

# קורס B

גלעד מואב

30 בנובמבר 2021

חלק I

חלק א'

## 1 גבול של סדרה

נגדיר גבול של סדרה באינסוף

$$\lim_{n \rightarrow \infty} a_n = L \iff \forall \epsilon > 0. \exists N. \forall n > N. |a_n - L| < \epsilon$$



## 2 גבול של פונקציה

### 2.1 גבול הפונקציה באינסוף

בדומה לגבול של סדרה, גבול הפונקציה יהיה

$$\lim_{x \rightarrow \infty} f(x) = L \iff \forall \epsilon > 0. \exists N. \forall x > N. |f(x) - L| < \epsilon$$

### 2.2 גבול הפונקציה בנקודה כלשהי

$$\lim_{x \rightarrow x_0} f(x) = L \iff \forall \epsilon > 0. \exists \delta > 0. \forall x \in (x_0 - \delta, x_0 + \delta). |f(x) - L| < \epsilon$$

### 2.3 גבול הפונקציה שווה לאינסוף

$$\lim_{x \rightarrow \infty} f(x) = \infty \iff \forall \Delta \exists N \forall x > N. f(x) > \Delta$$

$$\lim_{x \rightarrow x_0} f(x) = \infty \iff \forall \Delta \exists \delta \forall x \in (x_0 - \delta, x_0 + \delta). f(x) > \Delta$$

### 2.4 גבולות חד צדדיים

#### 2.4.1 גבול מימין

$$\lim_{x \rightarrow x_0} f(x) = L \iff \forall \epsilon > 0. \exists \delta > 0. \forall x \in (x_0 - \delta, x_0). |f(x) - L| < \epsilon$$

$$\lim_{x \rightarrow x_0} f(x) = L \iff \forall \epsilon > 0. \exists \delta > 0. \forall x \in (x_0, x_0 + \delta). |f(x) - L| < \epsilon$$

### 3 רציפות הפונקציה ומשפט ערך הביניים

#### 3.1 רציפות פונקציה

תהא פונקציה  $f$ , נגיד כי  $f$  רציפה בנקודה  $x_0$  אם

$$\lim_{x \rightarrow x_0} f(x) = f(x_0)$$

נגיד כי פונקציה  $f$  רציפה בקטע  $I$  אם  $f$  רציפה בכל נקודה בקטע הנתון.

דרך קלה להראות שפונקציה  $f$  אינה רציפה בנקודה  $x_0$  היא להוכיח כי הגבולות החד צדדיים שונים, קרי

$$\lim_{x \rightarrow x_0^-} f(x) \neq \lim_{x \rightarrow x_0^+} f(x)$$

#### 3.2 משפט ערך הביניים

תהא  $f$  פונקציה רציפה בקטע  $I = [a, b]$ . משפט ערך הביניים אומר כי לכל ערך ב  $[f(a), f(b)]$  קיים מקור

$$\forall y \in [f(a), f(b)] \rightarrow \exists \sigma \in I. f(\sigma) = y$$

## 4 נגזרת

#### 4.1 הגדרת הנגזרת

נגיד כי  $f$  גזירה בנקודה  $x_0$  אם הגבול  $\lim_{h \rightarrow 0} \frac{f(x_0+h) - f(x_0)}{h}$  קיים. נגיד כי  $f$  גזירה בקטע  $I$  אם כל נקודה בקטע גזירה. נשים לב כי אם  $f$  גזירה בקטע  $I$  היא רציפה בקטע.

תהא  $f$  פונקציה גזירה בנקודה  $x_0$  נגדיר את הנגזרת בנקודה  $x_0$  להיות

$$f'(x_0) = \lim_{h \rightarrow 0} \frac{f(x_0+h) - f(x_0)}{h}$$

#### 5 קבוע אוילר $e$

נגדיר את קבוע אוילר בתור הגבול  $e = \lim_{x \rightarrow \infty} (1 + \frac{1}{x})^x \approx 2.718$ . בנוסף  $(e^x)' = e^x$ .

