שאלה 1

שאלה 1 (10 נקודות)

יהי $x \in \mathbf{Z}$. הוכיחו כי $x \equiv 2025 \pmod{2026}$ וגם $x \equiv 2026 \pmod{2025}$

אם ורק אם: $x \equiv 2025 + 2026 \pmod{2025 \cdot 2026}$

מומלץ להיעזר בלמה 3.15 או שאלות 3.10 ו־3.11, גם כאן וגם בשאלה 3, ובכל מקום שאפשר.

כיוון 1

נתון:

$$x \equiv 2025 + 2026 \pmod{2025 \cdot 2026}$$

לפי הגדרה `3.6` נקבל:

$$2025 \cdot 2026 | x - 2025 - 2026$$

כלומר, לפי הגדרה `2.2` קיים $n \in \mathbb{Z}$ כאשר:

$$2025 \cdot 2026 \cdot n = x - 2025 - 2026$$

ביטוי זה שקול ל2 הביטויים האלה:

$$2025 \cdot (2026 \cdot n + 1) = x - 2026$$

$$2026 \cdot (2025 \cdot n + 1) = x - 2025$$

ולכן קיימים $k_1, k_2 \in \mathbb{Z}$ כאשר:

$$2025 * k_1 = x - 2026$$

$$2026 * k_1 = x - 2025$$

ונקבל:

$$2025 | x - 2026$$

$$2026 | x - 2025$$

ולפי הגדרה `3.6` :

$$x \equiv 2026 \pmod{2025}$$

$$x \equiv 2025 \pmod{2026}$$

מש"ל

כיוון 2

נתון:

$$x \equiv 2026 \pmod{2025}$$
$$x \equiv 2025 \pmod{2026}$$

לפי הגדרה `3.6` :

$$2025 | x - 2026$$
$$2026 | x - 2025$$

לפי שאלה `2.8` ניתן לטעון כי מתקיים:

$$2025 \cdot 2026 | 2026x - 2026^2$$
$$2026 \cdot 2025 | 2025x - 2025^2$$

לפי למה `2.3` נחסיר את הביטוי השני מהראשון
ונקבל:

$$2025 \cdot 2026 | x - (2026^2 - 2025^2)$$

לפי הגדרה `3.6` נקבל:

$$x \equiv (2026^2 - 2025^2) \pmod{2025 \cdot 2026}$$

כלומר,

$$x \equiv (2026 - 2025)(2026 + 2025) \pmod{2025 \cdot 2026}$$
$$x \equiv (2026 + 2025) \pmod{2025 \cdot 2026}$$

מש"ל

שאלה 2

שאלה 2 (15 נקודות)

יהיו a ו־b מספרים טבעיים. הוכיחו כי אם $(a,b)=1$ אז $(a+b,a-b)\in\{1,2\}$.

נגדיר $a, b \in \mathbb{N}$ כאשר $(a, b) = 1$
נניח בשלילה כי מתקיים $(a + b, a - b) \notin \{1, 2\}$
לכן נקבל כי קיים $(a + b, a - b) = m > 2$.
כלומר, קיימים $k_1, k_2 \in \mathbb{N}$ כאשר:

$$a + b = mk_1, a - b = mk_2$$

לכן (מחיסור משוואות):

$$2b = m(k_1 - k_2)$$

ונקבל:

$$b = \frac{1}{2}m(k_1 - k_2)$$

וכן נקבל:

$$b = \frac{1}{2}m(k_1 - k_2), a = \frac{1}{2}m(k_1 + k_2)$$

לכן, נקבל כי אם m זוגי אזי יש להם גורם משותף גדול או שווה ל-2, ואם m אי זוגי (אזי $k_1 + k_2$ מספר זוגי (וכך גם $(k_1 - k_2$)), אז יש להם גורם אי זוגי גדול מ2.
בשני המקרים, זו סתירה לטענה ש $(a, b) \neq 1$
לכן הטענה נכונה
מש"ל

שאלה 3

שאלה 3 (15 נקודות)

יהי k מספר שלם. הוכיחו כי $k^5 \equiv k \pmod{30}$.

