מטלה מספר 3 – ת.המספרים

.1

נראה כי אם $n \equiv 3(\mathrm{mod}\ 4)$ אזי n לא יכול להירשם כסכום של שני ריבועים שלמים, דהיינו:
לא קיימים x,y שלמים כך ש- $n = x^2 + y^2$.
ע"פ הגדרת שקלויות מתקיים $4k = n - 3 \gg n \equiv 3(\mathrm{mod}\ 4)$
נחלק למקרים.

<u>כאשר x , y אי-זוגיים</u> אזי שניהם מהצורה 2x+1 ולכן נקבל:

$$4k = 4x^2 + 4x + 1 + 4y^2 + 4y + 1 - 3$$
$$3 = 2(2x^2 + 2x + 2y^2 + 2y + 1 - 2k)$$

סתירה. קיבלנו באגף שמאל איבר בעל גורם ראשוני יחיד 3 ואילו באגף ימין קיבלנו איבר בעל גורם ראשוני 2 לכן אינם שווים.

<u>כאשר x , y זוגיים</u> אזי שניהם מהצורה של 2x+0 ולכן נקבל:

$$4k = 4x^2 + 4y^2 - 3$$
$$3 = 4(x^2 + y^2 - k)$$

סתירה. קיבלנו באגף שמאל איבר בעל גורם ראשוני יחיד 3 ואילו באגף ימין קיבלנו איבר בעל גורם ראשוני 2 לכן אינם שווים.

<u>כאשר x , y אינם שניהם זוגיים או אינם שניהם אי-זוגיים</u>. נניח בה"כ x זוגי כלומר, x מהצורה של 2x ואילו y מהצורה של 2y+1 ונקבל:

$$4k = 4x^2 + 4y^2 + 4y + 1 - 3$$
$$2 = 4(x^2 + y^2 + y - k)$$
$$2 = 2 \cdot 2(x^2 + y^2 + y - k)$$

סתירה. קיבלנו באגף שמאל איבר בעל גורם ראשוני יחיד 2 ואילו באגף ימין קיבלנו איבר בעל שני גורמים ראשוניים של 2 לכן אינם שווים.

מאחר וע"פ החלוקה למקרים הראנו שעבור כל האפשרויות נקבל סתירה אזי נובע מכך ש-n לא יכול להירשם כסכום של שני ריבועים שלמים.

מ.ש.ל

.2

יהי p_i הראשוני ה- i ברשימת הראשוניים. כלומר, $p_1 = 2 , p_2 = 3 , p_3 = 5 , \dots$.

נוכיח כי:

$$\forall i \in \mathbb{N}: p_i < 2^{2^i}$$

נוכיח באינדוקציה שלמה.

<u>בסיס:</u>

עבור $i = 1$ נקבל:

$$p_1 = 2 < 2^{2^1} = 4$$

<u>הנחה:</u>

נניח כי הטענה נכונה עבור כל המקרים $n \in \{1,2,\dots,i\}$ ונבדוק אם נכונותה לכל אלה גוררת נכונות עבור $n = i + 1$. כלומר, שמתקיים:

$$p_{i+1} < 2^{2^{i+1}}$$

<u>צעד:</u>

תחילה, נשים לב כי מתקיים האי שוויון הבא:

$$2^{2^i} \cdot 2^{2^{i-1}} \cdot \dots \cdot 2^{2^2} \cdot 2^{2^1} < 2^{2^i} \cdot 2^{2^i} = 2^{2^i} \cdot 2^{2^{i-1}} \cdot 2^{2^{i-1}}$$

$$= 2^{2^i} \cdot 2^{2^{i-1}} \cdot 2^{2^{i-2}} \cdot \dots \cdot 2^{2^4} \cdot 2^{2^3} \cdot 2^{2^2} \cdot 2^{2^1} \cdot 2^{2^1}$$

נשים לב שבאגף ימין הביטוי גדול פי 4 ולכן:

$$2^{2^i} \cdot 2^{2^{i-1}} \cdot \dots \cdot 2^{2^2} \cdot 2^{2^1} + 1 < 2^{2^i} \cdot 2^{2^{i-1}} \cdot 2^{2^{i-2}} \cdot \dots \cdot 2^{2^4} \cdot 2^{2^3} \cdot 2^{2^2} \cdot 2^{2^1} \cdot 2^{2^1}$$

