מטלה מספר 4 – תורת המספרים

1. ה

נחשב את 4 הספרות האחרונות במספר 2^{2020}

נצטרך לחשב:

$$2^{2020}(\mathrm{mod}10{,}000)$$

מכיוון שמתקיים:

$$2^{2020}(\mathrm{mod}2^4\cdot 5^4)$$

מכיוון שמתקיים $\left(2^{2020},2^4\cdot 5^4\right)=2^4$ כי 2,5 ראשוניים זרים,

נשתמש בחוק הצימצום ונקבל:

$$2^{2016}(\mathrm{mod}5^4)$$

נשתמש בפונקציית אויילר.

נחשב את $\varphi(625)$:

$$\varphi(625)=\ \varphi(5^4\ )=\ 625\ \cdot\ \left(1\ -\frac{1}{5}\right)=500$$

מכיוון ש- $2\in\mathbb{Z}$ ומכיוון ש- $625\in\mathbb{Z}$ ומתקיים $(2,625)=(2,5^4)=1$ כי 2,5 ראשוניים זרים, אזי, ע"פ משפט אויילר מתקיים:

$$2^{\varphi(625)}\equiv 2^{500}\equiv 1(\mathrm{mod}625)$$

ולכן:

$$2^{2016}\equiv 2^{16}\cdot 2^{2000}\equiv 2^{16}\cdot(2^{500})^4\equiv 2^{16}\cdot(1)^4\equiv 2^{16}(\mathrm{mod}5^4)$$

$$2^{16}\equiv 2^3\cdot 2^{13}\equiv 2^3\cdot 8192\equiv 2^3\cdot 67\equiv 536(\mathrm{mod}5^4)$$

ומכיוון שמתקיים:

$$2^{2016}\equiv 536(\mathrm{mod}5^4)$$

ומכיוון ש- $(2^4,5^4)=1$

נקבל:

$$2^{2016}\cdot 2^4\equiv 536\cdot 2^4(\mathrm{mod}5^4\cdot 2^4)$$

כלומר,

$$2^{2020}\equiv 8576(\mathrm{mod}10{,}000)$$

קיבלנו כי 4 הספרות האחרונות במספר 2^{2020} הם 8576 .

מ.ש.ל

2. א.

יהיו $a, n \in \mathbb{N}$ שני שלמים זרים, ויהי $m \in \mathbb{N}$

א. נוכיח כי אם $\varphi(n)|m$ אזי $a^m \equiv 1 \pmod n$

מכיוון שע"פ הנתון $\varphi(n)|m$ כלומר, ע"פ משפט החלוקה, ישנו k

כך שמתקיים $m = k \cdot \varphi(n)$

אזי, מכיוון ש- $a, n \in \mathbb{N}$ שני שלמים זרים, ע"פ משפט אויילר נקבל:

$$a^m \equiv a^{k\cdot\varphi(n)} \equiv (a^k)^{\varphi(n)} \equiv 1 \pmod n$$

מ.ש.ל.

ב.

נוכיח כי אם $(m, \varphi(n)) = 1$ וגם $a^m \equiv 1 \pmod n$ אזי $a \equiv 1 \ (mod\ n)$

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 $n \in \mathbb{N}$ 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 ליניארי 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 לינארי 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 $1 \leq b \leq a \leq 2020$ 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 $1 \leq b < a$ מתקיים $\text{amodb} \leq \frac{a}{2}$.

(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