אלגברה מודרנית: תרגילים

1 מספרים טבעיים

1. בכל סעיף, מצאו את המחלק המשותף המרבי:
   (א) $(5,10)$
   (ב) $(22,9)$
   (ג) $(18,27)$
   (ד) $(2n,3n)$ כאשר $n\in\mathbb{N}$.

2. בכל דוגמא, מצאו את השארית כאשר מחלקים את n ב m:
   (א) $n=72, m=5$
   (ב) $n=523, m=11$
   (ג) $n=7^4, m=8$
   (ד) $n=3, m=2010$.

3. מצאו פירוק לראשוניים של כל אחד מהמספרים הבאים:
   (א) 60
   (ב) 83
   (ג) 111
   (ד) 111111
   (ה) 729.

4. הוכיחו את הנוסחא הבאה:

$$1+2+\cdots+n=n(n+1)/2.$$

5. הוכיחו שלכל מספר שלם $n\geq 3$ מתקיים $5^n>4^n+3^n+2^n$.

6. סדרת פיבונצ'י היא סדרה $f_0,f_1,f_2,\ldots$ המוגדרת על ידי $f_0=0, f_1=1$ ולכל $n\in\mathbb{N}$, $f_{n+1}=f_n+f_{n-1}$. הוכיחו שלכל $n\in\mathbb{N}$, $f_n=\frac{1}{\sqrt{5}}(\alpha^n-\beta^n)$, כאשר $\alpha=\frac{1+\sqrt{5}}{2}$, $\beta=\frac{1-\sqrt{5}}{2}$.

7. תהי A קבוצת כל המספרים הטבעיים n כך שניתן לכתוב את n כסכום של שני ריבועים חיוביים בלפחות שתי דרכים, כלומר קיימים $a,b,c,d \in \mathbb{N}$ כך ש $n = a^2+b^2 = c^2+d^2$, $a \leq b, c \leq d$ ו $(a,b) \neq (c,d)$.

   (א) מצאו את האיבר הקטן ביותר ב A (לכן A אינה ריקה!)

   (ב) הראו ש A אינסופית.

8. עבור כל אחד מהסעיפים הבאים, מצאו את השארית של x מודולו n.

   (א) $x = 72, n = 5$.

   (ב) $x = 14455 + 35 \times 489 - 2^{300}$, $n = 4$.

   (ג) $x = 2^{101}, n = 13$

9. (א) יהי p מספר ראשוני ויהי $a \in \mathbb{N}$. נניח ש $p \nmid a$. הוכיחו ש a ו p הם זרים זה לזה.

   (ב) יהיו p,q ראשוניים שונים. הוכיחו שלכל $e,f \in \mathbb{N}$ מתקיים $(p^e,q^f)=1$.

10. מספר ריבועי הוא מספר שניתן לכתוב אותו בצורה של x^2 כאשר x מספר שלם. יהיו m,n מספרים חיוביים כך ש $(m,n)=1$. אם mn מספר ריבועי, הוכיחו ש m,n שניהם מספר ריבועיים.

11. יהי $z = a+bi$ מספר מרוכב על מעגל היחידה, כלומר $|z| = a^2+b^2 = 1$. נניח שקיים $k \in \mathbb{N}$ כך ש $z^k = 1$. יהי $m \in \mathbb{N}$ המספר הטבעי הקטן ביותר כך ש $z^m = 1$. הוכיחו שלכל $n \in \mathbb{N}$ מתקיים $z^n = 1$ אם ורק אם $m|n$.

12. יהי $n \in \mathbb{N}$. יהיו $a_1,a_2,b_1,b_2 \in \mathbb{Z}$ כך ש $a_1 \equiv a_2 \mod n$ ו $b_1 \equiv b_2 \mod n$. הוכיחו ש

   (א) $a_1+b_1 \equiv a_2+b_2 \mod n$.

