





מבוא לתורת המספרים (104157)

אביב 2024

רשימות תרגולים

אלן סורני

הרשימות עודכנו לאחרונה בתאריך ה-16 ביולי 2024



# תוכן העניינים

2	1	תרגול 3 - שימושים בפריקות יחידה
2	1.1	תזכורת . . . . .
2	1.2	תרגילים . . . . .
6	2	תרגול 4 - עוד פריקות יחידה, וחשבון מודולרי
9	3	תרגול 5 - עוד חשבון מודולרי
11	4	תרגול 6 - הדדיות ריבועית
15	5	תרגול 7 - הדדיות
18	6	תרגול 8 - עוד הדדיות

## סימונים

-  $\mathbb{N} = \{0, 1, 2, \dots\}$  אוסף המספרים הטבעיים.

-  $\mathbb{N}_+ = \{1, 2, 3, \dots\}$  אוסף המספרים הטבעיים החיוביים (כלומר, לא כולל אפס).

-  $[n] = \{1, \dots, n\}$

-  $\lfloor x \rfloor$  המספר הכי גדול שקטן או שווה ל- $x \in \mathbb{R}$ .

-  $\lceil x \rceil$  המספר הכי קטן שגדול או שווה ל- $x$ .

-

$$\gcd(a_1, \dots, a_n)$$

$$\text{lcm}(a_1, \dots, a_n)$$

בהתאמה, המחלק המשותף הגדול ביותר של המספרים  $a_1, \dots, a_n$ , והכפולה המשותפת המינימלית שלהם.

## פרק 1

# תרגול 3 - שימושים בפריקות יחידה

### 1.1 תזכורת

הגדרה 1.1.1. יהי  $n \in \mathbb{N}_+$  נגדיר

1.  $\nu(n) := \sum_{d|n} 1$  זה מספר המחלקים של  $n$ .

2.  $\sigma(n) := \sum_{d|n} d$  זה סכום המחלקים של  $n$ .

3.

$$\varphi(n) := \sum_{\substack{\gcd(d,n)=1 \\ 1 < d < n}} 1$$

זה מספר המספרים הטבעיים שקטנים מ- $n$  וזרים לו. זאת נקראת פונקציית אוילר (Euler totient function).

4.  $\pi(n)$  מספר האיברים הראשוניים הקטנים או שווים ל- $n$ . זאת נקראת פונקציית המספרים הראשוניים (prime-counting function).

5.

$$\mu(n) = \begin{cases} (-1)^\ell & \forall p \text{ prime} : p^2 \nmid n \\ 0 & \text{otherwise} \end{cases}$$

כאשר  $\ell$  מספר הראשוניים שמחלקים את  $n$ . זאת נקראת פונקציית מביוס (Möbius function).

### 1.2 תרגילים

תרגיל 1.1 (פרק 2, תרגיל 7). הסיקו מתרגיל 6 כי

$$\text{ord}_p(n!) \leq \frac{n}{p-1}$$

וכי

$$\sqrt[n]{n!} \leq \prod_{p|n!} p^{1/(p-1)}$$

פתרון. לפי תרגיל 6 מהתרגול הקודם,

$$\text{ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

נקבל כי

$$\begin{aligned} \text{ord}_p(n!) &\leq \sum_{k=1}^{\infty} \frac{n}{p^k} \\ &= n \sum_{k=1}^{\infty} \left(\frac{1}{p}\right)^k \end{aligned}$$

וכיוון ש- $p \in \mathbb{N}_+$  ראשוני מתקיים  $\left| \frac{1}{p} \right| < 1$ . מסכום סדרה הנדסית נקבל כי

$$\begin{aligned} \sum_{k=1}^{\infty} \left( \frac{1}{p} \right)^k &= \frac{1 - \left( 1 - \frac{1}{p} \right)}{1 - \frac{1}{p}} - 1 \\ &= \frac{\frac{1}{p}}{1 - \frac{1}{p}} \\ &= \frac{1}{p-1} \end{aligned}$$

ולכן

$$\text{ord}_p(n!) \leq \frac{n}{p-1}$$

אז מתקיים גם

$$\begin{aligned} n! &= \prod_{\substack{p|n \\ p \text{ prime}}} p^{\text{ord}_p(n!)} \\ &\leq \prod_{\substack{p|n \\ p \text{ prime}}} p^{\frac{n}{p-1}} \\ &\leq \prod_{p|n} p^{\frac{n}{p-1}} \\ &= \left( \prod_{p|n} p^{\frac{1}{p-1}} \right)^n \end{aligned}$$

ולכן

$$\sqrt[n]{n!} \leq \prod_{p|n} p^{\frac{1}{p-1}}$$

כנדרש.

**תרגיל 1.2 (פרק 2, תרגיל 8).** השתמשו בתוצאת התרגיל הקודם כדי להראות שיש אינסוף ראשוניים. רמז: הראו קודם שמתקיים  $(n!)^2 \geq n^n$  לכל  $n \in \mathbb{N}_+$ .

**פתרון.** ראשית, נראה כי  $(n!)^2 \geq n^n$  לכל  $n \in \mathbb{N}_+$  מתקיים

$$\begin{aligned} n! &= \prod_{k=0}^{n-1} (k+1) \\ n! &= \prod_{k=0}^{n-1} (n-k) \end{aligned}$$

ולכן

$$(n!)^2 = \prod_{k=0}^{n-1} (k+1)(n-k)$$

נראה כי הגורמים הנסכמים גדולים או שווים ל- $n$ . כאשר  $k=0$  מתקיים  $(k+1)(n-k) = n$ . כאשר  $0 < k \leq \frac{n}{2}$  מתקיים  $n-k \geq \frac{n}{2}$  ואז

$$(k+1)(n-k) \geq \frac{(k+1)n}{2} \geq \frac{2n}{2} = n$$

כאשר  $n-1 < k < \frac{n}{2}$  נקבל כי  $n-k \geq 2$  ולכן

$$(k+1)(n-k) > 2 \cdot \frac{n}{2} = n$$

כאשר  $k = n - 1$  נקבל

$$(k+1)(n-k) = (n-1+1) \cdot (n-n+1) = n \cdot 1 = n$$

לכן  $(n!)^2 \geq \prod_{k=0}^{n-1} n = n^n$  כנדרש.  
כעת, מהוכחת הסעיף הקודם ניתן לראות כי

$$\sqrt[n]{n!} \leq \prod_{\substack{p|n! \\ p \text{ prime}}} p^{\frac{1}{p-1}}$$

ואם נראה שאגף שמאל לאינסוף נקבל שגם אגף ימין שואף לאינסוף, ובפרט שיש אינסוף ראשוניים.  
אכן, מכך שמתקיים  $(n!)^2 \geq n^n$  נובע כי  $\sqrt[n]{n!} \geq \sqrt{n}$  ולכן  $\lim_{n \rightarrow \infty} \sqrt[n]{n!} = \infty$ .

