

א. צייל - ציילן פון אונזערע זאכן פון אונזערע זאכן

אונז

אונזערע זאכן

1. דאס איז 2

2. ציילן פון אונזערע זאכן פון אונזערע זאכן
נאך (2)

3. ציילן פון אונזערע זאכן פון אונזערע זאכן
דאס איז 8

4. ציילן פון אונזערע זאכן פון אונזערע זאכן
דאס איז 23

5. ציילן פון אונזערע זאכן פון אונזערע זאכן
דאס איז 27

הקדמה

העבודה שלפנינו נעוץ בקצת צסיפא של מאלא-
קאכרעל. תחילה נסתם על מאלא-זמ מסו
נעלים ייחודים מסו תבואה של מורדל.
נחיה קאלא פרק אה הידע אנהל זמ אלדן
על רבספא של מתקם חלדע"ם (א. יק היאלאניס).
פרק השלישי נעוץ במתקם היאלאניס של מאלא-
קאכרעל. אהז אנהל קדקי תבואה של
Schulze (א) תואה מכן פסיק הרביעי נאכיה כי
הרבספא של מתקם היאלאניס של מאלא קאכרעל
מחבורה אדפס + χ ה"א ו ז כן שנהל
ש"א אנהל מתקם היאלאניס זכ"א אדפס.

2.1. המשפט הראשון (Weil) F היא פולינום מונומיאלי מעלה n מעל $\mathbb{F}_p$

אז מספר הפתרונות של $F(x) \equiv 0 \pmod{p}$ הוא לכל היותר n .

הוכחה: נניח $F(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ ונניח שיש $n+1$ פתרונות שונים $\alpha_1, \dots, \alpha_{n+1}$ של $F(x) \equiv 0 \pmod{p}$. אז

לפי (2.1) $F(x) \equiv 0 \pmod{p}$ אם ורק אם x הוא שורש של $F(x)$ ב- $\mathbb{F}_p$. מכאן שיש $n+1$ שורשים שונים של $F(x)$ ב- $\mathbb{F}_p$. אבל $\mathbb{F}_p$ הוא שדה עם p איברים, ולכן יש לכל היותר p שורשים שונים. מכאן שיש לכל היותר n שורשים שונים של $F(x)$ ב- $\mathbb{F}_p$.

לכן מספר הפתרונות של $F(x) \equiv 0 \pmod{p}$ הוא לכל היותר n .

2.2. המשפט השני (Weil) $N(F, p)$ מספר הפתרונות של $F(x) \equiv 0 \pmod{p}$ הוא

$$|N(F, p) - p^{n-1}| \leq c(F) p^{n-1/2} \quad (2.2)$$

כאשר $c(F)$ הוא קבוע תלוי ב- F ו- p .

הוכחה: נניח $F(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ ונניח שיש $n+1$ פתרונות שונים $\alpha_1, \dots, \alpha_{n+1}$ של $F(x) \equiv 0 \pmod{p}$. אז

היחסים בין המעלות והצורה של המרחב

המעלה של F היא n והמעלה של F היא n (המעלה של F היא n)
 (2.1) F היא פולינום של $x_1, \dots, x_n$ מעל $\mathbb{F}_p$ ויש לה מעלה n ב- x_1 .
 מרחב F הוא n -ממדי, $1, 2, \dots, n-1$.

המעלה של F היא n והמעלה של F היא n

$$F(x_1, \dots, x_n) = a_1 x_1^{l_1} + a_2 x_2^{l_2} + \dots + a_n x_n^{l_n}$$

3. F היא

המעלה של F היא n

$$F(x_1, \dots, x_n) = a_1 x_1^{l_1} + a_2 x_2^{l_2} + \dots + a_n x_n^{l_n} \equiv 0 \pmod{p}$$

