

$R \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_k$  (Chinese Remainder Theorem) 227  
 $a \rightarrow (a+I_1, \dots, a+I_k)$  5/28, 22/31/16  
 $a \bmod I_i$

$I_1 \cap \dots \cap I_k$  ? מה נקרא?

$$\left( \begin{array}{c} a+I = I = 0+I \\ \Downarrow \\ a \in I \end{array} \right)$$

$R/I_1 \times \dots \times R/I_k$  אם יש לי פתרון בכולם אז יש לי פתרון בכולם?

$i \neq j, I_i + I_j = R$  הקשר בין  $I_i, I_j$  הוא  $I_i + I_j = R$  הקשר

מה קשר בין  $M, I$  אם  $M \subseteq I$  אז  $M+I = I$  אחרת  $M+I = R$

$(M \subseteq M+I = R \iff I \cap (M+I) = M)$   
 $I \cap (I+I) = I \cap I = I$

Chinese Remainder Theorem (CRT): אם  $I_1, \dots, I_k$  הם אידיאלים ראשוניים זרים  
 $R/I_1 \times \dots \times R/I_k \cong R / (I_1 \cap \dots \cap I_k)$

קיימת  $x \in R$  אם  $I_1, I_2$  זרים אז  $I_1 + I_2 = R$  ולכן  $\exists r_1 \in I_1, r_2 \in I_2$  כגון  $r_1 + r_2 = 1$   
 $p_i Z + p_j Z = \gcd(p_i, p_j) Z$

קיימת  $x \in R$  אם  $I_1, \dots, I_k$  זרים אז  $\exists x \in R$  כגון  $x \equiv a_i \pmod{I_i}$   
 $p_i Z + p_j Z = \gcd(p_i, p_j) Z$

$$\left\{ \begin{array}{l} x = a_1 \pmod{p_1} \\ \vdots \\ x = a_k \pmod{p_k} \end{array} \right.$$

$p_1 Z \cap \dots \cap p_k Z = p_1 \dots p_k Z$  אם  $p_1, \dots, p_k$  זרים אז  $p_1 \dots p_k = \gcd(p_1, \dots, p_k)$

$$\begin{aligned}
 x &= 2 \pmod{3} & \text{עיקרון } x \in \mathbb{Z} & \text{עבור } 1 \leq i \leq n \\
 x &= 2 \pmod{4} \\
 x &= 1 \pmod{5}
 \end{aligned}$$

$$x = \underbrace{4 \cdot 5 \cdot n_1}_{\pmod{3}} + \underbrace{3 \cdot 5 \cdot n_2}_{\pmod{4}} + \underbrace{3 \cdot 4 \cdot n_3}_{\pmod{5}}$$

$$x = 20n_1 = 2n_1 \pmod{3} \quad -3 \text{ חזרו על המספר}$$

$$x = 15n_2 = 3n_2 = 2 \quad n_1 = 1 \quad \text{על } 4 \text{ חזרו}$$

$$n_2 = 3^{-1} \cdot 2 = 3 \cdot 2 = 6 = 2 \pmod{4}$$

-5 חזרו על המספר

$$x = 12n_3 = 2n_3$$

$$n_3 = 2^{-1} = 3 \pmod{5}$$

$$x = 20 \cdot 1 + 15 \cdot 2 + 12 \cdot 3 = 86 = 26 \pmod{60}$$

העיקרון הזה פועל גם עבור מספרים רבים יותר. Powerful "psn" יס

העיקרון הזה פועל גם עבור מספרים רבים יותר. Powerful "psn" יס

העיקרון הזה פועל גם עבור מספרים רבים יותר. Powerful "psn" יס

העיקרון הזה פועל גם עבור מספרים רבים יותר. Powerful "psn" יס





אם  $e_1, e_2 \in \{0\}$  אז  $e_1 \cdot e_2 = 0 \in \{0\}$  (אובדנות)

אם  $e_1, e_2 \notin \{0\}$  אז

"3"

אם  $R$  קומוטטיבית  $\Rightarrow ab \in P \iff ba \in P$

$ab \notin P \iff ba \notin P$

משפט: אם  $R$  קומוטטיבית אז  $P$  הוא אידיאל ראשוני אם ורק אם  $R/P$  הוא שדה.

