מטלה מספר 2 – תורת המספרים

1. א.

ע"פ הנתון ניתן לבחור n+1 איברים מתוך $1 \leq a_1 < a_2 < \cdots < a_{n+1} \leq 2n$ אופציות.
כלומר, ניתן לחלק את האופציות ל3 חלקים: איברים אי זוגיים, איברים זוגיים בעלי גורמים זוגיים, איברים זוגיים (הקטנים מ2n) בעלי גורמים אי-זוגיים (שבהכרח קטנים מn).
נגדיר את תאי השובך להיות n קבוצות הבאות:
שובך 1 = 2^x כך ש: $X \in \mathbb{N} \cup \{0\}$
כלומר, בשובך אחד נקבל את כל האיברים המתקבלים מכפולות של 2 ו-1
$2^0, 2^1, 2^2, 2^3 \ldots = 1 \;\; ,1 \cdot 2 \;\; ,1 \cdot 2 \cdot 2 \;\; ,1 \cdot 2 \cdot 2 \cdot 2 \ldots$
כך שכל איבר מחלק את האיברים הבאים אחריו (כי כל איבר הוא גורם באיבר שלאחריו)
n-1 שובכים = מאחר וישנם n-1 איברים אי זוגיים הקטנים מ2n (פרט ל1 שנמצא בקבוצה 1)
אזי נגדיר n-1 שובכים כך שבכל שובך יש איבר אי זוגי כזה (הקטן מ2n פרט ל1) וגם הכפולה שלו ב2. כך שישנו שובך עבור כל איבר זוגי (בעל גורם אי-זוגי הקטן מ2n).
$\{3,6\}, \{5,10\} \ldots$
כלומר, בשאר השובכים נקבל את כל האיברים האי-זוגיים (פרט ל1) וגם את האיברים הזוגיים שהם הכפולות ב2 של אותם איברים אי-זוגיים (וא"כ אינם מהצורה של 2^x).

נרצה להוכיח שעבור כל קבוצת מספרים שלמים בעלת n+1 איברים $\{a_1, a_2 \ldots a_{n+1}\}$ המקיימים: $1 \leq a_1 < a_2 < \cdots < a_{n+1} \leq 2n$
מכילה לפחות שני איברים כך שהאחד מחלק את האחר.
במידה ויהיו שתי יונים בשובך מספר 1 אז סיימנו. כיוון שכבר הראנו שכל שניים מחלקים אחד את השני.
באותה מידה, מאחר ובשאר השובכים קיימים זוגות כך שבכל זוג ישנו מספר אי-זוגי עם הכפולה שלו ב-2 (כך שהאי זוגי מחלק את הזוגי) אז גם סיימנו.
אך מאחר ונרצה להכניס n+1 יונים לn שובכים, ומאחר שהראנו שהשובכים יכולים להכיל את כל טווח המספרים האפשריים עבור n מסויים, אזי נובע מעקרון שובך היונים שיש לפחות שתי יונים באותו תא.

מ.ש.ל.

ב.

נרצה להוכיח שעבור כל קבוצת מספרים שלמים בעלת n+1 איברים $\{a1,a2,\ldots,an+1\}$ המקיימים: $1 \leq a_1 < a_2 < \cdots < a_{n+1} \leq 2n$
מכילה לפחות שני אברים זרים.
ע"פ הנתון ניתן לבחור n+1 איברים מתוך $1 \leq a_1 < a_2 < \cdots < a_{n+1} \leq 2n$ אופציות.
נחלק את כל האופציות ל- n שובכים כך שבכל שובך ישנו זוג של מספרים עוקבים, כך:
$\{a_{2n-1}+1, a_{2n-1}\} \ldots \{3+1,3\}\{1+1,1\}$
על מנת להראות שעבור כל זוג $\{a_{n-1}+1, a_{n-1}\}$ המספרים אינם זרים, נצטרך להראות שישנו מחלק משותף הגדול מ1. אך מכיוון שעבור כל איבר a_{n-1} ישנו איבר נוסף $a_{n-1}+1$ (בעל אותם גורמים של a_{n-1} ובסכימה של 1). אזי כשנרצה להוציא גורם משותף גם לאיבר a_{n-1} וגם לאיבר "1"אזי נראה שמאחר והגורם של "1" הוא "1" בלבד, א"כ, הגורם המחלק המקסימלי של כל זוג מהצורה $\{a_{n-1}+1, a_{n-1}\}$ הוא 1.
לכן, ניתן להסיק, שכשנרצה להכניס n+1 יונים ל- n שובכים אזי נובע מעקרון שובך היונים שיש לפחות שתי יונים באותו תא.

