שאריות ריבועיות

1. הלמה של $Thue$: יהי $n > 1$ שלם, לכל a שזר ל-n קיימים $0 < |x|, |y| < \sqrt{n}$ כך ש-$a \equiv \frac{x}{y} \ mod \ n$.

<u>פתרון:</u> כמות הזוגות (x, y) כך ש-$0 \leq x, y \leq \lfloor \sqrt{n} \rfloor$ היא $\left(\lfloor \sqrt{n} \rfloor + 1\right)^2 > n$ ולכן יש שני זוגות $(x_1, y_1), (x_2, y_2)$ כך ש-

$$x_1 + ay_1 \equiv x_2 + ay_2 \ mod \ n$$

ולכן $(x_1 - x_2) \equiv a(y_2 - y_1)$ צריך רק להעיר ש-$x_1 - x_2$ ו-$y_1 - y_2$ שונים מ-0, אכן אם אחד מהם 0 אז גם השני ואז הזוגות שמצאנו אינם שונים.

2. יהי p ראשוני שהוא 3 מוד 4. הוכיחו כי אם יש כפולה של p מהצורה $a^2 + 5b^2$ אזי גם $2p$ הוא מהצורה $a^2 + 5b^2$.

<u>פתרון:</u> הנתון הוא שקיימים a, b כך ש-$p|a^2 + 5b^2$ כלומר ש--5 זו שארית ריבועית. מהלמה של תו נסיק שקיימים $0 < |c|, |d| < \sqrt{p}$ כך ש-$c \equiv \sqrt{-5}d \ mod \ p$ ולכן $p|c^2 + 5d^2 < 6p$. נסתכל מוד 4, ברור ש-c, d מזוגיות שונה ולכן $c^2 + 5d^2 \equiv c^2 + d^2 \equiv 1 \ mod \ 4$ ולכן $c^2 + 5d^2 \neq p, 4p, 5p$. נשאר לטפל במקרה ש-$c^2 + 5d^2 = 3p$. נכפיל את שני האגפים ב-$\frac{2}{3}$ ונחפש זהות מהצורה

$$(\alpha_1 c + \beta_1 d)^2 + 5(\alpha_2 c + \beta_2 d)^2 = \frac{2}{3}c^2 + \frac{10}{3}d^2$$

הגיוני לבקש $\alpha_1 = \alpha_2, \beta_1 = -5\beta_2$

ונקבל ש-$\beta_1^2 + 5\beta_2^2 = 30\beta_2^2 = \frac{10}{3}$ כלומר $\beta_2 = \pm\frac{1}{3}$ ו-$\alpha_1 = \pm\frac{1}{3}$.

נשאר לשים לב שאם $c \equiv d \ mod \ 3$ אז $\frac{c+5d}{3}, \frac{c-d}{3}$ שלמים, אחרת $\frac{c-5d}{3}, \frac{c+d}{3}$ שלמים. צריך להעיר גם שהנחנו ש-c, d לא מתחלקים ב-3 אבל במקרה זה p מתחלק ב-3 ולכן $p = 3$ ואכן $2 \cdot 3 = 1^2 + 5 \cdot 1^2$.

3. יהי $p > 3$ ראשוני ו-$\{q_1, q_2, \dots, q_{\frac{p-1}{2}}\}$ היא קבוצת כל השאריות הריבועיות מודולו p. האם קיימים a, b שלמים וזרים ל-p כך שהקבוצה $\{aq_1 + b, aq_2 + b, \dots, aq_{\frac{p-1}{2}} + b\}$ לא מכילה שאריות ריבועיות?

<u>פתרון:</u> נניח בשלילה שקיימים כאלו a, b, אז כל קבוצה

$$\{q_1 + \frac{b}{a}, q_2 + \frac{b}{a}, \dots, q_{\frac{p-1}{2}} + \frac{b}{a}\}$$

מכילה את כל השאריות הריבועיות או את כל השאריות הלא ריבועיות (כתלות באם a שארית ריבועית או לא).