כלומר, נקבל שמתקיים:

$$2^{2^i} \cdot 2^{2^{i-1}} \cdot \dots \cdot 2^{2^2} \cdot 2^{2^1} + 1 < 2^{2^i} \cdot 2^{2^i}$$

מאחר ואנו רוצים להוכיח נכונות עבור $n = i + 1$

נגדיר את האיבר הבא: $D = p_i \cdot p_{i-1} \cdot \dots \cdot p_2 \cdot p_1 + 1$

יתכן ש- D הוא ראשוני, אם D אינו ראשוני אזי הוא פריק ולפי למה 2 בהרצאת "פירוק ייחודי לגורמים ראשוניים" יש לו מחלק ראשוני q כך ש- $q = p_j$ עבור $j \in \{1,2,\dots,i\}$ כלשהו.

לכן, נקבל:

$$q | D - p_i \cdot p_{i-1} \cdot \dots \cdot p_2 \cdot p_1$$

כלומר $q|1$ שזה לא אפשרי כי $q \geq 2$. סתירה.

לכן, נסיק אחת משתי האפשרויות הבאות – 1. ישנו ראשוני נוסף (הקטן מ- D) שאינו מהקבוצה $p_i , p_{i-1} , \dots , p_2 , p_1$. 2. האיבר D בעצמו ראשוני.

ע"פ ההנחה מתקיים:

$$D = p_i \cdot p_{i-1} \cdot \dots \cdot p_2 \cdot p_1 + 1 < 2^{2^i} \cdot 2^{2^{i-1}} \cdot \dots \cdot 2^{2^2} \cdot 2^{2^1} + 1$$

ע"פ האי שוויון שהוכחנו מתקיים:

$$2^{2^i} \cdot 2^{2^{i-1}} \cdot \dots \cdot 2^{2^2} \cdot 2^{2^1} + 1 < 2^{2^i} \cdot 2^{2^i}$$

כלומר, בחיבור האי שוויוניים נקבל שמאחר והראשוני הנוסף ש"מצאנו" אינו גדול מ- D אזי ראשוני זה קטן מהביטוי $2^{2^i} \cdot 2^{2^i}$.

נובע מכך, שישנם i+1 מספרים ראשוניים הקטנים מהביטוי $2^{2^i} \cdot 2^{2^i}$ ולכן בהכרח:

$$p_{i+1} < 2^{2^{i+1}} = 2^{2 \cdot 2^i} = 2^{2^i} \cdot 2^{2^i} = 2^{2^{i+1}}$$

מ.ש.ל

3.

יהי p ראשוני כך ש $p+4, p+2$ גם הם ראשוניים. נוכיח כי p=3.

נחלק למקרים לפי שאריות החלוקה האפשרויות של p ב3.

שארית חלוקה 2: כלומר, כאשר p מהצורה p=3k+2.
שארית חלוקה 1: כלומר, כאשר p מהצורה כאשר p=3k+1.
שארית חלוקה 0: כלומר, כאשר p מהצורה p=3k+0. מאחר וp ראשוני וע"פ הגדרה מספר ראשוני מתחלק רק בעצמו וב1 לכן בהכרח נובע כי k=1 . כך ש- p=3.

נניח p מהצורה של p=3k+2.
ע"פ הנתון מתקיים שהאיבר p+4 גם הוא ראשוני. ע"פ ההנחה נקבל:

$$p+4=3\mathrm{k}+2+4=3\mathrm{k}+6=3(\mathrm{k}+2)$$

מאחר ו- p+4 ראשוני וע"פ הגדרה מספר ראשוני מתחלק רק בעצמו וב1 לכן בהכרח נובע כי k=-1 (כי k שרירותי), כך ש- $p+4=3$. אך ע"פ הנתון נקבל שמתקיים:

$$\mathrm{p}+2=\mathrm{p}+4-2=3-2=1$$

כלומר, נקבל:

$$\mathrm{p}+2=1$$

בסתירה לנתון ש- p+2 ראשוני.

נניח p מהצורה של p=3k+1.
ע"פ הנתון מתקיים שהאיבר p+2 גם הוא ראשוני. ע"פ ההנחה נקבל:

$$p+2=3\mathrm{k}+1+2=3\mathrm{k}+3=3(\mathrm{k}+1)$$

מאחר ו- p+2 ראשוני וע"פ הגדרה מספר ראשוני מתחלק רק בעצמו וב1 לכן בהכרח נובע כי k=0 (כי k שרירותי), כך ש- $p+2=3$. אך ע"פ הנתון נקבל שמתקיים:

$$\mathrm{p}=\mathrm{p}+2-2=3-2=1$$

כלומר, נקבל:

$$\mathrm{p}=1$$

בסתירה לנתון ש- pראשוני.