המעלה של F היא n והמעלה של F היא n

$$a_1, a_2, \dots, a_n \not\equiv 0 \pmod{p} \quad x_1, x_2, \dots, x_n \not\equiv 0 \pmod{p}$$

$$(p-1)^{n-1} p^{-n/2} > l_1 l_2 \dots l_n \quad (2.3)$$

המעלה של F היא n

המעלה של F היא n והמעלה של F היא n

המעלה של F היא n והמעלה של F היא n

$$l_1 | p-1, \dots, l_n | p-1 \quad (2.3) \quad F$$

$$x_1 x_2 \dots x_n \not\equiv 0 \pmod{p}$$

$$\chi(x) = \chi(2\pi i x/p)$$

המעלה של F היא n והמעלה של F היא n

$$P_N(F, p) = \sum_{t=0}^{p-1} \sum_{x_1, \dots, x_n=1}^{p-1} \chi(t F(x_1, \dots, x_n)) \quad (2.4)$$

$$F(x_1, \dots, x_n) \not\equiv 0 \pmod{p} \quad \text{אם } x_1, \dots, x_n \text{ אינם } 0 \pmod{p}$$

$$F(x_1, \dots, x_n) \equiv 0 \pmod{p} \quad \text{אם } x_1, \dots, x_n \text{ אינם } 0 \pmod{p}$$

$$PN(F, P) - (P-1)^n = \sum_{t=1}^{P-1} \sum_{x_1, \dots, x_n=1}^{P-1} \ell(t F(x_1, \dots, x_n))$$

$$\left((P-1)^n \right) \quad \text{for } P \text{ prime, } t=0 \text{ is not counted}$$

$$\left| PN(F, P) - (P-1)^n \right|^2 = \sum_{t_1, t_2=1}^{P-1} \sum_{\substack{x_1, \dots, x_n=1 \\ y_1, \dots, y_n=1}}^{P-1} \ell(t_1 F(x_1, \dots, x_n) - t_2 F(y_1, \dots, y_n)) \quad (2.5)$$

$$0 \leq a_i < P \quad \text{for } i=1, \dots, n$$

$$y_1, \dots, y_n \mid x_1, \dots, x_n \quad \text{for } x_i, y_i \in \{1, \dots, P-1\}$$

$$t_1 x_1^{l_1} \equiv t_2 y_1^{l_1} \quad \dots \quad t_1 x_n^{l_n} \equiv t_2 y_n^{l_n} \pmod{P} \quad (2.6)$$

$$M \leq (P-1)^{2+n} l_1 l_2 \dots l_n$$

$$\sum_{a_1, \dots, a_n} \left| PN(F, P) - (P-1)^n \right|^2 \leq P^n (P-1)^{2+n} l_1 l_2 \dots l_n$$

$$f(x) = \sum_{i=1}^n a_i x_i^{l_i} \quad \text{for } x_i \in \{1, \dots, P-1\}$$

$$a_1, \dots, a_n \not\equiv 0 \pmod{P} \quad \text{for } i=1, \dots, n$$

$$\frac{(p-1)^n}{l_1 l_2 \dots l_m} \left| PN(F, p) - (p-1)^n \right|^2 \leq p^n (p-1)^{2+m} l_1 l_2 \dots l_m$$

$$\left| PN(F, p) - (p-1)^n \right| \leq p^{n/2} (p-1) l_1 l_2 \dots l_m$$

$$\text{slc } PN(F, p) \neq 0 \quad \text{p. de Legendre}$$

$$(p-1)^n > p^{n/2} (p-1) l_1 l_2 \dots l_m$$

$$(p-1)^{n-1} p^{-n/2} > l_1 l_2 \dots l_m$$

: 4 Goren

$$F(x_1, \dots, x_n) = a_1 x_1^{e_1} + \dots + a_n x_n^{e_n} + a \equiv 0 \pmod{p}$$

$$a, a_1, \dots, a_n \not\equiv 0 \pmod{p} \quad \text{slc } p \quad \text{slc } p$$

$$(p-1)^{n-1} p^{-n/2} > l_1 l_2 \dots l_m \quad \text{slc } x_1, x_2, \dots, x_n \not\equiv 0 \pmod{p} \quad \text{p. de Legendre}$$