למה: סכום השאריות הריבועיות/לא ריבועיות, מודולו p, מתחלק ב-p.
הוכחה: סכום השאריות הריבועיות מודולו p שקול ל-

$$\frac{1}{2}\sum_{i=1}^{p-1} i^2 \equiv \frac{p \cdot (p+1) \cdot (2p+1)}{12} \equiv 0 \; mod \; p$$

בשוויון האחרון השתמשנו בכך ש-$p > 3$. הוכחנו שסכום השאריות הריבועיות הוא 0 מוד p אך כיוון שסכום כלל השאריות הוא 0 נקבל שגם סכום השאריות הלא ריבועיות גם הוא מתחלק ב-p.

מהלמה נסיק ש-$\sum q_i \equiv 0$ ולכן מהנחת השלילה נקבל ש-

$$0 \equiv \sum_{i=1}^{\frac{p-1}{2}} q_i + \frac{a}{b} \equiv \frac{a}{b} \cdot \frac{p-1}{2}$$

וזו סתירה.

4. יהי $p \geq 7$ ראשוני. הוכיחו כי אחד מבין המספרים

$$p + 1, 2p + 1, 3p + 1, \dots, (p-3)p + 1$$

ניתן להצגה כסכום של שני ריבועים.

<u>פתרון ראשון:</u> $(3,4,5)$ זו שלשה פיטגוראית ולכן

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 \equiv 1 \; mod \; p$$

נשים לב שאפשר לשנות סימן ל-$\frac{3}{5}$ ו-$\frac{4}{5}$ כך שהם יהיו בטווח בין 1 ל-$\frac{p-1}{2}$ ולכן ניתן לבחור את הסימנים כך שיתקיים ש-

$$\left(\pm\frac{3}{5}\right)^2+\left(\pm\frac{4}{5}\right)^2<(p-1)^2$$

כלומר אגף שמאל הוא לכל היותר p^2-3p+1 כנדרש.

<u>פתרון שני:</u> בעצם גם הטענה הכללית יותר נכונה. לכל a שזר ל-p, בקבוצה $p+a,2p+a,\dots,\frac{(p-3)}{2}p+a$ יש מספר שניתן להציג כסכום שני ריבועים.

הטענה הכללית נובעת די בקלות מהשאלה הקודמת: אנחנו יודעים שבקבוצה $\{-x^2+a,1\le x\le\frac{p-1}{2}\}$ יש שארית ריבועית, כלומר קיים $1\le y\le\frac{p-1}{2}$ כך ש-$-x^2+a\equiv y^2$ ולכן

$$p|x^2+y^2-a<x^2+y^2\le\frac{(p-1)^2}{2}$$

וזה מנצח.

5. יהי p ראשוני אי-זוגי ויהיו $a\neq0,b,c$ שלמים. ידוע שקיימים $2p-1$ שלמים עוקבים עבורם ax^2+bx+c ריבוע שלם.
הוכיחו כי b^2-4ac מתחלק ב-p.

<u>פתרון:</u> נוסיף ל-$2p-1$ המספרים גם את המספר הבא ונסכום את סימני לז'אנדר של $2p$ המספרים. מהנתון נובע שהתוצאה אמורה לצאת $2p-2$ או $2p-1$ או $2p$. נחשב את הסכום הזה בדרך אחרת, נחלק אותו לשני רצפים באורך p ולכן בעצם צריכים לחשב את הסכום הבא:

$$\sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right)$$

נניח בשלילה ש-$D=b^2-4ac$ לא מתחלק ב-p, נניח גם ש-a לא מתחלק ב-p ובמקרה שהוא כן מתחלק נטפל בסוף.
נכפיל את הסכום שלנו ב-$\left(\frac{4a}{p}\right)=\left(\frac{a}{p}\right)$ ונקבל:

$$\left(\frac{4a}{p}\right)\cdot\sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right)=\sum_{x=1}^{p}\left(\frac{4a^2x^2+4abx+4ac}{p}\right)$$
$$=\sum_{x=1}^{p}\left(\frac{(2ax+b)^2-b^2+4ac}{p}\right)=\sum_{x=1}^{p}\left(\frac{x^2-D}{p}\right)$$
$$=\sum_{x=1}^{p}(x^2-D)^{\frac{p-1}{2}}=\sum_{x=1}^{p}\sum_{i=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{i}x^{p-1-2i}\cdot D^i$$
$$=\sum_{i=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{i}\cdot D^i\cdot\sum_{x=1}^{p}x^{p-1-2i}$$

