

מבוא לתורת המספרים האלמנטרית

תזכורת

לכל a ולכל $b \neq 0$, קיימים q, r כך ש:

$$a = q \cdot b + r$$

:1

$$0 \leq r < |b|$$

תזכורת

יהיו $a, b \in \mathbb{Z}$, לא שניהם 0.

אז קיימים $\alpha, \beta \in \mathbb{Z}$, כך ש:

$$(a, b) = \alpha a + \beta b$$

תזכורת

אם $(a, b) = 1$ ו- $a|bc$, אז $a|c$.

תזכורת

a אי פריק אם מתקיים: אם $b|a$, אז $b = \pm 1, \pm a$.

p ראשוני אם מתקיים: אם $p|bc$, אז $p|b$ או $p|c$.

משפט

מספר ראשוני הוא אי פריק.

הוכחה

יהי $p \in \mathbb{Z}$ ראשוני.

נניח כי:

$$p = bc$$

מתקיים:

$$p \mid p$$

לכן:

$$p \mid bc$$

p ראשוני, לכן:

$$p \mid b \vee p \mid c$$

עפ"י ההנחה:

$$b \mid p \wedge c \mid p$$

לכן:

$$\begin{array}{l} b = \pm p \quad c = \pm p \\ \vee \\ c = \pm 1 \quad b = \pm 1 \end{array}$$

לכן, p אי פריק.

■

משפט

מספר אי פריק הוא ראשוני.

הוכחה

יהי $p \in \mathbb{Z}$ אי פריק.

נניח כי:

$$p \mid bc$$

אם $p \mid b$, סיימנו.

אחרת, $p \nmid b$.

עפ"י הגדרת המחלק המשותף המקסימלי:

$$(p, b) \mid p$$

p אי פריק, לכן:

$$(p, b) = \pm 1, \pm p$$

עפ"י הגדרת המחלק המשותף המקסימלי:

$$(p, b) \mid b$$

לכן:

$$(p, b) = 1$$

עפ"י משפט:

$$p \mid c$$

לכן, בכל מקרה:

$$p \mid b \vee p \mid c$$

לכן, p ראשוני.

■

משפט (המשפט היסודי של האריתמטיקה)

כל מספר שלם שווה, עד כדי סדר וסימן, למכפלה של אי פריקים, באופן יחיד.

הוכחה

קיום

נוכיח באינדוקציה שלמה על $n \in \mathbb{N}$.

אם n אי פריק, סיימנו.

אחרת, n פריק.

לכן קיימים $a, b < n$, כך ש:

$$n = ab$$

עפ"י הנחת האינדוקציה, a, b הם מכפלה של אי פריקים.

לכן, גם n הוא מכפלה של אי פריקים.

לכן, בכל מקרה, n שווה למכפלה של אי פריקים.

יחידות

נניח כי:

$$p_1 \cdots p_t = n = \pm q_1 \cdots q_s$$

כאשר לכל $p_i, q_j, 1 \leq i \leq t, 1 \leq j \leq s$ אי פריקים.

עפ"י משפט, ראשוני.

לכן, קיים $1 \leq j \leq s$, כך ש:

$$p_t \mid q_j$$

q_j אי פריק, לכן:

$$p_t = \pm q_j$$

נצמצם אותם מהמכפלה, ונסיים באינדוקציה על t .

■

הערה (משפט של אוקלידס)

קיימים אינסוף מספרים ראשוניים.

הוכחה

נניח בשלילה כי קיים מספר סופי של מספרים ראשוניים:

$$p_1, \dots, p_n$$

נתבונן במספר:

$$N := p_1 \cdots p_n + 1$$

נוכיח כי N אינו מתחלק באף ראשוני מבין p_1, \dots, p_n .

נניח בשלילה כי קיים $1 \leq i \leq n$ כך ש:

$$p_i \mid N$$

מתקיים:

$$p_i \mid p_1 \cdots p_n$$

לכן:

נכתב על ידי יהונתן רגב

שקילות מודולו n

$$p_i \mid N - p_1 \cdots p_n$$

$$\mid 1$$

סתירה.