Lemma

$$\text{Für 3 Goren } a, b, c \text{ mit } a \equiv b \pmod{p} \quad \text{slc } p \quad \text{slc } p$$

$$M \leq (p-1)^{1+m} l_1 l_2 \dots l_m \quad \text{slc } (p-1) \quad \text{slc } p$$

$$1+m \rightarrow \text{slc } p \quad 2+m \quad \text{slc } p$$

$$(p-1)^{n-1} p^{-n/2} > l_1 l_2 \dots l_m$$

$\sigma_{\text{max}} C_2$ $\sigma_{\text{min}} C_1, C_2$ $\sigma_{\text{max}} S_1$ $\sigma_{\text{min}} S_2$

[illegible]

היה אמר המלך הלאה חתן
המלך הלאה חתן ח'י חתן חתן חתן
החתן חתן חתן חתן חתן חתן
ח'י חתן חתן חתן חתן חתן חתן
ח'י חתן חתן חתן חתן חתן חתן

ההנחה הראשונה היא ש- $P_5 = \infty$ כלומר אין תלות בין P_5 לבין P_1, P_2, P_3, P_4 .
 ההנחה השנייה היא ש- P_5 היא פונקציה של P_1, P_2, P_3, P_4 .
 ההנחה השלישית היא ש- P_5 היא פונקציה של P_1, P_2, P_3, P_4 .
 ההנחה הרביעית היא ש- P_5 היא פונקציה של P_1, P_2, P_3, P_4 .
 ההנחה החמישית היא ש- P_5 היא פונקציה של P_1, P_2, P_3, P_4 .

החשבון של הנהלת החשבונות
הנהלת החשבונות של החשבון

Spalte von M-1 nach N

$$M = \{ m \mid \exists x_1, \dots, x_n, m \mid E(x_1, \dots, x_n) \}$$

10/03/04

$$1 > \lim_{N \rightarrow \infty} \frac{\# N \text{ is prime}}{N} \geq \prod_1^m \left(1 - \frac{1}{p_i}\right) > 0$$

ה'תשנ"ח - 1/11/98
ה'תשנ"ח - 1/11/98

3. פולינומים ממעלה ראשונה

הצגה כללית

משפט 1: נאמן

הפונקציה $f(x)$ היא פולינום ממעלה ראשונה אם ורק אם היא יכולה להיכתב בצורה:

$$f(x) = a(x - \alpha)$$

כאשר a הוא מספר ממשי, α הוא מספר ממשי, ו- $f(x)$ היא פונקציה ממעלה ראשונה. נאמן.

הפונקציה $f(x)$ היא פולינום ממעלה ראשונה אם ורק אם היא יכולה להיכתב בצורה:

$$f(x) = (x - b)g(x)$$

כאשר b הוא מספר ממשי, $g(x)$ היא פונקציה ממעלה ראשונה, ו- $f(x)$ היא פונקציה ממעלה ראשונה.

הצגה כללית

N - מספר ממשי

P - מספר ממשי

Z - מספר ממשי

Q - מספר ממשי

P - מספר ממשי

הפונקציה $f(x)$ היא פולינום ממעלה ראשונה אם ורק אם היא יכולה להיכתב בצורה:

משפט 1: נאמן

$$f(x) = a(x - \alpha)$$

כאשר a הוא מספר ממשי, α הוא מספר ממשי, ו- $f(x)$ היא פונקציה ממעלה ראשונה.

משפט P_f נוסף (הוא נוסף ל-1.5) $P_f(x) = \sum_{\substack{p \in P_f \\ p \leq x}} 1$

$$1 \geq c(f) = c_f \quad \text{and} \quad p_f(x) \sim c_f \frac{x}{\log x}$$

$$\left[\lim_{x \rightarrow \infty} \frac{P_f(x) \log x}{x} = C_f \quad \text{h.c.s} \right]$$

מה ש'רואים זה פונקציה של x וזה $f(x)$

P_f $\gamma \cdot n \cdot f_c$ f_a $n' r p l_n$ $1/b \cdot c \cdot z_n$ $c_f - f$ $k_p p$

[illegible]

סעיף ב: קראו בן ט.א.ר. ל.בן פולין א.א.ר. פולין

נראה שהם שניהם זכאים במקום ב- P_f באלו ההקשרים
האלו של פולינום ממעלה n וזה יהיה פולינום ממעלה
אם היותו אי-פריקם ב- $Z[x]$ (ולכן גם ב- $Q[x]$).

