

# תורת המספרים

מאיה פרבר ברודסקי

סיכומי ההרצאות של פרופ' דורון פודר, סמסטר ב' תשפ"א, אוניברסיטת תל אביב.

## תוכן עניינים

2	.....	1	אריתמטיקה בסיסית של השלמים
2	.....	1.1	חלוקה עם שארית
2	.....	1.2	מחלקים ו- $\gcd$
4	.....	1.3	משוואות דיופנטיות לינאריות
5	.....	2	ראשוניים והמשפט היסודי של האריתמטיקה
6	.....	2.1	משפט המספרים הראשוניים
9	.....	3	קונגרואנציות
9	.....	3.1	חוג השלמים מודולו $n$
11	.....	4	חבורת ההפיכים ושורשים פרימיטיביים
11	.....	4.1	החבורה הכפלית $\mathbb{Z}_n^*$
12	.....	4.2	שורש פרימיטיבי וקריטריון אוילר
13	.....	5	שאריות ריבועיות
13	.....	5.1	סימן לז'נדר וחוק ההדדיות הריבועית
15	.....	5.2	סימן יעקובי
16	.....	6	הצפנה ומבחני ראשוניות
16	.....	6.1	הצפנת RSA
17	.....	6.2	מבחני ראשוניות
18	.....	7	הלמה של הנזל
19	.....	8	שברים משולבים וקירובים דיופנטיים
19	.....	8.1	שברים משולבים
20	.....	8.2	קירובים דיופנטיים
22	.....	9	סכומי ריבועים
22	.....	9.1	חוג השלמים של גאוס
22	.....	9.2	משפט פרמה-גאוס
24	.....	10	הרחבות ריבועיות
24	.....	10.1	הרחבות ריבועיות דמיוניות וממשיות
24	.....	10.2	משוואת פל

# 1 אריתמטיקה בסיסית של השלמים

## 1.1 חלוקה עם שארית

**הגדרה 1.1** ערך שלם עבור  $x \in \mathbb{R}$ , נסמן  $[x] = \min\{n \in \mathbb{Z} \mid n \leq x\}$  את הערך השלם של  $x$ .

**טענה 1.2 חלוקה עם שארית** יהיו  $a, b \in \mathbb{Z}$  עם  $a > 0$ . אזי קיימים יחידים  $q, r \in \mathbb{Z}$  כך  $b = qa + r$  ו- $0 \leq r < a$ . במקרה זה,  $r$  נקראת השארית בחלוקת  $b$  ב- $a$ .

**הוכחה:** נגדיר  $q = \lfloor \frac{b}{a} \rfloor$  וכן  $r = b - qa$ . כמובן מתקיים  $b = qa + r$ , נותר להוכיח  $0 \leq r < a$  ויחידות. מתקיים  $\lfloor \frac{b}{a} \rfloor \leq \frac{b}{a} < \lfloor \frac{b}{a} \rfloor + 1$  מאי השוויון  $\frac{b}{a} - 1 < q$  נובע  $\frac{b}{a} - 1 < q$  ולכן  $b - a < qa$  כלומר  $r = b - qa < a$ . מאי השוויון  $\frac{b}{a} \leq \lfloor \frac{b}{a} \rfloor + 1$  נובע  $q \leq \frac{b}{a}$  ולכן  $qa \leq b$  כלומר  $r = b - qa \geq 0$ . בסך הכל,  $0 \leq r < a$ . עבור יחידות, נניח  $b = q'a + r'$  עם  $0 \leq r' < a$  אז  $(q' - q)a = (b - qa) - (b - q'a) = r - r'$  כלומר  $r - r' = (q' - q)a$  של  $a$  אבל מתוך  $0 \leq r, r' < a$  מקבלים  $0 \leq r - r' < a$  ולכן בהכרח  $(q' - q)a = r - r' = 0$  כלומר  $r = r'$  וכן  $q' - q = 0$  (כי  $a > 0$ ) ולכן  $q = q'$ , וקיבלנו יחידות. ■

## 1.2 מחלקים ו-gcd

**הגדרה 1.3 מחלק** עבור  $a, b \in \mathbb{Z}$  נסמן  $a \mid b$  אם  $a$  מחלק את  $b$ , כלומר אם קיים  $c \in \mathbb{Z}$  כך  $ac = b$ .

## טענה 1.4 תכונות בסיסיות

1.  $1 \mid n$  לכל  $n \in \mathbb{Z}$  - כי  $n = 1 \cdot n$ .
2.  $n \mid 0$  לכל  $n$  - כי  $0 = 0 \cdot n$ .
3.  $0 \nmid n$  אלא אם  $n = 0$  - כי  $0 \cdot m = 0$  לכל  $m$ .
4. אם  $b \neq 0$  וגם  $a \mid b$  אז  $|a| \leq |b|$  - קיים  $c$  כך  $ac = b$ , ואז  $|a||c| = |b|$ ,  $b \neq 0$  לכן  $c \neq 0$  כלומר  $|c| \geq 1$ , ולכן  $|a| \leq |b|$ .
5. אם  $a \mid n$  וגם  $n \mid b$  אז  $n \mid xa + yb$  לכל  $x, y \in \mathbb{Z}$  - קיימים  $\alpha, \beta \in \mathbb{Z}$  כך  $\alpha n = a, \beta n = b$  ולכן  $xa + yb = x\alpha n + y\beta n = (x\alpha + y\beta)n$ .
6. אם  $a \mid b$  וגם  $b \mid a$  אז  $a = b$  או  $a = -b$  - אם  $b = 0$  הטענה ברורה, אחרת מתקיים  $a = mb, b = na$  ולכן  $b = na = n \cdot mb$  ולכן  $b(1 - nm) = 0$  ולכן  $b \neq 0$  בפרט  $|n||m| = 1$  אבל  $|n|, |m| \geq 1$  ולכן  $|n| = |m| = 1$ , אם  $n = m = 1$  אז  $a = b$  ואם  $n = m = -1$  אז  $a = -b$ .

**הגדרה 1.5 מחלק משותף**,  $\gcd(a, b)$  יהיו  $a, b \in \mathbb{Z}$  כך ש- $(a, b) \neq (0, 0)$ . מחלק משותף של  $a, b$  הוא שלם  $d \in \mathbb{Z}$  המקיים  $d \mid a, d \mid b$ . מחלק משותף מקסימלי, או  $\gcd$ , הוא  $D \in \mathbb{Z}$  שהוא מחלק משותף של  $a, b$  ומקסימלי ביחס לסדר החלוקה, כלומר אם  $d \in \mathbb{Z}$  מחלק משותף של  $a, b$  אז  $d \mid D$ . מסמנים  $D = \gcd(a, b) = (a, b)$ .

**טענה 1.6 יחידות**  $\gcd$  הוא יחיד עד כדי כפל בהפיך, כלומר  $\pm 1$ .

**הוכחה:** אם  $D_1, D_2$  שניהם  $\gcd$  אז  $D_1 \mid D_2, D_2 \mid D_1$  ולכן  $D_1 = D_2$  או  $D_1 = -D_2$ . ■

**משפט 1.7 קיום** לכל  $a, b \in \mathbb{Z}$  לא שניהם 0 יש  $\gcd$ .

**הוכחה:** נתבונן בקבוצה  $I = \{xa + yb \mid x, y \in \mathbb{Z}\}$ . נשים לב כי  $I$  סגורה לחיבור ולכפל בסקלר שלם, כלומר אם  $i_1, i_2 \in I$  אז  $i_1 + i_2 \in I$  וכן אם  $i \in I, m \in \mathbb{Z}$  אז  $mi \in I$ . אכן, אם  $i_1 = x_1a + y_1b, i_2 = x_2a + y_2b \in I$  אז  $i_1 + i_2 = (x_1 + x_2)a + (y_1 + y_2)b \in I$  מסגירות השלמים לחיבור, ואם  $i = xa + yb, m \in \mathbb{Z}$  אז  $mi = mxa + mby \in I$  מסגירות השלמים לכפל.

ב  $I$  יש מספרים חיוביים, יהי  $D \in I$  החיובי המינימלי ב  $I$ . נטען שכל  $i \in I$  הוא כפולה של  $d$ . יהי  $i \in I$  ונחלק אותו עם שארית ב  $D$ ,  $i = qD + r$ , כאשר  $0 \leq r < D$ . מתקיים  $D \in I, q \in \mathbb{Z}$  לכן מהתכונות שהראינו  $qD \in I$  ומכאן גם  $r = i - qD \in I$ . קיבלנו  $r \in I$  וכן  $0 \leq r < D$  ולכן  $r = 0$ , כי  $D$  הוא החיובי המינימלי ב  $I$ . אז  $i = qD$ , כלומר  $i$  כפולה של  $D$ .

כעת נראה  $D = \gcd(a, b)$ . הוא מחלק משותף כי  $a, b \in I$  ולכן כפי שהראינו שניהם כפולה של  $D$ . הוא מקסימלי כי אם  $d \mid a, b$  אז  $d \mid xa + yb$  לכל  $x, y \in \mathbb{Z}$  ולכן  $d$  מחלק כל איבר ב  $I$  ובפרט את  $D$ , כלומר  $d \mid D$ . ■

**מסקנה 1.8 הלמה של בזו** לכל  $a, b \in \mathbb{Z}$  לא שניהם 0 יש  $x, y \in \mathbb{Z}$  כך ש  $\gcd(a, b) = xa + yb$ .

**הוכחה:** נובע ישירות מההוכחה, בחרנו  $D = \gcd(a, b) \in I = \{xa + yb \mid x, y \in \mathbb{Z}\}$ . ■

**הערה 1.9 חוגים קומוטטיביים כלליים**  $\mathbb{Z}$  היא דוגמה לחוג קומוטטיבי עם יחידה, מבנה אלגברי שמקיים את כל אקסיומות השדה פרט לקיום הופכי כפלי. דוגמאות נוספות הן  $\mathbb{F}[x]$  חוג הפולינומים מעל שדה  $\mathbb{F}$ ,  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  חוג השלמים של גאוס.

בתוך חוג קומוטטיבי  $A$ , תת קבוצה  $I \subseteq A$  נקראת אידיאל אם היא מקיימת את התכונות של הקבוצה  $I$  לעיל, כלומר אם  $i_1, i_2 \in I$  אז  $i_1 \pm i_2 \in I$  ואם  $a \in A, i \in I$  אז  $ai \in I$ .

**אלגוריתם 1.10 אוקלידס לחישוב gcd** בהינתן  $a, b \in \mathbb{Z}$  לא שניהם 0, נחלק עם שארית שוב ושוב:

$$\begin{array}{ll} a = q_1 b + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & \\ r_{k-2} = q_k r_{k-1} + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} = q_{k+1} r_k + 0 & \end{array}$$

עוצרים כאשר מקבלים שארית אפס, ואז ה- $\gcd$  הוא  $r_k$ .

**טענה 1.11 נכונות האלגוריתם** האלגוריתם תמיד עוצר, אחרי לכל היותר  $c \cdot \log(\min\{a, b\})$  צעדים עבור  $c > 0$  קבוע. הוא מחזיר את התוצאה הנכונה, כלומר  $r_k = \gcd(a, b)$ , והוא מספק גם דרך למצוא את מקדמי בזו.

**הוכחה:** מתקיים  $b > r_1 > r_2 > \dots$  זו סדרה יורדת של שלמים חיוביים ולכן חייבים להגיע לאפס, כלומר האלגוריתם חייב לעצור. את הסיבוכיות לא הוכחנו בכיתה.

על מנת להראות נכונות נראה שאם  $a = qb + r$  אז  $\gcd(a, b) = \gcd(b, r)$ . אכן, לשני הזוגות אותם מחלקים משותפים כי אם  $d \mid a, b$  אז  $d \mid a - qb = r$ ,  $d \mid b$  אז  $d \mid r, d \mid b$  להיפך, אם  $d \mid r, d \mid b$  אז  $d \mid qb + r = a$ ,  $d \mid b$  כעת, נשתמש בכך עבור ה- $r_i$  ונקבל

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$$

כדי למצוא את מקדמי בזו מהאלגוריתם, נכתוב בצורה איטרטיבית את השאריות כקומבינציות לינאריות

$$\begin{array}{l} r_1 = a - q_1 b \\ r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_2 q_1) b \\ \vdots \\ r_k = \gcd(a, b) = \dots \end{array}$$

■

**הגדרה 1.12**  $a, b \in \mathbb{Z}$  נקראים זרים אם  $\gcd(a, b) = \pm 1$ .

### 1.3 משוואות דיופנטיות לינאריות

**הגדרה 1.13** משוואה דיופנטית זו משוואה עם נעלמים שמחפשים עבורה פתרונות בשלמים.

**פתרון משוואה דיופנטית לינארית במשתנה אחד** יהיו  $a, b \in \mathbb{Z}$ , יש פתרון ל  $ax = b$  אם ורק אם  $a \mid b$ , ואז יש פתרון יחיד  $\frac{b}{a}$ , אלא אם  $a = b = 0$  ואז יש אינסוף פתרונות.

**פתרון משוואה דיופנטית לינארית בשני משתנים** יהיו  $a, b, c \in \mathbb{Z}$ , יש פתרון ל  $ax + by = c$  אם ורק אם  $\gcd(a, b) \mid c$ , זאת כי ראינו  $I = \{ax + by \mid x, y \in \mathbb{Z}\}$  וב  $\gcd(a, b)$  הוא המינימלי, וכל איבר אחר ב  $I$  הוא כפולה שלו. נניח כי  $\gcd(a, b) \mid c$  אז אם  $(x_0, y_0)$  פתרון פרטי (ניתן למצוא לדוגמה מהלמה של בזו) אז קבוצת הפתרונות היא

$$\left\{ \left( x_0 - \frac{b}{\gcd(a, b)} k, y_0 + \frac{a}{\gcd(a, b)} k \right) \mid k \in \mathbb{Z} \right\}$$

**הוכחה:** נניח  $ax_1 + by_1 = c, ax_2 + by_2 = c$  אז  $a(x_1 - x_2) + b(y_1 - y_2) = 0$  ולכן  $a\Delta x = -b\Delta y$  ואז  $\Delta x = -\frac{b}{a}\Delta y$ . נרשום  $a = a' \cdot \gcd(a, b), b = b' \cdot \gcd(a, b)$  וכן  $\Delta x = \frac{b'}{a'}\Delta y$  אז  $a' = a' \cdot \gcd(a, b), b' = b' \cdot \gcd(a, b)$  וזה קורה אם ורק אם  $a' \mid \Delta y$ , כלומר  $\Delta y = ka' = k \frac{a}{\gcd(a, b)}$  ואז  $\Delta x = -\frac{b'}{a'}k \frac{a}{\gcd(a, b)} = -\frac{b}{\gcd(a, b)}k$  ■

## 2 ראשוניים והמשפט היסודי של האריתמטיקה

**הגדרה 2.1 ראשוני**  $p \in \mathbb{N}$  עם  $p \geq 2$  נקרא ראשוני אם המחלקים שלו הם רק  $\pm 1, \pm p$ .

**למה 2.2 אוקלידס** יהיו  $a, b, p \in \mathbb{Z}$  ראשוני. אם  $p \mid ab$  אז  $p \mid a$  או  $p \mid b$ .

**הוכחה:** נניח  $p \mid ab$  וכן  $p \nmid a$ , אז  $\gcd(a, p) = 1$  ולפי הלמה של בזו ניתן לרשום  $1 = xa + yp$  עבור  $x, y \in \mathbb{Z}$ , ואז  $b = b \cdot 1 = b(xa + yp) = bxa + byp$ . מתקיים  $p \mid bxa$  ולכן  $p \mid byp$  ולכן  $p \mid b$ . ■

**הערה 2.3** באופן כללי, בחוג קומטטיבי עם יחידה איבר  $x$  נקרא ראשוני אם הוא מקיים את התכונה של הלמה, ואיבר  $x$  נקרא אי פריק אם הוא מתחלק רק בעצמו או בהפכים בחוג. איבר ראשוני הוא תמיד אי פריק, אבל ההפך לא תמיד נכון (בשלמים כן, זו בדיוק הלמה של אוקלידס).

