

תוספת 4

הונגרות (החלק) $m|a-b \iff a \equiv b \pmod{m}$

$a \in \mathbb{Z}$ $b \in \mathbb{Z}$ $k \in \mathbb{Z}$ $b = a + km$: קוסיט a ו- b מוציאו m נקיים

חשיים $\mathbb{Z}/m\mathbb{Z}$ \leftarrow מחלקות שקילות. זו הקוצת שאריות מוציאו m
residues mod m

שאריות מוציאו m :

$a \in \mathbb{Z}$ $\bar{a} = a + m\mathbb{Z}$ מחלקת a

$\bar{1} = 1 + 2\mathbb{Z} = 2\mathbb{Z}_{add}$, $\bar{0} = 0 + 2\mathbb{Z} = 2\mathbb{Z}$: $m=2$

חוק: יש כציוק m מחלקות קוסטונציה מוציאו m

הוכחת: (צדד) $S = \{0, 1, \dots, m-1\}$. אגן ציון שיש $a, b \in S$, $a \equiv b \pmod{m}$

אם $a = b$, ו $c \in \mathbb{Z}$ הו קו c אקר m .

'ה' $a, b \in S$, אם $a \equiv b \pmod{m}$ $\iff m|a-b$ $\iff m|a-b$ $\iff m|a-b$ $\iff m|a-b$

אם $a = b \iff |a-b| = 0$

\square $r \in S$, $c \in \mathbb{Z}$ $\iff c = qm + r$ $\iff c \equiv r \pmod{m}$ כותים $c \in \mathbb{Z}$ $\iff r \in S$

חוק: אם $a' \equiv a \pmod{m}$, $b' \equiv b \pmod{m}$:
 קיי $\left\{ \begin{array}{l} a+b \equiv a'+b' \pmod{m} \quad (1) \\ ab \equiv a'b' \pmod{m} \quad (2) \end{array} \right.$

הצטרף: $(a+m\mathbb{Z}) + (b+m\mathbb{Z}) := a+b+m\mathbb{Z}$

$(a+m\mathbb{Z}) \cdot (b+m\mathbb{Z}) := ab+m\mathbb{Z}$

$\bar{0} = m\mathbb{Z}$
 $\bar{1} = 1+m\mathbb{Z}$

$5 \cdot 5 \equiv 25 \equiv 4$

$m=7$ - לט

$-\bar{2} = \bar{5}$

$-2 \equiv 5 \pmod{7}$

$-2 \cdot -2 = 4$

$-\bar{2} \cdot -\bar{2} = \bar{4}$

$\mathbb{Z}/m\mathbb{Z}$

אם $x^2 - 11x + 31 = 0 \rightarrow$ אין פתרונות \mathbb{Z} - ה

$x^2 - 11x + 31 \equiv 1 \pmod{2} \neq 0$

$x \equiv 0 \pmod{2}$

אם $m=2$

הוכחה:

$x^2 - 11x + 31 \equiv 1 \pmod{2} \neq 0$

$x \equiv 1 \pmod{2}$

צורת גאומטרית (נספח): עבור איזוף a

טענה: אם $a \equiv 3 \pmod{4}$ אז אין $x, y \in \mathbb{Z}$ כך ש- $x^2 + y^2 = a$

הוכחה: אם x זוגי אז $x = 2k$ אז $x^2 = 4k^2$ אם x אי זוגי אז $x = 2k+1$ אז $x^2 = 4k^2 + 4k + 1$

אם x אי זוגי אז $x^2 \equiv 1 \pmod{4}$ אם x זוגי אז $x^2 \equiv 0 \pmod{4}$

כ"כ נשים y^2 נס

$$x^2 + y^2 \not\equiv 3 \pmod{4} \leftarrow$$

טענה: במחלקת הנוכחיות $3+4\mathbb{Z}$ יש אינסוף ראשוניים

$$(3+4\mathbb{Z} = k \in \mathbb{Z}, 3+4k : 3, 7, 11, 15, 19, 23, \dots)$$

הוכחה: הערה- אם $b, c \equiv 1 \pmod{4}$ אז $bc \equiv 1 \pmod{4}$

כעת אם $a \in \mathbb{Z}, a \neq 1, a \equiv -1 \pmod{4}$, אז $a = q_1 q_2 \dots q_s$ שיהיה a ראשוניים, אז \exists

q_i הם אי זוגיים ואי אפשר שכל q_i מתק"פ $q_i \equiv 1 \pmod{4}$

אם ה"פ u כך ש- $q_i \equiv -1 \pmod{4}$. כעת כותבים תשובה סופית של ראשוניים $\equiv 3 \pmod{4}$

$$p_0 = 3, p_1 = 7, p_2, \dots, p_e$$

אני בונה את ראשוני חזים מאותה צורת (כזו): $N = 4p_0 p_1 \dots p_e - 1$

אז N אי זוגי, $N \equiv -1 \pmod{4}$. סוגו של מחלק ראשוני p' של N

כך ש- $p' \equiv -1 \pmod{4}$. $p' | N$ ויש i ש- $p_i | N$ כי $p_i | 4p_0 \dots p_e$ אבל $p_i \nmid -1$