אם  $R$  קומוטטיבית ו- $I$  אידיאל ראשוני אז  $R/I$  הוא שדה. (אם  $I = R$  אז  $R/I = \{0\}$  אינו שדה).

משפט: אם  $I$  אידיאל ראשוני אז  $R/I$  הוא שדה.

אם  $I$  אידיאל ראשוני אז  $R/I$  הוא שדה.  $I \subset R$  ו- $I \neq R$ .

אם  $i + r_1 a \in (I + R_a) \cap S \neq \emptyset$  ו- $j + r_2 b \in (I + R_b) \cap S \neq \emptyset$  אז  $I$  אידיאל ראשוני.

$(j) \in S, r_1, r_2 \in R$   
 $S \ni (i + r_1 a)(j + r_2 b) =$  (שדה ראשוני)

$$= \underbrace{ij + ir_2b + jr_1a + r_1r_2ab}_{\in I} \in S$$

קומוטטיביות  $\Rightarrow I \cap S \neq \emptyset$ !

דוגמה 1 (שני תת-חבורות מתאימות)

יהי  $R$  חבורת קומוטטיבית  $P_1, \dots, P_n$  אידיאלים ראשוניים של  $R$  ויהי  $I \subseteq R$  אידיאל  
 $I \subseteq P_i$   $\forall i$  ויהי  $I \subseteq \cup P_i$  נקיים  $I \subseteq R$

הוכחה  
 נניח  $I \not\subseteq P_1, P_2$  נניח  $a_1 \in P_1, a_2 \in P_2$  ונניח  $a_1 \notin P_2, a_2 \notin P_1$   
 אזי  $a_1 + a_2 \in I$  (כי  $I$  אידיאל) וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

אם  $a_1 \in P_2$  או  $a_2 \in P_1$  אז  $a_1 + a_2 \in P_1 \cap P_2$  וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

אם  $a_1 \in P_2$  אז  $a_1 + a_2 \in P_2$  וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

$$a_1 = x \cdot a_2 \in P_1 \text{ כיוון } x \in P_1$$

אז  $x \in P_1$  וכן  $a_1 \in P_1$  וכן  $a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

דוגמה 2 (שני אידיאלים מתאימים)

~~$I \subseteq R$  אידיאל~~

אם  $I \subseteq \cup P_i$  אז  $I \subseteq P_i$  לכל  $i$  וכן  $I \subseteq R$  וכן  $I \subseteq \cup P_i$

כמו קודם נניח  $a_1 \in P_1, a_2 \in P_2$  ונניח  $a_1 \notin P_2, a_2 \notin P_1$   
 $x = a_1 + a_2 \in I$  וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

אם  $a_1 \in P_2$  אז  $a_1 + a_2 \in P_2$  וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

אם  $a_1 \in P_2$  אז  $a_1 + a_2 \in P_2$  וכן  $a_1 \in P_1, a_2 \in P_2$  וכן  $a_1 \notin P_2, a_2 \notin P_1$

דוגמה 3

$$a_n = x - a_1 - a_2 \in P_j$$

לכן

מקומות אחרים:

$$22732 = 62$$

הצגת חוקי של האותיות והן כצירי כלל לא האותיות

דחוי מקומות: חוקי של איותו ומוקומות שניתן והן כל רגע לא האותיות

חוקים: וניה  $I$  מוקומות שניתן כל איותו לא ניה  
או חוקי ולכן אפשר למצוא איותו  
 $a \in I$   $b \in J$   
 $b \in J$

$$abc \in J \subseteq I \subseteq J = \text{איותו}$$

$b \in I \subseteq J$  או  $a \in I \subseteq J$  - ה- חוקי והן מושגי איותו  
 $b \notin I - 1$   $a \notin J$  אלא לפי הדרחורה שלני

חוקים

$$\boxed{a \in I \subseteq J \text{ או } I \subseteq J \text{ איותו האותיות איותו}} \in$$

נ"ל