**משפט 2.4 היסודי של האריתמטיקה** כל  $n \in \mathbb{N}$  נתון באופן יחיד (עד כדי שינוי סדר) כמכפלה של ראשוניים.

**הוכחה: קיום:** באינדוקציה על  $n$ ,  $n = 2$  ברור ועבור הצעד נניח שהטענה נכונה לכל  $2 \leq m \leq n-1$ , אז עבור  $n$ , אם  $n$  ראשוני סיימנו, ואחרת בהכרח יש  $k \in \mathbb{N}$  כך ש- $k \mid n$  וכן  $k \neq 1, n$ , כלומר  $2 \leq k \leq n-1$  ולכן ניתן לכתוב את  $k, \frac{n}{k}$  כמכפלה של ראשוניים, ונניח יהיה מכפלת המכפלות הללו.

**יחידות:** לכל  $n \geq 2$  נסמן ב- $k(n)$  את אורך המכפלה הקצרה ביותר של ראשוניים ששווה ל- $n$ . נראה באינדוקציה על  $k(n)$ , עבור  $k(n) = 1$  ראשוני ולכן אם  $n = p_1 \cdots p_k$  אז בפרט  $p_1 \mid n$  אבל  $n$  ראשוני ולכן  $p_1 = n$ , ואז  $p_2 \cdots p_k = 1$  כלומר זו שוב מכפלה של ראשוני אחד,  $n$ . עבור הצעד, נניח שהטענה נכונה לכל  $m$  עם  $k(m) < k(n)$  ונניח  $n = p_1 p_2 \cdots p_{k(n)} = q_1 q_2 \cdots q_r$  ולפי הפעלה חוזרת של הלמה של אוקלידס  $q_r \mid p_i$  לאיזה  $1 \leq i \leq k(n)$ , בה"כ  $q_r \mid p_{k(n)}$ , שניהם ראשוניים ולכן שווים. קיבלנו  $\frac{n}{q_r} = p_1 p_2 \cdots p_{k(n)-1} = q_1 q_2 \cdots q_{r-1}$  ולפי הנחת האינדוקציה אלו אותם ראשוניים עד כדי שינוי סדר, ולכן גם  $p_1, \dots, p_{k(n)}$  ו- $q_1, \dots, q_{r-1}$  הם אותם ראשוניים עד כדי שינוי סדר. ■

**הערה 2.5** גרסה של המשפט נכונה בכל חוג בו אי פריק שקול לראשוני.

**מסקנה 2.6** אם נכתוב  $n = p_1^{r_1} \cdots p_k^{r_k}$  עם  $p_1 < p_2 < \cdots < p_k$  וכן  $r_i \in \mathbb{N}$  אז המחלקים של  $n$  הם  $\pm p_1^{s_1} \cdots p_k^{s_k}$  כאשר  $0 \leq s_i \leq r_i$  ובפרט מספר המחלקים הוא  $2(r_1 + 1) \cdots (r_k + 1)$ .  
אם  $a = \pm p_1^{r_1} \cdots p_k^{r_k}$ ,  $b = \pm p_1^{s_1} \cdots p_k^{s_k}$  כאשר  $s_i, r_i \in \mathbb{N} \cup \{0\}$  אז  $\gcd(a, b) = \pm p_1^{\min\{r_1, s_1\}} \cdots p_k^{\min\{r_k, s_k\}}$ .

**הגדרה 2.7**  $\text{lcm}$  בהינתן  $a, b \in \mathbb{Z}$ , לא שניהם 0,  $\text{lcm}$  הוא  $L \in \mathbb{Z}$  שמקיים  $a, b \mid L$  וכן אם  $a, b \mid \ell$  אז  $L \mid \ell$ .

**טענה 2.8** אם  $a = \pm \prod_{i=1}^k p_i^{r_i}$ ,  $b = \pm \prod_{i=1}^k p_i^{s_i}$  אז  $\text{lcm}(a, b) = \pm \prod_{i=1}^k p_i^{\max\{r_i, s_i\}}$  וכן  $\text{lcm}(a, b) \gcd(a, b) = \pm ab$ .

**משפט 2.9 אוקלידס** יש אינסוף מספרים ראשוניים.

**הוכחה:** נניח בשלילה שיש מספר סופי  $p_1, \dots, p_n$  של ראשוניים, נסמן  $N = p_1 p_2 \cdots p_n + 1$  אז לכל  $i$  נניח בשלילה  $p_i \mid N$  אז מכך  $p_i \mid p_1 \cdots p_n$  נובע  $p_i \mid N - p_1 \cdots p_n = 1$ , בסתירה לכך ש- $p_i$  ראשוני. כלומר אף אחד מבין הראשוניים לא מחלק את  $N$ , ובפרט לא ניתן לרשום את  $N$  כמכפלה של ראשוניים, בסתירה למשפט היסודי של האריתמטיקה. אז יש אינסוף ראשוניים. ■

**משפט 2.10 דיריכלה** (ללא הוכחה) לכל  $a, d \in \mathbb{N}$  זרים יש אינסוף ראשוניים בסדרה  $a + d, a + 2d, a + 3d, \dots$ .

**דוגמה 2.11** בקבוצה  $\{4k + 3 \mid k \in \mathbb{N}\}$  נוכל להוכיח שיש, נניח בשלילה שיש מספר סופי  $q_1, \dots, q_r$ . אם המכפלה נותנת שארית 1 בחלוקה ב-4 נסמן  $N = q_1 \cdots q_r + 2$ , אם שארית 3 נסמן  $N = q_1 \cdots q_r + 4$ . בכל מקרה שארית החלוקה של  $N$  היא 3 ולכן בפירוק לראשוניים של  $N$  יש ראשוני מהצורה  $4k + 3$  (אחרת כולם עם שארית 1 ולכן גם  $N$ ), נניח  $q_i$ . אז  $q_i \mid N - q_1 \cdots q_r$  כלומר  $q_i \mid 2$  או  $q_i \mid 4$ , וזו סתירה.

**השערת התאומים הראשוניים** יש אינסוף ערכים של  $n \in \mathbb{N}$  כך ש- $n, n + 2$  שניהם ראשוניים (השערה פתוחה).

## 2.1 משפט המספרים הראשוניים

נסמן  $p_1 < p_2 < \dots$  את הראשוניים, ונגדיר  $\pi(x) = \#\{p \leq x \mid p \text{ is prime}\}$ . מתקיים  $\pi(p_n) = n$ , ולכן אם נבין טוב את  $\pi(x)$  נוכל להבין גם מהו סדר הגודל של  $p_n$ .

**טענה 2.12 חסם ראשון**  $p_n < 2^{2^n}$ , ולכן לכל  $x \geq 2$  מתקיים  $\pi(x) \geq \log_2 \log_2 x - 1$ .

**הוכחה:** לכל  $n$  נגדיר  $q_n = p_1 \cdots p_n + 1$  אז כל גורם ראשוני של  $q_n$  הוא  $p_k$  עם  $k < n$ , ובפרט  $p_{n+1} \leq p_k \leq q_n$ . באינדוקציה, עבור  $n = 1$  מתקיים  $p_1 = 2 < 2^{2^1} = 4$ , נניח עבור  $n$  אז

$$p_{n+1} \leq p_1 \cdots p_n + 1 < 2^{2^1} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}}$$

■

**משפט 2.13 המספרים הראשוניים (ללא הוכחה)**  $\pi(x) \sim \frac{x}{\log x}$  כלומר  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$ .

**הערה 2.14** משפט זה שקול ל  $p_n \sim n \log n$ , כי  $\frac{n \log n}{\log(n \log n)} = \frac{n \log n}{\log n + \log \log n} \sim \frac{n \log n}{\log n} = n$ . במילים אחרות, לכל  $0 < a < 1 < b$  יש  $x_0 > 0$  כך שלכל  $x_0 \leq x$  מתקיים  $a \frac{x}{\log x} < \pi(x) < b \frac{x}{\log x}$ .

**משפט 2.15 צ'בישב קיימים**  $0 < a < 1 < b$  כך שלכל  $x \geq 2$  מתקיים  $a \frac{x}{\log x} < \pi(x) < b \frac{x}{\log x}$ .

**הוכחה: חסם עליון**

**למה א':** לכל  $x \in \mathbb{R}$  מתקיים  $[2x] - 2[x] \in \{0, 1\}$ .

**הוכחה:**  $[x] \leq x < [x] + 1$  ולכן  $2[x] \leq 2x < 2[x] + 2$ , ומכאן  $2[x] \leq [2x] \leq 2[x] + 1$ , נחסיר  $2[x]$  ונקבל  $0 \leq [2x] - 2[x] \leq 1$ .

כעת נראה  $\pi(x) - \pi\left(\frac{x}{2}\right) < \beta \frac{x}{\log x}$  עבור  $1 < \beta$  כלשהו.

יהי  $n$  טבעי, אז  $\pi(2n) - \pi(n) = \#\{n < p \leq 2n \mid p \text{ is prime}\}$ . מתקיים  $\binom{2n}{n} = \frac{(2n)!}{n!n!}$  כי כל הראשוניים מופיעים רק במונה. בפרט  $n^{\pi(2n) - \pi(n)} < \prod_{n < p \leq 2n} p < \binom{2n}{n}$  נוציא  $\log$  ונקבל

$$(\pi(2n) - \pi(n)) \log n < \log \binom{2n}{n} < \log(2^{2n}) = 2n \cdot \log 2$$

ולכן  $\pi(2n) - \pi(n) < 2 \log 2 \frac{n}{\log n} = \beta_1 \frac{n}{\log n}$  עבור  $x \in \mathbb{R}$  כללי. נניח  $x \geq 8$ , אז

$$\begin{aligned} \pi(x) - \pi\left(\frac{x}{2}\right) &= \pi([x]) - \pi\left(\left[\frac{x}{2}\right]\right) \stackrel{\text{Lemma (a)}}{\leq} 1 + \pi\left(2 \cdot \left[\frac{x}{2}\right]\right) - \pi\left(\left[\frac{x}{2}\right]\right) < 1 + \beta_1 \frac{\left[\frac{x}{2}\right]}{\log \left[\frac{x}{2}\right]} \leq 1 + \beta_1 \frac{\frac{x}{2}}{\log \left(\frac{x}{2} - 1\right)} \\ &= 1 + \frac{\beta_1}{2} \cdot \frac{x}{\log \left(\frac{x}{2} - 1\right)} \stackrel{x \geq 8 \Rightarrow \frac{x}{2} - 1 \geq \sqrt{x}}{\leq} 1 + \frac{\beta_1}{2} \frac{x}{\log \sqrt{x}} = 1 + \beta_1 \frac{x}{\log x} < (1 + \beta_1) \frac{x}{\log x} \end{aligned}$$

עבור  $2 \leq x < 8$  נמצא  $\beta_2 > 0$  כך ש  $\pi(x) - \pi\left(\frac{x}{2}\right) \leq \beta_2 \frac{x}{\log x}$  קיים כי  $\pi(x) - \pi\left(\frac{x}{2}\right) \in \{1, 2\}$  ואילו  $\frac{x}{\log x}$  חסומה מלמטה על ידי איזה  $m > 0$ . נגדיר  $\beta = \max\{\beta_2, 1 + \beta_1\}$  וקיבלנו לכל  $x \geq 2$  את  $\pi(x) - \pi\left(\frac{x}{2}\right) < \beta \frac{x}{\log x}$ .

לסיום ההוכחה, מתקיים לכל  $x \geq 2$

$$\begin{aligned} \pi(x) \log x - \pi\left(\frac{x}{2}\right) \log\left(\frac{x}{2}\right) &= \pi(x) \log x - \pi\left(\frac{x}{2}\right) (\log x - \log 2) = \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) \log x + \pi\left(\frac{x}{2}\right) \log 2 \\ &< \beta \frac{x}{\log x} \cdot \log x + \frac{x}{2} \log 2 = \left(\beta + \frac{\log 2}{2}\right) x = \beta_3 x \end{aligned}$$

כעת, ניקח  $m$  כך ש  $\frac{x}{2^{m+1}} < 2 \leq \frac{x}{2^m}$  אז

$$\pi(x) \log x = \left( \sum_{i=0}^m \pi\left(\frac{x}{2^i}\right) \log\left(\frac{x}{2^i}\right) - \pi\left(\frac{x}{2^{i+1}}\right) \log\left(\frac{x}{2^{i+1}}\right) \right) < \sum_{i=0}^m \beta_3 \frac{x}{2^i} < 2\beta_3 x = bx$$

ולכן  $\pi(x) < b \frac{x}{\log x}$  לכל  $x \geq 2$ , כדורש.

### חסם תחתון:

**למה ב':** עבור  $n$  טבעי ו- $p$  ראשוני, נסמן ב- $r_p$  את החזקה הגבוהה ביותר של  $p$  שהיא קטנה מ- $n$ , כלומר  $p^{r_p} \leq n < p^{r_p+1}$ . אז החזקה הגבוהה ביותר של  $p$  שמחלקת את  $n!$  היא  $\sum_{k=1}^{r_p} \left\lfloor \frac{n}{p^k} \right\rfloor$ .

