תרגילים 1: תורת המספרים

שאלה 1 מצאו את הפירוק מנה-שארית של השלמים הבאים:

א) $a = 7503, b = 81$.

ב) $a = -7503, b = 81$.

ג) $a = 81, b = 7503$.

ד) $a = -81, b = 7503$.

שאלה 2 יהיו $a, b, n > 0$ שלמים. הוכיחו כי $a \mod n = b \bmod n$ אם ורק אם $a \equiv b \pmod{n}$.

שאלה 3 מצאו שלמים s, t, d עבורם $12327s + 409t = d$.

שאלה 4 הוכיחו כי 7563 ו- 526 מספרים זרים.

שאלה 5 יהיו a, b מספרים שלמים.
הוכיחו שאם קיימים שלמים s, t כך ש- $sa + tb = 1$ אז a ו- b זרים.

שאלה 6 יהיו a, b, n מספרים שלמים. הוכיחו את הטענה הבאה:
אם השלושה תנאים הבאים מתקיימים:

1) a ו- b זרים,

2) $a \mid n$,

3) $b \mid n$,

אז $ab \mid n$.

שאלה 7 הוכיחו את הטענות הבאות:

א) $\gcd(ma, mb) = m \gcd(a, b)$.

ב) אם $m > 0$ ואם $a \mid m$ ו- $b \mid m$ אז $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m}$.

ג) המספרים $\frac{a}{\gcd(a, b)}$ ו- $\frac{b}{\gcd(a, b)}$ מספרים זרים.

ד) אם $c \mid ab$ ו- c זר ביחס ל- b אז $c|a$.

ה) אם a, c מספרים זרים ואם b, c מספרים זרים אז c ו- ab מספרים זרים.

ו) $\gcd(a,b) = \gcd(a+cb, b)$.

שאלה 8 יהיו a, m מספרים זרים. הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod m$.

שאלה 9 יהיו a, m מספרים (לא בהכרח זרים).
הוכיחו כי $ab \equiv ac \pmod{m}$ אם ורק אם $b \equiv c \pmod{\frac{m}{\gcd(a,m)}}$.

שאלה 10

א) חשבו את $\gcd(285, 89)$.

ב) מצאו שלמים s, t, d עבורם $285s + 89t = d$.

שאלה 11 הוכיחו: אם $a \mid bc$ ו- a, b זרים אז $a \mid c$.

שאלה 12

א) הוכיחו: אם a, b זרים אז קיים c עבורו $ac \equiv 1 \pmod{b}$.

ב) הוכיחו: אם a, b לא זרים אז לא קיים c עבורו $ac \equiv 1 \pmod{b}$.

שאלה 13

א) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a + c \equiv b + c \pmod{m}$.

ב) הוכיחו: אם $a \equiv b \pmod{m}$ ו- $c \equiv d \pmod{m}$ אז $ac \equiv bd \pmod{m}$.

ג) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a^n \equiv b^n \pmod{m}$.

שאלה 14

א) חשבו את $\gcd(285, 89)$.

ב) מצאו שלמים s, t, d עבורם $285s + 89t = d$.

שאלה 15 הוכיחו: אם $a \mid bc$ ו- a, b זרים אז $a \mid c$.

שאלה 16

א) הוכיחו: אם a, b זרים אז קיים c עבורו $ac \equiv 1 \pmod{b}$.

ב) הוכיחו: אם a, b לא זרים אז לא קיים c עבורו $ac \equiv 1 \pmod{b}$.

שאלה 17

א) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a + c \equiv b + c \mod m$.

ב) הוכיחו: אם $a \equiv b \pmod{m}$ ו- $c \equiv d \pmod{m}$ אז $ac \equiv bd \pmod{m}$.

ג) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a^n \equiv b^n \pmod{m}$.