תרגיל 1.3 (פרק 2, תרגיל 15). הראו כי

(א) לכל  $n \in \mathbb{N}_+$  מתקיים

$$\sum_{d|n} \mu(n/d) \nu(d) = 1$$

(ב) לכל  $n \in \mathbb{N}_+$  מתקיים

$$\sum_{d|n} \mu(n/d) \sigma(d) = n$$

פתרון. ראשית נזכיר כי

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

לכל  $f, g: \mathbb{N}_+ \rightarrow \mathbb{C}$ , וכי ראינו שלכל  $f$  כנ"ל מתקיים  $f = (f * 1) * \mu$ .

(א) מתקיים

$$\sum_{d|n} \mu(n/d) \nu(d) = (\nu * \mu)(n)$$

ונשים לב כי

$$\nu(n) = \sum_{d|n} 1 = (1 * 1)(n)$$

אז

$$(\nu * \mu)(n) = (1 * 1 * \mu)(n) = 1(n) = 1$$

כנדרש.

(ב) מתקיים

$$\sum_{d|n} \mu(n/d) \sigma(d) = (\sigma * \mu)(n)$$

ונשים לב כי

$$\sigma(n) = \sum_{d|n} d = (\text{Id}_{\mathbb{N}_+} * 1)(n)$$

אז

$$(\sigma * \mu)(n) = (\text{Id}_{\mathbb{N}_+} * 1 * \mu)(n) = \text{Id}_{\mathbb{N}_+}(n) = n$$

כנדרש.

תרגיל 1.4 (פרק 2, תרגיל 16). הראו כי  $\nu(n)$  איזווגי אם ורק אם  $n$  ריבוע.

פתרון. נכתוב  $n = \prod_{i \in [k]} p_i^{r_i}$ . ראינו כי אז

$$\nu(n) = \prod_{i \in [k]} (r_i + 1)$$

מספר זה איזווגי אם ורק אם כל ה- $r_i$  זוגיים, מה שמתקיים אם ורק אם  $n$  ריבוע.



תרגיל 1.5 (פרק 2, תרגיל 16). הראו כי  $\sigma(n)$  אי זוגי אם ורק אם  $n$  ריבוע או ריבוע כפול 2.

פתרון.

תרגיל 1.6 (פרק 2, תרגיל 18). הראו כי

$$\forall m, n \in \mathbb{N}_+ : \varphi(n) \varphi(m) = \varphi(\gcd(n, m)) \varphi(\text{lcm}(n, m))$$

פתרון. נזכיר כי עבור  $x = p_1^{a_1} \cdot \dots \cdot p_\ell^{a_\ell}$  מתקיים באופן כללי

$$\varphi(x) = x \prod_{k \in [\ell]} \left(1 - \frac{1}{p_k}\right)$$

יהיו

$$n = \left( \prod_{i \in [k]} p_i^{\alpha_i} \right) \left( \prod_{i \in [\ell]} q_i^{r_i} \right)$$

$$m = \left( \prod_{i \in [k]} p_i^{\beta_i} \right) \left( \prod_{i \in [\tilde{\ell}]} \tilde{q}_i^{s_i} \right)$$

הפירוקים של  $n, m$  לראשוניים, כאשר  $p_1, \dots, p_k$  הראשוניים שמחלקים גם את  $n$  וגם את  $m$  אז

$$\varphi(n) = n \left( \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right) \right) \left( \prod_{i \in [\ell]} \left(1 - \frac{1}{q_i}\right) \right)$$

$$\varphi(m) = m \left( \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right) \right) \left( \prod_{i \in [\tilde{\ell}]} \left(1 - \frac{1}{\tilde{q}_i}\right) \right)$$

$$\varphi(\gcd(n, m)) = \gcd(n, m) \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(\text{lcm}(n, m)) = \text{lcm}(n, m) \left( \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right) \right) \left( \prod_{i \in [\ell]} \left(1 - \frac{1}{q_i}\right) \right) \left( \prod_{i \in [\tilde{\ell}]} \left(1 - \frac{1}{\tilde{q}_i}\right) \right)$$

וכיוון ש- $\gcd(n, m) \text{lcm}(n, m) = nm$  נקבל כי

$$\varphi(n) \varphi(m) = \varphi(\gcd(n, m)) \varphi(\text{lcm}(n, m))$$

כנדרש.

## פרק 2

# תרגול 4 - עוד פריקות יחידה, וחשבון מודולרי

תרגיל 2.1 (פרק 2, תרגיל 19). הראו כי

$$\forall m, n \in \mathbb{N}_+ : \varphi(mn) \varphi(\gcd(m, n)) = \gcd(m, n) \varphi(m) \varphi(n)$$

פתרון. כיוון שראשוני מחלק את  $mn$  אם ורק אם הוא מחלק את  $\text{lcm}(m, n)$ , נקבל כי

$$\begin{aligned} \frac{\varphi(mn)}{mn} &= \prod_{\substack{p|mn \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) \\ &= \prod_{\substack{p|\text{lcm}(m, n) \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) \\ &= \frac{\varphi(\text{lcm}(m, n))}{\text{lcm}(m, n)}. \end{aligned}$$

נקבל כי

$$\begin{aligned} \varphi(mn) &= \frac{mn}{\text{lcm}(m, n)} \cdot \varphi(\text{lcm}(m, n)) \\ &= \gcd(m, n) \varphi(\text{lcm}(m, n)). \end{aligned}$$

לכן

$$\begin{aligned} \varphi(mn) \varphi(\gcd(m, n)) &= \gcd(m, n) \varphi(\text{lcm}(m, n)) \varphi(\gcd(m, n)) \\ &= \gcd(m, n) \varphi(m) \varphi(n) \end{aligned}$$

כאשר בשוויון השני השתמשנו בתרגיל הקודם.

תרגיל 2.2 (פרק 2, תרגיל 20). הראו כי

$$\prod_{d|n} d = n^{\nu(n)/2}$$

היעזרו בעובדה הבאה:  $\nu(n)$  אי־זוגי אם ורק אם  $n$  ריבוע.

פתרון. יהי  $n = \prod_{i \in [k]} p_i^{r_i}$  פירוק של  $n$  לראשוניים. נניח ראשית כי  $n = m^2$  עבור  $m \in \mathbb{N}_+$ . מתקיים

$$n^{\nu(n)/2} = (m^2)^{\nu(n)/2} = m^{\nu(n)}$$

אז

$$\text{ord}_{p_i} \left( n^{\nu(n)/2} \right) = \nu(n) \cdot \text{ord}_{p_i}(m)$$

ולכן די להראות כי

$$\text{ord}_{p_i} \left( \prod_{d|n} d \right) = \nu(n) \cdot \text{ord}_{p_i}(m)$$

כיוון ש- $m^2 = n$ , מתקיים  $\text{ord}_{p_i}(n) = 2 \text{ord}_{p_i}(m)$ , לכן  $\text{ord}_{p_i}(m) = \frac{\text{ord}_{p_i}(n)}{2}$ . לכן די להוכיח כי

$$\text{ord}_{p_i} \left( \prod_{d|n} d \right) = \frac{\nu(n) \cdot \text{ord}_{p_i}(n)}{2}$$