**הוכחה:**  $\left\lfloor \frac{n}{p^k} \right\rfloor$  הוא מספר המספרים בין  $1, \dots, n$  שמתחלקים ב- $p^k$ , ולכן סופר תרומה אחת של כל מספר כזה לחזקה הכוללת של  $p$ . כך, המספר  $1 \leq r \leq n$ , אם  $p^j \mid r$  אבל  $p^{j+1} \nmid r$  אז סופרים את  $r$  בדיוק  $j$  פעמים, ב- $\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{n}{p^2} \right\rfloor, \dots, \left\lfloor \frac{n}{p^j} \right\rfloor$ .

כעת נראה  $\left( \frac{2n}{n} \right) \mid \prod_{p \leq 2n} p^{r_p}$  כאשר  $r_p$  מתאים ל- $2n$ ,  $p^{r_p} \leq 2n < p^{r_p+1}$ .

החזקה הגבוהה ביותר של  $p$  שמחלקת את  $(2n)!$  היא  $\sum_{k=1}^{r_p} \left\lfloor \frac{2n}{p^k} \right\rfloor$  ואת  $n!$  היא  $\sum_{k=1}^{r_p} \left\lfloor \frac{n}{p^k} \right\rfloor$ , ולכן חזקת  $p$  שמופיעה ב- $\left( \frac{2n}{n} \right)$  היא

$$\sum_{k=1}^{r_p} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \stackrel{\text{Lemma (a)}}{\leq} \sum_{k=1}^{r_p} 1 = r_p$$

ולכן אכן  $\left( \frac{2n}{n} \right) \mid \prod_{p \leq 2n} p^{r_p}$ , ובפרט

$$\left( \frac{2n}{n} \right) \leq \prod_{p \leq 2n} p^{r_p} \stackrel{p^{r_p} \leq 2n}{\leq} (2n)^{\pi(2n)} \stackrel{\log}{\Rightarrow} n \log 2 = \log(2^n) \leq \log \left( \frac{2n}{n} \right) \leq \pi(2n) \log 2n$$

קיבלנו  $a_1 \frac{2n}{\log 2n} = \frac{\log 2}{2} \cdot \frac{2n}{\log 2n} \leq \pi(2n)$  הוכחנו את הרצוי לכל הזוגיים וצריך להוכיח ל- $2 \leq x \in \mathbb{R}$  כללי. נניח  $x \geq 4$ , אז

$$\pi(x) \geq \pi \left( 2 \cdot \left\lfloor \frac{x}{2} \right\rfloor \right) \geq a_1 \frac{2 \left\lfloor \frac{x}{2} \right\rfloor}{\log \left( 2 \left\lfloor \frac{x}{2} \right\rfloor \right)} \stackrel{\text{Lemma (a)}}{\geq} a_1 \frac{[x] - 1}{\log \left( 2 \cdot \frac{x}{2} \right)} \geq a_1 \frac{x - 2}{\log x} \stackrel{x \geq 4}{\geq} \frac{x - 2}{x} \geq \frac{x - 2}{x} \geq \frac{1}{2} \geq \frac{a_1}{2} \frac{x}{\log x}$$

עבור  $x \in [2, 4]$  יש  $a_2$  כך ש- $\pi(x) \geq a_2 \frac{x}{\log x}$ , ניקח  $a = \min \{a_2, \frac{a_1}{2}\}$  ואז לכל  $x \geq 2$  מתקיים  $a \frac{x}{\log x} \leq \pi(x)$ . ■

**מסקנה 2.16** קיימים  $\alpha, \beta > 0$  כך שלכל  $n \geq 2$  טבעי מתקיים  $\alpha n \log n < p_n < \beta n \log n$ .

**הוכחה:** ראינו שקיימים  $0 < a < 1 < b$  כך ש- $a \frac{x}{\log x} < \pi(x) < b \frac{x}{\log x}$ . אז בפרט

$$n = \pi(p_n) < b \frac{p_n}{\log p_n} \Rightarrow p_n > \frac{1}{b} n \log p_n > \frac{1}{b} n \log n = \alpha n \log n$$

בכיוון השני, נשים לב כי לכל  $n \geq \frac{2}{a}$  מתקיים  $p_n \leq n^4$  שכן  $\frac{\sqrt{p_n}}{2} < \frac{p_n}{\log p_n} < \frac{1}{a} r < \frac{r^2}{2} = \frac{n^2}{2}$  וכעת לכל  $n \geq \frac{2}{a}$

$$n = \pi(p_n) > a \frac{p_n}{\log p_n} \Rightarrow p_n < \frac{1}{a} n \log p_n \leq \frac{1}{a} n \log n^4 = \frac{4}{a} n \log n$$

עבור  $2 \leq n \leq \frac{2}{a}$  יש מספר סופי של  $r$  וניקח  $\beta_1$  כך שלכל אחד מהם מתקיים אי השוויון הרצוי, ואז עבור  $\beta = \max \left\{ \frac{4}{a}, \beta_1 \right\}$  זה מתקיים. ■

**טענה 2.17**  $\sum_{n=1}^{\infty} \frac{1}{p_n}$  מתבדר.

**הוכחה:** לפי המסקנה מצ'בישב לכל  $n \geq 2$  מתקיים  $\frac{1}{\beta n \log n} < \frac{1}{p_n} < \frac{1}{\alpha n \log n}$ , ולכן

$$\sum_{n=1}^{\infty} \frac{1}{p_n} \text{ diverges } \iff \sum_{n=2}^{\infty} \frac{1}{n \log n} \text{ diverges } \iff \int_2^{\infty} \frac{1}{x \log x} dx \text{ diverges}$$

נחשב

$$\int_2^{\infty} \frac{1}{x \log x} dx = \left[ \frac{t = \log x}{\frac{dt}{dx} = \frac{1}{x}} \right] = \int_{\log 2}^{\infty} \frac{1}{t} dt = [\log t]_{\log 2}^{\infty} = [\log \log x]_2^{\infty} = \infty$$

כלומר אכן מתבדר. ■

**משפט 2.18 השערת ברטרנד** לכל  $n > 1$  טבעי יש לפחות ראשוני אחד  $n < p < 2n$ .

**הוכחה:** נוכיח בהסתמך על משפט המספרים הראשוניים, עבור  $n > N_0$  מספיק גדול.

נבחר  $0 < a < 1 < b$  כלשהם כך ש  $2a - b > 0$ , אז יש  $N_0$  כך שלכל  $n > N_0$  מתקיים  $a \frac{n}{\log n} < \pi(n) < b \frac{n}{\log n}$ , ואז

$$\pi(2n) - \pi(n) > a \frac{2n}{\log 2n} - b \frac{n}{\log n} = \frac{2an \log n - bn \log 2n}{\log n \cdot \log 2n} = n \cdot \frac{(2a - b) \log n - b \log 2}{\log n \cdot \log 2n}$$

בחרנו  $2a - b > 0$  אז עבור  $n$  גדול מספיק  $(2a - b) \log n - b \log 2 > 0$  ואז  $\pi(2n) - \pi(n) > 0$  ובפרט יש ראשוני ביניהם. ■

## השערת רימן

**הגדרה 2.19 פונקציית Li** מוגדרת  $\text{Li}(x) = \int_2^x \frac{1}{\log t} dt$

**טענה 2.20**  $\text{Li}(x) \sim \frac{x}{\log x}$ , כלומר  $\frac{\text{Li}(x)}{x/\log x} \xrightarrow{x \rightarrow \infty} 1$  (תרגיל). ממשפט המספרים הראשוניים נובע  $\text{Li}(x) \sim \pi(x)$ .

**הגדרה 2.21 פונקציית זטא של רימן** לכל  $s$  ממשי, מגדירים  $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ , זה מתכנס לכל  $s > 1$ .

**הערה 2.22** לכל  $s > 1$  מתקיים  $\zeta(s) = \prod_{p \text{ is prime}} \frac{1}{1 - \frac{1}{p^s}}$ , וכן ניתן להעריך את  $\zeta(s)$  גם עבור מרוכבים עם  $\Re z > 1$ . יותר מזה, רימן גילה שיש המשכה אנליטית ל  $\zeta$ , כלומר פונקציה אנליטית שמוגדרת על כל  $\mathbb{C} \setminus \{1\}$  שמזדהה עם  $\zeta$  בתחום ההגדרה שלה.

**השערת רימן (גרסה 1)** לכל  $\beta > \frac{1}{2}$  קיים  $x_0$  כך שלכל  $x \geq x_0$  מתקיים  $|\pi(x) - \text{Li}(x)| \leq x^\beta$ . כלומר,  $|\pi(x) - \text{Li}(x)|$  חסום בערך על ידי  $\sqrt{x}$  (אבל לא ממש על ידי, ידוע שהטענה לא נכונה עבור  $\beta = \frac{1}{2}$ ).

**השערת רימן (גרסה 2)** כל האפסים הלא טריויאליים (לא  $-2n$  כאשר  $n \in \mathbb{N}$ ) של פונקציית זטא של רימן הם על הציר הקריטי  $\Re z = \frac{1}{2}$ .



### 3 קונגרואנציות

**הגדרה 3.1** קונגרואנציה יהי  $n$  טבעי, נאמר כי  $a, b \in \mathbb{Z}$  שווים מודולו  $n$  ונסמן  $a \equiv b \pmod{n}$  אם  $n \mid a - b$ . נעיר כי זה יחס שקילות מודולו  $n$ , ובמילים אחרות טוען כי  $a, b$  נותנים אותה שארית חלוקה ב- $n$ .

**טענה 3.2** נניח  $a_1 \equiv a_2 \pmod{n}$  וכן  $b_1 \equiv b_2 \pmod{n}$  אז  $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$  וכן  $a_1 b_1 \equiv a_2 b_2 \pmod{n}$ . כלומר, ניתן להגדיר חיבור וכפל על מחלקות השקילות מודולו  $n$ , שנסמן  $\bar{a}$  או  $a + n\mathbb{Z}$ .

**הוכחה:** עבור חיבור, מתקיים  $n \mid b_1 - b_2$  וכן  $n \mid a_1 - a_2$  ולכן  $n \mid (a_1 + b_1) - (a_2 + b_2)$  וכן  $n \mid (a_1 - a_2) + (b_1 - b_2)$ . כלומר  $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ . עבור כפל, מתקיים  $n \mid b_1 - b_2$  וכן  $n \mid a_1 - a_2$  ולכן

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1 (b_1 - b_2) + b_2 (a_1 - a_2)$$

ו- $n$  מחלק אותו, כי זה צירוף לינארי. ■

**מסקנה 3.3** יהי  $f(x) \in \mathbb{Z}[x]$  פולינום עם מקדמים שלמים אז  $f(a_1) \equiv f(a_2) \pmod{n} \implies a_1 \equiv a_2 \pmod{n}$ .

#### 3.1 חוג השלמים מודולו $n$

**הגדרה 3.4** נסמן  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$  את קבוצת מחלקות השקילות מודולו  $n$ . זה אכן חוג קומטטיבי עם יחידה.

**טענה 3.5** יהי  $a \in \mathbb{Z}$   $n \geq 21$  טבעי. האיבר  $\bar{a}$  הפיך ב- $\mathbb{Z}_n$  אם ורק אם  $\gcd(a, n) = 1$ .

**הוכחה:**  $\bar{a}$  הפיך  $\iff$  קיים  $b \in \mathbb{Z}$  כך ש- $ab \equiv 1 \pmod{n}$   $\iff$  קיים  $b \in \mathbb{Z}$  כך ש- $ab - 1$  מתחלק ב- $n$   $\iff$  קיימים  $b, k \in \mathbb{Z}$  כך ש- $ab - kn = 1$   $\iff$  קיימים  $b, k \in \mathbb{Z}$  כך ש- $kn = ab - 1$   $\iff$  לפי הלמה של בזו,  $\gcd(a, n) = 1$ . ■

**מסקנה 3.6**  $\mathbb{Z}_n$  שדה  $\iff n$  ראשוני.

**הוכחה:** אם  $n$  ראשוני אז  $\gcd(a, n) = 1$  לכל  $1 \leq a \leq p-1$ , ולכן כל  $\bar{a} \neq \bar{0}$  ב- $\mathbb{Z}_p$  הוא הפיך, ו- $\mathbb{Z}_p$  מקיים את כל אקסיומות השדה. אם  $n$  אינו ראשוני אז יש לו מחלק לא טריויאלי  $d$ , ואז  $\gcd(d, n) = d$  ולכן  $\bar{d}$  אין הופכי. ■

**אלגוריתם 3.7 חישוב ההופכי מודולו  $n$**  כדי למצוא את ההופכי של  $a$  מודולו  $n$  נשתמש באלגוריתם אוקלידס כדי למצוא  $x, y \in \mathbb{Z}$  כך ש- $ax + ny = \gcd(a, n)$ . אם  $\gcd(a, n) \neq 1$  אין הופכי, ואם הוא 1 אז ההופכי הוא  $x$ .

**הגדרה 3.8 חבורת ההפיכים** נסמן  $\mathbb{Z}_n^*$  קבוצת ההפיכים ב- $\mathbb{Z}_n$ , זו חבורה אבלית ביחס לכפל.

**הגדרה 3.9 פונקציית אוילר**  $\varphi(n) = |\mathbb{Z}_n^*| = \#\{1 \leq a \leq n \mid \gcd(a, n) = 1\}$ . מתקיים  $\varphi(p) = p - 1$ .

**משפט 3.10 משפט השאריות הסיני** אם  $m, n \in \mathbb{N}$  זרים אז לכל  $a, b \in \mathbb{Z}$  יש פתרון יחיד מודולו  $mn$  של

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \text{המערכת}$$

**הוכחה: קיום:** נמצא  $\hat{n}, \hat{m} \in \mathbb{Z}$  כך ש- $n\hat{n} \equiv 1 \pmod{m}$ ,  $m\hat{m} \equiv 1 \pmod{n}$  (קיימים כי  $n, m$  זרים ולכן כל אחד מהם הפיך מודולו השני), ונגדיר  $x = an\hat{n} + bm\hat{m}$  אז  $x \equiv an\hat{n} \equiv a \pmod{m}$ ,  $x \equiv bm\hat{m} \equiv b \pmod{n}$ . **יחידות:** משיקולי ספירה, יש בדיוק  $mn$  מחלקות מודולו  $mn$  ויש פתרון לכל אחת מ- $mn$  המערכות האפשריות (בחירה של  $(a, b)$ , ולכן הפתרון הוא יחיד. ■

**אלגוריתם 3.11 פתרון מערכת מהצורה** 
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$
 כאשר  $n_1, \dots, n_k$  זרים בזוגות

לכל  $i$  נמצא  $\hat{n}_i$  הופכי ל- $\prod_{j \neq i} n_j$  מודולו  $n_i$  באמצעות אלגוריתם אוקלידס (קיים, כי  $n_1, \dots, n_k$  זרים בזוגות ולכן  $n_i$  זר ל- $\prod_{j \neq i} n_j$ ), אזי הפתרון היחיד הוא  $x \equiv \sum_{i=1}^k a_i \left( \prod_{j \neq i} n_j \right) \hat{n}_i \pmod{n_1 \cdots n_k}$ .