משפט 3.2.1

האלו P_f הן למעשה מספר סופי של וצא
מכאן, הן V של מספר סופי של ט.א.ר. של
פולינום ממעלה n אי-פריקם ב- $Z[x]$.

הוכחה:

אם $f(x)$ אינו פולינום $f(x)$ במכפלה $q_1(x) \dots q_m(x)$
כאשר $q_i(x)$ פולינום אי-פריק ב- $Z[x]$ אם לא ברורה
מחלק. ה ט.א.ר. של $q_v(x) = a_m x^m + \dots + a_0$ ($v=1, \dots, m$)

הן למעשה מספר סופי של האלו כמו זה של

$$q'_v(x) = a_m^{m-1} q_v(x) = (a_m x)^m + a_{m-1} (a_m x)^{m-1} + a'_{m-2} (a_m x)^{m-2} + \dots + a'_0$$

אם נראה שה ט.א.ר. של $q'_v(x)$ הן ט.א.ר. מספר

סופי של האלו כמו זה של $q''(y) = y^n + a_{n-1} y^{n-1} + a'_{n-2} y^{n-2} + \dots + a'_0$

ובזה יוכח משפט 3.2.1 כי $q'(x)$ גם $q''(x)$

אי-פריקם ב- $Z[x]$.

באלו $q''(x)$ הן ט.א.ר. של $q''(x)$ הן ט.א.ר. של $q''(x)$

אם $q'_v(x)$ הן ט.א.ר. של $q''(x)$ הן ט.א.ר. של $q''(x)$

האם P ו- a_m זיהו זה "לפני" (אשר על נכון) של
האזי למספר סופי של $(P-1)$ אזי האסטרטגיה של a_m ,
בן e $a+1, P$ כאלה בלתי של a_m .
גילוי P יעיל יותר מאשר של $q'(x)$.

למבחן קיום של צפיפות אסטרטגיה של P_f ב- P
ותחילה, מספיק עם קצת של P_f עד כדי מספר
סופי של וצבים מהבטל.
עכשיו נבדוק לקח את הקואורדינטה של a_m שכלול
המספר q ו- a האלו V שקבענו במספר האחרון.

דוגמה 3: צפיפות אחידה של האסטרטגיה q

במספר זה נבדוק תחילה את האסטרטגיה q אחידה
נאמר את שתי התוצאות הבאות:
(א) לכל האסטרטגיה q יש צפיפות אסטרטגיה חלופית ב- P .
(ב) לחלק של שני האסטרטגיות q יש צפיפות אחידה ב- P .
- במספר הכללי, נראה שהקואורדינטה של צפיפות
לפני של חלק של מספר סופי של האסטרטגיה q חלופית
שהיא עולה. כי האלו V מספר q חלופית
למספר סופי של צבים מהבטל מוכיח
של האסטרטגיה q .

$Q(x) \sim y(x)$ as $x \rightarrow \infty$

$\frac{d}{dt} \left(\frac{1}{2} m v^2 + U(r) \right) = 0$

הוא - ה'א' ק' נ'צ'י א'פ'טל (ק) מהחל של המסמך
השנים של עזר המסמך החלט ד"ר א' אפר
עסק נ' - האחל (P) ומכסה של האחל האחל
(במילים) - א' . עם א'פ'טל האחל מחלק

$G = N \quad S_2$ $\alpha^P = S_2(\alpha) \pmod{P}$

$\left(\frac{k}{p}\right)$

$(T \in G)$ p - f q/n $T(p)$ u/n f/n u/n
 $T^{-1}(q) = p$ q u/n f/n u/n
 T u/n f/n u/n

$$\alpha^p = TS_p T^{-1}(\alpha) \bmod T(P)$$

[illegible]

