הגדרה: נאמר ש $c \in \mathbb{Z}^+$ הוא **מכפלה משותפת** של $a, b \in \mathbb{Z}$ אם $a \mid c$ ו $b \mid c$.

הגדרה: $\boldsymbol{lcm}$ (מכפלה משותפת המינמלית) של שני מספרים שלמים a, b תסומן ע"י $lcm(a,b)$ ומקיימת:

1. $a \mid lcm(a,b)$ ו $b \mid lcm(a,b)$
2. $\forall c \in \mathbb{Z}$ כך ש $a \mid c$ ו $b \mid c$ אזי $c \geq lcm(a,b)$

משפט: עבור כל $a, b \in \mathbb{Z}$ מתקיים כי $lcm(a,b) \cdot (a,b) = a \cdot b$

מכפלה משותפת **מינמלית** — מחלק משותף **מקסמלי**

לדוגמא: $lcm(8,6) = \frac{8 \cdot 6}{(8,6)} = \frac{48}{2} = 24$

ואכן $\min\{8,16,\mathbf{24},32,40,48,\dots\} \cap \{6,12,18,\mathbf{24},30,36,42,48\} = 24$

קבוצת **המכפלות** של 8 — קבוצת **המכפלות** של 6

מספר ריבועי: יהא $n \in \mathbb{Z}$ אזי n הוא מספר ריבועי אם קיים $a \in \mathbb{Z}$ כך ש $n = a^2$

מספר חופשי מריבועים: יהא $n \in \mathbb{Z}$ אזי n הוא מספר חופשי מריבועים אם **לא** קיים $1 < a \in \mathbb{Z}$ כך ש $a^2 \mid n$

תרגיל 1 :

1. יהא $a = q_1 \cdot q_2 \cdot \dots \cdot q_t$ כאשר $\forall i \in [t]$ אזי q_i הינו מספר ראשוני.
   הוכח או הפרך האם a הוא חופשי מריבועים
2. השלימו את הטענה הבאה :
   כל מספר ריבוע הוא מהצורה _____, _____, $5k$ עבור $k \in \mathbb{Z}$
3. הוכח או הפרך:
   כל שלם $n \geq 1$ יכול להכתב בצורה $n = a \cdot b$ כאשר a חופשי מריבועים ו b הינו מספר שלם

פתרון:

1. נניח בשלילה ש– a אינו חופשי מריבועים, ולכן קיים $1 < b \in \mathbb{Z}$ כך ש $b^2 \mid a$. נשים לב כי $b > 1$ ולכן לפי המשפט היסודי של האריתמטיקה נוכל לכתוב את b ככפולה של מספרים ראשוניים, ולכן :

$$b = p_1^{a_1} \cdot \dots \cdot p_k^{a_k} \quad : \quad \forall i \in [k]: \ p_i \ is \ prime, a_i > 0$$

ולכן $b^2 = p_1^{2a_1} \cdot \dots \cdot p_k^{2a_k}$

לפי ההנחה, $b^2 \mid a$ ולכן a מכיל את כל הגורמים הראשוניים של b^2, אבל כל הגורמים הראשוניים של a הם ממעלה 1 בדיוק, ולכן הגענו לסתירה.

2. יהא n מספר ריבועי, ולכן לפי הגדרה $n = a^2$ עבור $a \in \mathbb{Z}$:

לפי משפט החלוקה, a יכול להיות באחת מהצורות $\{5k, 5k+1, 5k+2, 5k+3, 5k+4\}$ ולכן נחלק למקרים:

- $a = 5k$ אזי $a^2 = (5k)^2 = 25k^2 = 5 \cdot (5k^2)$ ולכן n מהצורה $\boldsymbol{5k}$
- $a = 5k+1$ אזי $a^2 = (5k+1)^2 = 25k^2 + 10k + 1 = 5 \cdot (5k^2 + 2k) + 1$ ולכן n מהצורה $\boldsymbol{5k+1}$

- $a = 5k + 2$ אזי $a^2 = (5k+2)^2 = 25k^2 + 20k + 4 = 5 \cdot (5k^2 + 4k) + 4$ ולכן n מהצורה $\mathbf{5k + 4}$
- $a = 5k + 3$ אזי $a^2 = (5k+3)^2 = 25k^2 + 30k + 9 = 5 \cdot (5k^2 + 6k + 1) + 4$ ולכן n מהצורה $\mathbf{5k + 4}$
- $a = 5k + 4$ אזי $a^2 = (5k+4)^2 = 25k^2 + 40k + 16 = 5 \cdot (5k^2 + 8k + 3) + 1$ ולכן n מהצורה $\mathbf{5k + 1}$

קבלנו כי סה"כ n יכול להיות באחת מהצורות $\{5k, 5k+1, 5k+4\}$

3. הטענה נכונה, יהא פירוק ראשוני של n מהצורה :

$$n = (p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}) \cdot (q_1^{b_1} \cdot \ldots \cdot q_t^{b_t})$$