שאלה 18 יהי $m \geq 2$ שלם. הוכיחו או הפריכו על ידי דוגמה נגדית את הטענות הבאות:

א) m מספר ריבועי אם ורק אם כל אחד מהגורמים הראשוניים שלו מופיע עם חזקה זוגית בפירוק לראשוניים שלו.

ב) אם $\sqrt{m}$ מספר רצונלי אזי m מספר ריבועי.

ג) אם m הוא לא מספר ריבועי אזי $\sqrt{m}$ לא רציונלי.

שאלה 19 הוכיחו או הפריכו:

א) $54 \equiv 3 \pmod{17}$.

ב) $56 \equiv 3 \pmod{2}$.

ג) $578 \equiv 9 \pmod{1}$.

ד) $-23 \equiv 4 \pmod{9}$.

ה) $1001 \equiv 1 \pmod{7}$.

ו) $2025 \equiv 5 \pmod{10}$.

ז) $85 \equiv -3 \pmod{11}$.

ח) $2^8 \equiv 1 \pmod{5}$.

ט) $45 \equiv 5 \pmod{8}$.

י) $72 \equiv -1 \pmod{9}$.

שאלה 20 חשבו:

א) $12^5 + 2^5 \mod 11$.

ב) $7^4 + 3^5 \bmod 5$.

ג) $9^6 - 4^7 \bmod 7$.

ד) $5^{2025} \bmod 13$.

ה) $2^{100} + 2^{50} \bmod 3$.

ו) $10^{2025} \bmod 9$.

ז) $14^{12} \bmod 13$.

ח) $8^{17} - 3^{17} \bmod 5$.

ט) $6^{20} + 1 \bmod 7$.

י) $11^{30} \bmod 12$.

שאלה 21

א) אם $x \equiv 3 \pmod 7$ ו־$y \equiv 5 \pmod 7$, חשבו $4x - 3y \pmod 7$.

ב) אם $x \equiv 2 \pmod 9$ ו־$y \equiv 7 \pmod 9$, חשבו $xy^2 \pmod 9$.

ג) אם $a \equiv 11 \pmod{15}$ ו־$b \equiv -4 \pmod{15}$, חשבו $(2a + 5b) \pmod{15}$.

ד) אם $p \equiv 4 \pmod 6$ ו־$q \equiv -1 \pmod 6$, חשבו $p^2q \pmod 6$.

ה) אם $r \equiv 17 \pmod{20}$ ו־$s \equiv 13 \pmod{20}$, חשבו $(r - s)(r + s) \pmod{20}$.

שאלה 22

א) הוכיחו: אם $a \equiv c \pmod n$ ו־$b \equiv d \pmod n$ אז לכל $u, v \in \mathbb{Z}$ מתקיים:

$$ua + vb \equiv uc + vd \pmod n .$$

ב) הוכיחו באינדוקציה: אם $a \equiv c \pmod n$ אז לכל $k \in \mathbb{N}$ מתקיים:

$$a^k \equiv c^k \pmod n.$$

ג) הוכיחו: אם $a \equiv c \pmod n$ אז לכל פולינום $P(x)$ עם מקדמים שלמים מתקיים:

$$P(a) \equiv P(c) \pmod n.$$

ד) תנו דוגמה לכך שמ־$ac \equiv bc \pmod n$ לא נובע $a \equiv b \pmod n$.

ה) הוכיחו: אם $\gcd(c,n)=1$ לכל n ו־ $ac \equiv bc \pmod{n}$ אז $a \equiv b \pmod{n}$.

ו) תנו דוגמה עם $\gcd(c,n) \neq 1$ שבה $ac \equiv bc \pmod{n}$ אך $a \not\equiv b \pmod{n}$.

שאלה 23

אם $x \equiv 5 \pmod{12}$ ו־$y \equiv 8 \pmod{12}$, חשבו:

א) $x+y \bmod 12$

ב) $x-y \bmod 12$

ג) $xy \bmod 12$

ד) $x^3+2y \bmod 12$.