מ.ש.ל.

ג.

נרצה להוכיח כי בכל בחירה של חמישה מספרים טבעיים שונים יש תמיד שלושה מתוכם שסכומם מתחלק

נגדיר את תאי השובך להיות 3 קבוצות הבאות:

א. קבוצת כל המספרים בעלי שארית חלוקה של 0 בחלוקה ב3 (כלומר, מהצורה של 3x+r כך שr=0)

ב. קבוצת כל המספרים בעלי שארית חלוקה של 1 בחלוקה ב3 (כלומר, מהצורה של 3x+r כך שr=1)

ג. קבוצת כל המספרים בעלי שארית חלוקה של 2 בחלוקה ב3 (כלומר, מהצורה של 3x+r כך שr=2)

a. המקרה הטריוויאלי הוא כאשר לפחות 3 מהמספרים הם בעלי אותה שארית חלוקה כך שנקבל:

$$(3x+r)+(3y+r)+(3z+r)=3(x+y+z)+3r=3(x+y+z+r\}$$

b. עבור המקרה בו אין 3 מהמספרים בעלי אותה שארית חלוקה אזי בהכרח נקבל ששתיים מתוך האיברים שנבחר הם בעלי שארית חלוקה x ושתיים מהאיברים הם בעלי שארית חלוקה y ואיבר אחד הוא בעל שארית חלוקה z.

כלומר, מאחר ונרצה להכניס 5 יונים ל3 שובכים כך שכל שובך מכיל 2 יונים לכל היותר אזי נובע מעקרון שובך היונים שיש לפחות יונה אחת בכל תא.

א"כ בהכרח עבור שלישייה זו (יונה אחת מכל תא) נקבל מספר המתחלק ב3:

$$(3x+0)+(3y+1)+(3z+2)=3(x+y+z)+3=3(x+y+z+1\}$$

מ.ש.ל

ד.

נרצה להוכיח שלכל $\mathrm{n}>1$ טבעי, ישנה קבוצה של $2\mathrm{n}-2$ מספרים טבעיים כך שסכום כל n מתוכם אינו מתחלק ב- n.

נבחר את הקבוצה:

$$\{n\ ,n+1\ ,2n\ ,2n+1\ ,3n\ ,3n+1\ \dots\}$$

כלומר, עבור כל $\mathrm{n}>1$ נקבל קבוצה של $2(n-1)$ איברים מהצורה:

$$\{n\ ,n+1\ ,2n\ ,2n+1\ ,3n\ ,3n+1\ \dots\}$$

כך ש$n-1$ מתוכם הינם כפולות של n (כלומר, שארית החלוקה שלהם ב- n הינה 0)

וכך ש$n-1$ מתוכם הינם כפולות של n בסכימה עם "1" (כלומר, שארית החלוקה שלהם ב- n הינה 1)

מאחר ונצטרך לסכום n איברים (מתוך האופציות: $n-1$ איברים עם שארית חלוקה של 0 בn, ומתוך $n-1$ איברים עם שארית חלוקה של 1 בn), אזי בהכרח לכל הפחות נסכום איבר אחד מתוך האיברים בעלי שארית החלוקה של 1. ולכל היותר n-1 איברים עם שארית חלוקה של 1.

כך שעבור כל n איברים שנבחר נקבל שארית חלוקה r כך ש- $1<\mathrm{r}<(\mathrm{n}-1)$ וא"כ מאחר ומתקבל ש- $\mathrm{r}<\mathrm{n}$ אזי בהכרח n אינו מחלק את r.

מ.ש.ל

2. א.