אם  $n$  אינו ריבוע,  $\nu(n)$  זוגי, ואז  $\nu(n)/2$  שלם. נקבל כי במקרה זה

$$\text{ord}_{p_i} \left( n^{\nu(n)/2} \right) = \frac{\nu(n) \cdot \text{ord}_{p_i}(n)}{2}$$

ולכן גם במקרה זה די להוכיח כי

$$\text{ord}_{p_i} \left( \prod_{d|n} d \right) = \frac{\nu(n) \cdot \text{ord}_{p_i}(n)}{2}$$

נקבע  $i \in [k]$  מתקיים

$$\text{ord}_{p_i} \left( \prod_{d|n} d \right) = \sum_{d|n} \text{ord}_{p_i}(d)$$

לכל  $r \in \{0, \dots, r_i\}$  נסמן

$$A_r = \left\{ d \mid \begin{array}{l} d|n \\ \text{ord}_{p_i}(d)=r \end{array} \right\}$$

ואז

$$\{d \mid d|n\} = \bigcup_{r=0}^{r_i} A_r$$

כל הקבוצות  $A_r$  מאותו גודל, כי עבור בחירת החזקה עבור  $p_i$  יש אותו מספר דרכים לבחור את שאר החזקות. מתקיים גם  $|\bigcup_{r=0}^{r_i} A_r| = \nu(n)$  ולכן

$$|A_r| = \frac{\nu(n)}{r_i + 1}$$

לכל  $r \in \{0, \dots, r_i\}$  נקבל

$$\begin{aligned} \sum_{d|n} \text{ord}_{p_i}(d) &= \sum_{r \in \{0, \dots, r_i\}} \sum_{d \in A_r} r \\ &= \sum_{r \in \{0, \dots, r_i\}} |A_r| r \\ &= \frac{\nu(n)}{r_i + 1} \cdot \sum_{r \in \{0, \dots, r_i\}} r \\ &= \frac{\nu(n)}{r_i + 1} \cdot \frac{r_i(r_i + 1)}{2} \\ &= \frac{\nu(n) r_i}{2} \\ &= \frac{\nu(n) \text{ord}_{p_i}(n)}{2} \end{aligned}$$

כנדרש.

**תרגיל 2.3 (פרק 3, תרגיל 1).** הראו שיש אינסוף ראשוניים  $p$  עבורם  $p \equiv 5 \pmod{6}$ .

**פתרון.** נניח בדרך השלילה שיש מספר סופי של ראשוניים  $p_1, \dots, p_\ell$  עבורם  $p_i \equiv 5 \pmod{6}$ . אם  $\ell$  אי-זוגי, נגדיר  $m = \prod_{i \in [\ell]} p_i + 6$  ואז

$$m \equiv (-1)^\ell \equiv -1 \pmod{6}$$

וזה מספר שזר לכל  $p_i$ . אבל,  $ab \equiv -1 \pmod{6}$  גורר שלפחות אחד מבין  $a, b$  שווה  $-1 \pmod{6}$ . מפריקות יחידה, נקבל כי  $m$  חייב להתחלק בראשוני ששווה  $-1 \pmod{6}$ , בסתירה לכך שהוא לא מתחלק באף  $p_i$ . אם  $\ell$  זוגי, נגדיר במקום זאת  $m = 5 \prod_{i \in [\ell]} p_i + 6$  ונחזור למקרה הקודם.

**תרגיל 2.4 (פרק 3, תרגיל 6).** יהי  $n > 0$ . קבוצת מספרים  $\{a_1, \dots, a_{\varphi(n)}\}$  נקראת מערכת שאריות מצומצמת מודולו  $n$  אם  $\gcd(a_i, n) = 1$  לכל  $i \in [\varphi(n)]$  וגם  $a_i \not\equiv a_j \pmod{n}$  כאשר  $i \neq j$ . תהי  $R := \{a_1, \dots, a_{\varphi(n)}\}$  מערכת שאריות מצומצמת מודולו  $n$  והי  $a \in \mathbb{Z}$  עבורו  $\gcd(a, n) = 1$ . הראו כי  $aR := \{aa_1, \dots, aa_{\varphi(n)}\}$  מערכת שאריות מצומצמת מודולו  $n$ .

**פתרון.** ראשית, נשים לב כי לכל  $i \in [\varphi(n)]$  מתקיים  $\gcd(aa_i, n) = 1$  כי  $a, a_i$  שניהם זרים ל- $n$ . נסמן ב- $G := (\mathbb{Z}/n\mathbb{Z})^\times$  את קבוצת השאריות מודולו  $n$  שזרות ל- $n$ , ונשים לב לניזכר שקבוצה זאת היא חבורה ביחס לכפל. אכן, עבור  $x \in G$  כיוון שמתקיים  $\gcd(x, n) = 1$  קיימים  $\alpha, \beta \in \mathbb{Z}$  עבורם  $\alpha x + \beta n = 1$  ואז  $\alpha x \equiv 1 \pmod{n}$ , כלומר  $\alpha \equiv x^{-1} \pmod{n}$ . בפרט, קיים איבר הופכי ל- $a$  מודולו  $n$ , ואז

$$\begin{aligned} \bar{a}^{-1} \overline{aa_1}, \dots, \bar{a}^{-1} \overline{aa_{\varphi(n)}} &= \bar{a}^{-1} \bar{a} \bar{a}_1, \dots, \bar{a}^{-1} \bar{a} \bar{a}_{\varphi(n)} \\ &= \bar{a}_1, \dots, \bar{a}_{\varphi(n)}. \end{aligned}$$

לכן ההעתקה

$$\begin{aligned} G &\rightarrow G \\ x &\mapsto \bar{a}x \end{aligned}$$

הינה הפיכה, ולכן פרמוטציה. לכן האיברים  $\bar{a}\bar{a}_1, \dots, \bar{a}\bar{a}_{\varphi(n)}$  כולם שונים, כנדרש.

### פרק 3

## תרגול 5 - עוד חשבון מודולרי

**תרגיל 3.1 (פרק 3, תרגיל 7).** היעזרו בתרגיל הקודם כדי להוכיח את משפט אוילר,  $a^{\varphi(n)} \equiv 1 \pmod{n}$  כאשר  $(a, n) = 1$ .

**פתרון.** יהיו  $a \in \mathbb{Z}, n \in \mathbb{N}_+$  עבורם  $\gcd(a, n) = 1$ . תהי  $\bar{a}$  השארית של  $a$  מודולו  $n$ . ראינו כי  $(\mathbb{Z}/n\mathbb{Z})^\times$  חבורה כפלית מסדר  $\varphi(n)$ , והחזקה של איבר בסדר של החבורה תמיד שווה ליחידה, לכן  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , כנדרש.

**תרגיל 3.2.** עבור משולש  $T$  נסמן את אורכי הצלעות בתור  $\ell(T)$ . נגיד כי  $T$  כמעט שווה צלעות אם  $d(T) = \{a, a, a \pm 1\}$  עבור  $n \in \mathbb{N}$  כלשהו.

