

תוחם 20

$p \equiv 1 \pmod{4}$ $11 \leq p \leq 2 \Leftrightarrow p = x^2 + y^2$: נכון

$$x^2 \equiv 0, 1 \pmod{4} \quad \text{if} \quad p \nmid x^2 + y^2 \quad \text{slc} \quad p \equiv 3 \pmod{4} \quad \text{slc} \quad \exists p \nmid \eta : \eta \mid 2 \mid \eta$$

x, y s.t. $x^2 + y^2 \equiv p$ $\text{if } p \equiv 3(4)$ $p \nmid p$ $x^2 + y^2 \equiv 0, 1, 2(4)$ $p \nmid p$ $y^2 \equiv 0, 1(4)$

שאלות ריבועיות? $0, 1$ סדרה חזרתית

(גמח) $p \equiv 1(4) \Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow -1 \equiv x^2(p) \pmod{p}$: 2-כיתוב

(2) פיתוק יחיד - 2×2 -

הערה: $p = x^2 + y^2 \Leftrightarrow p$ ראשוני נורמה ב- $\mathbb{Z}[i]$

דמורה: יהי q ראשוני רצוני (כ-2), אז q הוא פריק ב- $\mathbb{Z}$ $\Leftrightarrow$

פ הא נרמה

הוכחת הנאמה: $\Rightarrow$ אם p נכונה, נניח $N(\alpha) = \alpha \cdot \bar{\alpha}$. אז p פריק ב- $\mathbb{Z}$.

(ii) α ו- β הפיך - כל הפך $\exists$ (C) (הנחה 1)

α, β אינן הפיכים. אלס מתקיים: $\rho = \alpha\beta$ $\rightarrow \exists i \in \mathbb{Z}$ $\rho = \alpha\beta$

$p, q \in P, p \perp q \Rightarrow N(p), N(q) \neq 1$ so $p^2 = N(p) = N(\alpha) \cdot N(p)$

דף 10 $N(\beta) - N(\alpha) = p$ ויהי p נורמה (נורמה)

לעמוד: פאק $p \equiv 1 \pmod{4}$ האט שוין א פאקטאריזאציע $p = 2C_1$.

היבט זה: נ.ח. כפשוטה ש- p לא פ.י.ק. - $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$ ו- p "ראשוני" - $\mathbb{Z}/p\mathbb{Z}$.

זכור ממשל פרמה (אחר): $p \mid a \Rightarrow 1 \pmod{p}$. $\left(\frac{-1}{p}\right) = 1$ אם $p \equiv 1 \pmod{4}$ ו-1 אחרת.

$p \mid (x+i)(x-i)$ or $p \mid x^2+1 \iff -1 \equiv x^2 \pmod{p}$

$p \mid x-i$ וכן $p \mid x+i$ וכן $2 \mid i$ - הן "מאפשרות"

דבר נוסף: $\mathbb{Z}[i]$: $\chi_{\pm i} = p(m \pm ni) \iff \pm i = \pm p m i \iff p n = 1$ וכן סתירה.

הכסיבה לסתירה היא שהתחננו ש φ אי-פריק ב- $\mathcal{X}_i$ $\Leftarrow$ φ פריק ב- $\mathcal{H}$ $\square$

נחזור עכשיו מה שיש לנו:

$\rho = x^2 + y^2$ $\rho \geq 0$ $\rho = 3(4)$ $\rho \leq 4$

$$\sqrt{p} = 1^2 + 1^2 \quad \text{SLC} \quad p = 2 \quad \text{PLIC} \quad \times$$

$\exists x, y \in \mathbb{Z}$ s.t. $p = x^2 + y^2$ p פרט וזוגי, $p \leq 2$ p איז פארטיילבאר $p \leq p \equiv 1 \pmod{4}$ $p \nmid x$

!e73p

1. 3,7 3 111111

$$13 = 3^2 + 2^2 \quad ; \quad 5 = 2^2 + 1^2 \quad ; \quad 2 = 1^2 + 1^2 \quad : \text{p } 13, 5, 2$$

7. הערת סיום ה. שאני מאשן. (רצה לקבוע) האם סיום של ריכוז -

$$K = a \cdot \prod_i p_i^{e_i}$$

$$\sqrt{p^E} = (p^{E/2})^2 + \sigma^2 \quad \text{שכ } \underline{E_i} \text{ מ"קן } N \quad p_i = 3(A) \quad \text{בס } p/c$$

- פונקציע f ווערט גערופן k סטאביל פונקציע, $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$, $f(x) = Ax$ און $k = \max_{1 \leq i \leq n} |a_{ii}|$.

כי מכפר ה' שם גורמות (היא) גורמת!

p_i : $\pi(p_i)$ $\frac{1}{n}$ $p_i \equiv 1/n$

$\pi_i \cdot e_i$: i -th person's expected utility
 $p_i = 3(4)$

1) עבור $p=2$ היא תמיד סכום של שני ריבועים.