עבור הקבוצה $\mathcal{D}a = \{n \in N : a \mid n\}$ נוכיח:

$$a = b \Leftrightarrow D_a = D_b$$

<u>כיוון ראשון (מימין לשמאל):</u>

מאחר וע"פ הגדרת הקבוצה - הקבוצה D_a והקבוצה D_b מכילות את כל המספרים הטבעיים אשר מתחלקים בa או b בהתאמה, או בניסוח שונה, הקבוצות מכילות את כל המספרים הטבעיים אשר הינם כפולות של a או b בהתאמה,

אזי בהכרח אם הקבוצות שוות ומכיוון ש- a,b טבעיים, קיים להם איבר מינימלי חיובי המתקבל מכפולת a,b באיבר המינימלי של $n \in \mathbb{N}$,

א"כ, נקבל שהאיברים המינימליים הם $a \cdot 1 = b \cdot 1$ כך ש - $a = b$.

<u>כיוון שני (משמאל לימין):</u>

הכיוון השני מתקיים בהכרח על פי הגדרת הקבוצה.

מ.ש.ל

ב.

נרצה להוכיח:

$$\mathrm{lcm}(a_1, a_2, \dots, a_n) = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_{n-1}), a_n)$$

<u>כיוון ראשון (שמאל מחלק את ימין):</u>

נגדיר: $a = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_{n-1}), a_n)$

נגדיר: $b = \mathrm{lcm}(a_1, a_2, \dots, a_{n-1})$

נגדיר: $c = \mathrm{lcm}(a_1, a_2, \dots, a_n)$

ע"פ הגדרת LCM $a_1, a_2, \dots, a_{n-1}|b$ (כלומר, כל האיברים מ- a_1 עד a_{n-1} מחלקים את b)

א"כ, מכיוון ש- $a_n|a$ וגם $b|a$ וגם $a_1, a_2, \dots, a_{n-1}|b$ מתקיים ש:

$$\mathrm{lcm}(a_1, a_2, \dots, a_n)|a$$

כלומר, מאחר וכל האיברים מ- a_1 עד a_n מחלקים את a (a כפולה שלהם), אזי בהכרח $\mathrm{lcm}(a_1, a_2, \dots, a_n)$ (הכפולה המינימלית שלהם) מחלקת את a.

<u>כיוון שני (ימין מחלק את שמאל):</u>

ע"פ הגדרת LCM מתקיים:

$$a_1, a_2, \dots, a_n|c$$

א"כ, מכיוון ש- $a_n|a$ וגם $b|a$ וגם $a_1, a_2, \dots, a_{n-1}|b$ מתקיים ש:

$$\mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_{n-1}), a_n)|c$$

כלומר, מאחר וכל האיברים מ- a_1 עד a_n מחלקים את c (c כפולה שלהם), אזי בהכרח $\mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_{n-1}), a_n)$ (הכפולה המינימלית שלהם) מחלקת את c.

הראנו שכל אגף מחלק את האגף השני, לכן ניתן לומר ש:

$$\mathrm{lcm}(a_1, a_2, \dots, a_n) = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_{n-1}), a_n)$$

מ.ש.ל

ג.

אנו יודעים כי עבור זוג מספרים זרים a, b מתקיים. $\mathrm{lcm}(a,b) = a \cdot b$:

יהיו $a_1, a_2, \dots, a_n$ מספרים טבעיים <u>זרים בזוגות</u>

עבור $n \in N$ נוכיח באינדוקציה כי לכל $n \geq 2$ מתקיים:

$$\mathrm{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

<u>בסיס (n=2):</u>

$$\mathrm{lcm}(a_1, a_2) = \frac{a_1 \cdot a_2}{\gcd(a_1, a_2)}$$

על פי הגדרה שני מספרים שלמים נקראים מספרים זרים, אם המחלק המשותף המקסימלי שלהם הוא 1. במילים אחרות, GCD של שני מספרים זרים הוא 1, לכן נקבל:

$$\mathrm{lcm}(a_1, a_2) = a_1 \cdot a_2$$

<u>הנחה:</u>

נניח שהטענה נכונה עבור:

$$\mathrm{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

<u>צעד (נוכיח עבור n+1):</u>

נשתמש בהוכחת הסעיף הקודם:

$$\mathrm{lcm}(a_1, a_2, \dots, a_{n+1}) = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_n), a_{n+1})$$