הראו כי אם  $T$  מקיים  $d(T) = \{a, a, a \pm 1\}$  עבור  $a \in \mathbb{N}$ , וגם את זה שהשטח של  $T$  שלם, אז  $a$  אי-זוגי.

**פתרון.** נסמן  $b = a \pm 1$  את אורך הצלע השלישית, ונמקם את הקודקוד שמול הצלע הזאת על הראשית, ואת האנך לצלע על ציר ה- $x$ .

אז אורך האנך הוא  $h = \cos(\alpha) \cdot a$  כאשר  $\alpha$  הזווית מעל ציר ה- $x$  מקיימת  $\alpha = \arcsin\left(\frac{b}{2a}\right)$ . נקבל כי

$$\begin{aligned} h &= \cos\left(\arcsin\left(\frac{b}{2a}\right)\right) \cdot a \\ &= \sqrt{1 - \sin^2\left(\arcsin\left(\frac{b}{2a}\right)\right)} \cdot a \\ &= \sqrt{a^2 - \left(\frac{b}{2}\right)^2} \end{aligned}$$

השטח של  $T$  שווה

$$A = \frac{h \cdot b}{2} = \sqrt{\frac{a^2 b^2}{4} - \left(\frac{b^2}{4}\right)^2}$$

ולכן

$$A^2 = \frac{a^2 b^2}{4} - \left(\frac{b^2}{4}\right)^2$$

נכפול ב-16 ונקבל

$$16A^2 = 4a^2 b^2 - b^4$$

מוד 4 נקבל

$$0 \equiv -b^4 \pmod{4}$$

ולכן

$$b \equiv 0 \pmod{4}$$

כלומר,  $b = a \pm 1$  זוגי.

**תרגיל 3.3 (פרק 3, תרגיל 9).** הראו כי  $(p-1)! \equiv -1 \pmod{p}$  לכל  $p \in \mathbb{N}_+$  ראשוני.

**פתרון.** אם  $p = 2$ , הטענה ברורה. לכן נניח  $p \neq 2$ .

הביטוי  $(p-1)!$  הוא מכפלת כל האיברים השונים מאפס מודולו  $p$ , כלומר איברי  $\mathbb{Z}/p\mathbb{Z}$ .

כל איבר במכפלה יצתמצם עם ההופכי שלו, אלא אם הוא ההופכי של עצמו. האיברים  $a \in \mathbb{Z}/p\mathbb{Z}$  עבורם  $a = a^{-1}$  הם אלו עבורם  $a^2 = 1$ . אלו שורשי הפולינום  $x^2 - 1$ , וכיוון ש- $\mathbb{Z}/p\mathbb{Z}$  שדה, יש לפולינום הזה בדיוק שני שורשים  $\pm 1$ .

נקבל כי  $(p-1)! = -1$ .

תרגיל 3.4 (פרק 3, תרגיל 10). יהי  $n \in \mathbb{N}_+$  שאינו ראשוני. הראו כי

$$(n-1)! \equiv 0 \pmod{n}$$

חוץ מכאשר  $n = 4$ .

פתרון. נניח ראשית כי  $n = 4$  אז  $(n-1)! = 3! = 6 \equiv 2 \pmod{4}$ . נניח כעת כי  $n \neq 4$ . ניתן לכתוב  $n = ab$  עבור  $a, b \in \{2, \dots, n-1\}$ . אם  $a \neq b$  נקבל כי  $a, b$  שניהם מופיעים כגורמים במכפלה  $(n-1)!$ , ולכן  $(n-1)! \equiv 0 \pmod{n}$ . אחרת,  $n = p^2$  עבור  $p$  ראשוני שונה מ-2. נקבל כי  $(n-1)! \equiv 0 \pmod{n}$  ולכן  $n = p^2 \mid p(2p) \mid (n-1)!$ , כנדרש.

תרגיל 3.5 (פרק 3, תרגיל 11). תהי  $a_1, \dots, a_{\varphi(n)}$  מערכת שאריות מצומצמת מודלו  $n$  ויהי  $N$  מספר הפתרונות למשוואה  $x^2 \equiv 1 \pmod{n}$ . הראו כי

$$a_1 \cdot \dots \cdot a_{\varphi(n)} \equiv (-1)^{N/2} \pmod{n}$$

פתרון. ראשית, נשים לב כי  $N$  אכן זוגי כי אם  $a^2 \equiv 1 \pmod{n}$  גם  $(-a)^2 \equiv 1 \pmod{n}$ , ואם  $a \equiv -a \pmod{n}$  אז  $2a \equiv 0 \pmod{n}$  כלומר  $a \equiv 0 \pmod{n}$  לא הפיך ב- $\mathbb{Z}/n\mathbb{Z}$ , בסתירה. כעת, במכפלה

$$a_1 \cdot \dots \cdot a_{\varphi(n)}$$

מופיעים איברים וההופכיים שלהם, כאשר ב- $N$  מהאיברים המספר שווה להופכי של עצמו. נניח בלי הגבלת הכלליות שאיברים אלו הם  $a_1, \dots, a_N$  ונקבל כי

$$a_1 \cdot \dots \cdot a_{\varphi(n)} \equiv a_1 \cdot \dots \cdot a_N \pmod{n}$$

כאשר  $a_i^2 = a_i$  לכל  $i \in [N]$ . אם  $x^2 = 1$  גם  $(-x)^2 = 1$ , ולכן בביטוי  $a_1 \cdot \dots \cdot a_N$  מופיעות  $N/2$  כפולות של איבר והנגדי שלו. עבור  $x$  כזה מתקיים  $x(-x) = -x^2 = -1$  לכן

$$a_1 \cdot \dots \cdot a_N \equiv (-1)^{N/2} \pmod{n}$$

כנדרש.

תרגיל 3.6 (פרק 3, תרגיל 15). יהי  $p \in \mathbb{N}_+$  ראשוני. הראו כי המונה של  $\sum_{k=1}^{p-1} \frac{1}{k}$  מתחלק ב- $p$ .

פתרון. ניקח מכנה משותף  $(p-1)!$ . מספר זה זר ל- $p$  כי  $(p-1)! \equiv -1 \pmod{p}$  ממפשט ווילסון. לכן, המונה בשבר זה מתחלק ב- $p$  אם ורק אם המונה בשבר המצומצם מתחלק ב- $p$ . המונה יהיה  $\sum_{k=1}^{p-1} \frac{(p-1)!}{k}$ .

תרגיל 3.7 (פרק 3, תרגיל 17). יהי  $f(x) \in \mathbb{Z}[x]$  ויהי

$$n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$$

הראו כי למשוואה  $f(x) \equiv 0 \pmod{n}$  יש פתרון אם ורק אם למשוואה  $f(x) \equiv 0 \pmod{p_i^{a_i}}$  יש פתרון לכל  $i \in [k]$ .