רמ"מ ר"ח אדר א' תש"ח

Artin Synol

(Date Recd)

$$\left(\frac{k}{p}\right)$$

חקר האוכלוסיות היה "היסטורי"
 (3 קבוצות אוכלוסיות) : 3 קבוצות אוכלוסיות

3.3.1 Coen

9.11.1965 (שבת) חתונה של חתנים

השקבות מוד 100% (5 ש"ח ב"ח) 100% - צ"ח

$$D = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in P_s} p^{-s}}{\sum_{p \in P} p^{-s}} = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in P_s} p^{-s}}{\log \frac{1}{s-1}}$$

$\Gamma_{\text{ON}}(S)$ של c מראה את Γ של b וקראו

$\rho = \frac{m}{V}$

$(\text{Hansu}[2] \quad \sqrt{0} \quad \text{m} \cdot \text{m} \cdot \text{m}) \quad \cdot \quad G \rightarrow (S) \sim N$

$\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad e^{\pm} \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}$

(Schulze [1] 2010, p. 204) "Die ..."

היום בערב - 1/11 - 1977

3-3.2 Coen

p sollte sein Γ ρ ρ_3 ρ_{ollen} ρ_{er}

הע"כים פוסט פילד S נק"מ

... Schutze [1] ...

...
 $f(x), g(x)$...
 $3.3.3$...

...
 A, B ...
 L ...
 $\bar{K}$...

3.3.4 ...

...
 $\left(\frac{K}{P_2}\right) \left(\frac{K}{P_1}\right)$...
 $\left(\frac{K}{P_1}\right) \left(\frac{L}{P_1}\right)$...

... Schutze [1] ...

...
 Q, R ...

סעיף 4: החלקים הראשונים של פולינומים אי-פריקים מילקנים

פירוק זה נראה כאילו החלקים הראשונים של פולינומים אי-פריקים מילקנים $q(x)$ מעל השדה K , אינם חולקים חזית, ולא כל מספר סופי של פולינומים מהצורה $q(x)$ יכולים להיות חולקים חזית. נראה כי יש פולינומים $q(x)$ שאינם חולקים חזית עם אף פולינום אחר.

בסעיף 5 נראה כי $q(x)$ חולק חזית עם מספר סופי של פולינומים. כלומר, $q(x)$ חולק חזית עם $q(x)$ עצמו, וכל פולינום אחר $p(x)$ חולק חזית עם $q(x)$ אם ורק אם $p(x) = q(x) \cdot r(x)$ עבור פולינום $r(x)$.

יהי K שדה הסדר n של $q(x)$, $\{1, \dots, n\}$ הוא סדר n של K . $q(x)$ חולק חזית עם כל פולינום $p(x)$ אם ורק אם $p(x) = q(x) \cdot r(x)$ עבור פולינום $r(x)$. כלומר, $q(x)$ חולק חזית עם כל פולינום $p(x)$ אם ורק אם $p(x) = q(x) \cdot r(x)$ עבור פולינום $r(x)$.

3.4.1 משפט

עקרון האי-אזרח $q(x) \equiv 0 \pmod{p}$ יהיה בגובה n של $q(x)$. כלומר, $q(x) \equiv 0 \pmod{p}$ אם ורק אם $q(x) = p(x) \cdot r(x)$ עבור פולינום $r(x)$. כלומר, $q(x) \equiv 0 \pmod{p}$ אם ורק אם $q(x) = p(x) \cdot r(x)$ עבור פולינום $r(x)$.

המחלקה המלאה של $q(x)$ היא $q(x)$ מסביב
 סביב של יוצאים ממנה האחד של כל המערכת, המ"כים
 מחלקת - מיליוני שנים, זהו מה שחלק מיליוני שנים
 נמצא ב-H - זהו מה שחלק מיליוני שנים חלק זה
 כל המערכת המלאה של $q(x)$.

