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

Studiju kurss

Veselo skaitļu teorija

17.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Skaitļu teorija un ģeometrija

1.0.1. Veselo punktu skaitīšana

1.1. piezīme. Veselo punktu skaits intervālā $[a, b]$ ir saistīts ar $[b-a]$.

Lai atrastu veselus punktus uz taisnes

$$ax + by = c,$$

ir jāprot risināt lineāri vienādojumi.

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

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

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

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

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

PIERĀDĪJUMS Diskusija. ■

1.0.2. 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 $2 = (1 + i)(1 - i)$.

1.4. 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 $7 = (1 - 2\omega)(3 + 2\omega)$.

1.5. 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 $\zeta_m = e^{\frac{2i\pi}{m}}$.

1.1. Klasiski rezultāti

1.1.1. Gausa riņķa problēma

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

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

1.6. 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

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

■

1.1.2. Nejaušu veselu punktu LKD

Cik kvadrātā ar virsotnēm $(0,0,),(0,m-1),(m-1,0),(m-1,m-1)$ ir punktu (x,y), kuriem $LKD(x,y)=1$?

Kāda ir to attieciba pret visu veselo punktu skaitu šajā kvadrātā? Citiem vārdiem sakot, kāda ir varbūtība, ka nejaušs punkts apmierina nosacījumu?

Kāda ir šīs varbūtības robeža, kad $m \to \infty$?

1.7. teorēma. Varbūtība, ka nejaušs veselo skaitļu pāris (x,y) apmierina nosacījumu $LKD(x,y)=1$, ir vienāda ar

$$\frac{1}{\zeta(2)}.$$

PIERĀDĪJUMS

Kvadrātā K_m ar virsotnēm $(0,0,),(0,m-1),(m-1,0),(m-1,m-1)$ veselo punktu skaits ir vienāds ar m^2.

Izmantosim divus kombinatorikas principus:

- skaitīšana izmantojot papildinājumu,
- sieta (ieslēgšanas-izslēgšanas) principu.

Skaitīsim, cik K_m ir veselu punktu (x, y), kuriem

$$LKD(x, y) \geq 2$$

(cik punktu ir interesējošās kopas papildinājumā), apzīmēsim šo punktu kopu ar S, un pēc tam atņemsim to no m^2.

Definēsim S_n kā to K_m veselo punktu (x, y) kopu, kuriem izpildās nosacījums

$$n | LKD(x, y).$$

Redzam, ka

- $S = S_2 \cup S_3 \cup ... S_p$, kur p ir lielākais pirmskaitlis, kas dala m,
- $LKD(n, n') = 1 \implies S_{nn'} = S_n \cap S_{n'}$.

Sieta (ieslēgšanas-izslēgšanas) princips. Ir dotas vairākas galīgas kopas $A_1, ..., A_n$, ir zināmi elementu skaiti kopām A_i, $A_i \cap A_j$,...,$A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}$. Tad elementu skaitu apvienojumā $A_i \cup ... \cup A_n$ var atrast izmantojot šādu formulu:

$$|A_1 \cap ... A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \\ ... + (-1)^{n+1} |A_1 \cap ... \cap A_n|.$$

Redzam, ka

$$|S| = \sum_{p} |S_p| - \sum_{p_1<p_2} |S_{p_1} \cap S_{p_2}| + ... = \\ \sum_{p} |S_p| - \sum_{p_1<p_2} |S_{p_1 p_2}| + \sum_{p_1<p_2<p_3} |S_{p_1 p_2 p_3}| - ...$$

Novērtēsim S_k:

$$S_k \sim \frac{m^2}{k^2}.$$

Tādējādi

$$\begin{aligned} m^2 - |S| &= m^2 - \sum_p |S_p| + \sum_{p_1<p_2} |S_{p_1p_2}| - \sum_{p_1<p_2<p_3} |S_{p_1p_2p_3}| + \ldots \\ &\sim \underbrace{\frac{m^2}{2^2} + \frac{m^2}{3^2} + \ldots}_{\text{pirmskaitļi}} - \underbrace{\frac{m^2}{2^2 3^2}}_{\text{pirmskaitļu pāri}} - \ldots \\ &\sim m^2(1 - \frac{1}{2^2})(1 - \frac{1}{3^2})\ldots = m^2 \prod_p (1 - \frac{1}{p^2}) \end{aligned}$$