$$k^5 \equiv k \pmod{30}$$

לפי הגדרה `3.6` נקבל כי הטענה שקולה לכך:

$$30 | k^5 - k$$

אראה תחילה כי טענה זו מתקיימת לכל $k \in \mathbb{N}$.
אראה זאת בעזרת אינדוקציה.
כאשר $k = 1$, הטענה מתקיימת:

$$1^5 \equiv 1 \pmod{30} \iff 1 \equiv 1 \pmod{30}$$

נניח כי הטענה נכונה עבור $k = n$ כאשר $n \in \mathbb{N}$.
אראה כי הטענה מתקיימת גם עבור $k = n + 1$.
על פי הנחת האינדוקציה, נקבל כי:

$$30 | n^5 - n$$

אראה כי מתקיים גם:

$$30 | (n + 1)^5 - (n + 1)$$

נסתכל על הביטוי:

$$\begin{aligned}
&(n+1)^5-(n+1)\\
&=(n^2+2n+1)(n+1)^3-(n+1)\\
&=(n^3+3n^2+3n+1)(n+1)^2-(n+1)\\
&=(n^4+4n^3+6n^2+4n+1)(n+1)-(n+1)\\
&=n^5+5n^4+10n^3+10n^2+5n+1-n-1\\
&=(n^5-n)+(5n^4+10n^3+10n^2+5n)=(n+1)^5-(n+1)
\end{aligned}$$

אראה כי לכל $k\in\mathbb{Z}$ מתקיים

$$30|5n^4+10n^3+10n^2+5n$$

בעזרת חילוק ב5, ניתן לראות כי:

$$30|5n^4+10n^3+10n^2+5n \iff 6|n^4+2n^3+2n^2+n$$

נסתכל על הביטוי

$$\begin{aligned}
&n^4+2n^3+2n^2+n\\
&=n(n^3+2n^2+2n^1+1)\\
&=n(n+1)(n^2+n+1)\\
&=(n^2+n)(n^2+n+1)
\end{aligned}$$

ולכן אראה כי

$$6|(n^2+n)(n^2+n+1)$$

נסתכל על הביטוי

$$n^2+n$$

נפריד אותו ל-2 אפשרויות - זוגי ואי זוגי:

זוגי: $n=2m, m\in\mathbb{Z}$:

$$n^2+n=4m^2+2m=2(2m^2+m)$$

וקיבלנו מספר זוגי.

אי זוגי: $n=2m+1, m\in\mathbb{Z}$:

$$n^2+n=4m^2+2m+1+2m+1=2(2m^2+m+1)$$

ולכן קיבלנו גם כאן מספר זוגי.

לכן הביטוי n^2+n הוא תמיד זוגי.

לכן, מתקיים לכל $n\in\mathbb{Z}$:

$$\frac{n^2+n}{2} \in \mathbb{Z}$$

ולכן, מתקיים:

$$6|(n^2+n)(n^2+n+1) \iff 6|\left(2 \cdot \frac{n^2+n}{2}(n^2+n+1)\right)$$

ונקבל שזה שקול לביטוי:

$$3|\left(\frac{n^2+n}{2}(n^2+n+1)\right)$$

נפריד את n לשלוש אפשרויות:

אפשרות 1: $n=3m$ כאשר $m \in \mathbb{Z}$
נקבל:

$$3|\left(\frac{9m^2+3m}{2}(9m^2+3m+1)\right)$$

כלומר:

$$3|3\left(\frac{3m^2+1m}{2}(9m^2+3m+1)\right)$$

לפי שאלה `2.8` הביטוי הוא פסוק אמת.

אפשרות 2: $n=3m+1$ כאשר $m \in \mathbb{Z}$
נקבל:

$$3|\left(\frac{9m^2+6m+1+3m+1}{2}(9m^2+6m+1+3m+1+1)\right)$$

כלומר,

$$3|\left(\frac{9m^2+9m+2}{2}(9m^2+9m+3)\right)$$

ולכן הביטוי שקול לביטוי:

$$3|3\left(\frac{9m^2+9m+2}{2}(3m^2+3m+1)\right)$$

לפי שאלה `2.8` הביטוי הוא פסוק אמת.

אפשרות 3: $n=3m+2$ כאשר $m \in \mathbb{Z}$
נקבל:

$$3|\left(\frac{9m^2+12m+4+3m+2}{2}(9m^2+12m+4+3m+2+1)\right)$$

כלומר,

$$3|\left(\frac{9m^2+15m+6}{2}(9m^2+15m+7)\right)$$

ונקבל,

$$3|3\left(\frac{3m^2+5m+2}{2}(9m^2+15m+7)\right)$$

לפי שאלה `2.8` הביטוי הוא פסוק אמת.