כעת נוכל להשתמש בהנחה ולכן:

$$\mathrm{lcm}(\mathrm{lcm}(a_1, a_2, \dots, a_n), a_{n+1}) = \mathrm{lcm}((a_1 \cdot a_2 \cdot \dots \cdot a_n), a_{n+1})$$

לפי ההנחה לכל שני מספרים ב- $(a_1 \cdot a_2, \dots, a_n)$ מתקיים שה- GCD הוא 1, כלומר, אין גורמים משותפים. א"כ נוכל לחשב את הGCD של המספר $(a_1 \cdot a_2 \cdot \dots, a_n)$ והמספר a_{n+1} כך שמאחר וגם הם זרים ע"פ הנתון, אזי גם הGCD שלהם הוא 1. ולכן:

$$\mathrm{lcm}((a_1 \cdot a_2 \cdot \dots \cdot a_n), a_{n+1}) = \frac{(a_1 \cdot a_2 \cdot \dots \cdot a_n) \cdot a_{n+1}}{\gcd((a_1 \cdot a_2 \cdot \dots \cdot a_n), a_{n+1})}$$
$$= a_1 \cdot a_2 \cdot \dots \cdot a_n \cdot a_{n+1}$$

מ.ש.ל.

3. א.

נרצה להוכיח: $(a^n, b^n) = (a, b)^n$

נגדיר $d = (a, b)$. כלומר, a=dx, b=dy, כך ש- x,y זרים בהכרח, זאת מכיוון שלמדנו שכל מספר ניתן לפרק לכפולות של מספרים ראשוניים (ע"פ המשפט היסודי של האריתמטיקה) ובמידה והיה לx,y גורם (ראשוני) נוסף כלשהו שהוא משותף, אזי בהכרח הוא היה אחד מהגורמים של d.

עבור $\mathbf{a^n} = (dx)^n = d^n x^n,\ \mathbf{b^n} = (dy)^n = d^n y^n$ - כיוון ש- x,y זרים אזי גם x^n, y^n זרים מאחר והם כפולות של אותם גורמים ראשוניים כפי שהסברנו.

לכן אפשר להסיק שמכיוון שd מקסימלי עבור a,b, ומכיוון ש- x^n, y^n זרים, אזי עבור $d^n x^n, d^n y^n$ מתקיים ש- d^n הוא מחלק המשותף המקסימלי כי הוא כפולות של d (כאמור, d הוא היחיד בעל הגורמים המשותפים לa,b).

קיבלנו:

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

מ.ש.ל.

ב.

על פי הגדרת lcm:

$$\mathrm{Lcm}(a,b)\cdot\gcd(a,b)=ab$$

לכן, עבור:

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

נקבל:

a.

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

b.

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

c.

$$\frac{1}{\gcd\,(a^n,b^n)}=\frac{1}{\gcd\,(a,b)}$$

נותר להוכיח:

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

אכן, לפי סעיף א' מתקיים:

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

מ.ש.ל

4. א.

נמצא x,y שלמים כך ש: $2020x+243y=1$

ניתן לראות שבעצם מה שאנחנו מחפשים הוא צירוף לינארי של המספר 2020 והמספר 243 כך שנקבל את הספרה 1.

על פי המשפט שלמדנו: אוסף הצירופים הליניאריים של שני מספרים הם כפולות של הGCD שלהם, לכן ניתן לראות שגם כאן יש צירוף ליניארי מינימלי

נחשב את הGCD על פי האלגוריתם של אוקלידס. לאחר מכן, לפי גורמי המכפלה (שנקבל מתוצאות החילוק) נוכל "לחזור אחורה" בתהליך כך שנקבל את הצירוף הלינארי המבוקש.

$$2020=[8]\cdot 243+76$$
$$2020=[3]\cdot 76+15$$
$$2020=[5]\cdot 15+\mathbf{1}$$
$$76-5\cdot 15=1$$
$$76-5\cdot(243-3\cdot 76)=1$$
$$(2020-8\cdot 243)-5\cdot(243-3\cdot(2020-8\cdot 243))=1$$
$$2020-8\cdot 243-5\cdot 243+15\cdot 2020-120\cdot 243))=1$$
$$\mathbf{16}\cdot 2020-\mathbf{133}\cdot 243=1$$

מ.ש.ל

ב.

