem n.)

1.2. Rīmana ζ-funkcija

1.2.1. Definīcija

Rīmana ζ-funkcija tiek definēta ar vienādību

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

1.2.2. Vienkāršākās īpašības

1.6. teorēma.

1. Ja $s > 1$, tad $\zeta(s)$ konverģē.
2. Ja $s \leq 1$, tad $\zeta(s)$ diverģē.

PIERĀDĪJUMS
Izmantojam pozitīvu rindu konverģences Košī integrālo pazīmi -

$$\int_1^{+\infty} x^{-s} dx < \infty \iff s > 1.$$

■

1.7. teorēma. Ja $s > 1$, tad

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

PIERĀDĪJUMS Ievērosim, ka

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + ...$$

Definēsim

$$P_k(s) = \prod_{i=1}^{k} \frac{1}{1-p_i^{-s}}.$$

Redzam, ka

$$P_k(s) = \sum_{n \in D_k} \frac{1}{n^s},$$

kur kopa D_k satur visus naturālos skaitļus, kas dalās tikai ar pirmajiem k pirmskaitļiem.

$n \notin D_n \implies n > p_k$.

$$|P_k(s) - \zeta(s)| = \sum_{n \notin D_k} \frac{1}{n^s} \leq \sum_{n > p_k} \frac{1}{n^s} = \zeta(s) - \sum_{n \leq p_k} \frac{1}{n^s}.$$

Redzam, ka

$$k \to \infty \implies \zeta(s) - \sum_{n \leq p_k} \frac{1}{n^s} \to 0.$$

■

2. Skaitļu teorija un ģeometrija

2.1. Vienkārši rezultāti

2.1.1. Režģi

Punktu Dekarta koordinātu sistēmā (taisnē, plaknē, telpā) sauksim par *veselu punktu* ja tā koordinātes ir veseli skaitļi. Tādējādi ģeometriskajās telpā veselu punktu koordinātes ir veseli skaitļi, veselu skaitļu pāri vai trijnieki.

Visu virkņu $(x_1, x_2, ..., x_n)$, $x_i \in \mathbb{R}$, kopu sauc par n-dimensionālu telpu, apzīmē ar $\mathbb{R}^n$, x_i sauc par koordinātēm. n-dimensionālas telpas elementu sauc par veselu punktu, ja visas koordinātes ir veseli skaitļi.

Telpā $\mathbb{R}^n$ var definēt vektorus, operācijas ar vektoriem. Var definēt *mēru* - lielumu, kas vispārina laukumu un tilpumu. Ja paralēlskaldnis tiek konstruēts uz vektoriem $v_1, ..., v_n$ un $v_i = (v_{i1}, v_{i2}, ..., v_{in})$, tad tā

mērs ir vienāds ar lieluma

$$\det \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{12} & v_{22} & \dots & v_{2n} \\ \dots & \dots & \dots & \dots \\ v_{n1} & v_{n2} & \dots & v_{nn} \end{bmatrix}$$

absolūto vērtību.

Veselu punktu kopā $\mathbb{R}^n$ sauc arī par *režģa punktu* un visu veselo punktu kopu - par *režģi*, to apzīmē ar $\mathbb{Z}^n$. $\mathbb{Z}^2$ sauc arī par *kvadrātisku režģi*, $\mathbb{Z}^3$ - par *kubisku režģi*.

Vispārīgāk, par režģi sauc arī punktu kopu formā

$$\lambda_1 v_1 + \dots + \lambda_n v_n,$$

kur katram i skaitlis λ_i ir vesels skaitlis un vektori $v_1, \dots, v_n$ (*režģa bāze*) ir lineāri neatkarīgi (veido lineārās telpas $\mathbb{R}^n$ bāzi). Dažādas bāzes var ģenerēt vienu un to pašu režģi.

Divus punktus $x \in \mathbb{R}^n$ un $y \in \mathbb{R}^n$ sauksim par *salīdzināmiem (kongruentiem) attiecībā uz režģi* $\mathcal{R}$, ja

$$x - y \in \mathcal{R}.$$

Tā ir ekvivalences attiecība, kas sadala visu kopu $\mathbb{R}^n$ ekvivalences klasēs.

Par režģa $\mathcal{R}$ ar bāzi $v_1, ..., v_n$ fundamentālo apgabalu sauc kopu

$$\mathcal{D} = \{\alpha_1 v_1 + ...\alpha_n v_n | 0 \leq \alpha_i < 1\}.$$

Var redzēt, ka

- katrai punktu kongruences klasei ir pārstāvis kopā $\mathcal{D}$;
- kopas $\mathcal{D} + r$, $r \in \mathcal{R}$ pārklāj visu telpu $\mathbb{R}^n$.