הוכחה השנייה:

נניח כי $q(x)$ מתפצל ל- $q_1, \dots, q_m$
 כל $q(x) \equiv 0 \pmod{p}$ זהו α חלקי קבוצה של K
 מחלקת האחד של p כל (p) K

$$\prod_{v=1}^m (\alpha - \xi_v) \equiv 0 \pmod{p}$$

אז $\xi_v \equiv \alpha \pmod{p}$ זהו v אינסוף
 כך $\xi_v^p \equiv \xi_v \pmod{p}$ זהו v אינסוף

$\xi^p \equiv \xi \pmod{T(p)}$ זהו K כל T
 זהו $T(p)$ - זהו $T(p)$ זהו $T(p)$
 $\xi^p \equiv \xi \pmod{T(p)}$ זהו $T(p)$ זהו $T(p)$

זהו ξ זהו ξ זהו ξ זהו ξ
 זהו ξ זהו ξ זהו ξ זהו ξ

$$\xi - \xi_\mu \equiv 0 \pmod{T(p)}$$

זהו $T(p)$ זהו $T(p)$ זהו $T(p)$
 זהו $T(p)$ זהו $T(p)$ זהו $T(p)$

$\alpha \equiv \beta \pmod{p}$ נקרא α שקול ל β modulo p
 $q(\alpha) \equiv 0 \pmod{p}$ - α שורש של q modulo p
 ואלו

אם α הוא שורש של q modulo p אז $q(\alpha) \equiv 0 \pmod{p}$
 מספרים אלו

4.5: צורה חתומה של פולינום

נניח $f(x)$ פולינום מעלה n מעל $\mathbb{F}_p$.
 נניח $f(x)$ אינו מתפצל ל $\mathbb{F}_p$.
 לפי סדר 2 ופסוק 4 מאיבר $\mathbb{F}_p$, $f(x)$ מתפצל ל $\mathbb{F}_p$ מספר
 שלם של גורמים, מאחר ש $\mathbb{F}_p$ מספרים שלם של גורמים $\mathbb{F}_p$

$$P_f = \prod_{i=1}^r (x - \alpha_i)^{e_i}$$

הצורה הנורמלית של P_f היא $P_f = \prod_{i=1}^r (x - \alpha_i)^{e_i}$, כאשר α_i הם השורשים של P_f ו e_i הם המעצמות של α_i .
 לפי תהורם 3.4.1, P_f מתפצל ל $\mathbb{F}_p$ אם ורק אם P_f מתפצל ל $\mathbb{F}_p$.

המספר $P_f(x)$ שווה למספר השורשים של P_f

אם x הוא שורש של P_f אז $P_f(x) = 0$.
 לפי תהורם 3.4.1, P_f מתפצל ל $\mathbb{F}_p$ אם ורק אם P_f מתפצל ל $\mathbb{F}_p$.

$$P_f(x) = \sum_{i=0}^n a_i x^i$$

נחשב $(T_{i_1} \dots T_{i_r})(x)$ נאמן x נחשב
 הבה $x \geq 1$ הנמצאים מתחת $T_{i_1} \dots T_{i_r}$
 הן מתחת x כולם צבועים i צבועים x

ב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב

נחשב P_f נחשב P_f נחשב

נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב

נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב

נחשב P_f נחשב P_f נחשב

נחשב P_f נחשב P_f נחשב
 נחשב P_f נחשב P_f נחשב

$$\alpha_j K_{j,1} \rightarrow \alpha_j K_{j,N} (i=1, \dots, m) \quad D_i \rightarrow \alpha_j K_{j,0}$$

$\Gamma_e \sqrt{1/\beta_e}$ — חלקי Γ_e — חלקי $m c^2 / h \nu$ — חלקי

$\exists \epsilon > 0$ m. $\forall \delta > 0$ $f_i(x) \in \mathcal{B}_\delta$ $\forall x \in \mathcal{B}_\epsilon$

3.35. Coerl of per D in f² Δ/ω $\approx N_c$

3/10/11 ח'א'ל - 1820

Coent rsl /len

11/2/97 : 7 9.00

ה'תר"ק כ"ה שבט ה'תש"ח

similar

Handwritten text: Handwritten text: ...