Redzam, ka robežgadījumā proporcija $\frac{m^2 - |S|}{m^2}$ ir

$$\prod_p (1 - \frac{1}{p^2}) = \prod_p \frac{p^2 - 1}{p^2} = \frac{1}{\prod_p \frac{p^2}{p^2-1}} = \frac{1}{\prod_p \frac{1}{1-p^{-2}}} = \frac{1}{\zeta(2)}.$$

■

1.2. piezīme. Kā atrast $\zeta(2)$?

$$\int_0^1\int_0^1 \frac{1}{1-xy}dxdy = \int_0^1\int_0^1 \sum_{n=1}^{\infty}(xy)^n dxdy.$$

Apskatīsim funkciju $f(x)$, kas ir 2π-periodiska un definēta intervālā $[-\pi,\pi]$ kā $f(x)=x^2$, tad

$$f(x) = \frac{1}{3} + \frac{4}{\pi^2}\sum_{n=1}^{\infty}\frac{(-1)^n}{n^2}\cos(n\pi x).$$

Apskatot $f(\pi)$, iegūsim

$$\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Var pierādīt, ka

$$\sin(x) = x \prod_{n=1}^{\infty} (1 - \frac{1}{n^2\pi^2} x^2).$$

Pamatojums - "Bezū teorēma" ar bezgalīgu vienkāršu sakņu kopu, jāprecizē koeficients izmantojot pirmo ievērojamo robežu.

Apskatot abām pusēm Teilora koeficientu pie x^3, iegūsim to pašu rezultātu.

1.1.3. Pika teorēma

1.3. piezīme. Ja a un b ir veseli skaitļi, tad nogriežņa $[a, b]$ garums $b - a$ ir vienāds ar $I + \frac{B}{2}$, kur I ir nogriežņa iekšējo veselo punktu skaits, $B = 2$ ir galapunktu skaits. Šo formulu var pamatot tā, ka katrs iekšējs punkts "rada" ap sevi simetrisku nogriezni ar garumu 1, bet katrs galapunkts - tikai nogriezni ar garumu $\frac{1}{2}$.

1.4. piezīme. Taisnstūrim ar veselām virsotnēm (a,b), $(a+u,b)$, $(a,b+v)$, $(a+u,b+v)$, laukums uv ir vienāds ar $I+\frac{B}{2}-1$. Redzam, ka $I=(u-1)(v-1)$ un $B=2u+2v$, tāpēc

$$I+\frac{B}{2}-1=uv-u-v+1+u+v-1=uv.$$

1.8. teorēma. (*Pika teorēma*) Ja D ir plakans daudzstūris bez malu paškrustojumiem, kura virsotnes ir veseli punkti, I ir D iekšējo veselo punktu skaits, B ir veselo punktu skaits uz D robežas, tad D laukums ir vienāds ar

$$I+\frac{B}{2}-1$$

PIERĀDĪJUMS
Izmantosim matemātisko indukciju ar laukumu kā parametru.

No sākuma pierādīsim, ka apgalvojums ir patiess trijstūriem ar šādu soļu palīdzību:

1) pierādām, ka formula ir pareiza taisnstūriem, kuru malas ir paralēlas koordinātu asīm;
2) pierādām, ka formula ir pareiza taisnleņka trijstūriem, kuru katetes ir paralēlas koordinātu asīm;
3) pierādām, ka formula ir pareiza trijstūriem, kuru viena mala ir paralēla koordinātu asīm;
4) pierādām, ka formula ir pareiza visiem trijstūriem.

Pieņemsim, ka apgalvojums ir pierādīts visiem daudzstūriem, kuru laukums ir mazāks kā S un pierādīsim, ka tādā gadījumā tas ir patiess arī daudzstūriem ar laukumu S.

Pieņemsim, ka ir dots daudzstūris D ar laukumu S, iekšējo veselo punktu skaitu I un robežas veselo punktu skaitu B. Eksistē diagonāle, kas kopā ar divām malām veido trijstūri, tātad D ir kāda daudzstūra D' (ar laumu mazāku kā S) un trijstūra apvienojums. Daudzstūrim D' Pika formula ir pareiza saskaņā ar indukcijas pieņēmumu, trijstūrim Pika formula ir spēkā. Pierādīsim, ka no šiem diviem faktiem seko Pika formulas pareizība daudzstūrim D.