פתרון. נניח כי יש ל- $f(x) \equiv 0 \pmod{n}$  פתרון  $f(s) \equiv 0 \pmod{n}$ . ניקח את המשוואה מוד  $p_i^{a_i}$  לכל  $i \in [k]$  ונקבל  $f(s) \equiv 0 \pmod{p_i^{a_i}}$ .

נניח כעת כי ל- $f(x) \equiv 0 \pmod{p_i^{a_i}}$  יש פתרון לכל  $i \in [k]$ . ממשפט השאריות הסיני, כלומר שקיימים  $s_i \in \mathbb{Z}$  עבורם  $f(s_i) \equiv 0 \pmod{p_i^{a_i}}$ . ממשפט השאריות הסיני, כיוון ש- $p_i^{a_i}, p_j^{a_j}$  זרים עבור  $i \neq j$ , קיים  $s \in \mathbb{Z}$  עבורו  $s \equiv s_i \pmod{p_i^{a_i}}$  לכל  $i \in [k]$  או

$$f(s) \equiv f(s_i) \pmod{p_i^{a_i}} \equiv 0 \pmod{p_i^{a_i}}$$

לכל  $i \in [k]$ .

תרגיל 3.8. יהי  $f(x) \in \mathbb{Z}[x]$  ויהי

$$n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$$

יהי  $N$  מספר הפתרונות של  $f(x) \equiv 0 \pmod{n}$  ויהיו  $N_i$  מספר הפתרונות של  $f(x) \equiv 0 \pmod{p_i^{a_i}}$ . הראו כי

$$N = \prod_{i \in [k]} N_i$$

פתרון. בתרגיל הקודם בנינו התאמה חד-חד ערכית ועל בין פתרונות  $f(s) \equiv 0 \pmod{n}$  לבין  $(s_1, \dots, s_k)$  כך ש- $f(s_i) \equiv 0 \pmod{p_i^{a_i}}$ . מספר הדרכים לבחור פתרונות  $(s_1, \dots, s_k)$  כאלה הוא  $N_1 \cdot \dots \cdot N_k$ , ולכן  $N = N_1 \cdot \dots \cdot N_k$ .

## פרק 4

# תרגול 6 - הדדיות ריבועית

### תזכורת

נזכיר טענה מההרצאה.

**טענה 4.0.1.** יהי  $m \in \mathbb{N}_+$  עם פירוק לראשוניים

$$m = 2^e \cdot \prod_{i \in [\ell]} p_i^{e_i}$$

איבר  $a \in \mathbb{Z}/m\mathbb{Z}$ , הוא ריבוע אם ורק אם מתקיימים התנאים הבאים

1.  $a \equiv 1 \pmod{4}$  אם  $e \geq 3$ , או  $a \equiv 1 \pmod{4}$  אם  $e = 2$ .

2. לכל  $i \in [\ell]$  מתקיים  $a^{\frac{p_i-1}{2}} \equiv 1 \pmod{p_i}$ .

נזכיר גם את ההגדרה הבאה, ומספר תכונות לגביה.

**הגדרה 4.0.2** (סימן לוג'נדר). עבור  $p \in \mathbb{Z}$  ראשוני, ועבור  $a \in \mathbb{N}_+$ , סימן לוג'נדר  $\left(\frac{a}{p}\right)$  שווה:

- אם  $0 \mid a$  ו- $p$ .

- אם  $1 \nmid a$  ו- $p \nmid a$  וגם  $a$  ריבוע מוד  $p$ .

- אם  $1 \nmid a$  ו- $p \nmid a$  וגם  $a$  אינו ריבוע מוד  $p$ .

**טענה 4.0.3.** יהיו  $a, b, p, q \in \mathbb{Z}$  עבור  $p, q$  ראשוניים חיוביים. מתקיים:

$$1. a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

$$2. \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

$$3. \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ אם } a \equiv b \pmod{p}.$$

**משפט 4.0.4.** יהיו  $p, q$  ראשוניים אי-זוגיים חיוביים שונים. מתקיים

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$
$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

**מסקנה 4.0.5.** אם  $q \equiv 1 \pmod{4}$  או  $p \equiv 1 \pmod{4}$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

אחרת,

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

## תרגילים

תרגיל 4.1 (פרק 5, תרגיל 1). חשבו את הביטויים הבאים בעזרת הטענה והמשפט.

1.  $\left(\frac{5}{7}\right)$

2.  $\left(\frac{3}{11}\right)$

3.  $\left(\frac{6}{13}\right)$

פתרון. 1.

$$\begin{aligned}\left(\frac{5}{7}\right) &= \left(\frac{7}{5}\right) \\ &= \left(\frac{2}{5}\right) \\ &= (-1)^{\frac{5^2-1}{8}} \\ &= (-1)^3 \\ &= -1\end{aligned}$$

2.

$$\begin{aligned}\left(\frac{3}{11}\right) &= -\left(\frac{11}{3}\right) \\ &= -\left(\frac{2}{3}\right) \\ &= -(-1)^{\frac{3^2-1}{8}} \\ &= 1\end{aligned}$$

3.

$$\begin{aligned}\left(\frac{6}{13}\right) &= \left(\frac{2}{13}\right) \left(\frac{3}{13}\right) \\ &= (-1)^{\frac{13^2-1}{8}} \left(\frac{13}{3}\right) \\ &= \left(\frac{13}{3}\right) \\ &= \left(\frac{1}{3}\right) \\ &= 1\end{aligned}$$

תרגיל 4.2 (פרק 5, תרגיל 2). הראו שמספר הפתרונות של המשוואה  $x^2 \equiv a \pmod{p}$  הוא  $1 + \left(\frac{a}{p}\right)$ .

פתרון. נפריד למקרים.

1. אם  $a \mid p$ , הפתרון היחיד הוא  $x = 0$ , וגם  $\left(\frac{a}{p}\right) = 0$ , לכן מספר הפתרונות הוא  $1 + \left(\frac{a}{p}\right) = 1$ .

2. אם  $a \nmid p$  ו- $a$  ריבוע מוד  $p$ , יש שני פתרונות למשוואה, וגם  $\left(\frac{a}{p}\right) = 1$ .

3. אם  $a \nmid p$  ו- $a$  אינו ריבוע מוד  $p$ , אין פתרונות למשוואה, וגם  $\left(\frac{a}{p}\right) = -1$ .

תרגיל 4.3 (פרק 5, תרגיל 3). יהיו  $a, b, c \in \mathbb{Z}$  כך ש- $a \nmid p$ . הוכיחו כי מספר הפתרונות של המשוואה

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

הוא  $1 + \left(\frac{b^2-4ac}{p}\right)$ .



פתרון. לפי נוסחאת השורשים, פתרונות המשוואה הם איברי

$$\left\{ -b \pm \sqrt{b^2 - 4ac} \mid 2a \right\}$$

גודל הקבוצה הזאת הוא מספר השורשים של  $b^2 - 4ac$ , וזה שווה לפי התרגיל הקודם  $1 + \left(\frac{b^2 - 4ac}{p}\right)$ .