לכן, מכיוון וההנחות הנ"ל גוררות סתירה נותר לומר כי p=3 כך שנקבל:

$$p=3$$
$$p+2=3+2=5$$
$$p+4=3+4=7$$

ראשוניים.

מ.ש.ל

4.

יהי $p \geq 5$ ראשוני . נראה כי $\mathrm{p}^2 \equiv 1(\mathrm{mod}\ 24)$

ע"פ הנתון p ראשוני. ע"פ ההוכחה שהוכחנו בתרגול 3 של משפט החלוקה מתקיים כי 3 מספרים עוקבים מתחלקים ב3. כלומר, קיים גורם ראשוני 3 במכפלתם ובפרט עבור:

$$(p-1)(p)(p+1)$$

(1) ע"פ הנתון p הינו ראשוני כך ש- $p \geq 5$ ולכן בהכרח הינו גורם ראשוני השונה מ3.
א"כ, בהכרח נובע שבפירוק לגורמים של המכפלה:

$$(p-1)(p+1)$$

ישנו גורם ראשוני 3.

נשים לב כי ההפרש בין $p-1$ ל- $p+1$ הוא 2. ונשים לב כי אם $p \geq 5$ אזי $p-1 \geq 4$.
מאחר ו- p ראשוני וע"פ הגדרה מספר ראשוני מתחלק רק בעצמו וב1 לכן בהכרח נובע כי P מהצורה של p=2k+1.
א"כ, נוכל להציג את:

$$(p-1)(p+1)$$

כך:

$$((2k+1)-1)((2k+1)+1)$$
$$(2k)(2k+2)$$
$$(2k)2(k+1)$$
$$4k(k+1)$$

(2)
כאשר k זוגי. כלומר k מהצורה של k=2x, נקבל:

$$4(2x)(2x+1+1)$$
$$4(2x)(2x+2)$$
$$8x(2x+2)$$

כאשר k אי-זוגי. כלומר k מהצורה של k=2x+1, נקבל:

$$4(2x+1)(2x+1+1)$$
$$4(2x+1)(2x+2)$$
$$4(2x+2)(2x+1)$$
$$4 \cdot 2(x+1)(2x+1)$$
$$8(x+1)(2x+1)$$

כלומר, בשני המקרים קיבלנו שהביטוי $(p-1)(p+1)$ מתחלק ב8.

לכן נסיק שמאחר וע"פ (1) הביטוי $(p-1)(p+1)$ מתחלק ב3. ולכן בפירוק לראשוניים שלו ישנו גורם ראשוני 3.
ומאחר וע"פ (2) הביטוי $(p-1)(p+1)$ מתחלק ב8. ולכן בפירוק לראשוניים שלו קיימים הגורמים הראשוניים $2 \cdot 2 \cdot 2$.
אזי מתקיים ש:

$$24|\mathrm{p}^2-1$$

כך שבהכרח ע"פ הגדרה:

$$\mathrm{p}^2 \equiv 1(\mathrm{mod}\ 24)$$

מ.ש.ל

5.

הוכיח כי אם a מספר טבעי וגם $n \geq 2$ כך ש $a^n - 1$: ראשוני, אזי $a = 2$, n ראשוני.
נשתמש בזהות הבאה:
$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

<u>נוכיח a = 2.</u>
מאחר וע"פ הנתון $a^n - 1$ ראשוני וע"פ הגדרה מספר ראשוני מתחלק רק בעצמו וב1. לכן בהכרח נובע כי:
$$(a^{n-1} + a^{n-2} + \cdots + a + 1) = 1$$
או:
$$(a-1) = 1$$