יהיו $a, b, c \in N$ כך ש$(a, b) = 1$ וכן $c|a + b$. נוכיח כי $(c, b) = (c, a) = 1$.

מאחר ונתון ש:

$$(a, b) = 1$$

ניתן להסיק ע"פ המשפט שלמדנו "אוסף הצירופים הליניאריים של שני מספרים הם כפולות של הGCD שלהם" ולהציג את $(a, b) = 1$ כצירוף לינארי:

$$ax + by = 1$$

בנוסף, מאחר ונתון ש- $c|a + b$ ניתן, ע"פ מפשט החלוקה, להציגו כך:

$$ck = a + b$$

עבור c,a נבודד את b ונציבו במשוואה הראשונה:

a. $ck - a = b$

b. $ax + (ck - a)y = 1$

c. $ax + cky - ay = 1$

d. $a(x - y) + c(ky) = 1$

ניתן לראות שעבור צירוף מסויים עבור a,c נקבל תוצאה מינימלית 1 כך שבהכרח מתקיים:

$$(c, a) = 1$$

באופן דומה נוכיח עבור c,b:

e. $ck - b = a$

f. $bx + (ck - b)y = 1$

g. $bx + cky - by = 1$

h. $b(x - y) + c(ky) = 1$

ניתן לראות שעבור צירוף מסויים עבור b,c נקבל תוצאה מינימלית 1 כך שבהכרח מתקיים:

$$(c, b) = 1$$

מ.ש.ל.

5.

יהיו $1 \le b \le a \le 2020$ טבעיים. נרצה להראות חסם מלעיל טוב ככל הניתן על מספר האיטרציות של האלגוריתם של אוקלידס על הקלט (a,b).

ע"פ האלגוריתם של אוקלידס הצעדים הינם:

עבור כל איטרציה נבצע על הקלט (a, b) את השלבים הבאים:

a. חלוקת המספר השמאל בימני:

a=qb+amodb

b. את המחלק נשרשר שמאלה ואת השארית נשרשר ימינה:

(b,amodb).

נחזור לבצע שוב איטרציה עד לקבלת שארית 0.

הוכחנו בתירגול 3 של משפט החלוקה שעבור כל $1 \le b < a$ מתקיים $\text{amodb} \le \frac{a}{2}$.

(לא נשקול את האפשרות ש- a=b כי ברור שתבוצע איטרציה אחת).

אזי, עבור כל איטרציה נמצא שהשארית לכל היותר חצי מהמספר המחולק (במקרה שלנו, המספר השמאלי). נשים לב שלאחר איטרציה אחת אותו מספר מתמקם בצד ימין. ורק לאחר איטרציה נוספת מתמקם שוב בצד שמאל. לכן, נמצא שעבור כל 2 איטרציות האיבר במיקום השמאלי קטן לכל הפחות פי 2 בכל 2 צעדים.

אם כן, על מנת למצוא חסם מלעיל נבחר בה"כ מספר מקסימלי a ונרצה לחשב את כמות הפעמים בהם קטן המספר a=2020 פי 2 בכל פעם (מכיוון שהוא קטן לכל הפחות פי 2 נחשב מקרה קיצון).
נחפש את x במשוואה הבאה (ולאחר מכן נכפיל אותו ב2, מכיוון שהוא קטן כל 2 איטרציות):

$$2^x = 2020$$

או על פי הגדרת הלוג נחשב את:

$$\log_2 2020$$

ונקבל:

$$\log_2 2020 = 10.98..$$

את התוצאה נכפיל פי 2, כיוון שאותו המספר קטן עבור כל 2 איטרציות.
לכן נקבל:

$$2\log_2 2020 = 2(10.98..) = 21.96..$$

כלומר, על פי החסם שמצאנו, נדרשות לכל היותר 22 איטרציות לביצוע האלגוריתם במקרה זה.

מ.ש.ל