   (ב) $a_1b_1 \equiv a_2b_2 \mod n$.

   (ג) $1234 \times 3456 \equiv 3 \mod 7$ (**רמז:** אין צורך לחשב את 1234×3456).

13. הראו שלכל $n \in \mathbb{N}$ מתקיים $5^{2n} \equiv 3^n \mod 11$.

14. (א) יהי $x \in \mathbb{Z}$ כך ש $5 \nmid x$. הוכיחו ש $x^4 - 1$ מתחלק ב 5 ללא שארית. (**רמז:** השתמשו בלמה של אוקלידס על מנת להראות ש $x \equiv r \mod 5$ עבור איזשהו $r \in \{0,1,2,3,4\}$).

   (ב) הראו שאין פתרון בשלמים למשוואה $x^4+y^4 = z^4+3$.

15. הראו שלמשוואה $a^2+b^2 = 6(c^2+d^2)$ קיים פתרון יחיד בשלמים.

16. יהיו p,q ראשוניים שונים. הראו ש
   (א) $(p,q)=1$.
   (ב) $(p^m,q^n)=1$ לכל $m,n\in\mathbb{N}$.

17. נתון ש $(a,b)=1$ ו $(b,c)=1$. האם ניתן להסיק ש $(a,c)=1$? נמקו.

18. יהיו n,a,b מספרים טבעיים. אם $n|ab$ ו $(a,n)=1$, הראו ש $n|b$.

19. יהי p ראשוני ונניח ש $p|abc$, כאשר $a,b,c\in\mathbb{Z}$. הראו שלפחות אחד מהבאים מתקיים: $p|a$, $p|b$, או $p|c$.

20. מצאו את כל הפתרונות בשלמים למשוואות הבאות:
   (א) $x^2=y^3$
   (ב) $x^2-x=y^3$
   (ג) $x^3=4y^2+4y-3$

21. יהיו a,b מספרים שלמים ויהי $n\in\mathbb{N}$ כך ש $a|n$ ו $b|n$. אם a ו b זרים זה לזה, הראו ש $ab|n$.

22. יהי p מספר ראשוני. אם $ac+bd\equiv bc+ad \mod p$ כאשר $a,b,c,d\in\mathbb{Z}$, הראו ש $a\equiv b \mod p$ או $c\equiv d \mod p$.

2 חבורות

23. תהי G חבורה ויהי $g\in G$. הוכיחו שהופכי של g^2 הוא $(g^{-1})^2$. מהו ההופכי של g^n עבור $n\in\mathbb{N}$?

24. תהי $G=\left\{A\in\mathbb{R}^{2\times 2}\mid A^T=A\right\}$. נגדיר על G פעולת כפל מטריצות. האם $(G,\cdot)$ חבורה? אם כן, האם החבורה אבלית?

25. תהי $H=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\mid x\in\mathbb{R}\right\}$. נגדיר על H פעולת כפל מטריצות. האם $(H,\cdot)$ חבורה? אם כן, האם החבורה אבלית?

26. נתבונן בחבורה $S=\mathbb{C}\backslash\{0\}$, חבורת המספרים המרוכבים בלי אפס עם פעולת כפל. לכל אחת מהקבוצות הבאות, האם היא תת חבורה? נמקו.
   (א) $S_1=\{z\in S \mid |z|>1\}$.
   (ב) $S_2=\{z\in S \mid |z|=1\}$.

(ג) $S_3 = \{z \in S \mid |z| < 1\}$.

(ד) $S_4 = \{z \in S \mid z^n = 1\}$ כאשר $n \in \mathbb{N}$ קבוע.

(ה) $S_5 = \{e^{i\theta} \in S \mid \frac{n\theta}{2\pi} \in \mathbb{Z}\}$ כאשר $n \in \mathbb{N}$ קבוע.

(ו) $S_6 = \{e^{i\theta} \in S \mid 0 \leq \theta \leq \pi\}$.