כידוע

$$\sum_{x=1}^{p}x^k\equiv\begin{cases}-1 & p-1|k\\ 0 & p-1\nmid k\end{cases}\ mod\ p$$

הוכחה של הנוסחה הידועה: אם k מתחלק ב-$p-1$ אז כל המחוברים בסכום למעט $x=p$ יוצאים 1 ולכן סך הכל הסכום שקול ל-$p-1$. אם k לא מתחלק ב-$p-1$ אז נסמן ב-g שורש פרימיטיבי מוד p נקבל ש-

$$\sum_{x=1}^{p-1}x^k=\sum_{i=1}^{p-1}g^{ki}=g^k\cdot\frac{g^{(p-1)k}-1}{g^k-1}\equiv 0\ mod\ p$$

שימו לב שבשוויון האמצעי הנחנו ש-$g^k\neq 1$ כלומר ש-k לא מתחלק ב-$p-1$.

נחזור לחישוב בשאלה, מהנוסחה המוכרת נקבל:

$$\sum_{i=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{i}\cdot D^i\cdot\sum_{x=1}^{p}x^{p-1-2i}\equiv -1\ mod\ p$$

נסכם:

$$\sum_{x=1}^{p}\left(\frac{x^2-D}{p}\right)\equiv -1\ mod\ p$$

ברור שצד שמאל חסום בערכו המוחלט על ידי $p-1$ ולכן הוא שהוא שווה ל--1 או ל-$p-1$. אבל הסכום חייב לצאת אי-זוגי כיוון שיש בו כמות אי-זוגית של מחוברים אי-זוגיים: או ש-D לא שארית ריבועית ואז כל p המחוברים אי-זוגיים, או ש-D שארית ריבועית ואז שני מחוברים שווים ל-0 והשאר אי-זוגיים.

לפיכך הוכחנו ש-

$$(*)\sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right)=-\left(\frac{a}{p}\right)$$

ולכן הסכום המקורי (של $2p$ איברים) הוא לכל היותר 2, אבל מהנתון הסכנו שהוא לפחות $2p-3\geq 3$, סתירה.

נשאר לטפל במקרה ש-$p|a$, במקרה זה אפשר להניח ש-p לא מתחלק את b (אחרת ברור ש-b^2-4ac מתחלק ב-p) ואז נקבל ש-

$$\sum_{x=1}^{p}\left(\frac{bx+c}{p}\right)=0$$

וזו שוב סתירה.

<u>הערה:</u> לפי $(*)$ עבור $a=-1,b=0,c=1$ נקבל ש-

$$\sum_{x=1}^{p}\left(\frac{-x^2+1}{p}\right)=-\left(\frac{-1}{p}\right)$$

מכאן נוכל להסיק מסכנה מעניינת: כמות הפתרונות של המשוואה

$$x^2+y^2\equiv 1\ mod\ p$$

היא $p-(\frac{-1}{p})$, אכן עבור x קבוע יש $\left(\frac{-x^2+1}{p}\right)+1$, y-ים שעובדים ולכן סך הכל יש

$$\sum_{x=1}^{p} 1+\left(\frac{-x^2+1}{p}\right)=p-\left(\frac{-1}{p}\right)$$

שימו לב, מהנוסחה הזו ניתן לקבל עוד הוכחה לשאלה 4 (תוודאו).

הערה נוספת: ניתן לספור את כמות הפתרונות של $x^2+y^2\equiv 1$ גם בדרך אחר, למעשה רוצים לספור את כמות הנקודות על מעגל היחידה. במישור הפרויקטיבי המשוואה שלו היא $x^2+y^2-z^2\equiv 0$ ויש עליו $p+1$ נקודות (כמו על כל שניוינית לא מנוונת) כיוון שאפשר לבחור נקודה (לדוגמה $(0,1)$) על המעגל ולעביר דרכה ישר בכל אחד מ-$p+1$ הכיוונים האפשריים שיתנו $p+1$ נקודות חיתוך (אחת הפעמים מתאימה למשיק בנקודה שחברנו). בשביל לקבל את כמות הפתרונות צריך לחסר את כמות הנקודות באינסוף כלומר כמות הפתרונות כאשר $z=0$, כאשר -1 אינו שארית ריבועית אין נקודות באינסוף ובמקרה האחר יש בדיוק 2 באינסוף.
באותה השיטה מקבלים מייד את הנוסחה $(*)$ למקרה שהשניונית לא מנוונת (כלומר $p\nmid b^2-4ac$), מקרה שהשניונית מנוונת נדרשת יותר עבודה כיוון שצריך לעבור על המקרים השונים של הניוון.