**מסקנה 3.12** ההעתקה  $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  המוגדרת  $x \rightarrow (x \bmod m, x \bmod n)$  היא חח"ע ועל, ומצטמצמת להעתקה חח"ע ועל  $\mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ . באופן יותר חזק, היא איזו' של חוגים, כלומר גם משמרת חיבור וכפל.

**הוכחה:** נראה את החלק השני, לגבי צמצום להפיכים.

$\subseteq$  יהי  $x \in \mathbb{Z}_{mn}^*$  אז יש  $y \in \mathbb{Z}$  כך ש  $xy \equiv 1 \pmod{mn}$ , ולכן  $mn \mid xy - 1$  כלומר גם  $m \mid xy - 1$  ולכן  $xy \equiv 1 \pmod{m}$  וכן  $xy \equiv 1 \pmod{n}$ . כלומר  $x$  הפיך מודולו  $m$  ולכן  $x \bmod m \in \mathbb{Z}_m^*$  וכנ"ל עבור  $n$ . לכן  $f(x) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ .  
 $\supseteq$  יהי  $x \in \mathbb{Z}_{mn}$  כך ש  $f(x) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$  כלומר  $x$  הפיך מודולו  $m$  ומודולו  $n$ , אז יש  $y_1, y_2$  כך ש  $xy_1 \equiv 1 \pmod{m}$  ו  $xy_2 \equiv 1 \pmod{n}$ . לפי משפט השאריות הסיני יש פתרון יחיד מודולו  $mn$  למערכת  $x \equiv y_1 \pmod{m}, x \equiv y_2 \pmod{n}$ . נסמן אותו ב  $x_0$  אז  $x_0 \equiv 1 \pmod{m}, x_0 \equiv 1 \pmod{n}$  ומכך  $mx_0 \equiv 1 \pmod{mn}$  וזרים נובע  $xx_0 \equiv 1 \pmod{mn}$  כלומר  $x = x_0^{-1} \pmod{mn}$ .

■ אז התמונה של  $f$  על  $\mathbb{Z}_{mn}^*$  היא בדיוק  $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ , והיא גם חח"ע ועל כי היא חח"ע ועל בכל התחום.

**מסקנה 3.13**  $\varphi$  כפליית כלומר אם  $m, n \in \mathbb{N}$  זרים אז  $\varphi(mn) = \varphi(m) \varphi(n)$ .

**הוכחה:** הפונקציה  $f$  מהמסקנה היא חח"ע ועל בצמצום, ולכן

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \varphi(n)$$

■

**משפט 3.14** נוסחה עבור  $\varphi$  לכל  $n \in \mathbb{N}$   $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$

**הוכחה:** ראשית נוכיח עבור המקרה הפרטי  $n = p^k$ . אכן, מתקיים  $\gcd(a, p^k) = 1 \iff p \nmid a$ , ולכן כל המספרים מ  $1$  עד  $p^k$  זרים לו, מלבד  $p^{k-1}$  המספרים שמתחלקים ב  $p$ . כלומר  $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$ .  
כדורש. כעת, עבור  $n \in \mathbb{N}$  כללי נרשום מהמשפט היסודי של האריתמטיקה  $n = \prod_{i=1}^k p_i^{t_i}$  אז זרים ולכן מכפליות הפונקציה  $\varphi$  שהראינו

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{t_i}\right) = \prod_{i=1}^k \varphi(p_i^{t_i}) = \prod_{i=1}^k p_i^{t_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k p_i^{t_i} \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

■

**מסקנה 3.15** לכל  $n$  טבעי  $n = \sum_{d|n} \varphi(d)$

**הוכחה:** נרשום  $n = \prod_{i=1}^k p_i^{t_i}$  אזי המחלקים שלו הם בדיוק כל המספרים מהצורה  $\prod_{i=1}^k p_i^{s_i}$  כאשר  $0 \leq s_i \leq t_i$  אז

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{\substack{0 \leq s_1 \leq t_1 \\ \vdots \\ 0 \leq s_k \leq t_k}} \varphi\left(\prod_{i=1}^k p_i^{s_i}\right) = \sum_{\substack{0 \leq s_1 \leq t_1 \\ \vdots \\ 0 \leq s_k \leq t_k}} \left(\prod_{i=1}^k \varphi(p_i^{s_i})\right) = \prod_{i=1}^k \left(\sum_{0 \leq s_i \leq t_i} \varphi(p_i^{s_i})\right) \\ &= \prod_{i=1}^k \left(1 + \sum_{1 \leq s_i \leq t_i} (p_i^{s_i} - p_i^{s_i-1})\right) \stackrel{\text{telescopic sum}}{=} \prod_{i=1}^k p_i^{t_i} = n \end{aligned}$$

■

**אלגוריתם 3.16 פתרון קונגרואנציה מהצורה  $ax \equiv c \pmod{n}$**

ראינו שלמשוואה הדיופנטית הלינארית בשני נעלמים  $ax + by = c$  יש פתרון  $\iff \gcd(a, b) \mid c$  ואם  $(x_0, y_0)$  פתרון פרטי אז קבוצת הפתרונות נתונה על ידי

$$\left\{ \left( x_0 - k \frac{b}{\gcd(a, b)}, y_0 + k \frac{a}{\gcd(a, b)} \right) \mid k \in \mathbb{Z} \right\}$$

כעת נשים לב כי למשוואה  $ax \equiv c \pmod{n}$  יש פתרון  $\iff$  למשוואה  $ax + ny = c$  יש פתרון, כלומר  $\iff \gcd(a, n) \mid c$  ובמקרה זה יש  $\gcd(a, n)$  פתרונות ב  $\mathbb{Z}_n^*$  והם  $\left\{ x_0 + k \frac{n}{\gcd(a, n)} \mid k \in \{0, 1, \dots, n-1\} \right\}$ .

## 4 חבורת ההפיכים ושורשים פרימיטיביים

### 4.1 החבורה הכפלית $\mathbb{Z}_n^*$

**הגדרה 4.1** סדר בחבורת ההפיכים יהי  $2 \leq n$ ,  $a \in \mathbb{Z}_n^*$ . הסדר של  $a$  הוא  $\text{ord}_n(a) = \min \{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{n}\}$ .

**טענה 4.2** אם  $\text{ord}_n(a) = k$ , אז  $a^m \equiv 1 \pmod{n} \iff k \mid m$ .

**הוכחה:**  $\Leftarrow$  נניח  $a^m \equiv 1 \pmod{n}$ , נחלק את  $m$  ב- $k$  עם שארית  $m = qk + r$  כאשר  $0 \leq r < k$ . מתקיים

$$1 \equiv a^m \equiv a^{qk+r} \equiv (a^k)^q a^r \equiv a^r \pmod{n}$$

ולכן אם  $0 < r < k$  אז זו סתירה לכך ש- $\text{ord}_n(a) = k$ , ומכאן בהכרח  $r = 0$  כלומר  $qk = m$ .  $k \mid m$

$\Rightarrow$  נניח  $k \mid m$ , נרשום  $m = qk$  אז  $a^m \equiv a^{qk} \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}$ . ■

### משפט 4.3 פרמה-אویلר $\text{ord}_n(a) \mid \varphi(n)$

**הוכחה:** יהיו  $x_1, \dots, x_{\varphi(n)}$  איברי החבורה  $\mathbb{Z}_n^*$ , אזי גם  $ax_1, \dots, ax_{\varphi(n)}$  הם בדיוק כל איברי החבורה, אולי בסדר שונה. מכאן

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} ax_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i \pmod{n}$$

אך  $\prod_{i=1}^{\varphi(n)} x_i$  הפיך לכן ניתן לכפול בהופכי שלו, ואז נקבל  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , ומהטענה  $\text{ord}_n(a) \mid \varphi(n)$ . ■

**מסקנה 4.4 המשפט הקטן של פרמה** אם  $a \in \mathbb{Z}$  מקיים  $\gcd(a, p) = 1$  אז  $a^{p-1} \equiv 1 \pmod{p}$ . או, לכל  $a \in \mathbb{Z}$  מתקיים  $a^p \equiv a \pmod{p}$ .

**משפט 4.5 וילסון** אם  $p$  ראשוני אז  $\prod_{i=1}^{p-1} i \equiv -1 \pmod{p}$ , כלומר  $(p-1)! \equiv -1 \pmod{p}$ .

**הוכחה:** אם  $a \in \mathbb{Z}_p^*$  וכן  $a^{-1} \neq a$  אז  $a, a^{-1}$  מתבטלים במכפלה. האיברים היחידים שלא מתבטלים הם אלה עם  $a^{-1} = a$  כלומר  $a^2 = 1$ , ומכך  $p$  ראשוני שדה ולכן זה רק  $a \equiv \pm 1 \pmod{p}$ . כלומר המכפלה היא  $1 \cdot (-1) = -1$ . כדרוש. ■

**משפט 4.6 אורך המחזור של  $\frac{1}{N}$  בכתוב עשרוני** אם  $\gcd(N, 10) = 1$ , אז אורך המחזור של  $\frac{1}{N}$  הוא  $\text{ord}_N(10)$ .

**הוכחה:** נבצע חילוק ארוך:

$$\begin{aligned} 10 &= a_1 N + r_1 \\ 10r_1 &= a_2 N + r_2 \\ 10r_2 &= a_3 N + r_3 \\ &\vdots \end{aligned}$$

זה בדיוק התהליך שמבצעים בחילוק ארוך של  $\frac{1}{N}$ , והספרה ה- $i$  אחרי הנקודה בכתוב העשרוני היא  $a_i$ . מתקיים  $r_1 \equiv 10 \pmod{N}$  ובכל שלב  $r_{i+1} \equiv 10r_i \pmod{N}$ , ולכן  $r_i \equiv 10^i \pmod{N}$ . אורך המחזור הוא בדיוק ה- $i$  הקטן ביותר כך ש- $r_i \equiv 1 \pmod{N}$  (כי אז מקבלים בשורה  $10r_i = a_{i+1}N + r_{i+1}$  בדיוק את אותה חלוקה כמו בשורה הראשונה, ולכן  $a_{i+1} = a_1$ ), שזה בדיוק  $\text{ord}_N(10)$ . כדרוש. ■

## 4.2 שורש פרימיטיבי וקריטריון אוילר

**הגדרה 4.7** שורש פרימיטיבי מודולו  $N$  הוא איבר  $a \in \mathbb{Z}_N^*$  כך ש  $\varphi(N) = \text{ord}_N(a)$ .

**טענה 4.8**  $a$  הוא שורש פרימיטיבי מודולו  $N \iff a$  יוצר את  $\mathbb{Z}_N^*$ .

**הוכחה:**  $a$  ש"פ  $\iff |\langle a \rangle| = \text{ord}_N(a) = \varphi(N) = |\mathbb{Z}_N^*| \iff \langle a \rangle = \mathbb{Z}_N^*$  ■

**הערה 4.9** אם יש שורש פרימיטיבי אז יש  $\varphi(\varphi(n))$  כאלה, כי נניח  $a$  שורש פרימיטיבי אז כל איברי החבורה הם  $1, a, a^2, \dots, a^{\varphi(n)-1}$ , ומתקיים  $\text{ord}_n(a^i) = \frac{\text{ord}_n(a)}{\gcd(i, \text{ord}_n(a))}$  כלומר שווה ל  $\varphi(n)$  אם ורק אם  $i$  זר ל  $\varphi(n)$ , ויש בדיוק  $\varphi(\varphi(n))$  כאלה, מהגדרה.

**משפט 4.10** תנאי לקיום ש"פ יש שורש פרימיטיבי מודולו  $n \iff n = 2, 4, p^k, 2p^k$  כאשר  $p$  אי זוגי,  $k$  שלם.

**הוכחה:** נוכיח רק את המקרה  $n = p$ , זה נקרא משפט גאוס.

לכל  $d \mid p-1$ , נסמן  $\psi(d) = \#\{x \in \mathbb{Z}_p^* \mid \text{ord}_n(x) = d\}$ . אז  $\sum_{d \mid p-1} \psi(d) = p-1$ , כי לכל  $x \in \mathbb{Z}_p^*$  מתקיים  $\text{ord}_n(x) \mid \varphi(p) = p-1$  ולכן זה בדיוק סכום על כל האיברים מסדר כלשהו, ולכל איבר יש סדר. כמו כן ראינו בעבר  $\sum_{d \mid n} \varphi(d) = n$ , ובפרט עבור  $p-1$ . כלומר שוויון זה מתקיים עבור  $\psi, \varphi$ .

**למה:** אם  $\psi(d) > 0$  אז  $\psi(d) = \varphi(d)$ .

**הוכחה:** נניח  $\psi(d) > 0$ , אז יש  $x \in \mathbb{Z}_p$  עם  $\text{ord}_n(x) = d$ . יש בדיוק  $d$  איברים שונים ב  $\mathbb{Z}_p^*$  שהם חזקות של  $x$ , וכולם שורשים של הפולינום  $x^d - 1$ .  $\mathbb{Z}_p$  הוא שדה, ולכן לפולינום זה יש לכל היותר  $d$  שורשים, כלומר חזקות  $x$  הן בדיוק כל השורשים.

כמו כן, מתקיים  $\text{ord}_n(x^i) = \frac{\text{ord}_n(x)}{\gcd(i, \text{ord}_n(x))} = \frac{d}{\gcd(i, d)}$  ולכן יש בדיוק  $\varphi(d)$  חזקות של  $d$  מסדר  $d$ , אלה עם מעריך זר ל  $d$ . מכאן יש בדיוק  $\varphi(d)$  איברים ב  $\mathbb{Z}_p^*$  מסדר  $d$  בסך הכל, כי איברים שאינם חזקות של  $x$  לא יכולים להיות שורש של הפולינום  $x^d - 1$ , ובפרט לא יכולים להיות מסדר  $d$ . כלומר,  $\psi(d) = \varphi(d)$ . ■

כעת, בהינתן הלמה, לכל  $d \mid p-1$  מתקיים  $\psi(d) \in \{0, \varphi(d)\}$ , אך  $\sum_{d \mid p-1} \psi(d) = p-1 = \sum_{d \mid p-1} \varphi(d)$  ולכן בהכרח  $\psi(d) = \varphi(d)$  לכל  $d$ , בפרט  $\psi(p-1) = \varphi(p-1)$  ולכן יש  $\varphi(p-1) = \varphi(\varphi(p))$  איברים ב  $\mathbb{Z}_p^*$  מסדר  $p-1$ , כלומר  $\varphi(\varphi(p))$  שורשים פרימיטיביים, ובפרט לא אפס. ■

**משפט 4.11** קריטריון אוילר נניח כי ב  $\mathbb{Z}_n^*$  יש שורש פרימיטיבי, ויהי  $a \in \mathbb{Z}_N^*$ . אזי יש פתרון למשוואה  $x^m \equiv a \pmod{n} \iff a^{\frac{\varphi(n)}{\gcd(m, \varphi(n))}} \equiv 1 \pmod{n}$  ואם יש פתרון אז יש בדיוק  $\gcd(m, \varphi(n))$  פתרונות.