תרגיל 4.4 (פרק 5, תרגיל 4). הוכיחו כי

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

הוכחה. ההעתקה

$$\varphi: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^2$$

משרה איזומורפיזם של חבורות

$$(\mathbb{Z}/p\mathbb{Z}) / \{\pm 1\} \cong \{a^2 \mid a \in (\mathbb{Z}/p\mathbb{Z})\}$$

לכן, אם נסמן

$$S_p := \{a^2 \mid a \in (\mathbb{Z}/p\mathbb{Z})\}$$

נקבל כי  $|S_p| = \frac{p-1}{2}$  או

$$\begin{aligned} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) &= \sum_{a \in S_p} \left(\frac{a}{p}\right) + \sum_{a \in [p-1] \setminus S_p} \left(\frac{a}{p}\right) \\ &= \sum_{a \in S_p} 1 + \sum_{a \in [p-1] \setminus S_p} (-1) \\ &= \frac{p-1}{2} - \frac{p-1}{2} \\ &= 0 \end{aligned}$$

■

כנדרש.

תרגיל 4.5 (פרק 5, תרגיל 5). עבור  $a, b \in \mathbb{Z}$  עבורם  $a \not\equiv 0 \pmod{p}$ , הראו כי

$$\sum_{k=0}^{p-1} \left(\frac{ak+b}{p}\right) = 0$$

פתרון. עבור  $k_1, k_2 \in \{0, \dots, p-1\}$  מתקיים

$$ak_1 + b \equiv ak_2 + b \pmod{p}$$

אם ורק אם

$$ak_1 \equiv ak_2 \pmod{p}$$

וכיוון ש- $p \mid p$  נקבל שזה מתקיים אם ורק אם  $k_1 = k_2$ . לכן  $a, a+b \pmod{p}, 2a+b \pmod{p}, \dots, (p-1)a+b \pmod{p}$  הם בדיוק איברי  $\mathbb{Z}/p\mathbb{Z}$ , כאשר כל אחד מופיע פעם אחת. כיוון ש- $\left(\frac{0}{p}\right) = 0$ , נקבל מהתרגיל הקודם את הנדרש.

תרגיל 4.6 (פרק 5, תרגיל 6). הראו כי מספר הפתרונות של המשוואה

$$x^2 - y^2 \equiv a \pmod{p}$$

הוא

$$\sum_{k=0}^{p-1} \left(1 + \left(\frac{k^2 + a}{p}\right)\right)$$

פתרון. נכתוב את המשוואה בתור

$$x^2 \equiv y^2 + a \pmod{p}$$

אז עבור  $y = k$  מספר הפתרונות של המשוואה הוא מספר הפתרונות של המשוואה

$$x^2 \equiv k^2 + a \pmod{p}$$

וראינו שזה שווה  $1 + \left(\frac{k^2 + a}{p}\right)$ .

תרגיל 4.7 (פרק 5, תרגיל 7). הראו על ידי חישוב ישיר שמספר הפתרונות של המשוואה

$$x^2 - y^2 \equiv a \pmod{p}$$

הוא  $p-1$  אם  $p \nmid a$  או  $2p-1$  אם  $p \mid a$ .  
רמז: סמנו  $u = x + y, v = x - y$ .

פתרון. עם הסימונים שהוצעו, נקבל שהמשוואה היא באופן שקול

$$uv \equiv a \pmod{p}$$

אם  $p \mid a$ , מספר הפתרונות הוא מספר הזוגות  $(u, v)$  עבורם לפחות אחד מבין  $u, v$  שווה 0. זה שווה בדיוק  $2p-1$  כי כאשר כל אחד שווה אפס, השני יכול להיות כל ערך ב- $\mathbb{Z}/p\mathbb{Z}$ , אבל אז  $(0, 0)$  נספר פעמיים.  
אם  $p \nmid a$ , לכל בחירה של  $u$  הפיך נקבל כי  $v \equiv \frac{a}{u}$ . איבר יחיד הפותר את המשוואה. לכן במקרה זה יש  $p-1$  פתרונות.

תרגיל 4.8 (פרק 5, תרגיל 8). היעזרו בשני התרגילים הקודמים כדי להראות כי

$$\sum_{k=0}^{p-1} \left( \frac{k^2 + a}{p} \right) = \begin{cases} -1 & p \nmid a \\ p-1 & p \mid a \end{cases}$$

פתרון. נניח כי  $p \nmid a$ . אז משני התרגילים נקבל כי

$$p + \sum_{k=0}^{p-1} \left( \frac{k^2 + a}{p} \right) = \sum_{k=0}^{p-1} \left( 1 + \left( \frac{k^2 + a}{p} \right) \right) = p-1$$

ואז

$$\sum_{k=0}^{p-1} \left( \frac{k^2 + a}{p} \right) = -1$$

נניח כי  $p \mid a$ . משני התרגילים נקבל כי

$$p + \sum_{k=0}^{p-1} \left( \frac{k^2 + a}{p} \right) = \sum_{k=0}^{p-1} \left( 1 + \left( \frac{k^2 + a}{p} \right) \right) = 2p-1$$

ואז

$$\sum_{k=0}^{p-1} \left( \frac{k^2 + a}{p} \right) = p-1$$

תרגיל 4.9 (פרק 5, תרגיל 10). יהיו  $r_1, \dots, r_{\frac{p-1}{2}}$  הריבועים ההפיכים מוד  $p$ . הראו כי

$$\prod_{i \in [\frac{p-1}{2}]} r_i = \begin{cases} 1 & p \equiv 3 \pmod{4} \\ -1 & p \equiv 1 \pmod{4} \end{cases}$$

פתרון. נרצה לחשב את הביטוי

$$P := \prod_{k=1}^{\frac{p-1}{2}} k^2$$

נשים לב כי  $k = -(p-k)$ , לכן  $k^2 = (-1)k(p-k)$  לכל  $k \in \mathbb{Z}/p\mathbb{Z}$ . אז

$$\begin{aligned} P &= (-1)^{\frac{p-1}{2}} \cdot \prod_{k=1}^{\frac{p-1}{2}} k(p-k) \\ &= (-1)^{\frac{p-1}{2}} \cdot \prod_{k=1}^{p-1} k \\ &= (-1)^{\frac{p-1}{2}} \cdot (p-1)! \\ &= (-1)^{\frac{p+1}{2}} \end{aligned}$$

כאשר בשוויון האחרון השתמשנו במשפט ווילסון. ביטוי זה שווה 1 אם  $p \equiv 3 \pmod{4}$  או  $-1$  אם  $p \equiv 1 \pmod{4}$ .

## פרק 5

# תרגול 7 - הדדיות

תרגיל 5.1 (פרק 5, תרגיל 11). יהי  $p > 3$  ראשוני עבורו  $p \equiv 3 \pmod{4}$  וכך שגם  $q := 2p + 1$  ראשוני. הראו כי  $2^{p-1}$  אינו ראשוני.  
רמז: הראו כי  $2^{p-1} \mid q$ .