6. יהי n שלם חיובי, מה היא כמות הפתרונות של המשוואה

$$x^2+y^2+z^2=2nxyz$$

מודולו p?

<u>פתרון:</u> המשוואה שקולה ל-

$$(z-nxy)^2=(n^2y^2-1)x^2-y^2$$

כמות הפתרונות שווה ל-

$$\sum_{y=0}^{p-1}\sum_{x=0}^{p-1} 1+\left(\frac{(n^2y^2-1)x^2-y^2}{p}\right)=$$

כאשר $n^2y^2-1\neq 0$ הסכום הפנימי שווה ל-$p-\left(\frac{n^2y^2-1}{p}\right)$ בשני המקרים בהם $ny\equiv\pm 1\ mod\ p$ הסכום הפנימי שווה ל-$p\left(1+\left(\frac{-1}{p}\right)\right)$

ולכן סך הכל הסכום שווה ל-

$$p^2 + 2p\left(\frac{-1}{p}\right) - \sum_{y=0}^{p-1}\left(\frac{n^2y^2 - 1}{p}\right)$$

$$= p^2 + 2p\left(\frac{-1}{p}\right) - \left(-\left(\frac{n^2}{p}\right)\right) = \left(p + \left(\frac{-1}{p}\right)\right)^2$$

7. יהי n שלם, הוכיחו שאם למשוואה

$$n = x^2 + xy + y^2$$

קיים פתרון ברציונליים אז יש לה פתרון גם בשלמים.

<u>פתרון:</u> למה: עבור ראשוני p קיימים שלמים a, b כך ש-$p = a^2 + ab + b^2$ אם ורק אם $p \equiv 1 \; mod \; 3$ או $p = 3$.

הוכחה: אם $p = 3$ אז $a = b = 1$ עובדים ומעכשיו נניח $p \neq 3$.

נתחיל מהכיוון הקל, אם אכן קיימים כאלו a, b, נחלק ב-b^2 ונקבל ש-$\left(\frac{a}{b}\right)^2 + \left(\frac{a}{b}\right) + 1 \equiv 0 \; mod \; 1$ אבל למשוואה $x^2 + x + 1 \equiv 0$ יש פתרון אם ורק אם -3 זו שארית ריבועית מוד p וזה קורה בדיוק כאשר p הוא 1 מוד 3:

אכן אם $p \equiv 1 \; mod \; 4$ אז

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = 1 \cdot \left(\frac{p}{3}\right)$$

אחרת

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = -1 \cdot \left(-\left(\frac{p}{3}\right)\right) = \left(\frac{p}{3}\right)$$

בכיוון ההפוך: הצעד היחיד שלא היה דו כיווני בטיעון הקודם הוא הגרירה שאם למשוואה $x^2 + x + 1 = 0$ יש פתרון מוד p אז קיימים a, b. נוכיח זאת. יהי r שורש של המשוואה הנ"ל, מהלמה של תו קיימים $0 < |a|, |b| < \sqrt{p}$ כך ש-$\frac{a}{b} \equiv r$ ולכן $a^2 + ab + b^2 \equiv 0 \; mod \; p$ ונשארנו עם שתי אפשרויות $a^2 + ab + b^2 = p, 2p$. האפשרות של $2p$ נפסל בקלות בגלל מוד 4, אם a, b אי זוגיים אז כך גם $a^2 + ab + b^2$ וכנ"ל במקרה שאחד מהם זוגי והשני אי זוגי, אם שניהם זוגיים אז $a^2 + ab + b^2$ יתחלק ב-4 כאשר $2p$ רק ב-2.