Paralēlskaldņa tilpumu, kas ir uzbūvēts uz režģa bāzes tilpumu sauc par režģa *fundamentālo tilpumu*. Režģi, kas atbilst veseliem punktiem, sauc par *vienības režģi*. Vienības režģa fundamentālais tilpums ir vienāds ar 1.

2.1. piezīme. Režģis veido grupu attiecībā uz vektoru saskaitīšanas operāciju:

1. divu režģa vektoru summa ir režģa vektors;
2. 0 ir režģa elements;
3. ja v ir režģa elements, tad $-v$ arī ir režģa elements.

2.2. piezīme. Kubiskos režģus plaši pielieto kristalogrāfijā.

2.1.2. Veselo punktu skaitīšana

2.1. teorēma. Veselo punktu skaits intervālā $[a, b]$ ir vienāds ar $[b-a]$.

Lai atrastu veselus punktus uz taisnes

$$ax + by = c,$$

ir jāprot risināt lineāri vienādojumi.

2.2. teorēma. Veselo punktu skaits taisnstūrī ar virsotnēm $(0,0)$, $(m,0)$, $(0,n)$, (m,n) ir vienāds ar $(m+1)(n+1)$.

2.3. teorēma. Veselo punktu skaits līklīnijas trapecē $a \le x \le b$, $0 \le y \le f(x)$ ir vienāds ar

$$\sum_{a \le x \le b, x \in \mathbb{Z}} \lceil f(x) \rceil = \sum_{a \le x \le b, x \in \mathbb{Z}} ([f(x)] + 1).$$

2.4. teorēma. Veselo punktu skaits riņķī $x^2 + y^2 \le R^2$ ir vienāds ar

$$1 + 4[R] + 8 \sum_{0 < x \le \frac{R}{\sqrt{2}}} [\sqrt{R^2 - x^2}] - 4[\frac{R}{\sqrt{2}}]^2.$$

PIERĀDĪJUMS Diskusija. ■

2.1.3. Gausa un Eizenšteina skaitļi

Īss pārskats par kompleksajiem skaitļiem.

Kompleksos skaitļus formā $x + iy$, kur $x \in \mathbb{Z}$ un $y \in \mathbb{Z}$, sauc par *Gausa skaitļiem* vai *Gausa veselajiem skaitļiem*. Gausa skaitļu kopu apzīmē ar $\mathbb{Z}[i]$. Redzam, ka $\mathbb{Z} \subset \mathbb{Z}[i]$. Gausa skaitļus var domāt arī kā vektorus plaknē.

Par Gausa skaitļa $x + iy$ *normu* sauc lielumu

$$\sqrt{x^2 + y^2} = \sqrt{(x + iy)(x - iy)}.$$

Gausa skaitļu kopā var definēt dalāmību, pirmskaitļus. Piemēram, $2 \in \mathbb{Z}[i]$ nav pirmskaitlis, jo $2 = (1 + i)(1 - i)$.

2.5. teorēma.

1. Gausa skaitļi veido gredzenu attiecībā uz komplekso skaitļu saskaitīšanas un reizināšanas operācijām.
2. Gausa skaitļu gredzens nav lauks (skaitlim 2 nav inversā elementa).
3. $u \in \mathbb{Z}[i]$ ir invertējams tad un tikai tad, ja $u^2 = \pm 1$.
4. Gredzenā $\mathbb{Z}[i]$ nav nulles dalītāju.
5. Ja $a \in \mathbb{Z}[i]$, $b \in \mathbb{Z}[i]$ un $b \neq 0$, tad eksistē q un r, tāds, ka $|r| < |b|$ un
$$a = qb + r.$$

PIERĀDĪJUMS

5. Vektori b un ib veido režģi $\mathcal{R}_b$. Ja $q = q' + iq''$, tad
$$qb = (q' + iq'')b = q'b + q''(ib) \in \mathcal{R}_b$$
un, otrādi, katrs $\mathcal{R}_b$ vektors ir izsakāms formā $q'''b$. Maksimālais attālums no a līdz tuvākajam $\mathcal{R}_b$ punktam b' nav lielāks kā $\frac{|b|}{\sqrt{2}}$, tāpēc eksistē q tāds, ka $|a - qb| < |b|$. ■

Definēsim $\omega = e^{\frac{2i\pi}{3}} = \frac{-1+\sqrt{3}}{2}$. Citiem vārdiem sakot, ω ir viens no vienādojuma $z^3 = 1$ atrisinājumiem.

Kompleksos skaitļus formā $x + \omega y$, kur $x \in \mathbb{Z}$ un $y \in \mathbb{Z}$, sauc par *Eizenšteina skaitļiem*. Eizenšteina skaitļu kopu apzīmē ar $\mathbb{Z}[\omega]$. Redzam, ka $\mathbb{Z} \subset \mathbb{Z}[\omega]$. Eizenšteina skaitļus var domāt arī kā vektorus plaknē.

