17/10/18

הרצאה 1

ליאור בר-יוסף, שרייבר 302. barylior@post.tau.ac.il

ספרות:

Janusz, "Algebraic number fields"

(יש רשימות במודל)

יהיו רשימות (ספר — לפני המבחן) ותרגילים, ויהיה מבחן סופי

<u>משוואה דיופנטית</u>: משוואה עם מקדמים שלמים, ומחפשים להן פתרונות שלמים.

<u>דוגמה</u>: $x^2-y^2=5$ מחפשים פתרונות שלמים.

$$\Updownarrow$$

$$(x-y)(x+y)=5$$

$$\Leftarrow \quad x-y=s$$

$$x+y=t\ ,\ st=5$$

(הפתרונות ל-s,t הן $\pm5,\pm1$):

יוצא $x=\pm3,\ y=\pm2$

<u>דוגמה</u>: $y^3=x^2+2$. נעבוד ב-$\mathbb{Z}[\sqrt{-2}]$. (פירוק:)

$$y^3=(x+\sqrt{-2})(x-\sqrt{-2})$$

נשים לב ש-x אי-זוגי! (ומשתמש במושג הזרות (co-primality) בתוך $\mathbb{Z}[\sqrt{-2}]$. (נשים לב כי-

$$\gcd(x-\sqrt{-2},\ x+\sqrt{-2})=1$$

שכן,

$$\gcd(x-\sqrt{-2},x+\sqrt{-2})=\gcd(x-\sqrt{-2},\ 2\sqrt{-2})$$

! — $\sqrt{-2}$ ראשוני בתוך $\mathbb{Z}[\sqrt{-2}]$ ולכן נסיק שאם $\sqrt{-2}\mid x-\sqrt{-2}$, אז נכון כי x זוגי.

בנוסף $\mathbb{Z}[\sqrt{-2}]$ מקיים את המשפט היסודי של האריתמטיקה.

כמובן מקיים שקיים פירוק לראשוניים והוא יחיד.

$$\Leftarrow \quad x+\sqrt{-2}=(a+b\sqrt{-2})^3$$

$$\parallel$$

$$a^3-6ab^2+\sqrt{-2}(3a^2b-2b^3)$$

$$\Leftarrow \quad x=a^3-6ab^2$$

$$1=3a^2b-2b^3=b(3a^2-2b^2)$$

$$b=\pm1\ ,\ 3a^2-2b^2=\mp1 \Rightarrow 3a^2=\begin{cases}\cancel{1}\\ 3\end{cases} \Rightarrow a^2=1$$

$$\Rightarrow a=\pm1 \quad (b=1)$$

(b=-1 [illegible]

קיבלנו סה"כ,

$$x=\begin{cases}5\\-5\end{cases}=\pm 5$$

לסיכום הפתרונות הם $x=\pm 5$, $y=3$.

משפט <u>פרמה</u>: $x^n+y^n=z^n$, $n\geq 3$

נרשום -

$$z^n-y^n=x^n$$

$$\prod_{i=1}^{n}(z-\xi^i y)=x^n$$

בחוג הציקלוטומי, $\mathbb{Z}[\xi]$.

Kummer, Lamé – עשו את הטעות הבאה: "הניחו פירוק". בעצם הם הניחו שב-$\mathbb{Z}[\xi]$ יש פריקות יחידה, וזה שגוי. למעשה הטיעון עובד כאשר $n=p$ ראשוני אם p הוא ראשוני רגולרי.

<u>הגדרה</u>: p שזר למס' <u>המחלקה</u> של $\mathbb{Z}[\xi]$ נקרא רגולרי.

מספר המחלקה, באופן אינטואיטיבי, מודד כמה רחוק החוג מלהיות עם פריקות יחידה. משפט מרכזי בשדה מספרים - מס' <u>המחלקה הוא</u> סופי. הכלים הם "גאומטריית המספרים" (תורת מינקובסקי).

משפט נוסף שנוכיח קשור ליחידות,

האיברים ההפיכים $=U(\mathbb{Z})=\{\pm 1\}$

$$U(\mathbb{Z}[i])=\{\pm 1,\pm i\}\cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

<u>אינסופי</u> - $U(\mathbb{Z}[\sqrt{2}])=\{\pm 1=(x+\sqrt{2}y)(x-\sqrt{2}y)=x^2-2y^2\}$

$$=\underbrace{G}_{\text{משה סופי}}\times\mathbb{Z}$$

משפט היחידות של <u>דיריכלה</u> - בחוג שלמים, חבורת היחידות היא תמיד מהצורה -

$$\mathbb{Z}^r\times G$$

כאשר G חבורת שורשי היחידה ~~בשדה~~ בחוג, ו-

$$r_1=\text{מספר השיכונים } \mathbb{Q}(\alpha)\longrightarrow\mathbb{R}$$

$$2r_2=\text{מס' השיכונים שאינם ממשיים } \mathbb{Q}(\alpha)\longrightarrow\mathbb{C}$$

$$r=r_1+r_2-1$$

נושא: שוב, תיבה מינקובסקי.