(ז) $S_7 = \{z \in S \mid \mathrm{Re}(z) = z\}$.

(ח) $S_8 = \{z \in S \mid \mathrm{Re}(z) = 0\}$.

27. יהי $[a,b]$ קטע סגור כאשר $a,b \in \mathbb{R}$, $a < b$. האם קיימת תת חבורה $H \neq \mathbb{R}$ של $(\mathbb{R},+)$ כך ש $[a,b] \subseteq H$?

28. נגדיר תת חבורה $S = \{z \in \mathbb{C} \mid |z| = 1\}$ של $\mathbb{C}\backslash\{0\}$. יהי $[a,b]$ קטע סגור כאשר $a,b \in \mathbb{R}, 0 < b-a < 2\pi$. האם קיימת תת חבורה $K \neq S$ של $(S,\cdot)$ כך ש $\{e^{i\theta} \mid a \leq \theta \leq b\} \subseteq K$?

29. מצאו את כל תתי החבורה של:

(א) $\mathbb{Z}/6\mathbb{Z}$.

(ב) $\mathbb{Z}/5\mathbb{Z}$.

(ג) $\mathbb{Z}/p\mathbb{Z}$ כאשר p מספר ראשוני.

30. נגדיר תת קבוצה $Q[\sqrt{2}]^*$ של החבורה $(\mathbb{R}\backslash\{0\},\cdot)$ על ידי

$$Q[\sqrt{2}]^* = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}, a \neq 0\}.$$

(א) הראה שלכל $a,b \in \mathbb{Q}, a \neq 0$ מתקיים $a^2 - 2b^2 \neq 0$.

(ב) הראה שלכל $a + b\sqrt{2} \in Q[\sqrt{2}]^*$ קיים הופכי ב $Q[\sqrt{2}]^*$. **הצעה:** חשבו את $(a+b\sqrt{2})(a-b\sqrt{2})$.

(ג) הוכיחו ש $(Q[\sqrt{2}]^*,\cdot)$ תת חבורה של $(\mathbb{R}\backslash\{0\},\cdot)$.

31. נגדיר תת קבוצה U של החבורה $(\mathrm{GL}_2(\mathbb{R}),\cdot)$ על ידי $U = \left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{R}\right\}$. הוכיחו ש U תת חבורה אבלית של $\mathrm{GL}_2(\mathbb{R})$.

32. תהי G חבורה ויהיו $x,y \in G$. הוכיחו ש

(א) לכל $g \in G$ מתקיים $(g^{-1})^{-1} = g$.

(ב) לכל $g,h \in G$ מתקיים $(gh)^{-1} = h^{-1}g^{-1}$.

33. תהי G חבורה. נגדיר $Z = \{x \in G \mid g \in G$ לכל $xg = gx\}$. הוכיחו ש Z תת חבורה של G.

34. חשבו את הסדר של איבר x בחבורה G כאשר:

(א) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = i$.

(ב) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(2\pi/8)}$.

(ג) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(10\pi/8)}$.

(ד) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(12\pi/8)}$.

(ה) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(2\pi/n)}$ ($n \in \mathbb{N}$.)

(ו) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(2\pi k/n)}$ ($k, n \in \mathbb{N}$, $(n,k) = 1$.)

(ז) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(2\pi k/n)}$ ($k, n \in \mathbb{N}$, $(n,k) = a \in \mathbb{N}$.)

(ח) $G = (\mathbb{C}\backslash\{0\}, \cdot)$, $x = e^{i(2\pi\sqrt{2})}$.

(ט) $G = (\mathbb{Z}/6\mathbb{Z}, +)$, $x = [2]$.

(י) $G = (\mathbb{Z}/9\mathbb{Z}, +)$, $x = [2]$.

(יא) $G = (\mathbb{Z}/9\mathbb{Z}, +)$, $x = [3]$.