Pieņemsim, ka D' laukums ir S', iekšējo veselo punktu skaits ir I' un robežas veselo punktu skaits ir B'. Pieņemsim, ka trijstūrim laukums ir S_T, iekšējo veselo punktu skaits ir I_T un robežas veselo punktu skaits ir B_T. Zinām, ka

$$S' = I' + \frac{B'}{2} - 1$$

un

$$S_T = I_T + \frac{B_T}{2} - 1.$$

Pieņemsim, ka veselo punktu skaits uz diagonāles, kas atdala D' no trijstūra, ir vienāds ar δ. Redzam, ka

$$I = I' + I_T + \delta - 2.$$

un

$$B = B' + B_T - 2\delta + 2.$$

Redzam,ka

$$S = S' + S_T = (I' + \frac{B'}{2} - 1) + (I_T + \frac{B_T}{2} - 1) =$$
$$(I' + I_T + \delta - 2) + (2 - \delta) - 1 + \frac{B' + B_T - 2\delta + 2}{2} + \frac{2\delta - 2}{2} - 1 =$$
$$I + \frac{B}{2} - 1.$$

■

1.5. piezīme. Pika teorēmu var vispārināt uz gadījumu, kad daudzstūrim ir "caurumi" ar veselām virsotnēm. Ja daudzstūrim ir k "caurumi", tad tā laukums ir vienāds ar $I + \frac{B}{2} - 1 + k$.

1.6. piezīme. Pika teorēmu var izmantot, lai skaitītu veselos punktus plaknes figūrās.

1.1.4. Minkovska teorēma

Ģeometrisku figūru F sauc par *centrāli simetrisku*, ja $(x, y) \in F$ tad un tikai tad, ja $(-x, -y) \in F$. Ģeometrisku figūru F sauc par *izliektu*, ja no tā, ka $A \in F$ un $B \in F$ seko, ka $AB \subseteq F$.

1.7. piezīme. Taisnē centrāli simetrisks nogrieznis, kas ir garāks kā 2, satur nenulles veselu skaitli.

Kvadrāts ar virsotnēm $(\pm 1, \pm 1)$ un laukumu 4 robežojas ar veseliem punktiem.

1.9. teorēma. (*Minkovska teorēma fundamentālajam režģim plaknē*) Katra izliekta un centrāli simetriska plaknes figūra F, kuras laukums S ir lielāks kā 4, satur nenulles veselu punktu (punktu, kas nav $(0,0)$).

PIERĀDĪJUMS Katram naturālam t apskatīsim taisnes

$$x = \frac{2a}{t}$$

un

$$y = \frac{2b}{t},$$

kur a un b ir veseli skaitļi. Šīs taisnes sadala plakni kvadrātos ar virsotnēm $(\frac{2a}{t}, \frac{2b}{t})$, malas garumu $\frac{2}{t}$ un laukumu $\frac{4}{t^2}$.

Apzīmēsim ar $C(t)$ kvadrātu virsotņu skaitu, kas pieder F. Redzam, ka

$$\lim_{t\to\infty} \frac{4}{t^2} C(t) = S,$$

jo katrai virsotnei atbilst tieši viens kvadrāts, kuram tā ir, piemēram, augšējais kreisais stūris un, ja t ir liels, tas visi šādi kvadrāti, kas atbilst virsotnēm figūrā F, labi tuvina F.

$S > 4 \implies S = 4 + \sigma$, kur $\sigma > 0$, tāpēc

$$\lim_{t\to\infty} \frac{1}{t^2} C(t) = 1 + \frac{\sigma}{4}$$

un visiem pietiekoši lieliem t izpildās nosacījums

$$\frac{1}{t^2} C(t) > 1$$

jeb

$$C(t) > t^2$$

Dalot pāra (a, b) elementus ar t, var iegūt ne vairāk kā t^2 atlikumu pārus, tāpēc eksistē divi skaitļu pāri - punkti $P_1 = (a_1, b_1)$ un $P_2 = (a_2, b_2)$, kuriem atlikumu pāri ir vienādi:

$$a_1 \equiv a_2 \pmod{t} \text{ un } b_1 \equiv b_2 \pmod{t}.$$

Nogriežņa P_1P_2 viduspunkts

$$\left(\frac{2a_2 - 2a_1}{2t}, \frac{2b_2 - 2b_1}{2t}\right) = \left(\frac{a_2 - a_1}{t}, \frac{b_2 - b_1}{t}\right)$$

ir vesels punkts, kas pieder F. ■

1.10. teorēma. (*Minkovska teorēma fundamentālajam režģim telpā*) Katra izliekta un centrāli simetriska telpas figūra F, kuras tilpums V ir lielāks kā 8, satur nenulles veselu punktu (punktu, kas nav $(0, 0, 0)$).

PIERĀDĪJUMS Līdzīgi plaknes gadījumam. ■

1.8. piezīme. Vispārīgā gadījumā Minkovska teorēma tiek formulēta šādi: ja telpā $\mathbb{R}^n$ ir dots režģis ar fundamentālo tilpumu μ, tad katra izliekta un centrāli simetriska figūra F, kuras tilpums ir lielāks kā $2^n\mu$, satur nenulles veselu punktu.

Izmantojot Minkovska teorēmu pierādīsim kādu klasisku rezultātu.

1.11. teorēma. Naturālu skaitli n var izteikt kā divu veselu skaitļu kvadrātu summu, ja n pirmskaitļu pakāpju sadalījumā nav pirmskaitļu p tādu, ka $p \equiv 3 \pmod 4$.

PIERĀDĪJUMS
Izmantojot *Brahmaguptas-Fibonači identitāti*

$$(x^2+y^2)(z^2+t^2) =$$
$$(xz-yt)^2+(xt+yz)^2 =$$
$$(xz+yt)^2+(xt-yz)^2$$

redzam, ka pietiek pierādīt, ka katru nepāra pirmskaitli p, kuram izpildās nosacījums $p \equiv 1 \pmod 4$, var izteikt kā kvadrātu summu.

Zinām, ka

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

tāpēc -1 ir kvadrātisks atlikums mod p tad un tikai tad, ja

$$p \equiv 1 \pmod 4.$$

Pieņemsim, ka

$$a^2 \equiv -1 \pmod p.$$

Konstruēsim režģi $\mathcal{R}$ ar vektoriem

$$\overrightarrow{v}_1 = (a, 1),$$

$$\overrightarrow{v}_2 = (p, 0).$$

Tā fundamentālais tilpums ir vienāds ar

$$|\det \begin{bmatrix} a & 1 \\ p & 0 \end{bmatrix}| = p.$$

Ja $(x, y) \in \mathcal{R}$, tad

$$(x, y) = n_1 \overrightarrow{v}_1 + n_2 \overrightarrow{v_2} = (n_1 a + n_2 p, n_1),$$

tāpēc

$$x^2 + y^2 = n_1^2 a^2 + 2n_1 n_2 ap + n_2^2 p + n_1^2 \equiv n_1^2(a^2 + 1) \equiv 0 \pmod p.$$

Definēsim F kā riņķi ar rādiusu $\sqrt{(2-0.1)p}$:

$$(x,y) \in F \Leftrightarrow x^2 + y^2 \leq 1.9p.$$

F laukums ir vienāds ar $1.9\pi p > 5.6p > 4p$.

Saskaņā ar Minkovska teorēmu F satur režģa $\mathcal{R}$ nenulles punktu (x_0, y_0).

Zinām, ka

$$x_0^2 + y_0^2 \equiv 0 \pmod{p}$$

un

$$x_0^2 + y_0^2 > 0.$$

No otras puses

$$x_0^2 + y_0^2 \leq 1.9p \implies x_0^2 + y_0^2 = p.$$

■

1.12. teorēma. Katru $n \in \mathbb{N}$ var izteikt kā 4 veselu skaitļu kvadrātu summu.

2. 17.mājasdarbs

17.1 Pierādiet Pika formulas analogu daudzstūriem ar vairākiem caurumiem. (Izmantojot matemātisko indukciju ar caurumu skaitu kā indukcijas parametru).

17.2 Pierādiet, ka pirmskaitlis $p > 3$ ir izsakāms formā $x^2 + xy + y^2$ tad un tikai tad, ja $p \equiv 1 (\mathrm{mod}\ 3)$.