#### 6 שימושי הנגזרת

בעזרת הנגזרת לפונקציה בנקודה  $x_0$  נוכל למצוא את המשיק לפונקציה בנקודה זו ונוכל למצוא קירוב מסדר ראשון לפונקציה סביב  $x_0$



בנוסף נוכל להעזר בנגזרת בשביל למצוא גבולות מסוימים עם כלל לופיטל.

## נוסחאות נפוצות

לינאריות הנגזרת:

$$(\alpha \cdot f \pm \beta \cdot g)' = \alpha \cdot f' \pm \beta \cdot g'$$

כפל בנגזרת:

$$(f \cdot g)' = f' \cdot g + g' \cdot f$$

חלוקה בנגזרת:

$$\left(\frac{f}{g}\right)' = \frac{f' \cdot g - g' \cdot f}{g^2}$$

הרכבת הנגזרת:

$$(f \circ g)' = f'(g) \cdot g'$$

## 7 חקירת פונקציה

חקירת פונקציה מורכבת מהבאים:

1. דומיין
2. חיתוכים עם הצירים
3. נקודות קיצון
4. תחומי עליה וירידה
5. תחומי קעירות וקמירות
6. אסימפטוטות משופעות ומאונכות

**אסימפטוטה משופעת/אופקית**

$$y = mx + b$$

$$m = \lim_{\sigma \rightarrow \infty} \frac{f(\sigma)}{\sigma} / \lim_{\sigma \rightarrow \infty} f'(\sigma)$$

$$b = \lim_{\sigma \rightarrow \infty} f(\sigma) - m\sigma$$

## 8 כלל לופיטל

יהיו  $f, g$ , ומתקיים אחד מהבאים

$$\lim_{x \rightarrow x_0} f(x) = \lim_{x \rightarrow x_0} g(x) = 0 \quad 1.$$

$$\lim_{x \rightarrow x_0} f(x) = \pm\infty, \lim_{x \rightarrow x_0} g(x) \neq 0 \quad 2.$$

$$\lim_{x \rightarrow x_0} \frac{f(x)}{g(x)} = L \text{ קיים אז } \lim_{x \rightarrow x_0} \frac{f'(x)}{g'(x)} = L \text{ הגבול } L$$

## 9 פיתוח טיילור והערכת שגיאה

### 9.1 פיתוח טיילור

תהא  $f$ , נגדיר את טור טיילור סביב  $x_0$  כטור חזקות שמתקרב לפונקציה  $f$  סביב הנקודה  $x_0$

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!} (x - x_0)^n$$

נגדיר את פולינום טיילור מהדרגה  $m$  סביב  $x_0$  כסדרת הסכומים החלקיים מ-0 עד  $m$  של טור החזקות,

$$\sum_{n=0}^m \frac{f^{(n)}(x_0)}{n!} (x - x_0)^n$$

נקרא לטור טיילור סביב 0 טור מקלורן. פולינום טיילור נותן לנו קירוב טוב לפונקציה, את השגיאה נוכל לחשב בעזרת לגראנז.

### 9.2 הערכת שגיאה לפי לגראנז

נניח ורצינו למצוא את  $e^{0.1}$ , נעזר בפולינום מקלורן של הפונקציה  $e^x$  מהדרגה 3,

$$f(x) = 1 + (0.1) + \frac{1}{2!}(0.1)^2 + \frac{1}{3!}(0.1)^3 + R_3(0.1)$$

כך ש  $R_3(0.1)$  הוא השארית של הפולינום, במקרה הזה  $R_3(0.1) = f(x) - 1 + (0.1) + \frac{1}{2!}(0.1)^2 + \frac{1}{3!}(0.1)^3$  לפי לגראנז קיים  $c \in (0, 0.1)$  כך ש  $R_3(0.1) = \frac{f^{(4)}(c)}{4!}(0.1)^4$