לכן, בכל האפשרויות, הביטוי הוא פסוק אמת, ולכן,
מתקיים:

$$3|\left(\frac{n^2+n}{2}(n^2+n+1)\right)$$

לכן, מתקיים

$$6|(n^2+n)(n^2+n+1)$$

ולכן, מתקיים:

$$30|5n^4+10n^3+10n^2+5n$$

לפי הנחת האינדוקציה, נקבל בנוסף כי:

$$30|n^5-n$$

לפי למה `2.3`
מתקיים

$$30|(n^5-n)+(5n^4+10n^3+10n^2+5n)$$

ולכן

$$30|(n+1)^5-(n+1)$$

ולכן האינדוקציה מתקיימת.
לכן טענת השאלה נכונה.
מש"ל

שאלה 4

שאלה 4 (20 נקודות)

תהי $(A,\cdot)$ אגודה. נגדיר יוחסה (שתסומן בסימן $\approx$) על הקבוצה A כך:

לכל $x,y\in A$ הזוג (x,y) נמצא ביוחסה, כלומר $x\approx y$, אם ורק אם $x=y$ או שהקבוצה $\{x,y\}$ היא תת־אגודה של $(A,\cdot)$ שטבלת הכפל שלה נראית כך:

$\cdot$	x	y
x	x	y
y	x	y

א. הראו שהיוחסה $\approx$ היא יוחסת שקילות על A.

בסעיפים הבאים נניח בנוסף שכל תת־קבוצה של A היא תת־אגודה של A.

ב. הוכיחו שאם $x,y,z\in A$ ו־ $x\approx y$ אז מתקיים $xz\approx yz$ וגם $zx\approx zy$.

ג. הסיקו שאם $x,x',y,y'\in A$ ומתקיים $x\approx x'$ וגם $y\approx y'$ אז $xy\approx x'y'$.

ד. כמו בסימוני הגדרה 3.8, לכל $a\in A$ נסמן ב־ C_a את מחלקת השקילות של a, ונסמן ב־ $A/_{\approx}$ את קבוצת המנה: קבוצת כל מחלקות השקילות. נגדיר פעולה בינארית $\cdot$ על הקבוצה $A/_{\approx}$ כך:

לכל $x,y\in A$ נגדיר $C_x\cdot C_y=C_{xy}$. הוכיחו שפעולה זאת מוגדרת חד־ערכית – דהיינו אינה תלויה בבחירת המייצגים x ו־ y של מחלקות השקילות, וש־ $\left(A/_{\approx},\cdot\right)$ היא אגודה.

סעיף א

אראה כי היוחסה $\approx$ היא יוחסת שקילות.

אראה כי $\approx$ היא רקפלסיבית, סימטרי, וטרנזיטיבי

רפלקסיבית:

טריוויאלי לפי הגדרת $\approx$.

לכן רפלקסיבי

סימטרית:

נגדיר $x,y\in A$ שונים כך שמתקיים $x\approx y$, כלומר:

$\times$	x	y
x	x	y
y	x	y

.

נבדוק האם מתקיים $y\approx x$:

נקבל:

$\times$	y	x
y	y	x
x	y	x

.

וקיבלנו אותה תבנית בדיוק
לכן היוחסה סימטרית!

טרנזיטיבית:
נגדיר $x, y, z \in A$, כאשר $x \approx y$ וגם $y \approx z$.
אראה כי מתקיים $x \approx z$:
ידוע כי $x \cdot x = x$ ו- $z \cdot z = z$, מהטבלאות של כל אחד מהם עם y
נמצא מה הערך של xz:
ידוע כי $yz = z$.
נקבל (בעזרת קיומה של $(A, \cdot)$ כאגודה):

$$xz = xyz = (xy)z = yz = z$$

נמצא מה הערך של zx:
ידוע כי $x = yx$
ונקבל:

$$zx = zyx = (zy)x = yx = x$$

ולכן קיבלנו את הטבלה:

$\times$	x	z
x	x	z
z	x	z

.

ולכן היוחסה טרנזיטיבית!
לכן, היוחסה מקיימת את כל התנאים לשקילות
לכן הטענה נכונה!
מש"ל א

סעיף ב

יהי $x, y, z \in A$ כאשר $x \approx y$. אראה כי מתקיים $xz \approx yz$ וגם $zx \approx zy$

אראה כי $zx \approx zy$

נבחין ב2 מקרים:

מקרה 1: $zx = x$ או $zy = y$

נבחין בין 2 תתי מקרים:

מקרה 1.1: $zx = x$:

נקבל:

$$zy = z(xy) = (zx)y = xy = y$$

וידוע כי $y \approx x$.