המחלקה - חלק 1

$$f_n(x) = x^n + 1$$

$$q_2(x) = x^3 - 2p.$$

$$g_3(x) = x^4 - 54$$

$$E_i = Q(i) \quad \text{föör } i \in G, \quad \text{och} \quad u_k(a$$

$\sin^2 \theta / 4$ $\sin^2 \theta / 4$ Q Γ_{on} $g_r(x)$ Γ_e

i. $\frac{1}{2} \frac{d}{dt} \left(\frac{1}{2} m v^2 \right) = \frac{1}{2} m v \frac{dv}{dt}$

$$-1 \sim p \sim 2 \quad q_{-1}(x) \quad \Gamma_c$$

$P \rightarrow \mathbb{R}, \varepsilon_1 = \int \mu(\varepsilon_1)$

9-01/05 9-01/08

$$C(\varepsilon_1) = \frac{1}{2} \quad \text{--- } r_2 C \quad \text{--- } 10.02$$

היחס $q_2(x)$ בין σ_2 ו- τ_2 (b)

$$E_2 = Q(\sqrt[3]{28}, -\frac{1}{2} + \frac{i}{2}\sqrt{3})$$

היחס σ_2 ו- τ_2 בין σ_2 ו- τ_2

$$G_2 = \{E_2, \sigma_2, \sigma_2^2, \tau_2, \sigma_2\tau_2, \sigma_2^2\tau_2\}$$

היחס σ_2 ו- τ_2 בין σ_2 ו- τ_2

$$E_2 = -\frac{1}{2}$$

$$\sigma_2(\sqrt[3]{28}) = \left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right)\sqrt[3]{28}$$

$$\sigma_2\left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right) = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$$

$$\tau_2(\sqrt[3]{28}) = \sqrt[3]{28}$$

$$\tau_2\left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right) = \left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right)^2$$

$$\{E_2\}, \{\sigma_2, \sigma_2^2\}, \{\tau_2, \sigma_2\tau_2, \sigma_2^2\tau_2\}$$

היחס $q_2(x)$ בין σ_2 ו- τ_2

$$M(E_2) = \frac{1}{6} \quad M(\tau_2) = \frac{3}{6} \quad \text{היחס } q_2(x) \text{ בין } \sigma_2 \text{ ו-} \tau_2$$

$$E_3 = Q(\sqrt[3]{54}, i) \quad \text{היחס } q_3(x) \text{ בין } \sigma_3 \text{ ו-} \tau_3$$

$$G_3 = \{E_3, \sigma_3, \sigma_3^2, \tau_3, \sigma_3\tau_3, \sigma_3^2\tau_3, \sigma_3^3\tau_3\}$$

$$\xi_3 = -1/2$$

$$\sigma_3(\sqrt[4]{54}) = i\sqrt[4]{54}$$

$$\tau_3(\sqrt[4]{54}) = \sqrt[4]{54}$$

$$\sigma_3(i) = i$$

$$\tau_3(i) = -i$$

המרחב הממשי של $\mathbb{C}^4$ הוא $\mathbb{R}^4$

$$\{\xi_3\}, \{\sigma_3, \sigma_3^3\}, \{\sigma_3^2\}, \{\tau_3, \sigma_3^2 \tau_3\}, \{\sigma_3 \tau_3, \sigma_3^3 \tau_3\}$$

המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.
 $M(\tau_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ $M(\xi_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1/2 & i\sqrt{3}/2 & 0 \\ 0 & -i\sqrt{3}/2 & -1/2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
 $C(\tau_3) = \frac{2}{3}$ $C(\xi_3) = \frac{1}{3}$ $\rho = 1$

2. $\mathbb{C}^4$

המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.
 המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.

3. $\mathbb{C}^4$

המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.
 המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.

1. (חלק ב) $\alpha = -28$, $\alpha = -28$

המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.
 המרחב $\mathbb{C}^4$ הוא $\mathbb{R}^4$ עם בסיס $\{\xi_3, \sigma_3, \sigma_3^3, \tau_3\}$.