באופן כללי נסמן את שארית פולינום טיילור מדרגה  $n$  סביב  $x_0$  עבור  $x$  כ  $R_n(x)$  לפי לגראנז אם פונקציה  $f$  גזירה  $n+1$  פעמים, קיים  $c \in (x, x_0) \cup (x_0, x)$  כך ש

$$R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!} (x - x_0)^{n+1}$$

נוכל לחסום את שארית הפולינום ( $R_n(x)$ ) באופן הבא

$$|R_n(x)| \leq \left| \frac{\max \{f^{(n+1)}(b) | b \in (x, x_0) \cup (x_0, x)\}}{(n+1)!} (x - x_0)^{n+1} \right|$$

## 10 ניוטון ראפסון

בעזרת ניוטון ראפסון נוכל למצוא קירובים לשורשים של פונקציות תהא פונקציה  $f$  בעלת שורש יחיד בקטע  $I$ , ניקח נקודה  $x_0 \in I$  כלשהי נמצא את פולינום הטיילור ראשונה סביב  $x_0$  ומוצאים את החיתוך שלו עם ציר ה- $x$ , נסמן נקודה זו ב  $x_1$

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

באופן כללי נסמן  $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ , כאשר  $n$  גדל כך  $x_n$  מתקרב לשורש הפונקציה ומתקיים  $\lim_{n \rightarrow \infty} f(x_n) = 0$

## II חלק

### חלק ב'

## 11 פונקציה קדומה ואינטגרל לא מסוים

נקרא ל  $F$  פונקציה קדומה ל  $f$  אם  $F' = f$  בהנתן פונקציה  $f$  נסמן את  $\int f(x) dx$  כמשפחת הפונקציות הקדומות ל  $f$ , נקרא לסימון זה ( $\int$ ) האינטגרל הלא מסוים של  $f$

## 12 שיטות אינטגרציה ואינטגרלים מוכרים

### 12.1 שיטות אינטגרציה מוכרות

1. שימוש בשברים חלקיים

$$\int \frac{1}{1-x^2} dx = \int \frac{1}{1-x} \cdot \frac{1}{1+x} dx = \int \left( \frac{A}{1-x} + \frac{B}{1+x} \right) dx \left[ A = B = \frac{1}{2} \right] = \frac{\int \frac{1}{1-x} dx + \int \frac{1}{1+x} dx}{2}$$

2. שימוש בהצבה

$$\int \frac{x}{1-x^2} dx \left[ \begin{array}{l} u = x^2 \\ dx = \frac{du}{2x} \end{array} \right] = \int \frac{x}{1-u} \cdot \frac{du}{2x} = \int \frac{1}{1-u} du$$

3. אינטגרציה בחלקים

$$\int f \cdot g' = f \cdot g - \int f' \cdot g$$

4. דרך נוספת - שימוש בחלוקת פולינומים

ניקח לדוגמא את השאלה  $x^3 - x^2 + 0x - 4$  חלקה ב- $x-3$   
תחילה נחלק את האיברים המובילים אחד בשני

$$x-3 \overline{) x^3 - x^2 + 0x - 4}$$

כעת נחסר את  $(x-3)x^2$  מ- $x^3 - x^2$

$$\begin{array}{r} x-3 \overline{) x^3 - x^2 + 0x - 4} \\ \underline{x^3 - 3x^2 \phantom{+ 0x} \downarrow} \\ 2x^2 + 0x \end{array}$$

וכן הלאה....

$$\begin{array}{r} x-3 \overline{) x^3 - x^2 + 0x - 4} \\ \underline{x^3 - 3x^2 \phantom{+ 0x} \downarrow} \\ 2x^2 + 0x \\ \underline{2x^2 - 3x} \\ 3x - 4 \\ \underline{3x - 9} \\ 5 \end{array}$$