לכן, N אינו מתחלק באף ראשוני מבין p_1, \dots, p_n .עפ"י המשפט היסודי של האריתמטיקה, N ראשוני.

סתירה.

לכן, קיימים אינסוף מספרים ראשוניים.



תרגיל

קיימים אינסוף ראשוניים השקולים ל-1 מודולו 4.

הוכחה

נניח בשלילה כי קיים מספר סופי של ראשוניים השקולים ל-1 מודולו 4:

$$p_1, \dots, p_n$$

נתבונן במספר:

$$N := 4p_1 \cdots p_n - 1$$

עפ"י הגדרת N , N אינו מתחלק ב-2 ואינו מתחלק באף ראשוני השקול ל-1 מודולו 4.עפ"י המשפט היסודי של האריתמטיקה, קיים פירוק של N כמכפלה של ראשוניים, שכולם

שקולים ל-1 מודולו 4.

לכן:

$$N \equiv 1 \pmod{4}$$

עפ"י הגדרת N :

$$N \equiv -1 \pmod{4}$$

סתירה.

לכן, קיימים אינסוף ראשוניים השקולים ל-1 מודולו 4.

■

תרגיל

כ"ל:

$$p \equiv -1 \pmod{6}$$

$$p \equiv 1 \pmod{6}$$

$$p \equiv 1 \pmod{4}$$

הגדרה

יהי $n \geq 1$.

נגדיר יחס בינארי על השלמים:

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

טענה

יחס זה הוא יחס שקילות.

הוכחה

יהי $n \in \mathbb{N}$.

• רפלקסיביות:

יהי $a \in \mathbb{Z}$.

מתקיים:

$$n \mid 0$$

$$\mid a - a$$

לכן:

$$a \equiv a \pmod{n}$$

• סימטריות:

יהיו $a, b \in \mathbb{Z}$.

נניח כי:

נכתב על ידי יהונתן רגב

שקילות מודולו n

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

לכן:

$$n \mid a - b$$

$$\Downarrow$$

$$n \mid b - a$$

לכן:

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

• טרנזיטיביות:יהיו $a, b, c \in \mathbb{Z}$.

נניח כי:

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

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

לכן:

$$n \mid a - b$$

$$n \mid b - c$$

$$\Downarrow$$

$$n \mid (a - b) + (b - c)$$

$$\mid a - c$$

לכן:

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

לכן, יחס זה הינו יחס שקילות.

■

טענה

מחלקות השקילות של יחס זה הן:

$$[0], [1], \dots, [n-2], [n-1]$$

הוכחה

צ"ל כי לכל $a \in \mathbb{Z}$, קיים $0 \leq r < n$ יחיד כך ש:

$$a \equiv r \pmod{n}$$

יהי $a \in \mathbb{Z}$.

קיום

נחלק את a ב- n עם שארית:

$$a = q \cdot n + r, \quad 0 \leq r < n$$

מתקיים:

$$\begin{aligned} n &| q \cdot n \\ &| a - r \end{aligned}$$

לכן:

$$a \equiv r \pmod{n}$$

יחידות

נניח בשלילה כי קיימים $0 \leq r < r' < n$ כך ש:

$$r \pmod{n} \equiv a \equiv r' \pmod{n}$$

לכן:

$$\begin{aligned} n &| a - r \\ n &| a - r' \end{aligned}$$

↓

$$\begin{aligned} n &| (a - r) - (a - r') \\ &| r' - r \end{aligned}$$

לכן:

נכתב על ידי יהונתן רגב

שקילות מודולו n

$$n \leq r' - r < n$$

סתירה.

לכן:

$$r' = r$$

לכן, מחלקות השקילות של יחס זה הן:

$$[0], [1], \dots, [n-2], [n-1]$$

■

הגדרהיהי $n \geq 1$.