מקרה 1.2 $zy = y$

נקבל:

$$zx = z(yx) = (zy)x = yx = y$$

וידוע כי $y \approx x$.

מקרה 2: $zx \neq x$ וגם $zy \neq y$

מפני שכל תת קבוצה בA היא אגודה, נקבל כי:

$$zy = z,\ zx = z$$

ולכן נקבל כי $zx \approx zy$

לכן, בכל המקרים קיבלנו כי $zy \approx zx$.

אראה כי $yz \approx xz$

נבחין ב2 מקרים:

מקרה 1: $xz = z$ או $yz = z$

נבחין בין 2 תתי מקרים:

מקרה 1.1: $xz = z$:

נקבל:

$$yz = y(xz) = (yx)z = xz = z$$

וידוע כי $z \approx z$.

מקרה 1.2 $yz = z$

נקבל:

$$xz = x(yz) = (xy)z = yx = z$$

וידוע כי $z \approx z$.

מקרה 2: $xz \neq z$ וגם $yz \neq z$

מפני שכל תת קבוצה בA היא אגודה, נקבל כי:

$$yz = y,\ xz = x$$

ולכן נקבל כי $x \approx y$

לכן, בכל המקרים קיבלנו כי $zy \approx zx$.
לכן, הטענה נכונה!
מש"ל ב

סעיף ג

נגדיר $x, x', y, y' \in A$
כאשר:

$$x \approx x',\ y \approx y'$$

לפי הסעיף הקודם, נקבל כי:

$$xy \approx x'y, x'y \approx x'y'$$

ולפי הטרנזיטיביות, נקבל כי

$$xy \approx x'y'$$

משל ג

סעיף ד

נגדיר עבור $a, b \in A$:

$$C_a = \{b \in A | a \approx b\},\ C_a \cdot C_b = C_{ab}$$

יהי $x, y \in A$.
ניקח $x' \in C_x,\ y' \in C_y$
נמצא את $C_{x'} \cdot C_{y'}$

$$C_{x'} \cdot C_{y'} = C_{x'y'}$$

לפי סעיף ג נקבל כי $xy \approx x'y'$, ולכן $C_{xy} = C_{x'y'}$, ולכן הפעולה חד ערכית.
אראה כי $\left({}^{A}/_{\approx}, \cdot\right)$ היא אגודה.
נסתכל על $C_x \cdot C_y$:

$$C_x \cdot C_y = C_{xy}$$

מפני שכל תת קבוצה בA היא תת אגודה, נקבל כי xy שווה או לx או לy. לכן, הביטוי שווה לאחד מ"גורמיו". לכן, הפעולה סגורה.
יהי $x, y, z \in A$.
מפני שA אגודה לפי הפעולה $\cdot$, נקבל:

$$(C_xC_y)C_z = C_{xy}C_z = C_{(xy)z} = C_{xyz} = C_{x(yz)} = C_x(C_yC_z)$$

וקילבנו כי $({}^A/_{\approx}, \cdot)$ אגודה!
מש"ל ד

שאלה 5

שאלה 5 (20 נקודות)

יהי $n > 2$ מספר זוגי. תהי $\sigma \in A_n$ תמורה זוגית. הוכיחו שיש חילופים $\tau_1, \tau_2, \dots, \tau_{n-2} \in S_n$ כך

ש־ $\sigma = \tau_1\tau_2\cdots\tau_{n-2}$. הערה: ה־ τ_i אינם בהכרח שונים זה מזה.

נגדיר $2 < n \in \mathbb{N}$, $\sigma \in A_n$ תמורה זוגית
אראה כי קיימים חילופים $\tau_1, \dots \tau_{n-2} \in S_n$ כאשר מתקיים

$$\tau_1 \cdot \tau_2 \cdots \tau_{n-2} = \sigma$$

נפרק את σ ל- $m \in \mathbb{N}$ עגילים זרים (לפי משפט 6.6):

$$x_1 \cdot x_2 \cdots x_m = \sigma$$

נגדיר r_i הסדר עבור x_i (שהוא גם האורך של עגיל זה)
מפני ש $\{x_i\}_i$ היא קבוצה של עגילים זרים עבור K_n נקבל כי מתקיים:

$$\sum_{i=1}^{m} r_i \leq n$$

*נניח כי הסכום היה גדול יותר מ-n. מפני ש r_i מסמל את גודל העגיל, וכך את כמות אבריו, על פי עיקרון שובך היונים, היה מתקבל שאיבר בK_n מופיע פעמיים בשני x_i שונים בסתירה לכך שהם זרים.