**הוכחה:** נניח  $g$  ש"פ מודולו  $n$  ונסמן  $d = \gcd(\varphi(n), m)$ .

$\Leftarrow$  נניח  $x^m \equiv a \pmod{n}$ , אז

$$a^{\frac{\varphi(n)}{d}} \equiv (x^m)^{\frac{\varphi(n)}{d}} \equiv (x^{\varphi(n)})^{\frac{m}{d}} \equiv 1^{\frac{m}{d}} \equiv 1 \pmod{n}$$

$\Rightarrow$  נניח  $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$  ונרשום  $a \equiv g^r \pmod{n}$  (אפשר כי ש"פ), אז  $(g^r)^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$  ולכן  $g^{\frac{r \cdot \varphi(n)}{d}} \equiv 1 \pmod{n}$ , כלומר  $\frac{r \cdot \varphi(n)}{d} \equiv 0 \pmod{\varphi(n)}$  ולכן  $d \mid r$ . אז יש פתרון למשוואה הדיופנטית  $mt + \varphi(n)s = r$ , ולכן יש פתרון לקונגרואנציה  $mt \equiv r \pmod{\varphi(n)}$ . נגדיר  $x \equiv g^t \pmod{n}$ , אז

$$x^m \equiv (g^t)^m \equiv g^{mt} \equiv g^r \equiv a \pmod{n}$$

למעשה יש  $\gcd(m, \varphi(n))$  פתרונות לקונגרואנציה הנ"ל, ולכן גם למשוואה  $x^m \equiv a \pmod{n}$ . ■

**דוגמה 4.12**  $-1$  הוא ריבוע מודולו  $p > 2 \iff p \equiv 1 \pmod{4} \iff 1 \equiv (-1)^{\frac{\varphi(p)}{\gcd(2, \varphi(p))}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

## 5 שאריות ריבועיות

### 5.1 סימן לז'נדר וחוק ההדדיות הריבועית

**הגדרה 5.1** שארית ריבועית  $a \in \mathbb{Z}$  היא שארית ריבועית מודולו  $p$  אם קיים  $x \in \mathbb{Z}$  כך ש  $x^2 \equiv a \pmod{p}$ .

**טענה 5.2** יהי  $p > 2$  ראשוני, אז בדיוק חצי מאיברי  $\mathbb{Z}_p^*$  הם שאריות ריבועיות.

**הוכחה:** אם  $a \in \mathbb{Z}_p^*$  שארית ריבועית מודולו  $p$  אז יש  $x \in \mathbb{Z}_p^*$  כך ש  $x^2 \equiv a \pmod{p}$ , ומכאן גם  $(-x)^2 \equiv a \pmod{p}$ . אי זוגי לכן  $x \not\equiv -x \pmod{p}$ , כלומר  $x, -x$  שני שורשים שונים לפולינום  $x^2 - a$  ב  $\mathbb{Z}_p$ . ראשוני לכן  $\mathbb{Z}_p$  שדה לכן לפולינום זה יש לכל היותר 2 שורשים, ומכאן  $x, -x$  השורשים היחידים שלו.

כלומר לכל פולינום  $x^2 - a$  עם  $a \in \mathbb{Z}_p^*$  יש שני שורשים או אפס, וכל איבר ב  $\mathbb{Z}_p^*$  הוא שורש של בדיוק פולינום אחד כנ"ל, ולכן משיקולי ספירה בדיוק לחצי מהפולינומים הנ"ל יש שורשים, כלומר בדיוק חצי מאיברי  $\mathbb{Z}_p^*$  הם שאריות ריבועיות. ■

**הגדרה 5.3** סימן לז'נדר עבור  $p > 2$  ראשוני ו  $a \in \mathbb{Z}$  (בדרך כלל נניח  $p \nmid a$  כלומר  $a$  זר ל  $p$ ), נגדיר

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a, a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a, a \text{ is a quadratic nonresidue mod } p \\ 0 & p \mid a \end{cases}$$

**טענה 5.4** מסקנה מקריטריון אוילר יהי  $a$  זר ל  $p$ , אז  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

**הוכחה:** אם  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  אז מקריטריון אוילר (ניתן להשתמש בו, כי ממשפט גאוס  $\mathbb{Z}_p^*$  יש שורש פרימיטיבי) יש פתרון ל  $x^2 \equiv a \pmod{p}$  כלומר  $a$  שארית ריבועית מודולו  $p$ , ולכן מהגדרה גם  $\left(\frac{a}{p}\right) \equiv 1 \pmod{p}$ . אחרת, בכל מקרה ממשפט פרמה הקטן  $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p}$  ולכן  $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ , ולכן בהכרח  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ . במקרה זה מקריטריון אוילר  $a$  אינה שארית ריבועית, ואכן  $\left(\frac{a}{p}\right) \equiv -1 \pmod{p}$ . ■

### 5.5 טענה תכונות של סימן לז'נדר

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

2. אם  $p \nmid a$  אז  $\left(\frac{a^2}{p}\right) = 1$ .

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

**הוכחה:** 1 ו 2 קל להוכיח, נראה את 3. אם  $p \mid a$  או  $p \mid b$  אז שני האגפים הם אפס. אחרת, נניח  $a, b$  שניהם זרים ל  $p$  אז ממהמסקנה מקריטריון אוילר

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

■

**משפט 5.6** חוק ההדדיות הריבועית יהיו  $p \neq q$  ראשוניים אי זוגיים. אזי

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & p, q \equiv 3 \pmod{4} \end{cases}$$

נספח 1:  $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$  נספח 2:  $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$

**הוכחה:** נתבונן באיברי  $\mathbb{Z}_{pq}^*$ , הם מתחלקים לזוגות של איברים שונים  $\{x, -x\}$ .

נבחר באופן שרירותי נציג אחד מכל זוג, ונכפול את הנציגים מודולו  $pq$  - המכפלה  $P$  מוגדרת ביחידות עד כדי סימן. נעביר את  $P$  דרך האיזומורפיזם  $f: \mathbb{Z}_{pq}^* \rightarrow \mathbb{Z}_p^* \times \mathbb{Z}_q^*$  הנתונה ממשפט השאריות הסיני, ונקבל  $(a, b)$ . בבחירה אחרת של הנציגים, אם מקבלים את המכפלה  $-P$ , הפונקציה תחזיר  $(-a, -b)$ . נחשב:

**חישוב 1:** נבחר את הנציג הקטן ביותר בכל זוג (כמספרים בין 1 ל- $pq$ ), כלומר את הנציגים מבין  $1, 2, \dots, \frac{pq-1}{2}$ . כלומר, ניקח את כל המספרים הללו ונוריד את הכפולות של  $p, q$ :

$$\frac{[1 \cdots (p-1)] \cdot [(p+1) \cdots (2p-1)] \cdots [((\frac{q-1}{2}-1)p+1) \cdots (\frac{q-1}{2}p-1)] \cdots [(\frac{q-1}{2}p+1) \cdots (\frac{q-1}{2}p + \frac{p-1}{2})]}{q \cdot 2q \cdots (\frac{p-1}{2}q)}$$

נעביר את  $P$  הזו דרך  $f$  (כדי לחשב מודולו  $q$  מבצעים תהליך סימטרי, מורידים כפולות  $q$  ואז מחלקים ב- $p$ )

$$P \equiv \frac{(p-1)!^{\frac{q-1}{2}} \cdot (\frac{p-1}{2})!}{q^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})!} \equiv \frac{(p-1)!^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} \pmod{p}$$

$$P \equiv \frac{(q-1)!^{\frac{p-1}{2}}}{\left(\frac{p}{q}\right)} \pmod{q}$$

כלומר, קיבלנו  $f(P) = \left((p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\right)$ .

**חישוב 2:** קודם בחרנו נציגים מבין  $\{x, -x\}$  לפני ההפעלה של  $f$ , עכשיו נבחר נציגים מבין  $\{(a, b), (-a, -b)\}$  אחרי ההפעלה של  $f$ . נבחר את הנציגים  $\{1, 2, \dots, p-1\} \times \{1, 2, \dots, \frac{q-1}{2}\}$  הפונקציה  $f$  שומרת על כפל לכן  $f(P)$  זה בדיוק המכפלה של כל הנציגים שבחרנו, כלומר הקואורדינטות הן

$$\begin{aligned} (1 \cdot 2 \cdots (p-1))^{\frac{q-1}{2}} &\equiv (p-1)!^{\frac{q-1}{2}} \pmod{p} \\ \left(1 \cdot 2 \cdots \frac{q-1}{2}\right)^{p-1} &\equiv \prod_{j=1}^{\frac{q-1}{2}} j^{p-1} \equiv \prod_{j=1}^{\frac{q-1}{2}} j^{\frac{p-1}{2}} \cdot (-j)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \prod_{j=1}^{q-1} j^{\frac{p-1}{2}} \\ &\equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot (q-1)!^{\frac{p-1}{2}} \pmod{q} \end{aligned}$$

ולכן  $f(P) = \left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot (q-1)!^{\frac{p-1}{2}}\right)$

שני החישובים מובילים לאותה תוצאה עד כדי סימן, ולכן אם  $\left(\frac{q}{p}\right) = 1$  אז הסימן זהה ולכן

$$\begin{aligned} (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot (q-1)!^{\frac{p-1}{2}} \\ \implies \left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \end{aligned}$$

ואם  $\left(\frac{q}{p}\right) = -1$  אז הסימן הפוך ולכן  $\left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{p}{q}\right) = -(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

בכל מקרה קיבלנו את חוק ההדדיות הריבועית.

כעת נעבור לנספחים - נספח 1 נובע ישירות מקריטריון אוילר, נותר להוכיח את נספח 2. אכן, מתקיים

$$\begin{aligned} \left(\frac{2}{p}\right) &\equiv 2^{\frac{p-1}{2}} \equiv \frac{2 \cdot 4 \cdot 6 \cdots (p-1)}{1 \cdot 2 \cdot 3 \cdots (\frac{p-1}{2})} = \frac{1 \cdot (-1) \cdot 2 \cdot (-1)^2 \cdot 3 \cdot (-1)^3 \cdots \frac{p-1}{2} \cdot (-1)^{\frac{p-1}{2}}}{1 \cdot 2 \cdot 3 \cdots (\frac{p-1}{2})} \\ &\equiv (-1)^{\sum_{i=1}^{\frac{p-1}{2}} i} \equiv (-1)^{\frac{\frac{p-1}{2}(\frac{p-1}{2}+1)}{2}} \equiv (-1)^{\frac{2(p-1)+p^2-2p+1}{8}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p} \end{aligned}$$

■

## משפט 5.7 שימוש בחוק ההדדיות יש אינסוף ראשוניים שהם 1 מודולו 4.

**הוכחה:** הוכחנו בעבר שיש אינסוף עם 3 מודולו 4, נראה עבור 1.

נניח בשלילה שיש מספר סופי כאלה,  $q_1, \dots, q_r \equiv 1 \pmod{4}$ . נסמן  $Q = (2 \prod_{i=1}^r q_i)^2 + 1$ , אז  $Q \equiv 1 \pmod{4}$ . ניקח  $Q \mid p$  ראשוני כלשהו, הוא בהכרח אי זוגי כי  $Q$  אי זוגי. נניח בשלילה  $p \equiv 1 \pmod{4}$  כלומר  $p = q_i$  עבור  $i$  כלשהו, אז  $q_i \mid Q$ , אבל אז  $Q - (2 \prod_{i=1}^r q_i)^2 = 1$  בסתירה לכך ש  $q_i$  ראשוני. אז בהכרח  $p \equiv 3 \pmod{4}$ , ולכן לפי נספח 1 נובע  $\left(\frac{-1}{p}\right) = -1$  כלומר  $Q - (2 \prod_{i=1}^r q_i)^2 = 1$  אבל  $p \mid Q = (2 \prod_{i=1}^r q_i)^2 + 1$  כלומר  $Q \equiv -1 \pmod{p}$ ,  $(2 \prod_{i=1}^r q_i)^2 \equiv -1 \pmod{p}$  כלומר  $-1$  כן שארית ריבועית מודולו  $p$ , וקיבלנו סתירה. ■

## משפט 5.8 המספרים הראשוניים לסדרות חשבוניות

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x \mid p \equiv a \pmod{N}\}}{\pi(x)} = \frac{1}{\varphi(N)}$$

## 5.2 סימן יעקובי

**הגדרה 5.9 סימן יעקובי** עבור  $p_1 \cdots p_r = m \in \mathbb{N}$  אי זוגי, לכל  $a \in \mathbb{Z}$  נגדיר  $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$ , כאשר באגף שמאל זה סימן יעקובי ובאגף ימין מכפלת סימני לז'נדר.

**הערה 5.10** אם  $\left(\frac{a}{m}\right) = -1$  אז  $a$  לא שארית ריבועית מודולו אחד מה  $p_i$ ים ולכן אינה שארית ריבועית מודולו  $m$ . אבל הכיוון השני לא נכון, כלומר אם  $\left(\frac{a}{m}\right) = 1$  אז  $a$  לא בהכרח שארית ריבועית מודולו  $m$ .

## טענה 5.11 תכונות

1. אם  $a \equiv b \pmod{m}$  אז  $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ .
2. אם  $b$  זר ל  $m$  אז  $\left(\frac{b^2}{m}\right) = 1$ .
3.  $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ .
4. הדדיות ריבועית: אם  $m, n$  אי זוגיים אז  $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) (-1)^{\frac{n-1}{2} \frac{m-1}{2}}$ , וגם הנספחים מתקיימים.

**הוכחה:** נוכיח את חוק ההדדיות הריבועית המוכלל.

**למה:** אם  $m$  אי זוגי,  $m = k_1 \cdots k_\ell$ , אז  $\frac{m-1}{2} \equiv \frac{k_1-1}{2} + \frac{k_2-1}{2} + \cdots + \frac{k_\ell-1}{2} \pmod{2}$ .