נגדיר:

$$\mathbb{Z}_n := \{[0], [1], \dots, [n-2], [n-1]\}$$

כלומר, \mathbb{Z}_n הוא אוסף מחלקות השקילות מודולו n .נהפוך את \mathbb{Z}_n לחבורה.**הגדרה**נגדיר פעולת חיבור על \mathbb{Z}_n .לכל $a, b \in \mathbb{Z}$:

$$[a] + [b] := [a + b]$$

נוכיח כי הפעולה מוגדרת היטב.

נניח כי:

$$a \equiv a'$$

$$b \equiv b'$$

לכן:

נכתב על ידי יהונתן רגב

שקילות מודולו n

$$n \mid a - a'$$

$$n \mid b - b'$$

לכן:

$$n \mid (a - a') + (b - b')$$

$$\mid (a + b) - (a' - b')$$

לכן:

$$a + b \equiv a' + b'$$

■

דוגמה

לוח חיבור של \mathbb{Z}_4 :

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

הערה

נוכיח כי \mathbb{Z}_n חבורה ביחס לחיבור.

- אסוציאטיביות
לכל $a, b, c \in \mathbb{Z}$

$$[a] + ([b] + [c]) = [a] + [b + c]$$

$$= [a + b + c]$$

$$([a] + [b]) + [c] = [a + b] + [c]$$

$$= [a + b + c]$$

לכן:

$$[a] + ([b] + [c]) = ([a] + [b]) + [c]$$

• קיום איבר יחידה

לכל $a \in \mathbb{Z}$:

$$[0] + [a] = [0 + a]$$

$$= [a]$$

$$[a] + [0] = [a + 0]$$

$$= [a]$$

• קיום איבר הופכי

לכל $a \in \mathbb{Z}$:

$$[a] + [-a] = [a + (-a)]$$

$$= [0]$$

$$[-a] + [a] = [-a + a]$$

$$= [0]$$

לכן, $(\mathbb{Z}_n, +, [0])$ חבורה.

■

הגדרה

נגדיר פעולת כפל על \mathbb{Z}_n .

לכל $a, b \in \mathbb{Z}$:

$$[a] \cdot [b] := [a \cdot b]$$

נוכיח כי הפעולה מוגדרת היטב.

נניח כי:

$$a \equiv a'$$

$$b \equiv b'$$

לכן:

$$n \mid a - a'$$

$$n \mid b - b'$$

לכן:

$$n \mid a(b - b') + (a - a')b'$$

$$\mid ab - a'b'$$

לכן:

$$ab \equiv a'b'$$

■

הערה

לוח כפל של \mathbb{Z}_4 :

\odot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

הערה

נוכיח כי \mathbb{Z}_n מונויד ביחס לכפל.

- אסוציאטיביות
לכל $a, b, c \in \mathbb{Z}$

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c]$$

$$= [a \cdot b \cdot c]$$

$$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c]$$

$$= [a \cdot b \cdot c]$$

לכן:

$$[a] \cdot ([b] \cdot [c]) = ([a] \cdot [b]) \cdot [c]$$

• קיום איבר יחידה

לכל $a \in \mathbb{Z}$:

$$[1] \cdot [a] = [1 \cdot a]$$

$$= [a]$$

$$[a] \cdot [1] = [a \cdot 1]$$

$$= [a]$$

לכן, $(\mathbb{Z}_n, \cdot, [1])$ מונוידי.

■

שאלה

מהם האיברים ההפיכים ב- \mathbb{Z}_n ביחס לכפל?

טענה

$[a]$ הפיכה ב- $(\mathbb{Z}_n, \cdot, [1])$ אם ורק אם $(a, n) = 1$.

הוכחה



נניח כי $[a]$ הפיכה.