נעבור לפתרון השאלה עצמה:

נתון שקיים פתרון למשוואה

$$a^2 + ab + b^2 = c^2 n$$

נשים לב שאם $p \equiv 2 \; mod \; 3$ מחלק את n אז $a^2 + ab + b^2$ מתחלק ב-p שהוא 2 מוד 3 ומהוכחת הלמה נקבל ש-a, b צריכים להתחלק ב-p ולכן אגף שמאל מתחלק ב-p^2 ולכן ניתן לחלק ב-p^2, אפשר להמשיך לחלק ב-p^2 כל פעם ולכן נסיק $v_p(n)$ זוגי. כמובן ש-n ניתן להצגה בצורה $a^2 + ab + b^2$ אם ורק אם $\frac{n}{p^2}$ ניתן להצגה זו ולכן ניתן להניח ש-n חסר ריבועים ובעצם כל מה שנשאר להראות זה שאם n, m ניתן להצגה אז כך גם nm. זה נובע מהזהות:

$$\begin{aligned}(a^2 + ab + b^2) \cdot (c^2 + cd + d^2) \\ = (ac - bd)^2 + (ac - bd)(ad + bc + bd) \\ + (ad + bc + bd)^2\end{aligned}$$

מוטיבציה להמציא את הזהות.

$$\begin{aligned}\left(a + \frac{b}{2} + \frac{\sqrt{3}}{2} bi\right)\left(c + \frac{d}{2} + \frac{\sqrt{3}}{2} di\right) \\ = \left(ac - bd + \frac{ad}{2} + \frac{bc}{2} + \frac{bd}{2}\right) + \frac{\sqrt{3}}{2} i(ad + bd \\ + bc)\end{aligned}$$

8. הוכיחו כי לא קיימים a, b, c שלמים עבורם

$$3(ab + ac + bc) | a^2 + b^2 + c^2$$

<u>פתרון:</u> נניח בשלילה שקיימים a, b, c, n שלמים עבורם

$$3n(ab + ac + bc) = (a^2 + b^2 + c^2)$$

שזה שקול ל-

$$(a + b + c)^2 = (3n + 2)(ab + ac + bc)$$

נבחר ראשוני $p \equiv 2 \; mod \; 3$ שמחלק את $3n + 2$ בחזקה אי-זוגית, p מחלק את אגף ימין בחזקה זוגית ולכן p מחלק את $ab + ac + bc$ ולכן

$$a + b + c \equiv ab + ac + bc \equiv 0 \; mod \; p$$

כלומר

$$ab + c(a+b) \equiv ab - (a+b)^2 = -(a^2 + ab + b^2) \equiv 0$$

אם p מחלק את a אז הוא מחלק גם את b ואת c ואז אפשר לצמצם ב-p ואחרת קיבלנו שראשוני שהוא 2 מוד 3 מחלק את $a^2 + ab + b^2$ שזו סתירה.

9. יהי p ראשוני אי-זוגי. נסמן $n = \frac{p-1}{2}$, מצאו את כל ה-n-יות $(x_1, x_2, \dots, x_n)$ כך ש-

$$\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} x_i^2 \equiv \dots \equiv \sum_{i=1}^{n} x_i^n \ mod\ p$$

<u>פתרון:</u> ברור שאם כל ה-x_i-ים הם 0 או 1 אז כל הסכומים שווים. נראה שזו האופציה היחידה.

נסמן את הסומים הנתונים ב-S ונחשב את הסכום $\sum(x_i + 1)^n$:

$$\sum_{i=1}^{n}(x_i+1)^n = \sum_{i=1}^{n}\sum_{k}^{n}\binom{n}{k}x_i^k \equiv n - s + s \cdot \sum_{k}^{n}\binom{n}{k}$$
$$= n + s \cdot (2^n - 1) = n + s \cdot \left(\left(\frac{2}{p}\right) - 1\right)$$

אם 2 זו שארית ריבועית אזי $\sum(x_i + 1)^n = n$ ולכן כל המספרים מהצורה $x_i + 1$ הן שאריות ריבועיות (שונות מ-0).
נשים לב שהיינו יכולים לשנות במעט את הסכום שאנו מחשבים ובמקומו לחשב את $\sum(ax_i + 1)^n$ עבור a לבחירתינו. בתוצאה היינו מקבלים $n + s \cdot \left(\left(\frac{a+1}{p}\right) - 1\right)$, נבחר את $a + 1$ להיות שארית ריבועית ונקבל שכל המספרים מהצורה $ax_i + 1$ הן שאריות ריבועיות שונות מ-0.