כל p_i ויש: $p' \neq p_i \leftarrow p' \equiv -1 \pmod{4}$ ויש $3 \nmid p'$

קונסטרקציה אינארית $ax = b \pmod{m}$

צורת-משפט פתירות קונג' לא אינארית:

$$x^2 - 1 \equiv 0 \pmod{6}, x_1 = 1, x_2 = -1, x_3 = 0$$

משפט: פתירות

⊖ פתירות אינארית $ax = b \pmod{m}$ יש פתירות $\Leftrightarrow d | b$ כאשר $d = \gcd(a, m)$

⊗ אם $d | b$ אז יש כזו d פתירות

⊕ אם x פתרון, אז גם הפתרונות הם $x_0 + am', x_0 + m', \dots, x_0 + (d-1)m'$ כאשר $m' = \frac{m}{d}$

$$x, y \in \mathbb{Z} \quad ax + ym = b \quad \Leftrightarrow \oplus ax \equiv b \pmod{m}$$

ה"פ פתרון משמעותי $\Leftrightarrow d | b$. יהי x_0, y_0 פתרון פרימיטיבי

כתיבים: $m' = \frac{m}{d}, a' = \frac{a}{d}$ אז הפתרון הפרימיטיבי של המשוואה הוא \leftarrow

תמונת תחום 4:

$t \in \mathbb{Z} \quad \begin{cases} x = x_0 + mt \\ y = y_0 - at \end{cases}$ המשך תורת:

$t \in \mathbb{Z} \quad x = x_0 + mt$ פתרון \otimes של

$x_0, x_0 + m', x_0 + 2m', \dots, x_0 + (d-1)m'$ $\otimes \otimes$ פתרון קונגרואנטי "ר" של $x \equiv x_0 \pmod{m}$.

$0 \leq r < d \quad t = qd + r \quad x_1 = x_0 + mt$ פתרון, כותמים r כל

$x_1 = x_0 + qdm' + rm' = x_0 + qm + rm$ של

$\otimes \otimes$ $x_1 = x_0 + rm'$ הפתרון קונגרואנטי. כאן r כל

יש בדיוק d פתרונות \pmod{m} שקולים.

$\otimes x \equiv 3 \pmod{15}$ $\otimes x - 15y = 3$ מצא:

$d = \gcd(6, 15) = 3$

$2x - 5y = 1$
פתרון $x=3, y=1$

פתרון $x_0 = 3, m = 15, d = 3, m' = 5$ הפתרונות: $3, 3+5, 3+2 \cdot 5$
 $3, 8, 13$

שאלה 1: $m \neq 1, a$ זריק a כל d - $ax \equiv b \pmod{m}$ קבוצת פתרון אחת.

הקבוצה מתקמה זה $d=1$ כל $d \mid b$ כל d פתרון $d=1$ פתרון.

שאלה 2: $\mathbb{Z}/m\mathbb{Z}$ פתרון $a \neq 0$ כל b $ax \equiv b \pmod{m}$ פתרון.

$ax \equiv b \pmod{m}$ יש בדיוק פתרון אחד.

$\mathbb{Z}/m\mathbb{Z}$ \rightarrow $ax \equiv b \pmod{m}$ פתרון \mathbb{Z} \rightarrow $\bar{a}x \equiv \bar{b} \pmod{m}$ פתרון $\mathbb{Z}/m\mathbb{Z}$.

לפי זה $\mathbb{Z}/m\mathbb{Z}$ פתרון $\mathbb{Z}/m\mathbb{Z}$ \rightarrow $\bar{a}x \equiv \bar{b} \pmod{m}$ פתרון \mathbb{Z} .

$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ הפתרון $\bar{a}x \equiv 1 \pmod{m}$ $\Leftrightarrow \bar{a}$ הפתרון $\bar{a}x \equiv 1 \pmod{m}$ פתרון $\mathbb{Z}/m\mathbb{Z}$.

יש פתרון $\bar{a}x \equiv 1 \pmod{m}$ $\Leftrightarrow \gcd(a, m) = 1$ פתרון $\mathbb{Z}/m\mathbb{Z}$.

$\Leftrightarrow \gcd(a, m) = 1$ פתרון $\mathbb{Z}/m\mathbb{Z}$ \rightarrow \bar{a} הפתרון $\bar{a}x \equiv 1 \pmod{m}$ פתרון $\mathbb{Z}/m\mathbb{Z}$.

כמה יש פתרון $\bar{a}x \equiv 1 \pmod{m}$ $\Leftrightarrow \phi(m)$ פתרון $\mathbb{Z}/m\mathbb{Z}$ \rightarrow $\bar{a}x \equiv 1 \pmod{m}$ פתרון $\mathbb{Z}/m\mathbb{Z}$.

$\phi(3) = 2$ מצא:

$\phi(4) = 2$
 $\phi(6) = 2$