$x^4 + a$ $p \mid n-1$ $n \mid n$ $n \mid n$ $n \mid n$
 $(C \mid n)$ $1 \mid n$ $n \mid n$ $n \mid n$ $n \mid n$

ה'תשנ"א
ח' תשרי ה'תשנ"א
מזל חסידים

(מ) חסידים
ה'תשנ"א
מזל חסידים

בית חסידים
מזל חסידים

הצבים לא ידעו להימלט מהמים - משכא - מהם וכלה קהלת ירושלים
 רק חלל/מורס - חסיה - מהם וכלה קהלת ירושלים

צ'ביטאל - מחלקים האלמנטים של $x^2 + f(y)a$ מכלול

באשר $f(y)$ פאקטור אקססורצור

משפט 4.1

הצ'ביטאל של האלמנט $x^2 + b^2 + a$ זה 1
אם ורק אם יש אינסוף מחלקים האלמנטים של $b^2 + a$.
הוכחה:

נניח שיש אינסוף מחלקים האלמנטים של $b^2 + a$
אז נקח את כל האלמנטים המקסימליים של
נקרא

$$(x^2 + m_1 p_1)(x^2 + m_2 p_2) \dots (x^2 + m_m p_m) \dots$$

הצ'ביטאל של כל מחלקי האלמנטים של פאקטור צ'ביטאל
זה $1/2$. הציבאל של המכפלה תהיה פקטור

$$\sum_{m=1}^n (-1)^{m-1} \binom{n}{m} \frac{1}{2^m}$$

אבל יש לנו אינסוף האלמנטים נקרא

$$\lim_{n \rightarrow \infty} \sum_{m=1}^n (-1)^{m-1} \binom{n}{m} \frac{1}{2^m} = 1$$

אם פאקטור - זה רק מספר סופי של האלמנטים
מחלקים של $b^2 + a$ והיה לנו

$$(x^2 + m_1 p_1) \dots (x^2 + m_m p_m)$$

זה $b^2 + a$ - כל המחלקים p - נ

חבול - חבל / מלאכה
קל חבל - קל / מלאכה
הזאת - הזאת

1. למה $x^2 + b^2 + a$ אינה Ce - כלומר Γ_{CP} אינו הומומורפיק
 $-b^2+a$ Ce אינה $\text{sig}(\Gamma_{\text{CP}})$ ולכן יש להכניס Γ_{CP}

$\rho_{\ell/\omega} \rightarrow \rho_{\ell/\omega} \text{ as } \Gamma_{\ell/\omega}$
 $\cdot b^{\frac{q}{2}+1} \equiv 0 \pmod{p}$
 $\Gamma_r \quad \Gamma_{\ell/\omega}$
 $\cdot \Gamma_{\ell/\omega} \text{ as } \rho_{\ell/\omega} \cdot a=1 \cdot \rho_{\ell/\omega}$

9/10/16

$b^2 + a$ $1/2x$ $1/2x$ $1/2x$ $1/2x$ $1/2x$ $1/2x$

$b^{23} + a$ 10,25 5,5 9,75 4,2 5,00

$$\prod_{i=1}^{\infty} b^{y_i} + a \quad \text{for } C_{n+1}$$

ausleten spinnen 46/40 e. n. s. 10. Se nicht mit 1. k

$$\prod_{i=1}^n (b^{y_{i+a}}) = \sum a^{n-r} b^{y_{i_1} + y_{i_2} + \dots + y_{i_r}} \quad \text{L.P. c.} \quad (*)$$

b. f_2 - f_1 sind Γ -u.

מחירי המוצרים הנמכרים

1. $\frac{1}{\sqrt{a}}$ $x^2 + b^2 + a$ $\int e^{\frac{1}{\sqrt{a}}}$ $\int e^{-\frac{1}{2} \ln 3}$ in $\int p(x)$

4.2 | 4.1 σ -Coen μ in $\int p(x)$

- (1) Z.I. BOREVICH & I.R. SHAFAREVICH - Number Theory
- (1) L. J. MORDELL - The number of solutions of some congruences in two variables. Math. Z. 37 (1933) 193-209
- (2) L. J. MORDELL - DIOPHANTINE EQUATIONS. Academic Press
- (1) W. S. CASSELS & A. FRÖHLICH, Algebraic Number Theory, Washington 1967
- (1) H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Würzburg 1965 2. Auflage 1. Teil
- (2) H. HASSE. 2. Teil
- (1) V. - SCHULZE - Die Primteilerdichte von ganzzahligen Polynomen I. Crelle Journal, 253 (1972) (175-185)