לכל x_i, קיבלנו העתקה לינארית מקבוצת השאריות הריבועיות השונות מ-0,1 שמעבירה את השארית a לשארית $(a-1)x_i + 1$. אם $x_i \neq 0$ אז זו העתקה חח"ע ועל ולכן ניתן לסכום על כל השאריות הלא ריבועיות ששונות מ-0,1 ולקבל ש-

$$\sum_{a\neq 0,1,\left(\frac{a}{p}\right)=1} a = \sum_{a\neq 0,1,\left(\frac{a}{p}\right)=1} (a-1)x_i + 1$$
$$= \frac{p-3}{2}\cdot(1-x_i) + x_i \cdot \sum_{a\neq 0,1,\left(\frac{a}{p}\right)=1} a$$

ברור שהסכום על כל a-ים שווה ל--1 ולכן

$$-1 \equiv \frac{p-3}{2} - \frac{p-1}{2}x_i$$

כלומר $x_i \equiv 1$, ניצחון.

10. יהיו a, b, c שלמים חיוביים עבורם מתקיים ש-

$$\gcd(a,b) + lcm(a,b) = 2021^c .$$

אם ידוע ש-$|a-b|$ ראשוני, הוכיחו כי $(a+b)^2+4$ פריק.

<u>פתרון:</u> נניח ש-$a > b$ ונסמן $a - b = p$.
נחלק למקרים לפי האם a, b זרים או לא.

אם a, b זרים אז $ab = 2021^c - 1$ ולכן $bp + b^2$
$$(a+b)^2 + 4 = (p+2b)^2 + 4 = p^2 + 4bp + 4b^2 + 4$$
$$= p^2 + 4\cdot 2021^c$$

אם $p \neq 3$ ו-c אי זוגי אז $p^2 + 4\cdot 2021^c$ מתחלק ב-3 ולכן הביטוי שלנו פריק. אם $p = 3$ אז

$$(a+b)^2 = 4\cdot 2021^c + 5 \equiv 5 \; mod \; 43$$

ולכן 5 אמורה להיות שארית ריבועית מודולו 43 אבל

$$\left(\frac{5}{43}\right) = \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = -1$$

נשאר המקרה ש-$p \neq 3$ ו-c זוגי, במקרה זה נניח ש-$(a+b)^2 + 4 = q$ ראשוני אזי $q = p^2 + \left(2\cdot 2021^{\frac{c}{2}}\right)^2$ אבל כיוון שכל ראשוני ניתן להצגה כסכום של שני ריבועים בדרך אחת לכל היותר נקבל ש-

$p=2$ או $p=a+b$, האפשרות השנייה כמובן לא יכולה להתקיים כי $p=a-b$ ולכן נשארנו עם $a-b=p=2$ ו-$a+b=2\cdot 2021^{\frac{c}{2}}$ ולכן $a+b\equiv a-b\equiv 2\ mod\ 4$ שזה לא אפשרי (a,b זרים ולכן אי-זוגיים).

נעבור למקרה שבו a,b לא זרים. במקרה זה

$$\gcd(a,b)=\gcd(a-b,b)=\gcd(p,b)=p$$

ולכן $p|2021$ כלומר $p=43$ או $p=47$. נסמן $b=xp$, ונקבל ש-$a=(x+1)p$

$$p(x^2+x+1)=2021^c$$

אם $c>1$ אז $47|x^2+x+1$ אבל $47\equiv 2\ mod\ 3$ שזו סתירה ולכן $c=1$ ו-$p=47$ ולכן $x^2+x+1=43$ ולכן $x=6$
ו-$a=329, b=282$. נציב בביטוי שלנו ונבדוק שהוא פריק.

11. יהי ראשוני p, חשבו את מכפלת כל השאריות x מודולו p כך שגם x וגם $4-x$ אינן שאריות ריבועיות.

<u>פתרון:</u> למספרים שמקיימים את תנאי השאלה נקרא סוג א'. למספרים כך שגם x וגם $4-x$ נקרא סוג ב', אם מספר הוא מסוג א' או מסוג ב' נקרא לו טוב.