(יב) $G = (\mathbb{Z}/12\mathbb{Z}, +)$, $x = [8]$.

(יג) $G = (\mathbb{Z}/n\mathbb{Z}, +)$, $x = [a]$ כאשר $(a, n) = 1$.

(יד) $G = (\mathbb{Z}/n\mathbb{Z}, +)$, $x = [a]$ כאשר $(a, n) = k$.

(טו) $G = ((\mathbb{Z}/8\mathbb{Z})^*, \cdot)$, $x = [3]$.

(טז) $G = ((\mathbb{Z}/8\mathbb{Z})^*, \cdot)$, $x = [5]$.

(יז) $G = ((\mathbb{Z}/10\mathbb{Z})^*, \cdot)$, $x = [3]$.

(יח) $G = ((\mathbb{Z}/11\mathbb{Z})^*, \cdot)$, $x = [3]$.

(יט) $G = ((\mathbb{Z}/11\mathbb{Z})^*, \cdot)$, $x = [6]$.

(כ) $G = ((\mathbb{Z}/15\mathbb{Z})^*, \cdot)$, $x = [2]$.

(כא) $G = ((\mathbb{Z}/15\mathbb{Z})^*, \cdot)$, $x = [4]$.

(כב) $G = ((\mathbb{Z}/15\mathbb{Z})^*, \cdot)$, $x = [11]$.

(כג) $G = (\mathrm{GL}_2(\mathbb{R}), \cdot)$, $x = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

(כד) $G = (\mathrm{GL}_2(\mathbb{R}), \cdot)$, $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(כה) $G = (\mathrm{GL}_2(\mathbb{R}), \cdot)$, $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

35. תנו דוגמא של חבורה G שאין לה איבר שונה מהאדיש מסדר סופי.

36. תנו דוגמא של חבורה G אינסופי שיש לה איבר שונה מהאדיש מסדר סופי ומצאו איבר כזה.

37. תהי $G=(\mathbb{C}\backslash\{0\},\cdot)$. יהי $z\in G$ מסדר סופי. הוכיחו ש $|z|=1$.

38. תהי $G=(\mathrm{GL}_2(\mathbb{R}),\cdot)$. תהי $A\in G$ מסדר סופי. הוכיחו ש $\det A=\pm 1$.

39. לכל $m,n\in\mathbb{N}$ ה lcm (lowest common multiple) שלהם, מסומן ב $\mathrm{lcm}(m,n)$, הוא הכפולה המשותפת הקטנה ביותר, כלמור הוא המספר הקטנה ביותר שמתחלק גם ב m וגם ב n. למשל, $\mathrm{lcm}(4,2)=4$, $\mathrm{lcm}(6,8)=24$, $\mathrm{lcm}(5,7)=35$.

(א) הוכיחו שאם $(m,n)=1$ אז $\mathrm{lcm}(m,n)=mn$.

(ב) הוכיחו שלכל $m,n\in\mathbb{N}$ מתקיים $\mathrm{lcm}(m,n)=\frac{mn}{(m,n)}$.

(ג) יהי $\sigma\in S_n$ מעגל באורך k. הראו ש $\mathrm{ord}(\sigma)=k$.

(ד) יהי $\sigma\in S_n$ ויהי $\sigma=\sigma_1\cdots\sigma_m$ ביטוי ל σ כהרכבה של מעגלים זרים. נסמן את האורך של כל σ_i על ידי r_i.

i. הוכיחו שלכל i מתקיים $r_i|\mathrm{ord}(\sigma)$.

ii. אם $\sigma=\sigma_1\sigma_2$ ו $(r_1,r_2)=1$ הוכיחו ש $\mathrm{ord}(\sigma)=r_1r_2$.

iii. אם $\sigma=\sigma_1\sigma_2$ הוכיחו ש $\mathrm{ord}(\sigma)=\mathrm{lcm}(r_1,r_2)$.