לכן  $\frac{x^3 - x^2 - 4}{x-3} = x-3 \overline{) x^3 - x^2 + 0x - 4} = x^2 + 2x + 3 + \frac{5}{x-3}$

### 12.2 אינטגרלים מוכרים

$$\int x^\alpha dx = \frac{x^{\alpha+1}}{\alpha+1} + C, x > 0; \alpha \neq -1$$

$$\int \frac{1}{x} dx = \ln |x|$$

$$\int \sin x dx = -\cos x + C$$

$$\int \cos x dx = \sin x + C$$

$$\int \sinh x dx = \cosh x + C$$

$$\int \cosh x dx = \sinh x + C$$

$$\int \frac{1}{1+x^2} dx = \arctan x + C$$

$$\int e^x dx = e^x + C$$

$$\int \sec^2 x dx = \tan x + C$$

$$\int \csc^2 x dx = -\cot x + C$$

$$\int \operatorname{sech} x dx = \tanh x + C$$

$$\int \operatorname{csch} x dx = -\coth x + C$$

$$\int \frac{1}{\sqrt{1-x^2}} dx = \arcsin x + C$$

## 13 סכומי דרבו ואינטגרל מסוים

### 13.1 סכומי דרבו

יהי קטע  $I = [a_0, a_{n+1}]$  נסמן חלוקה של הקטע הנ"ל  $I_{\langle a_1, \dots, a_n \rangle}$  כך ש  $a < \{a_i\}_{i=1}^n < b$  תהא חלוקה  $I_{\langle a_1, \dots, a_n \rangle}$ , סכומי דרבו העליונים על החלוקה הנ"ל יהיו

$$\sum_{i=0}^n (a_{n+1} - a_n) \cdot \max \{f(x) | x \in [a_{n+1}, a_n]\}$$

והתחתונים

$$\sum_{i=0}^n (a_{n+1} - a_n) \cdot \min \{f(x) | x \in [a_{n+1}, a_n]\}$$

נסמן  $D_{I_{\langle a_1, \dots, a_n \rangle}}^{\pm}$  כסכומי דרבו התחתונים/עליונים  
נסמן  $\Pi_n$  כ  $\langle a_1, \dots, a_n \rangle$  כך שלכל  $i, i$   $a_i = a_0 + \frac{b-a}{n} \cdot i$



### 13.2 פונקציה אינטגרבילית, אינטגרל רימן ואינטגרל מסוים

נגיד כי פונקציה  $f: I \rightarrow \mathbb{R}$  אינטגרבילית רימן בקטע  $I$  אם ומ"מ  $\lim_{n \rightarrow \infty} D_{\Pi_n}^+ - D_{\Pi_n}^- = 0$  או לחלופין  $\lim_{n \rightarrow \infty} D_{\Pi_n}^- = \lim_{n \rightarrow \infty} D_{\Pi_n}^+ = S$

במקרה זה נסמן  $\int_a^b f(x)dx = S$ , נקרא לפעולה זו אינטגרל מסוים

כל פונקציה רציפה היא אינטגרבילית ובפרט הפונקציות האלמנטריות (בסיסיות)

### 14 המשפט היסודי של החדו"א ומשפט ניוטון-לייבניץ

#### 14.1 המשפט היסודי של החדו"א

תהא  $f: I \rightarrow \mathbb{R}$  אינטגרבילית בקטע  $I = [a, b]$ , נגדיר את הפונקציה צוברת השטח

$$F(x) = \int_a^x f(t)dt$$

1.  $F$  פונקציה רציפה

2. אם  $f$  רציפה ב- $x_0$  אז  $F$  גזירה ב- $x_0$  וכן  $F'(x_0) = f(x_0)$

באופן כללי, אם  $f$  רציפה בקטע  $I$  אז  $F$  קדומה לה בקטע הנ"ל

#### 14.2 משפט ניוטון-לייבניץ

אם  $f$  רציפה בקטע  $I = [a, b]$  (לכן  $\int_a^x f$  של  $f$ ) ונניח כי  $F$  קדומה של  $f$ , מתקיים