ברור שלכל מספר טוב x, $x(4-x)$ זו שארית ריבועית. לכל זוג מספרים טובים מהצורה $(x,4-x)$ נוכל להתאים מספר מסוג ב': $x(4-x)$,
הרי ברור ש-$x(4-x)$ שארית ריבועית אבל גם
$4-\big(x(4-x)\big)=x^2-4x+4$ שארית ריבועית. ההעתקה זו היא כמעט 2 ל-1, אכן אם $x(4-x)=y(4-y)$ אז או ש-$x=y$ או ש-$x+y=4$ (כי זו משוואה ריבועית ב-y ואלו בדיוק הפתרונות שלה), הנקודה היחידה שבה ההעתקה היא 1 ל-1 היא 4 (ברור ש-4 מסוג ב') שאליה הולך רק הזוג $(2,2)$.

נטען שהעתקה זו היא גם על. אכן אם $x,4-x$ שאריות ריבועיות אז קיים y כך ש-$4-x=y^2$ או לחילופין

$$x=(2-y)(2+y)=(y+2)\big(4-(y+2)\big)$$

ולכן ניתן להציג את x בצורה $z(4-z)$ וכיוון ש-x ריבוע חייבים ש-$z,4-z$ יהיו שניהם מסוג א' או שניהם מסוג ב'.

עכשיו קל לסיים, מכפלת כל האיברים הטובים שווה מצד אחד למכפלה של כל האיברים מסוג א' ומכפלת כל האיברים מסוג ב'. מצד שני בגלל ההעתקה שלנו נוכל לזווג את האיברים הטובים לזוגות כך שהמכפלה בכל זוג שווה לאיבר מסוג ב', חוץ מהמספר הטוב 2 שמותאם למספר מסוג ב'-4 ולכן מכפלת המספרים הטובים שווה לפעמיים מכפלת המספרים מסוג ב' ולכן מכפלת המספרים מסוג א' שווה ל-2.

12. א. יהי p ראשוני, הוכיחו כי השארית הלא ריבועית הקטנה ביותר קטנה מ-$\sqrt{p}+1$.

פתרון ראשון: נראה שקבוצת השאריות שקטנות מ-$\sqrt{p}+1$ יוצרת את $\mathbb{Z}/p\mathbb{Z}$. נניח בשלילה שזה לא המצב ונבחר את השארית x הקטנה ביותר שלא נוצרת ידי השאריות הקטנות. נכפיל את x ב-y שהיא השארית הקטנה ביותר כך ש-$xy > p$, כלומר $y = \left\lfloor \frac{p}{x} \right\rfloor + 1$. מצד אחד ברור ש-

$$\left\lfloor \frac{p}{x} \right\rfloor + 1 \leq \frac{p-1}{x} + 1 < \frac{p-1}{\sqrt{p}+1} + 1 = \sqrt{p}$$

ולכן y קטנה ומצד שני

$$p < xy = x\left\lfloor \frac{p}{x} \right\rfloor + x \leq p - 1 + x$$

ולכן ל-xy שארית שקטנה מ-x ולכן ניתן ליצור אותה אבל אז אפשר לחלק ב-y ואז אפשר ליצור גם את x.

נשאר לציין שאי אפשר ליצור את כל החבורה הכפלית רק עם שאריות ריבועיות.

<u>פתרון שני</u> (ניסוח אחר של הפתרון הקודם): תהי x שארית לא ריבועית מינימלית. כמו בפתרון הקודם נגדיר $y = \left\lfloor \frac{p}{x} \right\rfloor + 1$ ונשים לב ש-$p < xy < p + x$ ולכן xy שארית ריבועית ולפיכך

$$1 = \left(\frac{xy}{p}\right) = -\left(\frac{y}{p}\right)$$

ולכן y שארית לא ריבועית ולכן $x \leq y < \frac{p}{x} + 1$ כלומר $x < \sqrt{p} + 1$.

ב. בנוסף יהי n שלם חיובי. הוכיחו כי הקבוצה
$\{n, n+1, \dots, n+2\lfloor\sqrt{p}\rfloor+1\}$ מכילה שארית לא ריבועית.

