

תולדות 13

תצבורת: כיטון נצ' (א): $\frac{a}{p} \equiv \pm 1$ אם a שירת ריבועית מודולו p
 $\leftarrow -1$ אחרת.

נמשך להוכיח את הטענה: (א) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(ב) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ג) אם $a \equiv bp \pmod{p}$ אז $\frac{a}{p} \equiv \frac{b}{p}$

הוכחנו א+, נראה ס':
 נ-א': $\frac{ab}{p} \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p}$
 $\Leftrightarrow \frac{ab}{p} \equiv \frac{a}{p} \cdot \frac{b}{p}$ (כיהיט שנועידה ± 1)

כי ב p , $2k$, $2k+1$ סין p , $p \nmid 2$, $p \nmid (-2)$
 אם $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$ אז $\left(\frac{ab}{p}\right) \equiv \pm 2$

ההסתקה $\cup (2/p) \rightarrow \pm 1$: $\bar{a} \rightarrow \left(\frac{a}{p}\right)$ כה הנומורוס

(כי הוכחנו שמכפלה זוטרת זמנפיה)

מסקנה: יש אלו מכפלי ש שירות ואי שירות ריבועיות מודולו p .

הכחתי: $a^{\frac{p-1}{2}} \equiv 1 - \delta$ יש $\frac{p-1}{2}$ פתרונות

$\leftarrow \frac{p-1}{2}$ שירות (!) $\frac{p-1}{2} = 1 - \frac{p-1}{2}$ אי שירות

מסקנה 2: מכפלה של שתי ~~שירות~~ שירות היא שירות. (כי $1 \cdot 1 = 1$)

מכפלה של שירות טו שירות היא אי שירות. (כי $-1 \cdot 1 = -1$)

מכפלה של אי שירות היא שירות. (כי $-1 \cdot -1 = 1$)

צורתי: $3 \cdot 5 = 7 \pmod{8}$

$\pmod{7}$:

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

 3, 5 נא ריבוע מודולו 7
 $3 \cdot 5 = 15 \equiv 1 \pmod{7}$ אז

$7^2 \equiv 1 \pmod{8}$ $5^2 \equiv 1 \pmod{8}$ $3^2 \equiv 1 \pmod{8}$, $1^2 \equiv 1 \pmod{8}$

מסקנה 3: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

הכחתי: $\left(\frac{-1}{p}\right) \equiv -1^{\frac{p-1}{2}} \pmod{p}$ אם $2k$ או $2k+1$ קונר אחרת שוון.

אם אי זכי היא מהצורה $4k+1$ או $4k+3$.

מסקנה 3': הקונר $x^2 \equiv -1 \pmod{p}$ ניתנת לפתרון $\Leftrightarrow p$ מהצורה $4k+1$

הכחתי: אם $p = 4k+1$ אז $(-1)^{2k} = (-1)^{\frac{p-1}{2}} = 1$ אחרת: $\left(\frac{-1}{p}\right)$

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

$$4k+1: 5, 13, 17, 29, \dots$$

1- הטו ריבוע מובטא

$$4k+3: 7, 11, 19, 23, \dots$$

אם לא ריבוע מובטא

צדמטא: $(5) 2^2 = -1$, אם $p=7$: $-1 \equiv 6$ אינו ריבוע מובטא 7.

טענה: יש אינסוף ראשוניים מהצורה $4k+1$

הוכחנו כבר שיש אותם. צדמטא שיש אינסוף ראשוניים! מהצורה: $2, 4k+1, 4k+3$

נבחרת הסענה: נניח p_1, p_2, \dots, p_m ראשוניים מהצורה $4k+1$.

נבנה זכרית אחת נכונה.

זכיר $N = (2p_1 p_2 \dots p_m)^2 + 1$. כעת יהי N מס' טיפני.

אם $p \neq p_i$ $\forall i$ כי $p_i \nmid 1$.

אז $x^2 \equiv -1 \pmod{p}$ יש פתרון $x = 2p_1 p_2 \dots p_m$.