40. תהי G חבורה אבלית.

(א) הראו שלכל $g,h\in G$ ו $n\in\mathbb{N}$ מתקיים $(gh)^n=g^nh^n$.

(ב) יהיו $x,y\in G$ כך ש $\mathrm{ord}(x)=m,\mathrm{ord}(y)=n$. הוכיחו שאם $(m,n)=1$ אזי $\mathrm{ord}(xy)=mn$.

(ג) יהיו $x,y\in G$ כך ש $\mathrm{ord}(x)=m,\mathrm{ord}(y)=n$. הוכיחו ש $\mathrm{ord}(xy)=\mathrm{lcm}(m,n)$. (המושג של lcm מוגדר בתרגיל 39.)

(ד) מצאו שני איברים $x,y\in S_3$ מסדר m,n בהתאמה כך ש $\mathrm{ord}(xy)\neq\mathrm{lcm}(m,n)$.

41. תהי G חבורה ויהי $x\in G$ מסדר סופי $k=\mathrm{ord}(x)$.

(א) יהי $m\in\mathbb{Z}$. הראו ש $m\in k\mathbb{Z}\iff x^m=1$. כאן $k\mathbb{Z}=\{kq\mid q\in\mathbb{Z}\}$.

(ב) אם G חבורה סופית, הוכיחו ש k מחלק את $|G|$.

(ג) תהי G חבורה כך ש $|G|=2^n$ כאשר $n\in\mathbb{N}$. הוכיחו שקיים $x\in G$, $x\neq e$ כך ש x הוא ההופכי של עצמו.

(ד) יהי $n\in\mathbb{N}$ ותהי $G=\mathbb{Z}/2^n\mathbb{Z}$. מצאו איבר $[x]\in G$ כך ש $[x]^{-1}=[x]$.

(ה) אם $G=S_n$ הוכיחו שלכל ראשוני p כך ש $p|k$ מתקיים $p\leq n$.

(ו) אם $G = S_n$ הוכיחו שלכל מספר טבעי t כך ש $t \leq n$ קיים איבר $\sigma \in S_n$ כך ש $\mathrm{ord}(y) = t$.

(ז) הוכיחו שלחבורה S_{24} אין איבר מסדר 29.

(ח) מצאו איבר $\sigma \in S_{24}$ מסדר 23.

(ט) האם קיים איבר של S_{24} מסדר 27?

42. תהי $G = \langle x \rangle$ חבורה ציקלית הנוצרת על ידי $x \in G$ ונסמן $n = |G|$.

(א) הוכיחו כל תת חבורה H ציקלית.

(ב) הוכיחו שלכל תת חבורה H של G קיים $k \in \mathbb{N}$ כך ש $H = \langle x^k \rangle$ ו $k|n$.

(ג) מצאו את כל תתי החבורה של

i. $(\mathbb{Z}/6\mathbb{Z}, +)$

ii. $(\mathbb{Z}/24\mathbb{Z}, +)$

iii. $((\mathbb{Z}/9\mathbb{Z})^*, \cdot)$

iv. $(\{z \in \mathbb{C} \mid z^6 = 1\}, \cdot)$

v. $\left(\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}, \cdot\right)$

vi. $(\{\sigma \in S_3 \mid \sigma^3 = 1\}, \circ)$

43. תהי $G = (\mathrm{GL}_2(\mathbb{R}), \cdot)$. תהי $A \in G$ מסדר סופי. הוכיחו ש $\det A = \pm 1$.

44. הוכיחו שכל תת חבורה של חבורה אבלית היא נורמלית.

45. הוכיחו שכל תת חבורה של חבורה ציקלית היא נורמלית.

46. תהי G חבורה ותהי N תת חבורה נורמלית של G.

(א) הוכיחו שאם G אבלית אז גם המנה G/N אבלית.

(ב) הוכיחו שאם G ציקלית אז גם המנה G/N ציקלית.