כך $\forall i \in [k]:\ p_i \text{ is prime}, a_i \text{ is even}$ ו $\forall i \in [t]:\ q_i \text{ is prime}, b_i \text{ is odd}$ ולכן $a_i = 2a_i'$ עבור $a_i' \in \mathbb{Z}$ עבור כל $i \in [k]$ ו $b_i = 2b_i' + 1$ עבור $b_i' \in \mathbb{Z}$ עבור כל $i \in [t]$ ולכן נוכל לשכתב את n באופן הבא:

$$\begin{aligned} n &= (p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}) \cdot (q_1^{b_1} \cdot \ldots \cdot q_t^{b_t}) = \left(p_1^{2a_1'} \cdot \ldots \cdot p_k^{2a_k'}\right) \cdot \left(q_1^{2b_1'+1} \cdot \ldots \cdot q_t^{2b_t'+1}\right) \\ &= \left(p_1^{2a_1'} \cdot \ldots \cdot p_k^{2a_k'} \cdot q_1^{2b_1'} \cdot \ldots \cdot q_t^{2b_t'}\right) \cdot (q_1 \cdot \ldots \cdot q_t) \\ &= \left(p_1^{a_1'} \cdot \ldots \cdot p_k^{a_k'} \cdot q_1^{b_1'} \cdot \ldots \cdot q_t^{b_t'}\right)^2 \cdot (q_1 \cdot \ldots \cdot q_t) \end{aligned}$$

מספר ריבועי

חופשי מריבועים לפי סעיף א'

תרגיל 2:

הוכח או הפרך

קיים n_0 כך שלכל $n \geq n_0$ יכול להכתב כסכום של שני מספרים פריקים

פתרון:

נסתכל על שני מקרים, מקרה ראשון כאשר n הינו מספר זוגי ומקרה שני הינו המקרה המשלים, כלומר המקרה שבו n הינו מספר אי זוגי.

- אם n זוגי אזי $n = 2k$ עבור $k \in \mathbb{Z}$ ולכן :
$$\begin{aligned} n &= 2k \\ &= 2(k-1) + 2 \\ &= 2(k-2) + 4 \end{aligned}$$
נשים לב כי במקרה זה, עבור $k \geq 4$ נקבל כי n הוא סכום של שני מספרים פריקים ו $n_0 = 8$ –
- אם n אי זוגי אזי $n = 2k + 1$ עבור $k \in \mathbb{Z}$ ולכן :
$$\begin{aligned} n &= 2k + 1 \\ &= 2(k-1) + 3 \\ &= 2(k-2) + 5 \\ &= 2(k-3) + 7 \\ &= 2(k-4) + 9 \end{aligned}$$
נשים לב כי במקרה זה, עבור $k \geq 6$ נקבל כי n הוא סכום של שני מספרים פריקים ו $n_0 = 13$ –

ולכן עבור $n_0 = \max(13,8) = 13$ אזי לכל $n \geq n_0$ יכול להכתב כסכום של שני מספרים פריקים

תרגיל 3:

יהי $p_1, p_2, \dots, p_n$ n המספרים הראשוניים ויהי $k \in [1,n]$. נגדיר :

$$Q \coloneqq p_1 \cdot p_2 \cdot \dots \cdot p_k$$

$$R \coloneqq p_{k+1} \cdot p_{k+2} \cdot \dots \cdot p_n$$

1. הוכיחו כי לכל $i \in [n]$ מתקיים כי $p_i \nmid Q + R$
2. העזרו בסעיף א' על מנת לתת הוכחה לכך שיש אינסוף ראשוניים.

פתרון:

1. יהי p_i ראשוני כלשהו כך ש $i \in [1,n]$, נניח בה"כ כי $p_i \in [p_{k+1}, p_n]$

$p_i \nmid Q$ ו $p_i \mid R$

נניח בשלילה כי $p_i \mid Q + R$ ולכן לפי תכונות חלוקה מתקיים כי $p_i \mid Q + R - R = Q$ בסתירה לכך ש $p_i \nmid Q$

2. נניח בשלילה ש $p_1, \dots, p_n$ הינם כל הראשוניים בעולם, מכוון ש 2,3 ראשוניים נקבל כי $n \geq 2$ ולכן קיים $k \in [1.n]$ כך ש :

$$Q \coloneqq p_1 \cdot p_2 \cdot \dots \cdot p_k$$

$$R \coloneqq p_{k+1} \cdot p_{k+2} \cdot \dots \cdot p_n$$

היות ו $Q + R$ גדול מכל הראשוניים נובע שהוא מספר פריק, כי אם אחרת, הוא דוגמא נגדית עצמאית להמצאות ראשוני נוסף.