על פי למה 6.7, נקבל כי ניתן לפרק כל x_i ל $r_i - 1$ חילופים.
לכן, מפני ש S_n היא אגודה לגבי פעולת הכפל, נקבל כי כמות החילופים המרכיבים את σ היא:

$$\sum_{i=1}^{m}(r_i - 1) = \left(\sum_{i=1}^{m} r_i\right) - m \leq n - m$$

נסתכל במקרה כאשר $m = 1, r_1 = n$:
נקבל כי σ היא עגיל מאורך n. לפני משפט 6.7, נקבל כי היא עגיל, אשר מורכבת מ- $n - 1$ חילופים, בסתירה לכך ש-σ היא תמורה זוגית
לכן מקרה זה לא רלוונטי!

כאשר $m=0$, קיים המקרה הטריוויאלי כאשר כל חילוף הוא חילוף של איבר עם עצמו $n-2$ פעמים.

כאשר $m\geq 2$:
נקבל שהאורך הוא

$$\left(\sum_{i=1}^{m} r_i\right)-2\leq n-2$$

ולכן, אם האורך קטן, אזי שאר החילופים יכולים להיות חילוף של איבר בעצמו.
*חשוב לציין כי גם אם כמות החילופים לא $n-2$ היא עדיין זוגית, לפי זוגיות σ.

לכן הטענה נכונה
מש"ל

שאלה 6

שאלה 6 (20 נקודות)

א. מצאו תמורה מסדר 20 ב־ S_9. האם יש ב־ S_9 תמורה מסדר 18? נמקו היטב!

ב. מצאו את המספר הטבעי m הקטן ביותר בעל התכונה שלכל $\sigma\in S_9$ מתקיים $\sigma^m=\varepsilon$.

סעיף א

ניקח את התמורה:

$$\sigma=(12345)(6789)$$

כאשר σ מורכבת מ2 עגילים זרים, אחד באורך 4, והשני באורך 5.
כאשר מכפילים את σ בעצמה, מפני שהעגילים זרים, לקבל:

$$\sigma^n=(12345)^n(6789)^n$$

נקבל כי $\sigma=\varepsilon$ רק כאשר שני העגילים "מתאפסים" ל- ε.
ידוע כי האורך של עגיל הוא גם הסדר שלו. לכן, צריך את המספר הקטן ביותר שמתחלק הן ב4, והן ב5.
זהו הקכ"מ (לפי למה 2.22).
הקכמ של 4,5 הוא 20!
לכן תמורה זו מקיימת את תנאי השאלה.

לגבי תמורה מסדר 18, צריך ש18 יהיה קכ"מ של הסדרים של העגילים הזרים.
18 הוא קכ"מ למספרים 9,2, אך 9 לא יכול להיות עגיל (בנוסף לעגילים אחרים) כי סכומם גדוך מ9 ולכן לא יכולים להיות עגילים זרים בS_n.
שאר הגורמים האפשריים של 18 הם 3,2,6, אך הקכ"מ שלהם הוא 6, לכן, בכל דרך שנבחר עגילים זרים

באורכים הללו, הסדר של התמורה לא תעלה על 6, כי הוא המספר שכל שאר המספרים מתחלקים בו.
לכן לא קיימת תמורה כזו!

מש"ל א

סעיף ב

צריך למצוא את הקכ"מ של K_9 - המספר הקטן ביותר המחלק את כל המספרים בK_9. ידוע שכל העגילים באורך 1 עד 9 שייכים לS_9, והתמורות האחרות מורכבות גם מעגילים באורך 1 עד 9. לכן, הקכ"מ של K_9 מקיימת את תנאי השאלה.
מספר זה הוא:

$$n = 5 \cdot 7 \cdot 9 \cdot 8 = 2520$$

כל מספר בK_n מתחלק בו!
אך אם מחלקים את n במספר כלשהוא, הוא כבר לא יחלק את כל אברי K_n.
לכן המספר הוא 2520
מש"ל ב