47. תנו דוגמא של חבורה G ותת חבורה נורמלית N של G כך ש N ציקלית אבל G אינה ציקלית.

48. תנו דוגמא של חבורה G ותת חבורה נורמלית N של G כך ש N אבלית אבל G אינה אבלית.

49. תנו דוגמא של חבורה G ותת חבורה נורמלית N של G כך ש N אבלית ו G/N אבלית אבל G אינה אבלית.

50. תהי G חבורה ותהי N תת חבורה נורמלית של G. הוכיחו שאם N סופית וגם G/N סופית אזי G סופית.

51. תהי $O = \{A \in \mathbb{R}^{2\times 2} \mid A^T A = I\}$ חבורת המטריצות האורתוגונליות מסדר 2×2 עם פעולת כפל. הוכיחו ש $S = \{A \in O \mid A$ סיבוב$\}$ תת חבורה נורמלית של O.

52. יהי $n \in \mathbb{N}$. תהי $S = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{2k\pi i/n} \mid k = 0, 1, \ldots, n-1\}$ עם פעולת כפל ותהי $\mathbb{Z}/n\mathbb{Z}$ חבורה עם פעולת חיבור מודולו n. נגדיר פונקציה $\varphi : \mathbb{Z}/n\mathbb{Z} \to S$ על ידי $\varphi(k) = (e^{2k\pi i/n})$.

(א) הוכיחו ש φ איזומורפיזם.

(ב) הוכיחו שלכל $0 \leq k \leq n-1$ מתקיים $\operatorname{ord}(e^{2k\pi i/n}) = \operatorname{ord}(k) = (k, n)$.

53. תהי $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_4$.

(א) הראו ש V תת חבורה נורמלית של S_4.

(ב) חשבו את הסדר של המנה S_4/V.

(ג) מצאו נציג לכל אחד מהקוסטים השמאליים של V ב S_4.

(ד) האם S_4/V אבלית? נמקו.

(ה) הראו ש S_4/V איזומורפית ל S_3.
הצעה: מצאו נציגים של הקוסטים של V ב S_4 שהם כולם מקיימים $\sigma(4) = 4$.

54. יהיו $(G, *), (K, \bullet)$ חבורות. נגדיר על מכפלת הקבוצות $G \times K$ פעולה על ידי $(g_1, k_1)\cdot(g_2, k_2) = (g_1 * g_2, k_1 \bullet k_2)$. נכתוב $G_0 = \{(g, e_K) \mid g \in G\}$ ו $K_0 = \{(e_G, k) \mid k \in K\}$ כאשר e_G האדיש ב G ו e_K האדיש ב K.

(א) הוכיחו ש $(G \times K, \cdot)$ היא חבורה.

(ב) הוכיחו ש $G_0 \cong G$ ו $K_0 \cong K$.

(ג) הוכיחו ש G_0, K_0 תתי חבורה נורמליות ב $G \times K$.

(ד) הוכיחו ש $(G \times K)/G_0 \cong K$ ו $(G \times K)/K_0 \cong G$.

(ה) הוכיחו שאם $g \in G, k \in K$ כך ש $\operatorname{ord}(g) = m, \operatorname{ord}(k) = n$ ובנוסף $(m, n) = 1$ אזי $\operatorname{ord}((g, k)) = mn$.

(ו) הראו שאם G, K שתיהן אבליות אז $G \times K$ גם אבלית.

55. תהי $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ תת חבורה נורמלית של S_4. הוכיחו ש $(V, \circ) \cong ((\mathbb{Z}/8\mathbb{Z})^*, \cdot) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ כאשר מכפלת חבורות מוגדרת בתרגיל 54.

56. תהי G חבורה עם תת חרובה נורמלית N. אם K תת חבורה נורמלית של N האם נובע ש K נורמלית ב G?
הצעה: חפשו דוגמא נגדית כאשר $G = S_4$.