$$\int_a^b f(x)dx = F(b) - F(a)$$

### 15 שימושי האינטגרל

#### 15.1 חישוב שטח מתחת לגרף

תהא  $f$  אינטגרבילית בקטע  $I = [a, b]$ ,  $\int_a^b f(x)dx$  הוא השטח מתחת ל- $f$  בקטע  $[a, b]$



#### 15.2 חישוב אורך עקומה

תהא  $f$  אינטגרבילית בקטע  $I = [a, b]$  ונרצה למצוא את אורך העקומה בין  $a$  ל- $b$ , נעזר במשפט פתגורס ונראה כי

$$\int_a^b \sqrt{dx^2 + dy^2} = \int_a^b \sqrt{1 + \frac{dy^2}{dx^2}} dx = \int_a^b \sqrt{1 + (f'(x))^2} dx$$



### 15.3 נפח גוף סיבוב

#### 15.3.1 נפח גוף סיבוב סביב ציר ה־ $x$

$$\pi \int_a^b f^2(x) dx$$

במקרה בו מדובר על נפח גוף סיבוב של שטח הכלוא בין 2 פונקציות  $f, g$

$$\pi \int_a^b |f^2(x) - g^2(x)| dx$$

#### 15.3.2 נפח גוף סיבוב סביב ציר ה־ $y$

$$2\pi \int_a^b x f(x) dx$$

## חלק III

## חלק ג'

### 16 הגדרות בסיסיות בתורת המספרים

#### 16.1 יחס ה־

יהיו  $m, k \in \mathbb{Z}$ , נגיד כי  $m|k$  אם קיים  $i \in \mathbb{Z}$  כך ש  $m \cdot i = k$  או באופן כללי

$$m|k \iff \exists i \in \mathbb{Z}. m \cdot i = k$$

#### 16.2 mod

נגיד כי  $b \bmod n = a$  אם  $m \in \mathbb{Z}$  כך  $b = m \cdot n + a$

$$b \bmod n = a \iff \exists m \in \mathbb{Z}. b = m \cdot n + a$$

#### 16.3 gcd

$\gcd(a, b)$  הוא המחלק המשותף הגדול ביותר של  $a$  ו  $b$

$$\gcd(a, b) = \max \{m \in \mathbb{Z} | m|a \wedge m|b\}$$

### 17 משפט אוקלידס לקיום אינסוף ראשוניים

משפט אוקלידס אומר כי קיימים אינסוף ראשוניים.

צ"ל קיימים אינסוף ראשוניים, נניח בשלילה כי קיים מספר סופי  $n$  של ראשוניים, נסמן  $p_1, p_2, \dots, p_n$ , נגדיר מספר  $p = 1 + \prod_{i=1}^n p_i$ ,

נשים לב כי  $p$  לא מתחלק באף  $p_i$  לכן  $p$  ראשוני וקיימים  $n+1$  ראשוניים, סתירה!  
לכן קיימים אינסוף ראשוניים



## 18 מחלק משותף מירבי

כפי שראינו  $\gcd(a, b)$  ימצא לנו את המחלק המשותף הגדול ביותר של  $a$  ו- $b$  עבור  $\gcd(a, b) = c$  קיים "ייצוג לינארי", כלומר קיימים  $t, s \in \mathbb{Z}$  כך ש

$$t \cdot a + s \cdot b = c$$

### מספרים זרים

עבור  $a, b$  כך ש  $\gcd(a, b) = 1$  נגיד כי  $a$  ו- $b$  זרים

### משפט

עבור  $a, b$  זרים אמ"מ קיימים  $s, t \in \mathbb{Z}$  כך ש  $t \cdot a + s \cdot b = 1$

## 19 אלגוריתם אוקלידס

### 19.1 אלגוריתם אוקלידס

יהיו  $a, b$  נרצה למצוא את  $\gcd(a, b)$  אלגוריתם אוקלידס נותן פיתרון יעיל ופשוט לבעיה זו האלגוריתם משתמש בעובדה ש  $\gcd(a, b) = \gcd(a, b + m \cdot a)$ , לכן

$$a = m_1 \cdot b + n_1$$

$$b = m_2 \cdot n_1 + n_2$$

.