שדות גלובליים – מספריים / על $\mathbb{F}_q$ שדה סופי עם q איברים.
נסתכל על החוג – $\mathbb{F}_q[T]$ של פולינומים מעל
$\mathbb{F}_q$ ועל $\mathbb{F}_q(T)$ של פונקציות רציונליות. [נסמן
אותם להיות המקביל של $\mathbb{Z}$ ושל $\mathbb{Q}$]

דמיון מפתיע –

$$\mathbb{F}_q[T] \leftrightsquigarrow \mathbb{Z}$$

$\mathbb{F}_q[T]$	$\mathbb{Z}$
- תחום עם שארית	- תחום עם שארית
- מס' סופי של יחידות	- מס' סופי של יחידות
- פירוק יחיד לראשוניים	- פירוק יחיד לראשוניים
- נורמה ($\lvert\mathbb{F}_q[T]/(f)\rvert$) $= q^{\deg(f)}$	- נורמה ($\lvert\mathbb{Z}/n\mathbb{Z}\rvert$)

למשל. מה קורה עם משפט,

PNT – $\pi(x) = \#\{p \leq x\}$, $\pi(x) = \frac{x}{\ln x} + o(x/\ln x)$, $x \to \infty$

יש אנלוג לפולינומים ראשוניים –

$$\pi_q(n) = \{P \in \mathbb{F}_q[T] \mid \deg P = n\}$$

P מתוקן ואי פריק.

PPT – $\pi_q(n) \approx \frac{q^n}{n}$, $q^n \longrightarrow \infty$

כמו שציפינו, תוצאה כזו תקפה יותר – $\pi_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$ ← $\log_q(q^n)$!

הוספה: נגדיר –

$$(\mathrm{Re}(s) > 1) \qquad \zeta_q(s) = \sum_{f \text{ מתוקן}} \frac{1}{|f|^s} = \sum_{f \text{ מתוקן}} \frac{1}{q^{\deg f \cdot s}} =$$

$$\overset{u=q^{-s}}{=} \sum_{d=0}^{\infty} \sum_{\substack{f \text{ מתוקן} \\ \deg f = d}} u^d = \sum_{d=0}^{\infty} (qu)^d = \frac{1}{1-qu}$$

$u = q^{-s}$, $|u| = q^{-\mathrm{Re}(s)}$, $|u| < \frac{1}{q}$.

– יש לה המשך אנליטי עם קוטב (פשוט) ב- $s=1$, או $u = 1/q$. ואפסים שלה הם ב- $\mathrm{Re}(s) = \frac{1}{2}$.
(כי אין לה אפסים...)
ויש מכפלת אוילר –

$$\zeta_q(s) = \prod_{P \text{ ראשוני}} (1 - |P|^{-s})^{-1} = \prod_{d=1}^{\infty} (1 - u^d)^{-\pi_q(d)}$$

משפט אופרטור $u\frac{d\log}{du}$:

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} \pi_q(d) \frac{d u^d}{1-u^d}$$

$$\sum_{k=1}^{\infty} (qu)^k = \sum_{d=1}^{\infty} d\pi_q(d) \sum_{r=1}^{\infty} u^{dr}$$

$$\sum_{k=1}^{\infty} q^k \cdot u^k = \sum_{k=1}^{\infty} \Big(\sum_{d\mid k} d\pi_q(d)\Big) u^k$$

$$\Longrightarrow \sum_{d\mid k} d\pi_q(d) = q^k$$

ומוביוס ההיפוך של מוביוס

$$k\pi_q(k) = \sum_{d\mid k} q^d \cdot \mu(k/d)$$

$$\Longrightarrow \pi_q(n) = \frac{1}{n}\sum_{d\mid n} q^d \cdot \mu(n/d)$$

$$\pi_q(n) = \frac{q^n}{n} + \frac{1}{n}\sum_{d\mid n} \mu(n/d)\, q^d = \frac{q^n}{n} + O\Big(\frac{q^{n/2}}{n}\Big)$$

הגד': ראשוניים תאומים – אם p ראשוני וגם $p+2$ ראשוני, נאמר ש-$(p,p+2)$ הם תאומים ראשוניים. האם יש אינסוף כאלה?

יש אינסוף ראשוניים – $\sum \frac{1}{p} = \infty$

אבל, Brun הוכיח ש- $\sum_{p \text{ תאום ראשוני}} \frac{1}{p} < \infty$ - מספר סופי

$$\pi(X;2) = \#\{p \le x : p, p+2 \text{ - ראשוניים תאומים}\}$$

$$\pi(X;2) \approx \frac{x}{\log x \log x} \quad \text{(ניחוש)}$$

זה לא נכון, אבל יש לו מובן נכון. צריך לשקול את ראשוני עם המובן ש-p ראשוני ומתן את על $p+2$, ואז לתקן סיכויים לפי השגיאות המקריים

יצא: $\pi(X;2) \sim C \cdot \frac{x}{(\log x)^2}$ (ראשוניים).

השערת הארדי-ליטלווד

$$C = 2\cdot\prod_{p>2} \frac{\left(1-\frac{2}{p}\right)}{\left(1-\frac{1}{p}\right)^2}$$

נסתכל: תאומים של ראשוניים -

$F_q[T]$, f ו-$f+1$

$$\pi_q(n;1) = \#\{\text{מתוקנים ראשוניים } f, f+1, \deg f = n\}$$

השערה -

$$\pi_q(n;1) \approx C_q \cdot q^n/n^2 \;,\; q^n \to \infty$$

רוצים $\lim_{n\to\infty}$. (לא יודעים אם אף מצליחים)

מסוגלים ב- $\lim_{q\to\infty}\lim_{n\to\infty}$. (לא גם מצליחים...)

מסוגלים ב- $\lim_{n\to\infty}\lim_{q\to\infty}$ - עם כבר משהו, שלוקח כסמנטר ζ.

רעיון: לוקחים הרחבה $L/\mathbb{Q}$ גלואה, עם חבורת גלואה $G = \mathrm{Gal}(L/\mathbb{Q})$. לכל ראשוני p שאינו מסועף ב-L, יש איבר פרובניוס שמוגדר עד כדי הצמדה.

Frob_p

משפט. צ'בוטרב - Frob_p מתפלג אחיד, עבור $1 \le p < x$ וכש $x \to \infty$.