[illegible][illegible]

הנורמה: $\|x\| = \sqrt{x^2 + y^2}$

אם p_i/x אז p_i/y שכן p_i^2/h וכל יחידה של h מתחלקת ב- p_i^2 אז

לפי χ, y ב p_i ו p_i ב p_i - $n' = \frac{n}{p_i^2}$ מופים בחזקה n' או n' יות.

כומר $n' = x^2 + y^2$ $p_i - 1$ מופס n' מחלק n' כומר

(חצוי עס תרפון מה עד א-א יא קא יא קא כימקרה העזום נים למכ)

ש- (קצת). ואכן ניתן זאת בהר"ב. נ"ח

$$y \neq 0(p) \quad \text{w.k.} \quad x^2 + y^2 \equiv 0(p) \quad \text{p.d.} \quad p \nmid n$$

(ח) γ - מרחק p מרחק p , $\exists y' \in Z$ כך $yy' = 1(p)$. (ב) y'^2 - ריבוע y' .

$$(xy')^2 + \underbrace{(yy')^2}_1 = 0(p) \Rightarrow (xy')^2 = -1(p) \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod{4}$$

130 בתורה! אם לא, הן מופיע בחסרה א. 215 ת. 39-1 של $P_i \equiv 39-1$ $12 \neq x^2 + y^2$ $2 \rightarrow 7$ 5

כאן צוה.

$$27=3^3 \quad \text{in } 27 \neq 0+0, \quad 9=3^2+0^2, \quad 5=1^2+2^2 \quad \text{is allowed}$$

$$3 \cdot 5 = 15 \neq \square + \square \quad \text{re} \quad 54 = 2 \cdot 3^3 \quad \text{so } 54 \neq \square + \square \quad \text{p wo}$$

$3 \cdot (1+2i)$ (רשום) $3^2 = 3^2 + 0$: $3^2 \cdot 5 = 45$ כאילו (מכאן את המס' 2 עקור
 (חשבו ונרמז) $5 = 2^2 + 1^2$

$2^5 \cdot 5^3 \cdot 7^2$ (רשום) : $(1+i)^5 \cdot (1+2i)^3 \cdot 7$ ← נחשק את המכפר ונמצא נורמה
 $\downarrow$ $\downarrow$ $\downarrow$
 נורמה = s נורמה = 2

תורת תחום 20

Hensel - חזקה

נתון פולינום $f \in \mathbb{Z}[x]$ ואם $f(x) \equiv 0 \pmod{p}$ אז $f(x) \equiv 0 \pmod{p^2}$.

$$2x^3 + 7x - 4 \equiv 0 \pmod{200}$$

$$2x^3 + 7x - 4 \equiv 0 \pmod{2^3} \quad 200 = 2^3 \cdot 5^2$$

$$2x^3 + 7x - 4 \equiv 0 \pmod{5^2}$$

אז יש לנו, נבדוק עבור 2^3 פתרון.

נניח שיש פתרון $x_2 \pmod{2^3}$ ונבדוק $x_5 \pmod{5^2}$. כעת נבדוק $x_5 \pmod{5^2}$ ונסיק.

$$\begin{cases} x_2 \equiv x_5 \pmod{2^3} \\ x_2 \equiv x_5 \pmod{5^2} \end{cases} \quad \text{יש פתרון היחיד x_2 ונבדוק $f(x_2) \equiv 0 \pmod{200}$ }$$

$$2x^3 + 7x - 4 \equiv 0 \pmod{5^2} \quad \text{נפתור}$$

נבדוק עבור 5 . נבדוק $x \equiv 1 \pmod{5}$ זה הפתרון היחיד.

עבור 5^2 : נבדוק $x = 1 + 5t \pmod{5^2}$, $t \in \mathbb{Z}$.

$$2(1+5t)^3 + 7(1+5t) - 4 \equiv 0 \pmod{25}$$

$$\Rightarrow 2(1 + 3 \cdot 5t + 3 \cdot 5^2 t^2 + 5^3 t^3) + 7 + 35t - 4 \equiv 0 \pmod{25}$$

$$2 + 30t + 3 + 35t - 4 \equiv 0 \pmod{25}$$

$$5(1 + 13t) \equiv 0 \pmod{25}$$

$$5 \mid 5(1+13t) \Rightarrow 5 \mid 1+13t$$

אם $13 \equiv 0 \pmod{5}$ אז זה הפתרון!

$$1 + 13t \equiv 0 \pmod{5}$$

$$3t \equiv -1 \pmod{5}$$

$$t \equiv 3 \pmod{5}$$

$\Downarrow$

$$x \equiv 1 + 3 \cdot 5 \pmod{25}$$

⚠️ (נסתכל) $f(x) = 2x^3 + 7x - 4$, $f'(x) = 6x^2 + 7$ ונבדוק $f'(1) = 13$ $\leftarrow$ פתרון!