.

$$n_{i-3} = m_{i-1} \cdot n_{i-2} + c$$

$$n_{i-2} = m_i \cdot c + 0$$

לכן  $\gcd(a, b) = c$  באופן פשוט יותר נוכל לעבוד באופן הבא  $\gcd(a, b) = \gcd(b, a \bmod b) = \dots = \gcd(c, 0) = c$

### 19.2 אלגוריתם אוקלידס המורחב

האלגוריתם המורחב עוזר לנו למצוא ייצוג לינארי לשיוויון מהסוג  $\gcd(a, b) = c$  הוא עובד כמו האלגוריתם הקודם, רק אחורה, כלומר נתחיל מהשלב האחרון ונראה כי

$$n_{i-3} - m_{i-1} \cdot n_{i-2} = c$$

השלב הבא יהיה הצבת הערכים מהשוויונים שראינו מהאלגוריתם הקודם

$$n_{i-3} - m_{i-1} \cdot (n_{i-4} - m_{i-2} \cdot n_{i-3}) = c$$

וכן הלאה

נרצה למצוא את  $\gcd(840, 138)$  ואת הייצוג הלינארי שלו

$$840 = 6 \cdot 138 + 12$$

$$138 = 11 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0$$

לכן  $\gcd(840, 138) = 6$   
 כעת נמצא את הייצוג הלינארי שלהם

$$6 = 138 - 11 \cdot 12$$

$$6 = 138 - 11 \cdot (840 - 6 \cdot 138)$$

$$6 = 67 \cdot 138 - 11 \cdot 840$$

## 20 משפט על פריקות יחידה לראשוניים

לכל מספר שלם קיימת פריקות יחידה למספרים ראשוניים

## 21 משוואות דיאופנטיות לינאריות

תהא משוואה דיאופנטית  $a \cdot x + b \cdot y = c$

### 21.1 קיום פתרון למשוואה

נראה כי אם  $\gcd(a, b) \mid c$  קיים פתרון ולחלופין אם  $\gcd(a, b) \nmid c$  לא קיים פתרון למשוואה

### 21.2 מציאת פתרון פרטי

בהנחה ולמשוואה קיים פתרון  $\gcd(a, b) \mid c$ , נסמן  $d = \gcd(a, b)$ , ונראה כי מכיון ש  $d \mid c$  קיים  $e$  כך ש  $d \cdot e = c$ , כלומר  $e = \frac{c}{d}$ . בנוסף מכיון ש  $d = \gcd(a, b)$  קיים ייצוג לינארי  $t \cdot a + s \cdot b = d$ , נכפיל את שני האגפים ב  $e$  ונקבל

$$e \cdot t \cdot a + e \cdot s \cdot b = e \cdot d \rightarrow (e \cdot t) \cdot a + (e \cdot s) \cdot b = \frac{c}{d} \cdot d = c$$

לכן הפתרון הפרטי למשוואה  $a \cdot x + b \cdot y = c$  יהיה  $x_0 = e \cdot t, y_0 = e \cdot s$

### 21.3 מציאת כל הפתרונות

קבוצת כל הפתרונות היא

$$\left\{ \left\langle x_0 + \frac{b}{d} \cdot z, y_0 - \frac{a}{d} \cdot z \right\rangle \mid z \in \mathbb{Z} \right\}$$