פתרון. נכתוב  $p = 4k + 3$  עבור  $k \in \mathbb{N}_+$ . אז

$$q = 2p + 1 = 8k + 7 \equiv -1 \pmod{8}.$$

לכן

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = 1$$

אז

$$2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$$

כלומר

$$2^p \equiv 1 \pmod{q}$$

נקבל כי  $2^p - 1 \mid q$ , ולכן  $2^p - 1$  אינו ראשוני.

תרגיל 5.2 (פרק 5, תרגיל 16). מיצאו בעזרת הדדיות ריבועית את הראשוניים עבורם 7 הוא ריבוע ב- $\mathbb{Z}/p\mathbb{Z}$ .

פתרון. ראשית,  $p = 2$  עונה על הדרישה כי  $7 \equiv 1 \pmod{2}$ . נניח בהמשך כי  $p$  אי-זוגי. מתקיים כי 7 ריבוע מוד  $p$  אם ורק אם  $p = 7$  או  $p \neq 7$  וגם  $\left(\frac{7}{p}\right) = 1$ . נניח כי  $p \neq 7$ . לפי הדדיות ריבועית,

$$\begin{aligned} \left(\frac{7}{p}\right) &= (-1)^{\frac{7-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{7}\right) \\ &= (-1)^{\frac{3(p-1)}{2}} \left(\frac{p}{7}\right). \end{aligned}$$

אם  $p \equiv 1 \pmod{4}$  נקבל כי  $\frac{3(p-1)}{2}$  זוגי ואז

$$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right).$$

אחרת, נקבל כי

$$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right).$$

לכן התשובה היא ראשוניים  $\{2, 7\}$  וגם  $p \notin \{2, 7\}$  עבורם

$$\left(\frac{p}{7}\right) = 1, \quad p \equiv 1 \pmod{4}$$

או

$$\left(\frac{p}{7}\right) = -1, \quad p \equiv 3 \pmod{4}.$$

נחפש את ערכי  $p$  שמקיימים זאת. מוד 7 מתקיים

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 2$$

$$4^2 = 2$$

$$5^2 = 4$$

$$6^2 = 1$$

נחפש קודם ערכי  $p$  עבורם  $p \equiv 1 \pmod{4}$ ,  $\left(\frac{p}{7}\right) = 1$ , נכתוב  $a \equiv p \pmod{7} \in \{1, 2, 4\}$ . מתקיים  $\gcd(4, 7) = 1$  ונוכל לכתוב  $1 = 2 \cdot 4 + (-1) \cdot 7$ . אז שפותר את המערכת

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

$$p \equiv a \pmod{7}$$

הוא כל ראשוני מהצורה

$$1. \quad a = 1 + 28k \text{ אם } a = 1$$

$$2. \quad a = 9 + 28k \text{ אם } a = 2$$

$$3. \quad a = 25 + 28k \text{ אם } a = 4$$

באופן דומה, עבור  $p \equiv 3 \pmod{4}$  נצטרך למצוא פתרונות ראשוניים למערכת

$$p \equiv 3 \pmod{4}$$

$$p \equiv a \pmod{7}$$

כאשר  $a \in \{3, 5, 6\}$ . אלו יהיו כל הראשוניים מהצורה

$$1. \quad a = 3 + 28k \text{ עבור } a = 3$$

$$2. \quad a = 19 + 28k \text{ עבור } a = 5$$

$$3. \quad a = 27 + 28k \text{ עבור } a = 6$$

**הגדרה 5.0.1 (סימן יקובי).** עבור  $b$  חיובי אי-זוגי עם פירוק לראשוניים  $b = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$ , נגדיר את סימן יקובי  $\left(\frac{a}{b}\right)$  בתור

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)^{a_1} \cdot \dots \cdot \left(\frac{a}{p_k}\right)^{a_k}$$

**טענה 5.0.2.** 1.  $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$  אם  $a_1 \equiv a_2 \pmod{b}$

$$2. \quad \left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \left(\frac{a_2}{b}\right)$$

$$3. \quad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \left(\frac{a}{b_2}\right)$$

**טענה 5.0.3.** 1.  $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$

$$2. \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

3. אם  $a, b$  שניהם אי-זוגיים,

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

**תרגיל 5.3 (פרק 5, תרגיל 18).** יהי  $D$  שלם חיובי חסר-ריבועים. הראו שיש  $b$  שלם חיובי זר ל- $D$  עבורו  $\left(\frac{b}{D}\right) = -1$ .

פתרון. נכתוב  $D = \prod_{i \in [k]} p_i$  עבור ראשוניים זרים בזוגות. אז

$$\frac{b}{D} = \prod_{i \in [k]} \left( \frac{b}{p_i} \right)$$

יהיו  $a_i \in \mathbb{Z}/p_i\mathbb{Z}$  שונים מאפס כך ש- $a_1$  ריבוע ב- $\mathbb{Z}/p_1\mathbb{Z}$  ו- $a_i$  אינו ריבוע ב- $\mathbb{Z}/p_i\mathbb{Z}$  לכל  $i \geq 2$ . ממשפט השאריות הסיני קיים  $b \in \mathbb{Z}$  עבורו  $b \equiv a_i \pmod{p_i}$  לכל  $i \in [k]$ . אז

$$\left( \frac{b}{p_i} \right) \equiv \left( \frac{a_i}{p_i} \right) = (-1)^{\delta_{i,1}}$$

לכן

$$\frac{b}{D} = \prod_{i \in [k]} \left( \frac{b}{p_i} \right) = -1$$

כנדרש.

**תרגיל 5.4 (פרק 5, תרגיל 19).** תהי  $(a_1, \dots, a_{\varphi(D)})$  מערכת שאריות מצומצמת מוד  $D$ . ת שאריות מצומצמת מוד  $D$ .

1. הראו כי

$$\sum_{i \in [\varphi(D)]} \left( \frac{a_i}{D} \right) = 0$$

היזכרו כי לכל  $a$  הפיך מוד  $D$ , גם  $(aa_1, \dots, aa_{\varphi(D)})$  מערכת שאריות מצומצמת מוד  $D$ .

2. הסיקו כי בדיוק חצי מאיברי  $(\mathbb{Z}/D\mathbb{Z})^\times$  מקיימים  $\left( \frac{a}{D} \right) = 1$ .

פתרון. 1. מתקיים

$$\sum_{i \in [\varphi(D)]} \left( \frac{a_i}{D} \right) \in \{1, 0, -1\}$$

ניקח  $b \in \mathbb{Z}$  עבורו  $\left( \frac{b}{D} \right) = -1$ , שקיים מהתרגיל הקודם. אז

$$\begin{aligned} \sum_{i \in [\varphi(D)]} \left( \frac{a_i}{D} \right) &= \sum_{i \in [\varphi(D)]} \left( \frac{ba_i}{D} \right) \\ &= \sum_{i \in [\varphi(D)]} \left( \frac{b}{D} \right) \left( \frac{a_i}{D} \right) \\ &= - \sum_{i \in [\varphi(D)]} \left( \frac{a_i}{D} \right) \end{aligned}$$

ולכן

$$\sum_{i \in [\varphi(D)]} \left( \frac{a_i}{D} \right) = 0$$

כנדרש.

