

משפט: נניח, $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}$, $n \neq 0$

$$ax \equiv b \pmod{n}$$

(א) יש פתרון אם ורק אם $\gcd(a, n) \mid b$
 (ב) אם יש פתרון, הקושר הוא יחידה בקושר -

$$x \equiv \frac{b}{\gcd(a, n)} \pmod{\frac{n}{\gcd(a, n)}}$$

ולכן יש פתרון יחיד מודול $\frac{n}{\gcd(a, n)}$. אם $\gcd(a, n) \neq 1$ אז יש פתרון יחיד מודול $\frac{n}{\gcd(a, n)}$.

הוכחה:

(א) נניח $\gcd(a, n) \nmid b$. אז אין פתרון. אם $\gcd(a, n) \mid b$ אז יש פתרון.

$$ax \equiv b \pmod{n} \iff n \mid ax - b$$

$$\downarrow$$

$$\exists k \in \mathbb{Z} : n \mid ax - b$$

$$\downarrow$$

$$b = ax - kn$$

אם $\gcd(a, n) \nmid b$ אז אין פתרון. אם $\gcd(a, n) \mid b$ אז יש פתרון.

$$a = \gcd(a, n) \cdot L$$

$$b = \gcd(a, n) \cdot m$$

$$\downarrow$$

$$ax \equiv b \pmod{n}$$

$$\gcd(a, n) \cdot Lx \equiv \gcd(a, n) \cdot m \pmod{n}$$

$$Lx \equiv m \pmod{\frac{n}{\gcd(a, n)}}$$

$$\frac{Lx}{\frac{n}{\gcd(a, n)}} \equiv \frac{m}{\frac{n}{\gcd(a, n)}} \pmod{\frac{n}{\gcd(a, n)}}$$

$$\gcd\left(\frac{a}{\gcd(a, n)}, \frac{n}{\gcd(a, n)}\right) = 1$$

$$\frac{a'}{\frac{n}{\gcd(a, n)}} \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$$

נבדוק ק"ו ונבדוק

$$x \equiv \frac{b}{gcd(a,n)} a' \pmod{\frac{n}{gcd(a,n)}}$$

היכחתי שה' x בתוך $\frac{n}{gcd(a,n)}$ מוקדו
גם x הוא, כהחזרות של x מוקדו n

נניח x_0 - x בתוך $\frac{n}{gcd(a,n)}$ K מוקדו.

אם x כל ההחזרות של x מוקדו

$$x_r = x_0 + r \cdot \frac{n}{gcd(a,n)}, r \in \mathbb{Z}$$

$$= x_0 + r \cdot \frac{n}{d} \quad (d = gcd(a,n))$$

נניח $x_0, x_1, \dots, x_{d-1}$

הם נייטים וכל ההחזרות של x

מוקדו n .

כאשר x הוא, ההחזרות של x מוקדו n ,

כ' x מוקדו n $0 \leq r_1 < r_2$ K

$$x_{r_2} - x_{r_1} = (r_2 - r_1) \cdot \frac{n}{d} < n$$

$$x_{r_1} \not\equiv x_{r_2} \pmod{n}$$

כ' x מוקדו n $r \in \mathbb{Z}$ n מוקדו n

$$r = kd + q, \quad 0 \leq q < d, \quad k \in \mathbb{Z}$$

$$x_r = x_0 + \frac{r \cdot n}{d} = x_0 + (kd + q) \frac{n}{d}$$

$$= x_0 + q \frac{n}{d} + kn = x_0 + q \frac{n}{d} \pmod{n}$$

הם נייטים $x_0, \dots, x_{d-1}$ n מוקדו n

הם נייטים $x_0, \dots, x_{d-1}$ n מוקדו n

ס' חנוכה, מסכת הוללותא קדושת ק' ב' / ס' א' ח' פ'

