

תורת q

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1))$$

סדרה 1: p - $\mathbb{F}_p[x]$ מרחב וקטורי

$$f(x) = (x^{p-1} - 1) - (x-1)\dots(x-(p-1))$$

תוצאה: (צדד)

$$f(1)=0, f(2)=0, \dots, f(p-1)=0 \quad \deg f \leq p-2$$

אם f לא אפס אז צדד פולינום ממעלה $\deg f \leq p-2$ ויש f שונים

שונים - כתיבה! לכן $f=0$

מכונה-למשל Wilson: $(p) \equiv -1 \pmod{p}$ כל p ראשוני

תוצאה: אם $p=2$ כתיבה: $1! \equiv -1 \pmod{2}$

אם $p > 2$ אז $p-1$ כתיבה. כותבים $x = p-1$ במונחים של סדרה 1:

$$-1 = (-1)(-2)\dots(-(p-1)) = (p-1)! \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p} \quad \leftarrow (p-1)! = -1 \pmod{p}$$

⚠️ (הערה): אם $n > 4$ ו- n מורכב אז $(n-1)! \equiv 0 \pmod{n}$

סדרה 2: אם $d \mid (p-1)$ אז נקרא (צדד) $x^d \equiv 1 \pmod{p}$ יש קבוצה d פתוחה.

תוצאה: נניח $dd' = p-1$ אז מתקיים:

$$\frac{x^{p-1} - 1}{x^d - 1} = \frac{(x^d)^{d'} - 1}{x^d - 1} = (x^d)^{d'-1} + (x^d)^{d'-2} + \dots + x^d + 1 =: g(x)$$

$$x^{p-1} - 1 = (x^d - 1)g(x)$$

יש $d-1$ שונים $\leq d$ שונים. יש $p-1$ שונים (סדרה 1)

כעת מנסים להניח $x^{p-1} - 1$ יש מ' קטן או שווה $p-1$ של שונים.

אם $x^d - 1$ היה מ' שונים הקטן מ- d אז $x^{p-1} - 1$ היה מספר שונים

קטן מ- $d + (p-1) - d$ וצדד כתיבה! ■

⊗ אנו רוצים להוכיח: $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ חבורה ציקלית

למשל: $n = \sum_{d \mid n} \psi(d)$ $n > 1$ מתקיים:

תוצאה:

אם $d \mid n$, $d > 1$, (צדד) קבוצה $\{m \mid 1 \leq m \leq n, \gcd(m, n) = d\}$ $S_d = \{m \mid \gcd(m, n) = d\}$

$$\gcd(m, n) = d \Leftrightarrow d \mid m, \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

$$\# S_d = \# \{s \mid \gcd(s, \frac{n}{d}) = 1, 1 \leq s \leq \frac{n}{d}\} = \psi\left(\frac{n}{d}\right) \quad p \delta$$

$$\{1, a, \dots, n\} = \bigcup_{d|n} S_d \quad (\text{איחוד זר})$$

כעת נרדיון על-

$$n = \sum_{d|n} \psi\left(\frac{n}{d}\right)$$

אנו מקבלים על-

אם d עובר על התחלקים של n אז $\frac{n}{d}$ גם הוא עובר על

על התחלקים של n לכן:

$$\sum_{d|n} \psi\left(\frac{n}{d}\right) = \sum_{d|n} \psi(d) = \sum_{d|n} \psi(d)$$

$$\boxed{n = \sum_{d|n} \psi(d)}$$

משפט 1 (זאוס): אם d ראשוני p ראשוני אז $\psi(d) = U(2/p^2)$ כל ψ יש

בדיוק $\psi(d)$ איברים מסדר d .

מסקנה: יש $1 \leq \psi(p-1)$ איברים מסדר $p-1$ כל ψ איברי מסדר

$p-1$ יוצרי יש בחקורה בדיוק ψ איברים).

הוכחת משפט 1:

יה $d | (p-1)$ ויה $\psi(d)$ מספר האיברים $\psi(d)$ מסדר d .

המסדר של $U(2/p^2)$ הוא $p-1$. עבור $x \in U(2/p^2)$ המסדר של x הוא

$$p-1 = \sum_{d|p-1} \psi(d) \quad \text{מכיוון של } p-1 \text{ כל}$$

$$p-1 = \sum_{d|p-1} \psi(d) \quad \text{מכיוון של } p-1 \text{ כל}$$

$$(3) \sum_{d|p-1} \psi(d) = \sum_{d|p-1} \psi(d) \quad \text{כל}$$

כעת נרצה להראות של $d | (p-1)$ מתקיים $\psi(d) \leq \psi(d)$ (יחס $\psi(d) = \psi(d)$).

יש 2 אפשרויות: או $\psi(d) = 0$, או $\psi(d) \neq 0$. אם $\psi(d) = 0$ אז $\psi(d) \leq \psi(d)$.

אם $\psi(d) \neq 0$ אז קיים $x \in U(2/p^2) = \mathbb{F}_p^*$ מסדר d . כל האיברים $1, x, x^2, \dots, x^{d-1}$

שונים זה מזה. כתם שורשים של המשוואה $x^d - 1 = 0$ ב- $\mathbb{F}_p$.

$$(x^k)^d = (x^d)^k = 1^k = 1 \quad \text{כל } k$$

שנים הפעמים מסתבר d כל השורשים של המשוואה הזו.

כל $y \in U(2/p^2)$ מסדר d הוא אחד מ- $1, x, x^2, \dots, x^{d-1}$ אבל לא

$$y = x^a \quad \text{!} \quad \gcd(a, d) = 1 \quad \text{כל } y = x^a \quad \text{כל } y = x^a \quad \text{כל } y = x^a$$

המסדר של y שונה מ- d . כל $\text{ord}(y) = d$ כל $\gcd(a, d) = 1$.

יש $\psi(d)$ איברים מסדר d כל $\psi(d) \leq \psi(d)$ כל $\psi(d) \leq \psi(d)$.

$$\forall d | (p-1). \psi(d) = \psi(d) \quad \Leftarrow$$

המושג תחילת

משפט: יהי G חבורה אבליה סופית מסדר $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$

יהי $x \in G$ אז $x^{n/p_i} \neq 1$ $\forall i$ אז x יוצר G .

(כוכבה)

$$n = p_1^{a_1} \dots p_r^{a_r}$$

(נניח קטן. נניח $x \neq 1$, $\text{ord } x \neq n$, אז $m \mid n$, $m < n$.

מכיוון $m \neq n$ קיים i כך $b_i < a_i$, $b_i \leq a_i - 1$.

ז"א $\frac{n}{p_i} \leftarrow m \leftarrow \text{עבור } x^{n/p_i} = 1 \leftarrow \text{סתם!}$

$$\frac{12}{2} = 6, \frac{12}{3} = 4, p-1 = 12 = 2^2 \cdot 3, p = 13$$

שורש פרימיטיבי עבור 13, $G = (2/13)^+$, $\#G = 12$

$$a=2, a^4 = 16 \not\equiv 1(13), a^6 = 64 \equiv -1 \not\equiv 1(13), a^8 = 256 \equiv 1(13) \leftarrow \text{זוהי שורש פרימיטיבי מסדר 8}$$