$(2p_1 \dots p_m)^2 + 1 \equiv 0 \pmod{p}$ (היי)
 $(2p_1 \dots p_m)^2 \equiv -1 \pmod{p}$

אין 1- הטו ריבוע מובטא p , לכן p מהצורה $4k+1$ קבוע!

2. מובטא אוצר p א הטו ריבוע $\frac{p-1}{2}$

עבור $a = -1$ אנו יוצעים (טוינו) $\leftarrow p = 4k+1$.

טענה:

(1) 2 הטו שארית ריבועית \pmod{p} אם p מהצורה $8k+1$ או $8k+7$

(2) 2 הטו אראשונית \pmod{p} אם p מהצורה $8k+3$ או $8k+5$

(3) טיפני: $\frac{p-1}{2} = (-1)^{\frac{p-1}{8}}$ (\leftarrow נותן את 1 מת 2)

הוכחה:

$8k \pm 1$

(1) אם $p = 8k \pm 1$ אז $\frac{p-1}{8} = 2k \pm \frac{1}{8}$

$\frac{p^2-1}{8} = 8k^2 \pm 2k$

$\frac{p^2-1}{8} = 1$ לכן 2 שארית \pmod{p}

$\frac{p^2-1}{8} = 8k^2 + 8k + 2 \pm (2k+1)$

(2) אם $p = 8k+4 \pm 1$ אז

$\frac{p^2-1}{8} = -1 \Rightarrow$ א שארית \pmod{p}

$10 = 2 \cdot 5$

$2 = 2 \cdot 1$

$8 = 2 \cdot 4$

$4 = 2 \cdot 2$

$6 = 2 \cdot 3$

$\frac{11-1}{2} \cdot \left(\frac{11-1}{2}\right)!$

$p=11$

$12 = 2 \cdot 6$

$2 = 2 \cdot 1$

$10 = 2 \cdot 5$

$4 = 2 \cdot 2$

$8 = 2 \cdot 4$

$6 = 2 \cdot 3$

צדמטא: $p=13$

$\frac{p-1}{2} = 6!$
 $\left(\frac{13-1}{2}\right)$

(3) $1 \equiv (-1)^1 (p-1) \pmod{p}$

$2 \equiv (-1)^2 \cdot 2 \pmod{p}$

$3 \equiv (-1)^3 (p-3) \pmod{p}$

$4 \equiv (-1)^4 \cdot 4 \pmod{p}$

:

$\frac{p-1}{2}$

המשך תוכנית 13

המשך תוכנית הפוכה:

מתקיים

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{S(p)} \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$S(p) = \sum_{i=1}^{\frac{p-1}{2}} i = \frac{1}{2} \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}\right) = \frac{p^2-1}{8}$$

כאשר

$$\left(\frac{2}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

ובעצם קיבולנו -

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}}$$

$$\frac{q}{p} \equiv \frac{p}{q}$$

צוואה: מסתבר על q, p ראשוניים או $13, 5$ ראשוניים.

$$\left(\frac{13}{5}\right) = \left(\frac{5}{13}\right) = -1$$

• עבור $5, 13$

$$\left(\frac{5}{13}\right) = \left(\frac{-8}{13}\right) = \frac{-1}{13} \cdot \frac{2}{13} \cdot \left(\frac{2}{13}\right)^2 = 1 \cdot (-1) = -1$$

$$\frac{5}{3} = \frac{2}{3} = -1$$

$$\frac{3}{5} = -1$$

• עבור $5, 3$

$$\frac{3}{7} = \frac{-4}{7} = \left(\frac{-1}{7}\right) \left(\frac{2}{7}\right)^2 = \frac{-1}{7} = -1$$

• עבור $7, 3$

$$\frac{7}{3} = \left(\frac{1}{3}\right) = 1$$

חוק ההדדיות הריבועית שני גורמים:

משפט (חוק ההדדיות הריבועית): יהיו q, p ראשוניים או $13, 5$ ראשוניים.

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (ב)$$

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \quad (ג)$$

(ג) ← אומר שאם p מהצורה $4k+1$ או q מהצורה $4k+1$ אז $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

אם p מהצורה $4k+3$ ו- q מהצורה $4k+3$ אז $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$