$$a, x \equiv b, (\text{mod } m)$$

$$a_2 x \equiv b_2 \pmod{n_2}$$

$$x \equiv c \pmod{h}, \quad \forall h \in \mathcal{H}$$

1754-1755

$$x \equiv c \pmod{m} \left(\bigwedge_{i=1}^k (A_i : i \in \mathbb{N}, i \leq k) \right)$$

$$x \equiv c \pmod{n}$$

$$n/x - c$$

$$n_i / x - 0$$

$$x \equiv c \pmod{n_i}$$

$$a, b \neq 0, b/h, a/h$$

$$gcd(a, b) = 7$$

pt : 25 + 100

$$ab/n$$

קטן כח קו, $\sqrt{\cdot}$ יונקטור וי' נ' א' $a, b \in \mathbb{Z}$ - ער $a+b=1$ ו' ד' n $\vdash$

$$m = \sqrt{a_m + v_b m}$$

q_b/m

$pc, //, ab/bm, ab/am$
 $(a/m) \quad (b/m)$

ה'תשנ"ח - 2018

מעל העקר/ה הס"ח

בית המדרש (מאה 7) סוף ג'ת"ס, נאמר ונתייאר מן ג'ת"ס ארץ ישראל

שבת ג' י"א אדר, בארמון א"ת ישראל שבת 2 באדר 2' 1908

[illegible]

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$

המקרה "רגיל" $(x \in \mathbb{Z}, x \geq 0)$

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases}$$

המשפט הכללי: $\gcd(h_1, h_2, \dots, h_k) = 1$ ייתכן למצוא $c_1, c_2, \dots, c_k$ כאלו $x \equiv c_i \pmod{h_i}$

$$x \equiv c_1 \pmod{h_1}$$

$$\vdots$$

$$x \equiv c_k \pmod{h_k}$$

אם $h_1, h_2, \dots, h_k$ זרים בזוגות, אז $\gcd(h_1, h_2, \dots, h_k) = 1$ ויש פתרון.

$$x \equiv c \pmod{h_1 h_2 \dots h_k}$$

$$h = h_1 h_2 \dots h_k$$

$$m_i = \frac{h}{h_i}$$

$$\gcd(m_i, h_i) = 1$$

לכן $\exists$ a_i כאלו $a_i m_i \equiv 1 \pmod{h_i}$

אם $p \nmid h_i \Leftrightarrow i \neq j, p \nmid h_j$ אז $p \nmid m_i$ ויש פתרון.

אם $\gcd(h_i, h_j) = 1$ אז $\exists$ a_i, a_j כאלו $a_i m_i \equiv 1 \pmod{h_i}$ ויש פתרון.

$$m_i x_i \equiv c_i \pmod{h_i}$$

$$x = m_1 x_1 + \dots + m_k x_k$$

אם $x \equiv c_i \pmod{h_i}$ אז $m_i x_i \equiv c_i \pmod{h_i}$ ויש פתרון.

$$x = m_1 x_1 + \dots + m_k x_k \equiv c_i \pmod{h_i}$$

אם $x \equiv c_i \pmod{h_i}$ אז $m_i x_i \equiv c_i \pmod{h_i}$ ויש פתרון.

אם $x \equiv c_i \pmod{h_i}$ אז $m_i x_i \equiv c_i \pmod{h_i}$ ויש פתרון.

$$h_i | c_i - c_j \Leftrightarrow c_i \equiv c_j \pmod{h_i}$$

$$h_i | c_i - c_j \Leftrightarrow c_i \equiv c_j \pmod{h_i}$$

לפי (עמ' 155) ופנייה, $(h_1, h_2, \dots, h_k) \in \mathbb{Z}_n^k$

$$\Downarrow$$

$$x_i \equiv c_i \pmod{n}$$

אם $x + k_n \equiv x \pmod{n}$ נכון, אז $x + k_n \equiv c_i \pmod{n}$

אכן, בהנחה כי $x \equiv c_i \pmod{n}$ הוא נכון, אז $x + k_n \equiv c_i \pmod{n}$

$$x \equiv c_i \pmod{n}$$