אם:
$$(a^{n-1} + a^{n-2} +,,,, + a + 1) = 1$$
אזי a=0 ונקבל:
$$a^n - 1 = (0-1)(0+1) = -1.$$
אך 1- אינו ראשוני.
לכן נאמר:
$$(a-1) = 1$$
כך ש- a=2 ונקבל:
$$a^n - 1 = (1)(2^{n-1} + 2^{n-2} +,,,, + 2 + 1).$$
ע"פ הנתון $2^n - 1$ ראשוני ולכן $2^n - 1 \geq 2$. כלומר, $2^n \geq 3$ ולכן $n \geq 2$.
<u>נוכיח ש- n ראשוני.</u>
נניח בשלילה כי n פריק כך שקיימים $a, b > 1$ כך ש- $n = a \cdot b$.
נציג את הביטוי:
$$a^n - 1 = (a^{n-1} + a^{n-2} +,,,, + a + 1).$$
כך:
$$2^n - 1 = (2^{ab-1} + 2^{ab-2} + \cdots + 2^{ab-(b-1)a} + 2^{ab-ab}).$$
נשים לב שמאחר ו- n פריק אזי קיימים $a \cdot b$ איברים (מחזקת 0 עד חזקת $ab - 1$) ולכן ניתן יהיה לחלקם לקבוצות. נחלק את האיברים בה"כ ל- b קבוצות של a איברים ונקבל את הביטוי:
$$2^n - 1 = ((2^{ab-1} + \cdots + 2^{ab-a}) + (2^{(ab-a)-1} + \cdots + 2^{(ab-2a)}) + \cdots + (2^{ab-(b-1)a} + \cdots + 2^{ab-ab}).$$
נוציא גורם משותף $2^{(a-1)} + \cdots + 1$ עבור כל קבוצה כזאת:
$$2^n - 1 = ((2^{(ab-a)})(2^{(a-1)} + \cdots + 1) + (2^{(ab-2a)})(2^{(a-1)} + \cdots + 1) + \cdots + (2^{(ab-ab)})(2^{(a-1)} + \cdots + 1).$$
ונקבל:
$$2^n - 1 = (2^{(a-1)} + \cdots + 1)(2^{(ab-a)} + 2^{(ab-2a)} + \cdots + 2^{(ab-ab)}).$$
נשים לב כי עבור כל חזקה x בביטוי הנ"ל מתקיים $x \geq 0$ וע"פ חוקי מעריכית $2^x \geq 1$ עבור כל x כזה. לכן, מההנחה ש- n פריק נובע כי הביטוי $2^n - 1$ פריק (לגורמים הגדולים מ1).
נסיק כי מאחר ועל סמך הזהות ניתן לייצג את הביטוי $a^n - 1$ כך:
$$(a-1)(a^{n-1} + a^{n-2} +,,,, + a + 1)$$
ומאחר וזהות זו היא הכללה, כלומר, אף אם $a^n - 1$ ראשוני. נותר לומר שמכיוון שההנחה ש- n פריק גוררת סתירה, בהכרח n ראשוני.

מ.ש.ל.

6.

יהי n מספר טבעי המקיים $n \equiv 1 (\mathrm{mod}\ 4)$. נראה עבור אילו ערכים יכול n להיות שקול מודולו 8.

ע"פ הגדרת שקלויות מתקיים $n \equiv 1 (\mathrm{mod}\ 4) \gg 4k = n - 1$

כלומר, מתקיים:

$$n = 4k + 1$$

צ"ל את ערכי z האפשריים בשקילות הבאה:

$$4k + 1 \equiv z (\mathrm{mod}\ 8)$$

נחלק למקרים.

<u>כאשר k זוגי</u>. כלומר, k מהצורה של 2x. נקבל:

$$4(2x) + 1 \equiv z (\mathrm{mod}\ 8)$$
$$8x + 1 \equiv z (\mathrm{mod}\ 8)$$

ע"פ הגדרת שקלויות מתקיים:

$$8x \equiv 0 (\mathrm{mod}\ 8)$$

ולכן נקבל:

$$8x + 1 \equiv 1 \equiv z (\mathrm{mod}\ 8)$$
$$1 \equiv z (\mathrm{mod}\ 8)$$

<u>כאשר k אי-זוגי</u>. כלומר, k מהצורה של 2x+1. נקבל:

$$4(2x + 1) + 1 \equiv z (\mathrm{mod}\ 8)$$
$$8x + 4 + 1 \equiv z (\mathrm{mod}\ 8)$$
$$8x + 5 \equiv z (\mathrm{mod}\ 8)$$

ע"פ הגדרת שקלויות מתקיים:

$$8x \equiv 0 (\mathrm{mod}\ 8)$$

ולכן נקבל:

$$8x + 5 \equiv 5 \equiv z (\mathrm{mod}\ 8)$$
$$5 \equiv z (\mathrm{mod}\ 8)$$

לכן, נסיק כי עבור הערכים 1 , 5 יכול n להיות שקול מודולו 8.

מ.ש.ל