**הוכחה:** נסמן  $A_1 = \#\{k_i \equiv 1 \pmod{4}\}$ ,  $A_3 = \#\{k_i \equiv 3 \pmod{4}\}$ .

אם  $k_i \equiv 1 \pmod{4}$  אז  $\frac{k_i-1}{2} \equiv 0 \pmod{2}$ , ואם  $k_i \equiv 3 \pmod{4}$  אז  $\frac{k_i-1}{2} \equiv 1 \pmod{2}$ , ולכן

$$\frac{m-1}{2} \equiv 0 \pmod{2} \iff m \equiv 1 \pmod{4} \iff A_3 \text{ is even} \iff \frac{k_1-1}{2} + \frac{k_2-1}{2} + \cdots + \frac{k_\ell-1}{2} \equiv 0 \pmod{2}$$

כעת, נרשום  $m = p_1 \cdots p_k$ ,  $n = q_1 \cdots q_\ell$  אז

$$\begin{aligned} \left(\frac{m}{n}\right) &= \prod_{i=1}^k \left(\frac{p_i}{n}\right) = \prod_{i=1}^k \prod_{j=1}^\ell \left(\frac{p_i}{q_j}\right) = \prod_{i=1}^k \prod_{j=1}^\ell \left(\frac{q_j}{p_i}\right) (-1)^{\frac{q_j-1}{2} \frac{p_i-1}{2}} = \left(\frac{n}{m}\right) \prod_{i=1}^k \prod_{j=1}^\ell (-1)^{\frac{q_j-1}{2} \frac{p_i-1}{2}} \\ &= \left(\frac{n}{m}\right) (-1)^{\sum_{i=1}^k \sum_{j=1}^\ell \frac{q_j-1}{2} \frac{p_i-1}{2}} = \left(\frac{n}{m}\right) (-1)^{\left(\sum_{i=1}^k \frac{p_i-1}{2}\right) \left(\sum_{j=1}^\ell \frac{q_j-1}{2}\right)} \stackrel{\text{Lemma}}{=} \left(\frac{n}{m}\right) (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \end{aligned}$$

■

## 6 הצפנה ומבחני ראשוניות

### 6.1 הצפנת RSA

תהליך יצירת המפתח הפרטי והפומבי:

1. איילת בוחרת שני ראשוניים גדולים  $p, q$ . נסמן  $N = pq$ .
2. איילת מחשבת את  $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$ .
3. איילת מוצאת מספר  $e$  זר ל  $\varphi(N)$ .
4. איילת מפרסמת את המפתח הפומבי  $(N, e)$ , ושומרת את המפתח הפרטי  $\varphi(N)$ .

תהליך הצפנת הודעה:

1. בועז משיג את המפתח הפומבי של איילת אליה הוא רוצה לשלוח את ההודעה,  $(N, e)$ .
2. בועז מקודד את ההודעה למספר  $1 \leq P < N$ .
3. בועז מחשב את  $C \equiv P^e \pmod{N}$ , ושולח לאיילת.

תהליך פענוח הודעה:

1. איילת מקבלת הודעה  $C$  מבוועז.
2. איילת מחשבת את ההופכי  $d$  של  $e$  מודולו  $\varphi(N)$ .
3. איילת מחשבת את  $P \equiv C^d \pmod{N}$ , זו ההודעה המקורית.

**טענה 6.1 נכונות הפענוח עובד**, כלומר תחת ההגדרות הנ"ל אם  $C \equiv P^e \pmod{N}$  אז  $P \equiv C^d \pmod{N}$ .

**הוכחה:** נניח  $C \equiv P^e \pmod{N}$  ההודעה המוצפנת, מכך ש  $e, d$  הופכיים מודולו  $\varphi(N)$  נובע  $ed \equiv 1 \pmod{\varphi(N)}$ , כלומר  $ed = 1 + k\varphi(N)$  עבור  $k \in \mathbb{Z}$  כלשהו.

אם  $P$  זר ל  $N$ : מתקיים

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k\varphi(N)} \equiv P \cdot (P^{\varphi(N)})^k \equiv P \cdot 1^k \equiv P \pmod{N}$$

אם  $P$  אינו זר ל  $N$ : הסיכוי לכך הוא זניח  $(\frac{1}{p} + \frac{1}{q})$ , לכן לוקחים  $p, q$  גדולים מאוד, אבל הטענה עדיין נכונה. אכן, נניח בה"כ  $q \mid P$ , אז

$$C^d \equiv (P^e)^d \equiv (0^e)^d \equiv 0 \equiv P \pmod{q}$$

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k\varphi(N)} \equiv P \cdot (P^{\varphi(p)})^{\varphi(q)k} \equiv P \pmod{p}$$

כלומר  $C^d \equiv P \pmod{pq}$ , ולכן מכך ש  $p, q$  ראשוניים שונים ובפרט זרים  $C^d - P$  מתחלק ב  $qp$  כלומר  $C^d \equiv P \pmod{pq}$  כלומר מודולו  $N$ , כדרוש. ■



## 6.2 מבחני ראשוניות

נסיון ראשון - מבחן ראשוניות לפי המשפט הקטן של פרמה

בהינתן  $N$ , אם נמצא  $a \in \mathbb{Z}$  זר ל $N$  כך ש $a^{N-1} \not\equiv 1 \pmod{N}$ , אז  $N$  פריק. כזה נקרא עד פרמה עבור  $N$ . אבל יש בעיה - לא לכל  $N$  פריק יש עד פרמה. לכן האלגוריתם לא יעבוד.

**הגדרה 6.2 מספר קרמייקל**  $N$  פריק כך שלכל  $a \in \mathbb{Z}$  זר ל $N$ ,  $a^{N-1} \equiv 1 \pmod{N}$ . לדוגמה, 561.

**משפט 6.3** (ללא הוכחה)  $N$  הוא קרמייקל  $\iff N = p_1 p_2 \cdots p_\ell$  כאשר  $\ell \geq 2$ ,  $p_i$  ראשוניים שונים, וכן  $p_i - 1 \mid N - 1$  לכל  $i$ .

נסיון שני - מבחן Solovay-Strassen לפי קריטריון אוילר

בהינתן  $N$  אי זוגי, אם נמצא  $a \in \mathbb{Z}$  זר ל $N$  כך ש $a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \pmod{N}$ , כזה נקרא עד אוילר-יעקובי של  $N$ .

**הערה 6.4** כל עד פרמה הוא עד אוילר-יעקובי, כי אם הוא לא עד אוילר-יעקובי אז  $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}$  ולכן  $a^{N-1} \equiv \left(\frac{a}{N}\right)^2 \equiv (\pm 1)^2 \equiv 1 \pmod{N}$  כלומר הוא לא עד פרמה.

**משפט 6.5 נכונות** לכל  $N$  פריק אי זוגי יש עד אוילר-יעקובי (לא צריך לדעת להוכיח).

**טענה 6.6** נסמן ב $L_N$  את קבוצת השקרנים עבור  $N$ , כלומר את קבוצת האיברים  $a \in \mathbb{Z}_N^*$  שאינם עדי אוילר-יעקובי עבור  $N$ . אזי  $L_N$  היא תת חבורה של  $\mathbb{Z}_N^*$ .

■ **הוכחה:** לא הקלדתי, לא קשה.

**מסקנה 6.7**  $|L_N| \leq \frac{1}{2} |\mathbb{Z}_N^*|$ .

■ **הוכחה:** מקרה פרטי של לגראנז', לוקחים  $g \in G \setminus H$  ומסתכלים על  $H, gH$ , הן זרות ומגודל שווה.

## 7 הלמה של הנזל

**מוטיבציה - איך ניתן לקבוע אם  $a$  הוא ריבוע מודולו  $N$ ?** נפרק את  $N$  לראשוניים שונים  $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ , אז לפי משפט השאריות הסיני  $a$  ריבוע מודולו  $n \iff a$  ריבוע מודולו  $p_i^{\alpha_i}$  לכל  $i$ . לכן המקרה המעניין הוא לבדוק אם  $a$  ריבוע מודולו  $p^\alpha$ .

**גישה 1:** אם  $p \neq 2$ , ניתן להשתמש בקריטריון אוילר (כי יש ש"פ מודולו  $p^\alpha$ ), ולפיו  $a$  ריבוע מודולו  $p^\alpha \iff a^{\frac{1}{2}\varphi(p^\alpha)} \equiv a^{\frac{\varphi(p^\alpha)}{\gcd(2, \varphi(p^\alpha))}} \equiv 1$ .

**גישה 2:** אם  $a$  ריבוע מודולו  $p^\alpha$ , אז הוא ריבוע מודולו  $p$ .

אם  $\alpha = 2$  ויש פתרון מודולו  $p^2$  הנתון  $a \equiv y^2 \pmod{p^2}$ , אז  $y$  הוא גם פתרון מודולו  $p$ . כלומר, אם נכתוב  $y = bp + y_1$  כאשר  $0 \leq y \leq p^2 - 1$  וכן  $0 \leq b, y_1 \leq p - 1$ , אז  $a \equiv y^2 \equiv (bp + y_1)^2 \equiv y_1^2 \pmod{p}$  כלומר  $a \equiv y_1^2 \pmod{p}$  הוא פתרון מודולו  $p$ .

נניח שמצאנו את  $y_1$  כך ש  $y_1^2 \equiv a \pmod{p}$ , נמצא את  $y$  על ידי כך שנרשום  $y = bp + y_1$  וננסה לפתור את המשוואה

$$\begin{aligned} a &\equiv y^2 \equiv (bp + y_1)^2 \equiv 2bpy_1 + y_1^2 \pmod{p^2} \\ \implies 0 &\equiv 2bpy_1 + \underbrace{(y_1^2 - a)}_{\equiv 0 \pmod{p}} \pmod{p^2} \\ \implies 0 &\equiv 2by_1 + \frac{y_1^2 - a}{p} \pmod{p} \\ \implies b &\equiv \frac{a - y_1^2}{p} \cdot (2y_1)^{-1} \pmod{p} \end{aligned}$$

כאשר המעבר האחרון מתקיים אם  $y_1 \not\equiv 0 \pmod{p}$  וכן  $p \neq 2$ , אם זה לא מתקיים הלמה של הנזל לא עוזרת.

**מסקנה 7.1** יהי  $p \neq 2$  ראשוני. אם  $\left(\frac{a}{p}\right) = 1$  אז  $a$  הוא ריבוע גם מודולו  $p^2$ , ולמעשה מודולו  $p^\alpha$  לכל  $\alpha$ . מכאן נובע **מקרה פרטי של הלמה של הנזל**: יהי  $p \neq 2$  ראשוני,  $a$  זר ל  $p$ ,  $\alpha \geq 2$ , ונניח שיש פתרון למשוואה  $x^2 \equiv a \pmod{p}$ . אז לכל פתרון  $y_1^2 \equiv a \pmod{p}$  יש פתרון יחיד  $y_\alpha^2 \equiv a \pmod{p^\alpha}$  המקיים  $y_\alpha \equiv y_1 \pmod{p}$ , והוא נקרא הרמה של  $y_1$ .

**דוגמה 7.2** נפתור את  $x^2 \equiv 14 \pmod{125}$ . נפתור את  $y_1^2 \equiv 4 \pmod{5}$ , הפתרונות הם 2, 3, נבחר  $y_1 = 2$ . נמצא הרמה מודולו 25: נרשום  $y_2 = 5b + 2$ , אז המשוואה היא  $14 \equiv y_2^2 \equiv 20b + 4 \pmod{25}$  ולכן  $2 \equiv 4b \pmod{5}$ , הפתרון הוא  $b \equiv 3 \pmod{5}$ , ולכן  $y_2 \equiv 17 \pmod{25}$ . נמצא הרמה מודולו 125: נרשום  $y_3 = 25b + 17$ , אז המשוואה היא  $14 \equiv y_3^2 \equiv 850b + 289 \equiv -25b + 39 \pmod{125}$  ולכן  $25b \equiv 25 \pmod{125}$ , כלומר  $b \equiv 1 \pmod{5}$ , ולכן  $y_3 \equiv 42 \pmod{125}$ .

**משפט 7.3 הלמה של הנזל** יהי  $f(x) \in \mathbb{Z}[x]$  פולינום עם מקדמים שלמים,  $p \neq 2$  ראשוני,  $\alpha \geq 2$  (ללא הוכחה). אזי לכל פתרון לא סינגולרי  $y_1$  של  $f(x) \equiv 0 \pmod{p}$  (כלומר  $f(y_1) \equiv 0 \pmod{p}$  אבל  $f'(y_1) \not\equiv 0 \pmod{p}$ ) יש הרמה יחידה  $y_k \in \mathbb{Z}_{p^k}$  כך ש  $y_k \equiv y_1 \pmod{p}$  וכן  $f(y_k) \equiv 0 \pmod{p}$ .

**הערה 7.4** במקרה  $p = 2$ , יש שיטה אחרת: כדי לפתור את  $x^2 \equiv a \pmod{2^k}$  מוצאים פתרון  $x_0$  ל  $x^2 \equiv a \pmod{2}$  ואז לוקחים  $x = x_0 + 2^{k-1}s$  ומציבים. יש פתרון אחד עבור  $k = 1$ , שניים עבור  $k = 2$ , ו-4 ל  $k \geq 3$ .

## 8 שברים משולבים וקירובים דיפונטיים

**טענה 8.1 כתיב עשרוני של ממשיים** כל ממשי ניתן לכתיבה כמספר עשרוני (אולי אינסופי).

יש ייצוג סופי  $\iff$  המספר הוא רציונלי מהצורה  $\frac{p}{2^n \cdot 5^k}$   $\iff$  הייצוג אינו יחיד (לדוגמה  $1 = 0.9999$ ).  
יש ייצוג מחזורי (החל ממקום מסוים)  $\iff$  המספר הוא רציונלי.

### 8.1 שברים משולבים

**הגדרה 8.2 שבר משולב של מספר ממשי** יהי  $\theta \in \mathbb{R}$ , נגדיר  $a_0 = \lfloor \theta \rfloor$ . אם  $a_0 \neq \theta$  (כלומר  $\theta \notin \mathbb{Z}$ ), מתקיים  $0 < \theta - a_0 < 1$ . נסמן  $\theta_1 = \frac{1}{\theta - a_0} > 1$ , אז מתקיים  $\theta = a_0 + \frac{1}{\theta_1}$ , נמשיך רקורסיבית על  $\theta_1, \theta_2, \dots$  עד אינסוף, או עד שנקבל  $\theta_i$  שלם.

הביטוי המתקבל  $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$  נקרא השבר המשולב של  $\theta$ . מסמנים

$$[a_0, a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

**טענה 8.3 ייצוג שברי של שבר משולב** יהיו  $a_0 \in \mathbb{R}, a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}$  נגדיר

$$\begin{aligned} p_0 &= a_0 \\ p_1 &= a_1 a_0 + 1 \\ \forall k \geq 2. p_k &= a_k p_{k-1} + p_{k-2} \\ q_0 &= 1 \\ q_1 &= a_1 \\ \forall k \geq 2. q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

אזי  $[a_0, a_1, \dots, a_k] = \frac{p_k}{q_k}$ .