Par Eizenšteina skaitļa $x + \omega y$ *normu* sauc lielumu

$$|x + \omega y| = \sqrt{x^2 - xy + y^2}.$$

Eizenšteina skaitļu kopā var definēt dalāmību, pirmskaitļus. Piemēram, $3 \in \mathbb{Z}[\omega]$ nav pirmskaitlis, jo $3 = (2 + \omega)(1 - \omega)$. 7 nav pirmskaitlis, jo $7 = (1 - 2\omega)(3 + 2\omega)$.

2.6. teorēma.

1. Eizenšteina skaitļi veido gredzenu attiecībā uz komplekso skaitļu saskaitīšanas un reizināšanas operācijām.
2. Eizenšteina skaitļu gredzens nav lauks (skaitlim 2 nav inversā elementa).
3. $u \in \mathbb{Z}[\omega]$ ir invertējams tad un tikai tad, ja $u \in \{\pm 1, \pm\omega, \pm\omega^2\}$.
4. Gredzenā $\mathbb{Z}[\omega]$ nav nulles dalītāju.
5. Ja $a \in \mathbb{Z}[\omega]$, $b \in \mathbb{Z}[\omega]$ un $b \neq 0$, tad eksistē q un r, tāds, ka $|r| < |b|$ un
$$a = qb + r.$$

PIERĀDĪJUMS ■

Var definēt *Kummera gredzenu* $\mathbb{Z}[\zeta_m]$, kur $\zeta_m = e^{\frac{2i\pi}{m}}$.

2.2. Klasiski rezultāti

2.2.1. Gausa riņķa problēma

Apzīmēsim ar $r_2(n)$ veidu skaitu kā n ir iespējams izteikt divu veselu skaitļu kvadrātu sakārtotas summas veidā.

2.1. piemērs. $4 = (\pm 2)^2 + 0^2 = 0^2 + (\pm 2)^2$, tāpēc $r_2(4) = 4$.

2.7. teorēma.

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} r_2(n) = \pi.$$

PIERĀDĪJUMS $r_2(n)$ ir veselo punktu skaits uz riņķa līnijas

$$x^2 + y^2 = n.$$

Redzam, ka $\sum_{n=0}^{N} r_2(n)$ ir veselo punktu skaits riņķī R_N, kuru nosaka nevienādība $x^2 + y^2 \leq N$.

Katram veselam punktam P riņķī R_N piekārtosim kvadrātu ar malas garumu 1, kura malas ir paralēlas koordinātu asīm, un kuram P ir augšējais kreisais stūris.

Šādu kvadrātu laukumu summa ir vienāda ar veselo punktu skaitu $\sum_{n=0}^{N} r_2(n)$.

Jo lielāks ir N, jo tuvāka šī kvadrātu laukumu summa ir riņķa R_N laukumam πN. Tātad pārejot uz robežu, kad $N \to \infty$, iegūsim

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} r_2(n) = \lim_{N\to\infty} \frac{\pi N}{N} = \pi.$$

■

2.2.2. Dirihlē dalītāju problēma

Apzīmēsim ar $d(n)$ naturāla skaitļa n naturālo dalītāju skaitu.

Teiksim, ka $a_n = O(b_n)$, ja eksistē pozitīva konstante c un vesels skaitlis n_0 tādi, ka

$$0 \leq a_n \leq cb_n$$

visiem $n > n_0$. Virkni b_n sauksim par virknes a_n *augšējo asimptotisko robežu*. Alternatīva definīcija: $a_n = O(b_n)$, ja

$$\lim_{n\to\infty} \frac{a_n}{b_n} < \infty.$$

2.8. teorēma.

$$\sum_{n=0}^{N} d(n) = N \ln N + cN + O(\sqrt{N}).$$

PIERĀDĪJUMS $d(n)$ ir vienāds ar veselo punktu skaitu uz hiperbolas $xy = n$ valējā pirmajā kvadrantā. $\sum_{n=0}^{N} d(n)$ ir veselo punktu skaits valējā pirmajā kvadrantā, kas apmierina nevienādību $xy \leq N$. ■

3. 16.mājasdarbs

16.1 Atrodiet veselo punktu skaitu šādās ģeometriskās figūrās:

(a) nogrieznī ar veselām koordinātēm (x_i, y_i), $i \in \{1, 2\}$;
(b) trijstūrī ar veselām virsotnēm (x_i, y_i), $i \in \{1, 2, 3\}$;
(c) nogrieznī ar veselām koordinātēm (x_i, y_i, z_i), $i \in \{1, 2\}$.