לכן, קיים b כך ש:

$$[a] \cdot [b] = [1]$$

לכן:

$$ab \equiv 1 \pmod{n}$$

לכן:

$$n \mid ab - 1$$

עפ"י הגדרת המחלק המשותף המקסימלי:

$$(a, n) \mid n$$

$$\mid ab - 1$$

עפ"י הגדרת המחלק המשותף המקסימלי:

$$(a, n) \mid a$$

$$\mid ab$$

לכן:

$$(a, b) \mid ab - (ab - 1)$$

$$\mid 1$$

לכן:

$$(a, n) = 1$$



נניח כי: $(a, n) = 1$.

עפ"י משפט, קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש:

$$\alpha a + \beta n = 1$$

מתקיים:

$$n \mid \beta n$$

$$\mid 1 - \alpha a$$

לכן:

$$\alpha a \equiv 1 \pmod{n}$$

לכן:

$$[\alpha] \cdot [a] = [1]$$

לכן, $[a]$ הפיכה.



מסקנה

$$\mathcal{U}(\mathbb{Z}_n, \cdot, [1]) = \{[a] \mid (a, n) = 1\}$$

חבורה זו נקראת חבורת אוילר של n , ומסומנת:

$$U_n := \mathcal{U}(\mathbb{Z}_n, \cdot, [1])$$

הגדרה

$$\varphi(n) := |U_n|$$

דוגמה

לוחות הכפל של U_8, U_{12} :

	U_8	\cong	U_{12}																																																			
	<table style="border-collapse: collapse; width: 100%;"> <thead> <tr> <th style="border-right: 1px solid black; padding: 5px;">\odot</th> <th style="padding: 5px;">1</th> <th style="padding: 5px;">3</th> <th style="padding: 5px;">5</th> <th style="padding: 5px;">7</th> </tr> </thead> <tbody> <tr> <th style="border-right: 1px solid black; padding: 5px;">1</th> <td style="padding: 5px;">1</td> <td style="padding: 5px;">3</td> <td style="padding: 5px;">5</td> <td style="padding: 5px;">7</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">3</th> <td style="padding: 5px;">3</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">7</td> <td style="padding: 5px;">5</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">5</th> <td style="padding: 5px;">5</td> <td style="padding: 5px;">7</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">3</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">7</th> <td style="padding: 5px;">7</td> <td style="padding: 5px;">5</td> <td style="padding: 5px;">3</td> <td style="padding: 5px;">1</td> </tr> </tbody> </table>	\odot	1	3	5	7	1	1	3	5	7	3	3	1	7	5	5	5	7	1	3	7	7	5	3	1		<table style="border-collapse: collapse; width: 100%;"> <thead> <tr> <th style="border-right: 1px solid black; padding: 5px;">\odot</th> <th style="padding: 5px;">1</th> <th style="padding: 5px;">5</th> <th style="padding: 5px;">7</th> <th style="padding: 5px;">11</th> </tr> </thead> <tbody> <tr> <th style="border-right: 1px solid black; padding: 5px;">1</th> <td style="padding: 5px;">1</td> <td style="padding: 5px;">5</td> <td style="padding: 5px;">7</td> <td style="padding: 5px;">11</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">5</th> <td style="padding: 5px;">5</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">11</td> <td style="padding: 5px;">7</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">7</th> <td style="padding: 5px;">7</td> <td style="padding: 5px;">11</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">5</td> </tr> <tr> <th style="border-right: 1px solid black; padding: 5px;">11</th> <td style="padding: 5px;">11</td> <td style="padding: 5px;">7</td> <td style="padding: 5px;">5</td> <td style="padding: 5px;">1</td> </tr> </tbody> </table>	\odot	1	5	7	11	1	1	5	7	11	5	5	1	11	7	7	7	11	1	5	11	11	7	5	1	
\odot	1	3	5	7																																																		
1	1	3	5	7																																																		
3	3	1	7	5																																																		
5	5	7	1	3																																																		
7	7	5	3	1																																																		
\odot	1	5	7	11																																																		
1	1	5	7	11																																																		
5	5	1	11	7																																																		
7	7	11	1	5																																																		
11	11	7	5	1																																																		

■