לפי ההנחה $Q + R$ פריק ולכן קיים מחלק ראשוני q כך ש $q \mid Q + R$ ולכן לפי לפי סעיף א' מתקיים כי $q \neq p_i$ עבור כל $i \in [1,n]$ ולכן $q \notin \{p_1, \dots, p_n\}$ בסתירה לכך שהקבוצה $\{p_1, \dots p_n\}$ היא קבוצת כל הראשוניים בעולם.

תרגיל 4:

1. עבור $a, b, n \in \mathbb{Z}^+$ הוכיחו כי $(a^n, b^n) = (a, b)^n$
2. עבור $a, b, n \in \mathbb{Z}^+$ הוכיחו כי $lcm(a^n, b^n) = lcm(a, b)^n$

פתרון:

1. יהי $d = (a, b)$ ולכן $a = dk_1$ ו-$b = dk_2$ עבור $k_1, k_2 \in \mathbb{Z}$ כך שמתקיים $(k_1, k_2) = 1$

(לפי טענת עזר 1)

כלומר, k_1 ו-k_2 לא חולקים גורמים ראשוניים משותפים (לפי פירוק לגורמים לראשוניים), ולכן גם $(k_1^n, k_2^n) = 1$. נשים לב:

$$(a^n, b^n) = (d^n k_1^n, d^n k_2^n)$$

$$= d^n (k_1^n, k_2^n) \quad \text{(לפי טענת עזר 2)}$$

$$= d^n$$

$$= (a, b)^n$$

2.

$$\forall a, b \in \mathbb{Z}: (a, b) \cdot lcm(a, b) = a \cdot b$$

ולכן

$$lcm(a^n, b^n) = \frac{a^n b^n}{(a^n, b^n)}$$

לפי הסעיף הקודם מתקיים

$$\frac{a^n b^n}{(a^n, b^n)} = \frac{a^n b^n}{(a, b)^n}$$

ובנוסף מתקיים

$$\frac{a^n b^n}{(a, b)^n} = \left(\frac{ab}{(a, b)}\right)^n$$
$$= lcm(a, b)^n$$

שזה מה שצריך להוכיח.

<u>טענת עזר 1:</u>

אם $d = (a, b)$ אז $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

<u>הוכחה:</u>

<u>דרך ראשונה – לפי משפט בז'ו</u>

ידוע כי $d = (a, b)$ ולכן קיימים $m, n \in \mathbb{Z}$ לפי בז'ו כך ש $d = ma + nb$.

היות ו-d מחלק משותף מקסימלי של a, b מתקיים בפרט כי $d \mid a$ ו-$d|b$ ולכן ניתן לחלק ב-d ולהישאר עם מספרים שלמים:

$$d = ma + nb$$
$$1 = m\left(\frac{a}{d}\right) + n\left(\frac{b}{d}\right)$$

ולכן קיבלנו כי 1 הוא קומבינציה ליניארית של $\left(\frac{a}{d}\right), \left(\frac{b}{d}\right)$. בנוסף מתקיים כי 1 הוא איבר מינימלי ב-$\mathbb{Z}^+$ ולכן 1 הוא ה-gcd המבוקש.

<u>דרך שנייה – תכונות חלוקה</u>

יהי $e > 0$ מחלק משותף של $\frac{a}{d}$ ו-$\frac{b}{d}$. ולכן מתקיים כי $\left(\frac{a}{d}\right) = ek$ וגם $\left(\frac{b}{d}\right) = eq$ עבור $q, k \in \mathbb{Z}$. לכן מתקיים $a = edk, b = edq$, נקבל כי $ed \mid a$ וגם $ed \mid b$ אבל ידוע כי d הוא המחלק המשותף המקסימאלי של $\left(\frac{a}{d}\right), \left(\frac{b}{d}\right)$ ולכן מתקיים כי $d \leq ed$. ולכן קיבלנו בהכרח $e = 1$.

<u>טענת עזר 2:</u>

$$(ca, cb) = c(a, b)$$

<u>הוכחה:</u>

יהי $d = (ca, cb)$ ו-$e = (a, b)$. נראה כי $ce \mid d$ וכי $d \mid ce$ ולכן $d = ce$.

<u>כיוון ראשון:</u> משום ש-$e \mid a$ ו-$e \mid b$ נקבל כי $ce \mid ca$ וכי $ce \mid cb$ ולכן $ce \mid d$ (כי d הוא המחלק המשותף המקסמלי של ca ו-cb).

<u>כיוון שני:</u> לפי משפט בז'ו $e = am + bn$ עבור $m, n \in \mathbb{Z}$, ולכן $ce = cam + cbn$. ידוע כי $d \mid ca$ וכי $d \mid cb$, ולכן $d \mid cam + cbn = ce$.

הוכחנו כי $ce \mid d$ וכי $d \mid ce$ ולכן $d = ce$, כלומר $(ca, cb) = c(a, b)$.