2. כיוון שכל הגורמים  $\left( \frac{a_i}{D} \right)$  בסכום הם אחד מבין  $1, -1$ , וכיוון ש- $\varphi(D) < \varphi(D)$ , נקבל כי הסכום יכול להיות אפס אם ורק אם חצי מהגורמים בו שווים 1 וחצי מהם שווים -1. כיוון שמחלקות השקילות של  $a_1, \dots, a_{\varphi(D)}$  הן איברי  $\mathbb{Z}/D\mathbb{Z}$ , נקבל את הנדרש.

**תרגיל 5.5 (פרק 5, תרגיל 20).** יהיו  $a_1, \dots, a_{\varphi(D)/2} \in \mathbb{Z}/D\mathbb{Z}$  האיברים עבורם  $\left( \frac{a_i}{D} \right) = 1$ . יהי  $p \nmid D$  ראשוני שמקיים  $p \equiv 1 \pmod{4}$ . הראו כי  $D$  שארית ריבועית מוד  $p$  אם ורק אם קיים  $i \in [\varphi(D)]$  עבורו  $p \equiv a_i \pmod{D}$ .

פתרון.  $D$  שארית ריבועית מוד  $p$  אם ורק אם  $\left( \frac{D}{p} \right) = 1$ .

נניח כי  $p \equiv a_i \pmod{D}$  עבור איזהו  $i \in [\varphi(D)/2]$ . אז

$$\left( \frac{p}{D} \right) = \left( \frac{a_i}{D} \right) = 1$$

כיוון ש- $p \equiv 1 \pmod{4}$ , נקבל כי  $\frac{p-1}{2}$  זוגי ולכן

$$\left( \frac{D}{p} \right) = \left( \frac{p}{D} \right) = 1$$

נניח כעת כי  $p \not\equiv a_i \pmod{D}$  לאף  $i \in [\varphi(D)/2]$ . אז  $\left( \frac{p}{D} \right) = -1$  ובאותו אופן נקבל כי  $\left( \frac{D}{p} \right) = -1$ , לכן  $D$  לא שארית ריבועית מוד  $p$ .

## פרק 6

### תרגול 8 - עוד הדדיות

תרגיל 6.1 (פרק 5, תרגיל 21). השתמשו בשיטה משני התרגילים הקודמים כדי למצוא את כל הראשוניים  $p$  עבורם 21 הוא שארית ריבועית מוד  $p$ .

פתרון. ההפיכים מוד 21 הם המספרים מ-1 עד 20 שזורים ל-3, 7. אלו 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.

$$\begin{aligned}\left(\frac{1}{21}\right) &= \left(\frac{1}{3}\right)\left(\frac{1}{7}\right) \\ &= 1\end{aligned}$$

$$\begin{aligned}\left(\frac{2}{21}\right) &= (-1)^{\frac{21^2-1}{8}} \\ &= (-1)^{55} \\ &= -1\end{aligned}$$

$$\begin{aligned}\left(\frac{4}{21}\right) &= \left(\frac{2}{21}\right)^2 \\ &= 1\end{aligned}$$

$$\begin{aligned}\left(\frac{5}{21}\right) &= \left(\frac{21}{5}\right) \\ &= \left(\frac{1}{5}\right) \\ &= 1\end{aligned}$$

$$\begin{aligned}\left(\frac{8}{21}\right) &= \left(\frac{2}{21}\right)^3 \\ &= -1\end{aligned}$$

$$\begin{aligned}\left(\frac{10}{21}\right) &= \left(\frac{2}{21}\right)\left(\frac{5}{21}\right) \\ &= -1 \cdot 1 \\ &= -1\end{aligned}$$

$$\begin{aligned}\left(\frac{11}{21}\right) &= \left(\frac{21}{11}\right) \\ &= \left(\frac{10}{11}\right) \\ &= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \\ &= -(-1)^{\frac{11^2-1}{8}}\left(\frac{11}{3}\right) \\ &= -(-1)^{15}\left(\frac{2}{3}\right) \\ &= (-1)^3 \\ &= -1\end{aligned}$$

$$\begin{aligned}
\left(\frac{13}{21}\right) &= \left(\frac{21}{13}\right) \\
&= \left(\frac{8}{13}\right) \\
&= \left(\frac{2}{13}\right)^3 \\
&= (-1)^{3 \cdot \frac{13^2-1}{8}} \\
&= (-1)^{3 \cdot 21} \\
&= -1 \\
\left(\frac{16}{21}\right) &= \left(\frac{2}{21}\right)^4 \\
&= 1 \\
\left(\frac{17}{21}\right) &= \left(\frac{21}{17}\right) \\
&= \left(\frac{4}{17}\right) \\
&= \left(\frac{2}{17}\right)^2 \\
&= 1 \\
\left(\frac{19}{21}\right) &= \left(\frac{21}{19}\right) \\
&= \left(\frac{2}{19}\right) \\
&= (-1)^{\frac{19^2-1}{8}} \\
&= (-1)^{45} \\
&= -1 \\
\left(\frac{20}{21}\right) &= \left(\frac{2}{21}\right) \left(\frac{10}{21}\right) \\
&= (-1)^2 \\
&= 1
\end{aligned}$$

ולכן האיברים  $a \in \mathbb{Z}/21\mathbb{Z}$  עבורם  $\left(\frac{a}{21}\right) = 1$  הם 1, 4, 5, 16, 17, 20. נשים לב שזה מספר האיברים האלו שאנו אמורים לקבל, כי  $\frac{\varphi(21)}{2} = \frac{12}{2} = 6$ .  
 לכן שארית ריבועית מוד  $p$  אם ורק אם  $\bar{p} \pmod{21} \in \{1, 4, 5, 16, 17, 20\}$ .

**תרגיל 6.2 (פרק 5, תרגיל 23).** יהי  $p \equiv 1 \pmod{4}$  ראשוני.

1. הראו שקיימים  $s, t \in \mathbb{Z}$  עבורם  $pt = 1 + s^2$ .

2. הסיקו כי  $p$  אינו ראשוני ב- $\mathbb{Z}[i]$ .

זיכרו כי יש ב- $\mathbb{Z}[i]$  פירוק יחיד לראשוניים.

**פתרון.** 1. מכך ש- $p \equiv 1 \pmod{4}$  נקבל כי

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$$

ולכן  $(-1)$  ריבוע מוד  $p$ . לכן יש  $s \in \mathbb{Z}$  עבורו  $s^2 \equiv -1 \pmod{p}$ , כלומר  $s^2 + 1 \equiv 0 \pmod{p}$ , כלומר קיים  $t \in \mathbb{Z}$  עבורו  $pt = s^2 + 1$ .

2. נקבל כי עבור  $s, t$  שמצאנו מתקיים  $pt = (s+i)(s-i)$ . אם  $p$  היה ראשוני ב- $\mathbb{Z}[i]$  היינו מקבלים  $p \mid s+i$  או  $p \mid s-i$ . אבל אז  $p \mid 1$  או  $p \mid -1$ , מה שלא יתכן.