<u>פתרון:</u> נסמן את הקבוצה המבוקשת ב-X ונסמן $X' = X\backslash\{0\}$. נניח בשלילה שכל איברי X הם שאריות ריבועיות ונבחר את השארית הלא ריבועית t הגדולה ביותר שקטנה מ-$\sqrt{p}+1$.

מהנחת השלילה נקבל שכל המספרים בקבוצה $t \cdot X'$ הם שאריות לא ריבועיות. הקבוצה tX' לא נחתך עם X אבל ב-X יש $2\lfloor\sqrt{p}\rfloor+2$ שלמים עוקבים וההפרשים בין כל שני איברים ב-X הם לכל היותר $2t < 2\sqrt{p}+2$ (כי יכול להיות 0 ואז יש צעד כפול) ולכן כל המספרים ב-tX' נמצאים בין שתי הזזות (ב-p) של X. ב-tX' יש לפחות $2\lfloor\sqrt{p}\rfloor+1$ איברים ולכן ההפרש בין המספר הגדול לקטן ב-tX' הוא לפחות $2t\lfloor\sqrt{p}\rfloor$ מצד שני כל האיברים צריכים להיכנס בקטע באורך $p-2\lfloor\sqrt{p}\rfloor-3$ כלומר

$$t \le \frac{p-2\lfloor\sqrt{p}\rfloor-3}{2\lfloor\sqrt{p}\rfloor}$$

מכאן ברור ש-$2t < \lfloor\sqrt{p}\rfloor+1$ ואבל t נבחר להיות השארית הלא ריבועית הגדולה ביותר ולכן 2 זו לא שארית ריבועית אבל מצד שני

$$\frac{p-2\lfloor\sqrt{p}\rfloor-3}{2\lfloor\sqrt{p}\rfloor} < \left\lfloor\frac{\lfloor\sqrt{p}\rfloor+1}{2}\right\rfloor$$

ולכן $\left\lfloor\frac{\lfloor\sqrt{p}\rfloor+1}{2}\right\rfloor 2$ לא שארית ריבועית וגם כי הם גדולים מ-t אבל קטנים מ-$\lfloor\sqrt{p}\rfloor+1$ אבל היחס ביניהם הוא 2 וזו סתירה.

ג. יהי $p \equiv 1 \ mod\ 4$ ראשוני. נסמן ב-X את כמות השאריות הלא ריבועיות מודולו p שלא עולות על $\sqrt{p}$. הוכיחו כי

$$|2X - \sqrt{p}| \le \sqrt{\frac{p+1}{2}}$$

<u>פתרון:</u> -1 שארית ריבועית ולכן אם a שארית לא ריבועית אז כך גם $-a$. מהלמה של $Thue$, לכל a, נוכל למצוא $0 < |b|, |c| < \sqrt{p}$ כך ש-$\frac{b}{c} \equiv a \bmod p$. כמובן שגם $\frac{-b}{-c} \equiv a \bmod p$, בנוסף $\frac{-b}{c} \equiv \frac{b}{-c} \equiv -a \bmod p$ ולכן בכל אחד מהזוגות $(b,c),(-b,-c),(b,-c),(-b,c)$ אחד המספרים הוא שארית ריבועית והשני לא. בדיוק באחד מבין ארבעת הזוגות, שני המספרים חיוביים ולכן לכל זוג שאריות ריבועיות נגדיות מצאנו זוג מספרים $0 < b,c < \sqrt{p}$ שאחד מהם שארית ריבועית והשני לא. נשאר לשים לב שכמות הזוגות האלו שווה ל-$2X(\lfloor\sqrt{p}\rfloor - X)$ (ה-2 בגלל שיש חשיבות לסדר) ולכן נקבל:

$$X(\lfloor\sqrt{p}\rfloor - X) \geq \frac{p-1}{8}$$

$$\left(X - \frac{\lfloor\sqrt{p}\rfloor}{2}\right)^2 \leq \frac{1 + 2\lfloor\sqrt{p}\rfloor^2 - p}{8}$$

$$\left(2X - \lfloor\sqrt{p}\rfloor\right)^2 \leq \frac{p+1}{2}$$

וזה מנצח.