**הוכחה:** באינדוקציה על  $k$ . עבור הבסיס,

$$\begin{aligned} [a_0] &= a_0 = \frac{a_0}{1} = \frac{p_0}{q_0} \\ [a_0, a_1] &= a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1} \end{aligned}$$

נניח עבור  $k$ , אז

$$[a_0, a_1, \dots, a_{k-1}, a_k, a_{k+1}] = \left[ a_0, a_1, \dots, a_{k-1}, a_k + \frac{1}{a_{k+1}} \right] \stackrel{\text{ind. hyp.}}{=} \frac{p'_k}{q'_k}$$

עבור  $p'_k, q'_k$  המספרים שמתאימים ל  $a_0, a_1, \dots, a_{k-1}, a_k + \frac{1}{a_{k+1}}$ . לכל  $0 \leq i < k$  מתקיים  $p_i = p'_i, q_i = q'_i$ , ולכן

$$\frac{p'_k}{q'_k} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_{k+1} (a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1} (a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

■

**למה 8.4** לכל  $k \in \mathbb{N}$  מתקיים  $\det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$

**הוכחה:** עבור  $k = 1$ ,  $\det \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix} = \det \begin{pmatrix} a_1 a_0 + 1 & a_0 \\ a_1 & 1 \end{pmatrix} = (a_1 a_0 + 1) - a_1 a_0 = 1 = (-1)^{1-1}$ ,  
באינדוקציה, נניח עבור  $k-1$  אז מתכונות דטרמיננטה (לינאריות לפי עמודות, ...)

$$\begin{aligned} \det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} &= \det \begin{pmatrix} a_k p_{k-1} + p_{k-2} & p_{k-1} \\ a_k q_{k-1} + q_{k-2} & q_{k-1} \end{pmatrix} = a_k \underbrace{\det \begin{pmatrix} p_{k-1} & p_{k-1} \\ q_{k-1} & q_{k-1} \end{pmatrix}}_{=0} + \det \begin{pmatrix} p_{k-2} & p_{k-1} \\ q_{k-2} & q_{k-1} \end{pmatrix} \\ &= -\det \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} = -(-1)^{(k-1)-1} = (-1)^{k-1} \end{aligned}$$

■

**מסקנה 8.5** אם  $a_0, \dots, a_k \in \mathbb{Z}$  אז  $p_k, q_k$  זרים.

■

**הוכחה:** אם  $d \mid p_k, q_k$  אז  $d \mid p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$  ולכן  $d = \pm 1$ .

**משפט 8.6** יהי  $\theta \in \mathbb{R}$ . אזי השבר המשולב של  $\theta$  סופי  $\iff \theta$  רציונלי, ואם  $\theta$  אי רציונלי אז

$$\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \lim_{n \rightarrow \infty} [a_0, a_1, \dots, a_n] = \theta$$

**הוכחה:** אם השבר סופי אז  $\theta = [a_0, a_1, \dots, a_n] \in \mathbb{Q}$  (חיבור, מנה של רציונליים), ואם  $\theta$  רציונלי אז תהליך בניית השבר המשולב, שמתבסס על אלגוריתם אוקלידס עבור  $a, b$  כאשר  $\theta = \frac{a}{b}$ , חייב לעצור. כעת נניח כי  $\theta$  אי רציונלי. בסימונים מהגדרת שבר משולב

$$\theta = [a_0, a_1, \dots, a_k, \theta_{k+1}] = \frac{\theta_{k+1} p_k + p_{k-1}}{\theta_{k+1} q_k + q_{k-1}}$$

ולכן

$$\begin{aligned} \left| \theta - \frac{p_k}{q_k} \right| &= \left| \frac{\theta_{k+1} p_k + p_{k-1}}{\theta_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{\theta_{k+1} p_k q_k + p_{k-1} q_k - \theta_{k+1} q_k p_k - p_k q_{k-1}}{q_k (\theta_{k+1} q_k + q_{k-1})} \right| \\ &\stackrel{\text{lemma}}{=} \left| \frac{-(-1)^{k-1}}{q_k (\theta_{k+1} q_k + q_{k-1})} \right| = \frac{1}{q_k (\theta_{k+1} q_k + q_{k-1})} \stackrel{\theta_{k+1} > 1, q_i \geq 1}{<} \frac{1}{q_k^2} \xrightarrow{k \rightarrow \infty} 0 \end{aligned}$$

■ הגבול נובע מכך ש- $q_k = a_k q_{k-1} + q_{k-2}$  וכן  $a_k \geq 1$ , ולכן  $q_k$  זו סדרת טבעיים עולה ממש ולכן  $q_k \rightarrow \infty$ .

**טענה 8.7** יהיו  $p \in \mathbb{Z}, q \in \mathbb{N}, x \in \mathbb{R}$

$$\left\lfloor \frac{p+x}{q} \right\rfloor = \left\lfloor \frac{p + \lfloor x \rfloor}{q} \right\rfloor$$

**משפט 8.8 לגראנז'**  $\alpha \in \mathbb{R}$  הינו בעל ייצוג מחזורי בשברים משולבים, כלומר  $\alpha = [a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+m-1}}]$ , אם ורק אם  $\alpha$  שורש של משוואה ריבועית  $ax^2 + bx + c = 0$  כאשר  $a \neq 0$  וכן  $\Delta = b^2 - 4ac > 0$  לא ריבוע שלם (לא להוכחה).

## 8.2 קירובים דיופנטיים

**מסקנה 8.9** (מהמשפט שלפני לגראנז') לכל  $\theta \in \mathbb{R}$  אי רציונלי יש אינסוף קירובים דיופנטיים שמקיימים  $\left| \theta - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$ . מסקנה זו משפרת את החסם הטריויאלי, שיש קירוב עם  $\left| \theta - \frac{p}{q} \right| \leq \frac{1}{2q}$ .  
כמו כן היא ייחידות לאי רציונליים, כי עבור  $\frac{a}{b} \in \mathbb{Q}$ , אם  $b < q$  אז  $\frac{a}{b} > \frac{1}{q^2} \geq \left| \frac{aq-bp}{bq} \right| = \left| \frac{a}{b} - \frac{p}{q} \right|$ , ויש מספר סופי של אפשרויות עם  $q \leq b$  (כי בהינתן  $q, \frac{a}{b}$ , המספר  $p$  נקבע ביחידות).

**משפט 8.10** הרישיות של  $\frac{p_n}{q_n}$  של הפיתוח של  $\theta \in \mathbb{R}$  לשברים משולבים נותנות את הקירוב הטוב ביותר במובן הבא:

1. **המובן החלש:** לכל  $a, b \in \mathbb{Z}$  כך ש- $1 \leq b < q_n$  מתקיים  $|\theta - \frac{a}{b}| < |\theta - \frac{p_n}{q_n}|$ . כלומר, לא ניתן להגיע לקירוב טוב יותר מבלי להגדיל את המכנה.

2. **המובן החזק:** לכל  $a, b \in \mathbb{Z}$  כך ש- $1 \leq b < q_{n+1}$  מתקיים  $|q_n \theta - p_n| \leq |b \theta - a|$ . תכונה זו היא למעשה קריטריון הכרחי ומספיק לקירובים של  $\theta$ . אכן, בהינתן  $p_n, q_n$ , ניתן להגדיר את  $p_{n+1}, q_{n+1}$  להיות זוג השלמים עם  $q_{n+1}$  מינימלי כך ש- $|q_n \theta - p_n| > |q_{n+1} \theta - p_{n+1}|$ .

**הגדרה 8.11 מספר אלגברי**  $\alpha \in \mathbb{R}$  נקרא אלגברי אם הוא שורש של פולינום  $f \in \mathbb{Z}[x]$  (באופן שקול, שור של  $f \in \mathbb{Q}[x]$ ). אם  $\alpha$  אלגברי, המעלה של  $\alpha$  זו המעלה המינימלית של פולינום כזה ש- $\alpha$  שורש שלו. בנוסף, אם  $\alpha$  אינו אלגברי הוא נקרא טרנסצנדנטי.

**משפט 8.12 ליוביל** לכל  $\alpha \in \mathbb{R}$  אלגברי ממעלה  $d$  יש מספר  $c = c(\alpha) > 0$  כך שלכל רציונלי  $\frac{p}{q} \neq \alpha$  מתקיים  $|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}$ .

**הוכחה:** נפריד למקרים  $d = 1, d \geq 2$ .

אם  $d = 1$ ,  $\alpha$  רציונלי. נניח  $\alpha = \frac{a}{b}$  ונגדיר  $c(\alpha) = \frac{1}{b}$ , אז לכל  $\frac{p}{q} \neq \alpha$  מתקיים

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq} = \frac{c}{q}$$

אם  $d \geq 2$ , יהי  $f = \sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$  כך ש- $f(\alpha) = 0$ . ל- $f$  אין שורשים רציונליים, כי אם  $f(\frac{p}{q}) = 0$  אז  $f(x) = (x - \frac{p}{q})g(x)$  ואז  $g(\alpha) = 0$  ו- $g$  פולינום רציונלי ולכן מעלת  $\alpha$  היא לכל היותר  $d-1$ , סתירה.

הנגזרת  $f'(x)$  חסומה בקטע  $[\alpha-1, \alpha+1]$  ע"י  $M > 0$  (כי היא רציפה וזה קטע קומפקטי). ניקח את המקדם  $c(\alpha) = \min \{1, \frac{1}{M}\}$ , ונראה שלכל  $\frac{p}{q} \in \mathbb{Q}$  מתקיים  $|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}$ . אם  $|\alpha - \frac{p}{q}| \geq 1$  אז  $|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}$  ואם  $|\alpha - \frac{p}{q}| < 1$  אז לפי משפט לגראנז' יש  $x_0$  בין  $\alpha$  ל- $\frac{p}{q}$  שמקיים  $f'(x_0) = \frac{f(\frac{p}{q}) - f(\alpha)}{\frac{p}{q} - \alpha}$ . מתקיים  $f(\alpha) = 0$  וכן

$$0 \neq \left| f\left(\frac{p}{q}\right) \right| = \left| \sum_{i=0}^d a_i \frac{p^i}{q^i} \right| = \frac{1}{q^d} \left| \sum_{i=0}^d a_i q^{d-i} p^i \right| \geq \frac{1}{q^d}$$

ולכן

$$\left| \frac{p}{q} - \alpha \right| = \frac{\left| f\left(\frac{p}{q}\right) \right|}{|f'(x_0)|} \geq \frac{\frac{1}{q^d}}{M} \geq \frac{c}{q^d}$$

כדרוש. ■

**מסקנה 8.13** מספר שניתן לקרב לכל  $d \in \mathbb{N}$  על ידי  $\frac{p}{q}$  כך ש- $|\frac{p}{q} - \theta| < \frac{1}{q^d}$  הוא טרנסצנדנטי. מספרים אלו נקראים **מספרי ליוביל**, ויש טרנסצנדנטיים שאינם מספרי ליוביל (לדוגמה  $(\pi, e)$ ). לדוגמה,

$$\theta = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000100 \dots$$

הוא ליוביל ובפרט טרנסצנדנטי.

## 9 סכומי ריבועים

### 9.1 חוג השלמים של גאוס

**הגדרה 9.1** המספרים של גאוס  $\mathbb{Q}(i) = \{r + is \mid r, s \in \mathbb{Q}\} \subseteq \mathbb{C}$

**טענה 9.2**  $\mathbb{Q}(i)$  הוא תת-שדה של  $\mathbb{C}$ , כלומר הוא מכיל את  $0, 1$ , וסגור לחיבור, חיסור, כפל, והופכי כפלי.

**הוכחה:**  $0, 1 \in \mathbb{Q}(i)$  ברור, נניח  $r, r', s, s' \in \mathbb{Q}$  אז  $(r + is) + (r' + is') = (r + r') + i(s + s')$  והסגירות נובעת מסגירות רציונליים לחיבור. כפל תרגיל, ועבור הופכי נניח  $0 \neq r + is \in \mathbb{Q}(i)$  אז

$$\frac{1}{r + is} = \frac{r - is}{(r + is)(r - is)} = \frac{r - is}{r^2 + s^2} = \frac{r}{r^2 + s^2} + i \cdot \frac{-s}{r^2 + s^2} \in \mathbb{Q}(i)$$

שוב, מכך שהרציונליים הם שדה.

**הערה 9.3**  $\mathbb{Q}(i)$  הוא גם מרחב וקטורי מעל  $\mathbb{Q}$  מממד 2, וזו דוגמה להרחבת שדות ריבועית של  $\mathbb{Q}$ .

**הגדרה 9.4** הצמדה ונורמה לכל  $z = x + iy \in \mathbb{C}$ , הצמוד הוא  $\bar{z} = x - iy$  ומתקיים  $\overline{zw} = \bar{z}\bar{w}$ . כמו כן נגדיר נורמה  $N: \mathbb{C} \rightarrow \mathbb{R}_{\geq 0}$  על ידי  $N(z) = z \cdot \bar{z} = |z|^2$ , היא מקיימת  $N(z) = 0 \iff z = 0$  וכן  $N(zw) = N(z)N(w)$ . **השלמים של גאוס**  $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(i)$

**טענה 9.5**  $\mathbb{Z}[i]$  הוא תת-חוג של  $\mathbb{Q}(i)$  (או של  $\mathbb{C}$ ), כלומר הוא מכיל את  $0, 1$ , וסגור לחיבור, חיסור, וכפל. אבל, הוא אינו תת-שדה (לא סגור להופכי).

**הערה 9.6** נסתכל על הנורמה  $N: \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ , התמונה שלה היא בדיוק כל סכומי הריבועים.

**טענה 9.7** ההפיכים ב- $\mathbb{Z}[i]$  הם  $\pm 1, \pm i$ , כלומר האיברים עם  $N(\alpha) = 1$ .

**הוכחה:** אם  $\alpha\beta = 1$  אז  $1 = N(\alpha\beta) = N(\alpha)N(\beta)$  וכן  $N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}$  לכן שניהם 1.

**טענה 9.8**  $\mathbb{Z}[i]$  הוא חוג אוקלידי, כלומר קיים בו אלגוריתם חלוקה בשארית ביחס לנורמה. משמע, לכל  $\alpha, \beta \in \mathbb{Z}[i]$  עם  $\beta \neq 0$  יש  $q, r \in \mathbb{Z}[i]$  כך ש- $\alpha = q\beta + r$  ובנוסף  $N(r) < N(\beta)$ .