## 22 הפיכות מודולו, משפט פרמה הקטן ומשפט השארית הסיני

### 22.1 משפט פרמה הקטן

יהיו  $p \in \mathbb{P}$  ו  $a$  כך ש  $\gcd(a, p) = 1$  יתקיים

$$a^{p-1} = 1 \pmod{p}$$

## 22.2 הפיכות מודולו

ידוע לנו על פעולות החיבור, חיסור וכפל במודולו, אך מה לגבי חילוק?  
יהי  $k \in \mathbb{Z}$ , נרצה לדעת האם קיים  $m \in \mathbb{Z}$  כך ש  $m \equiv \frac{1}{k} \pmod{n}$  או באופן שקול  $m \cdot k \equiv 1 \pmod{n}$   
משפט על הפיכות המודולו אומר כי אם  $k$  ו  $n$  זרים קיים  $m$  כך ש  $m \cdot k \equiv 1 \pmod{n}$

$$\gcd(k, n) = 1 \iff \exists m \in \mathbb{Z}. m \cdot k \equiv 1 \pmod{n}$$

## 22.3 משפט השאריות הסיני

### 22.3.1 דוגמא

נרצה לפתור את מערכת המשוואות הבאה

$$\begin{cases} x \equiv 7 \pmod{19} \\ x \equiv 3 \pmod{5} \end{cases}$$

באופן שקול נוכל לפתור את

$$\begin{cases} x = 19a + 7 \\ x = 5b + 3 \end{cases}$$

נחסר את המשוואות אחת מהשנייה ונקבל

$$0 = 19a - 5b + 4 \rightarrow 4 = 5b - 19a$$

נראה כי קיים פתרון למשוואה מכיון ש  $\gcd(5, -19) = 1 \mid 4$ , למשל  $-12$

### 22.3.2 הכללה

באופן כללי כאשר נרצה לפתור מערכת משוואות מהצורה הבאה

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdot \\ \cdot \\ x \equiv a_n \pmod{m_n} \end{cases}$$

לפי משפט השאריות הסיני, זרים בזוגות שקול לקיום פתרון למערכת המשוואות

### 22.3.3 פתרון פרטי

נסמן  $n_i = \frac{m}{m_i}$ , נשים לב כי  $m_i, n_i$  זרים ( $\gcd(m_i, n_i) = 1$ ), לכן קיימים  $s_i, t_i$  כך ש  $s_i \cdot n_i + t_i \cdot m_i = 1$   
נסמן  $e_i = s_i \cdot n_i$  ונראה כי  $e_i + t_i \cdot m_i = 1$  לכן  $e_i \equiv -t_i \cdot m_i + 1$  לכן  $e_i \equiv 1 \pmod{m_i}$   
באופן כללי אם נקח  $i \neq j$  יתקיים  $e_i \equiv 0 \pmod{m_j}$  מכיון ש  $m_j \mid n_i e_i$  לכן כתלות ב  $i$  ו  $j$  נערכו של  $\delta_{i,j} \pmod{m_j} = e_i$

$$\delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

הפתרון הפרטי של מערכת המשוואות תהיה  $x_0 = \sum_{k=1}^n a_k \cdot e_k$  שכן

$$x_0 \pmod{m_i} = \left( \sum_{k=1}^n a_k \cdot e_k \right) \pmod{m_i} = \sum_{k=1}^n (a_k \pmod{m_i}) \cdot (e_k \pmod{m_i}) =$$

$$0 \cdot (a_1 \pmod{m_i}) + \dots + 1 \cdot (a_i \pmod{m_i}) + \dots = a_i \pmod{m_i}$$

קבוצת הפתרונות למערכת המשוואות הנ"ל תהיה

$$\{x_0 + m \cdot z \mid z \in \mathbb{Z}\}$$

## חלק IV

## חלק ד'

23 השערת הרצף

24 השערת רימן

25 השערת הנאד

26 סודרים