**הוכחה:** מתקיים  $|r|^2 = N(r) < N(\beta) = |\beta|^2$  אם ורק אם  $|r| < |\beta|$ , אם ורק אם  $\left|\frac{r}{\beta}\right| < 1$ . נרשום  $\frac{\alpha}{\beta} = r + is \in \mathbb{Q}(i)$ , נבחר  $\frac{\alpha}{\beta}$  נמצא באיזשהו ריבוע עם קודקודים ב- $\mathbb{Z}[i]$ , נבחר את הקרוב ביותר (נעגל את שתי הקואורדינטות) ונקבל  $q \in \mathbb{Z}[i]$  כך ש- $\left|\frac{r}{\beta} - q\right| \leq \frac{\sqrt{2}}{2} < 1$ , כדרוש.

**מסקנה 9.9** תכונות של החוג  $\mathbb{Z}[i]$  יש  $\gcd$  (יחיד עד כדי כפל בהפיך), מקדמי בזו, אי פריק שקול לראשוני, ויחידות פירוק לראשוניים כפול הפיך עד כדי כפל בהפיך ושינוי סדר הראשוניים.

### 9.2 משפט פרמה-גאוס

**משפט 9.10** אם  $p$  ראשוני וכן  $p \equiv 3 \pmod{4}$  אז  $p$  אי פריק ב- $\mathbb{Z}[i]$ .

**הוכחה:** נניח בשלילה שיש  $\alpha, \beta$  לא הפיכים כך ש- $\alpha\beta = p$ , אז  $N(\alpha)N(\beta) = N(p) = p^2$  וכן  $N(\alpha), N(\beta) > 1$  ולכן  $N(\alpha) = N(\beta) = p$ . לכן  $p$  סכום ריבועים (תמונת  $N$  היא בדיוק כל סכומי הריבועים), אבל זו סתירה לכך ש- $p \equiv 3 \pmod{4}$  (מהכיוון  $\iff$  במשפט הבא, שלא מסתמך על תוצאה זו).

**משפט 9.11** פרמה-גאוס מספר ראשוני  $p$  הוא סכום שני ריבועים  $\iff p \not\equiv 3 \pmod{4}$ .

**הוכחה:**  $\Leftarrow$  למעשה כיוון זה נכון עבור  $n \in \mathbb{N}$  כללי, לא בהכרח ראשוני. אכן, השאריות הריבועיות מודולו 4 הן 0, 1, ולכן סכום של שני ריבועים מודולו 4 הוא אחד מבין  $0+0=0, 0+1=1, 1+1=2$ , כלומר אם  $n$  סכום שני ריבועים אז  $n \not\equiv 3 \pmod{4}$ .

$\Rightarrow$  נניח  $p \equiv 1 \pmod{4}$  ראשוני. רוצים להראות ש  $p$  סכום ריבועים, באופן שקול פריק כאיבר של  $\mathbb{Z}[i]$  (זה שקול כי אם  $p = x^2 + y^2$  סכום ריבועים אז  $p = (x + iy)(x - iy)$  פריק, ובכיוון השני אם הוא פריק אז מהמשפט  $p \equiv 3 \pmod{4}$  בסתירה להנחה). כעת, נניח בשלילה  $p$  אי פריק ב  $\mathbb{Z}[i]$  אז הוא גם ראשוני. נזכר  $\left(\frac{-1}{p}\right) = 1$  כי  $p \equiv 1 \pmod{4}$ , ולכן יש  $x \in \mathbb{Z}$  כך ש  $x^2 \equiv -1 \pmod{p}$ , כלומר  $x^2 + 1 = (x + i)(x - i)$  ולכן  $p \mid x^2 + 1 = (x + i)(x - i)$  כלומר קיים  $m + ni$  כך ש  $p(m + ni) = x + i$  ■  
 אז  $pm + pni = p(m + ni) = x + i$  ■

**מסקנה 9.12** (תרגיל)  $n$  טבעי הוא סכום שני ריבועים  $\iff$  בפירוק לראשוניים  $n = \prod_{i=1}^r p_i^{e_i}$  החזקה של כל  $p_i$  שמקיים  $p_i \equiv 3 \pmod{4}$  היא זוגית.

**טענה 9.13** **אי פריקים ב  $\mathbb{Z}[i]$**  האיברים האי-פריקים היחידים ב  $\mathbb{Z}[i]$  הם  $1 - i$  ראשוניים עם  $p \equiv 3 \pmod{4}$  או  $x \pm iy$  כך שיש ראשוני  $p \equiv 1 \pmod{4}$  כך ש  $p = (x + iy)(x - iy)$ .

**הוכחה:** אם  $\alpha \in \mathbb{Z}[i]$  אי פריק אז  $\alpha \cdot \bar{\alpha} = p_1^{e_1} \cdots p_r^{e_r}$ ,  $\alpha \mid \alpha \cdot \bar{\alpha}$  בפירוק ב  $\mathbb{Z}[i]$  מופיעים רק איברים מהפירוק שכתבנו, ומיחידות הפירוק  $\alpha$  חבר של אחד האי פריקים בפירוק זה. ■

**דוגמה 9.14** נפרק לאי פריקים את  $8 - i \in \mathbb{Z}[i]$ . מתקיים  $8 - i \in \mathbb{Z}[i]$ ,  $N(8 - i) = 65 = 5 \cdot 13$ , נפרק:

$$5 = (2 + i)(2 - i)$$

$$13 = (2 + 3i)(2 - 3i)$$

בדיוק אחד מבין  $2 + i, 2 - i$  בפירוק של  $8 - i$ , במקרה הזה זה  $2 + i$  (מחלקים ובודקים אם יוצא שלם גאוס). בדיוק אחד מבין  $2 + 3i, 2 - 3i$  בפירוק של  $8 - i$ , במקרה הזה  $2 + 3i$ . נחשב  $(2 + i)(2 + 3i) = 1 + 8i$ , ואם מכפילים ב  $-i$  (הפיך) מקבלים בדיוק את הדרוש.

## 10 הרחבות ריבועיות

**הגדרה 10.1 הרחבה ריבועית** (לא לגמרי חלק מהקורס) תת שדה של  $\mathbb{C}$  (שמכיל את  $\mathbb{Q}$ , אבל זה נכון לכל תת שדה) וכמרחב וקטורי מעל  $\mathbb{Q}$  הוא דו-מימדי. לדוגמה, ראינו את  $\mathbb{Q}(i)$ .

**טענה 10.2** (תרגיל) השדות הללו הם בדיוק מהצורה  $\mathbb{Q}(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\}$  עבור  $d \in \mathbb{Z}$  שאינו ריבוע.

### 10.1 הרחבות ריבועיות דמיוניות וממשיות

#### הרחבות ריבועיות דמיוניות

הרחבה ריבועית כאשר  $d < 0$ , לדוגמה עבור  $d = -1$  מקבלים את  $\mathbb{Q}(i)$ .

**הגדרה 10.3 צמוד** הצמוד המרוכב  $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$

**נורמה**  $N(z) = z\bar{z} = x^2 - dy^2 = |z|^2$

**טענה 10.4 ההפיכים** ב  $\mathbb{Z}[\sqrt{d}]$  הם כל האיברים עם  $N(z) = 1$ .

**הערה 10.5** כדי למצוא את ההפיכים צריך לפתור את  $x^2 - dy^2 = 1$ , אם  $d = -1$  אז  $\alpha = \pm 1, \pm i$  ואם  $d \leq -2$  אז  $y = 0$  (כי  $-d \geq 2$ ) ולכן  $\alpha = \pm 1$ .

#### הרחבות ריבועיות ממשיות

הרחבה ריבועית כאשר  $d > 0$ , לדוגמה עבור  $d = 2$  מקבלים את  $\mathbb{Q}(\sqrt{2})$ .

**הגדרה 10.6 צמוד** הצמוד האלגברי של  $\alpha$  מוגדר  $\tilde{\alpha} = r - s\sqrt{d}$

**נורמה** (כעת עשויה להיות שלילית, אבל היא עדיין כפלית)  $N(\alpha) = \alpha\tilde{\alpha} = r^2 - ds^2$

**טענה 10.7**  $\tilde{\alpha}\tilde{\beta} = \tilde{\alpha\beta}$ ,  $\alpha + \tilde{\beta} = \tilde{\alpha} + \beta$ ,  $N(\alpha\beta) = N(\alpha)N(\beta)$  **ההפיכים** ב  $\mathbb{Z}[\sqrt{d}]$  הם כל האיברים עם  $N(z) = \pm 1$ , באופן שקול הפתרונות של המשוואה  $x^2 - dy^2 = \pm 1$ , שנקראת משוואת פל.

**הערה 10.8** לכל  $\alpha \in \mathbb{Q}(\sqrt{d})$  מתקיים  $0 \neq \alpha \in \mathbb{Q}(\sqrt{d})$  אחרת  $x^2 - dy^2 = 0$  ולכן  $\sqrt{d} = \frac{x}{y}$  אבל  $\sqrt{d}$  אינו רציונלי.

### 10.2 משוואת פל

**הערה 10.9** פתרונות משוואת פל מתאימים לאיברים ההפיכים ב  $\mathbb{Z}[\sqrt{d}]$ , ולכן יש להם מבנה של חבורה, כאשר הכפל הוא

$$(x, y) \cdot (a, b) = (ax + byd, ay + bx)$$

קבוצת הפתרונות סגורה לכפל, יש בה איבר יחידה  $(1, 0)$  והופכי לכל איבר.

**מסקנה 10.10** אם יש פתרון לא טריויאלי, כלומר לא  $(\pm 1, 0)$ , אז יש אינסוף פתרונות.

**הוכחה:** אם  $\pm 1 \neq x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$  הפיך, בה"כ ניתן להניח  $x \geq 0, y \geq 1$  ואז  $x + y\sqrt{d} > 1$  ואז

$$(x + y\sqrt{d})^n \xrightarrow{n \rightarrow \infty} \infty$$

וכל חזקה כזו מהווה פתרון, כי זו חבורה. ■

**למה 10.11**  $(x, y)$  פתרון חיובי  $\iff x + y\sqrt{d} > 1$



**הוכחה:** אם  $x, y > 0$  אז  $x + y\sqrt{d} > 1$ , אז  $x < 0, y < 0$  אז  $x + y\sqrt{d} < -1$  ואם  $x > 0, y < 0$  אז  $\frac{1}{\alpha} = \frac{\bar{\alpha}}{N(\alpha)} = \pm \tilde{\alpha} = \pm (x - y\sqrt{d})$  ובביטוי הנ"ל  $x, -y$  שווים סימן, ולכן  $-1 < \alpha < 1$ . ■

**משפט 10.12** לכל  $d > 0$  לא ריבוע יש פתרון לא טריויאלי למשוואת פל.

**הוכחה: למה:** קיים  $k \in \mathbb{Z}$  כך שיש אינסוף פתרונות בשלמים ל  $x^2 - dy^2 = k$ .

**הוכחה:**  $\sqrt{d} \notin \mathbb{Q}$ , לכן יש לו אינסוף קירובים דיופנטיים  $\left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{y^2}$ . עבור קירוב כזה

$$|x^2 - dy^2| = y^2 \left| \left( \frac{x}{y} \right)^2 - d \right| = y^2 \left| \frac{x}{y} - \sqrt{d} \right| \cdot \left| \frac{x}{y} + \sqrt{d} \right| < \frac{x}{y} + \sqrt{d} \leq 1 + 2\sqrt{d}$$

לכן לכל  $x, y > 0$  שמקיימים  $\left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{y^2}$  מתקיים  $|x^2 - dy^2| < 1 + 2\sqrt{d}$ ,  $\mathbb{Z} \ni$  יש מספר סופי של אפשרויות לכן אינסוף מבין ה  $(x, y)$  ים מקבלים אותו ערך.

נחזור להוכחת המשפט. עבור  $k$  זה, יש אינסוף פתרונות לכן ניתן למצוא שני פתרונות שונים  $\alpha_1 = x_1 + y_1\sqrt{d}, \alpha_2 = x_2 + y_2\sqrt{d}$  ששקולים מודולו  $k$ , כלומר  $x_1 \equiv x_2 \pmod{k}, y_1 \equiv y_2 \pmod{k}$ . נניח בה"כ  $\alpha_2 > \alpha_1$  ונראה ש  $\frac{\alpha_2}{\alpha_1}$  פתרון חיובי, שלם, לא טריויאלי ל  $x^2 - dy^2 = 1$ .

**פתרון:** מכפלות הנורמה  $N\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{N(\alpha_2)}{N(\alpha_1)} = \frac{k}{k} = 1$ . **חיובי ולא טריויאלי:**  $\frac{\alpha_2}{\alpha_1} > 1$  כי  $\alpha_2 > \alpha_1$ .

**שלם:** מתקיים  $\frac{\alpha_2}{\alpha_1} = \frac{\alpha_2 \bar{\alpha}_1}{\alpha_1 \bar{\alpha}_1} = \frac{\alpha_2 \bar{\alpha}_1}{k} = \frac{(x_1 x_2 - y_1 y_2 d) + \sqrt{d}(x_1 y_2 - x_2 y_1)}{k}$  והמונה מתחלק ב  $k$  כי

$$(x_1 x_2 - y_1 y_2 d) + \sqrt{d}(x_1 y_2 - x_2 y_1) \equiv (x_1 x_1 - y_1 y_2 d) + \sqrt{d}(x_1 y_1 - x_1 y_1) \equiv k + 0 \equiv 0 \pmod{k}$$

ולכן  $\frac{\alpha_2}{\alpha_1} \in \mathbb{Z}[\sqrt{d}]$  כדרוש. ■

**מסקנה 10.13** יש פתרון  $(x, y)$  עם  $x + y\sqrt{d} > 0$ .

כמו כן יש פתרון מינימלי מעל 1,  $1 < \varepsilon_d = x_1 + y_1\sqrt{d}$ .

**הוכחה:** הראשון כי יש פתרון חיובי, והשני כי אם  $x + y\sqrt{d}$  פתרון חיובי אז יש מספר סופי של פתרונות בקטע  $(1, x + y\sqrt{d})$  ולכן יש ביניהם מינימלי. ■

**משפט 10.14** הפתרונות של משוואת פל הם  $\{\pm \varepsilon_d^n \mid n \in \mathbb{Z}\}$ .

**הוכחה:** לכל פתרון  $(x, y)$  מתאים פתרון חיובי על ידי שינוי סימן  $\alpha = x + y\sqrt{d}$ . כעת קיים  $n \in \mathbb{Z}$  כך ש  $\varepsilon_d^n \leq \alpha < \varepsilon_d^{n+1}$  ואז  $1 \leq \frac{\alpha}{\varepsilon_d^n} < \varepsilon_d$  פתרון כי הוא הפיך. ממינימליות  $\varepsilon_d$  נובע  $\frac{\alpha}{\varepsilon_d^n} = 1$  כלומר  $\alpha = \varepsilon_d^n$ , ולכן הפתרון המקורי הוא  $\pm \varepsilon_d^n$ . ■