תרגיל 3

1. שני מספרים טבעיים a ו-b ומספר ראשוני p מקיימים משוואה $a^2-b^2=p$. האם בהינתן p ניתן לשחזר את a ו-b? אם כן מצאו ביטוי מפורש ל-a ול-b באמצעות p. אם לא מצאו דוגמא נגדית.

פתרון. נשים לב שבהכרח $a>b$ כי p חיובי, בנוסף:

$$p=a^2-b^2=(a-b)\cdot(a+b)$$

ולכן אחד מהנכפלים 1 והשני p, אם $a+b=1$ אז בבירור $a=1,b=0$ וזה אינו פתרון עבור אף p, לכן:

$$\begin{cases} a-b=1 \\ a+b=p \end{cases}$$

ולאחר פתירת המשוואות נקבל $a=\frac{p+1}{2},b=\frac{p-1}{2}$ וזהו הפתרון היחיד.

2. p ראשוני גדול מ-5, הוכיחו שאפשר למצוא a,b,c שונים מבין $1,2,...,p-1$ כך ש:

$$\begin{cases} p\,|\,abc-1 \\ p|\,a+b+c \end{cases}$$

פתרון. בתור התחלה נשים לב שהשאלה היא לגמרי מודולו p, ולכן אין צורך לבחור את המספרים בין $1,2,...,p-1$, אלה רק שיהיו שונה מודולו p.

אם קיים מספר x כך ש:

$$p\,|\,1+x+x^2$$

אז נטען ש-$1,x,x^2$ פתרון, מכיוון ש-$p\neq 3$ קל לראות ש-$x\neq\pm 1(\mathrm{mod}\,p)$ ולכן שלושת המספרים שונים מודולו p. המשוואה השנייה בשאלה בבירור מתקיימת, בנוסף:

$$p\,|\,(1+x+x^2)\cdot(x-1)=x^3-1=1\cdot x\cdot x^2-1$$

ולכן גם המשוואה הראשונה מתקיימת, וסיימנו.

אם אין פתרון למשוואה הזו, אזי אם $x^3 = 1 (\mathrm{mod}\ p)$ נקבל ש:

$$(x-1)\cdot(x^2+x+1) = x^3 - 1 = 0 (\mathrm{mod}\ p)$$

המוכפל השני אינו מתחלק ב- p לפי ההנחה, ולכן נקבל ש- $x = 1 (\mathrm{mod}\ p)$.

מכאן שאם $x^3 = y^3 (\mathrm{mod}\ p)$ ושניהם לא מתחלקים ב p אז:

$$\left(\frac{x}{y}\right)^3 = 1 (\mathrm{mod}\ p)$$

$$\frac{x}{y} = 1 (\mathrm{mod}\ p)$$

$$x = y (\mathrm{mod}\ p)$$

לכן העלה בשלישית היא חד-חד-ערכית מודולו p , ולכן גם על, בפרט אפשר למצוא α כך ש:

$$\alpha^3 = -6 (\mathrm{mod}\ p)$$

נסתכל על המספרים $\frac{1}{\alpha}, \frac{2}{\alpha}, -\frac{3}{\alpha}$, הם מקיימים:

$$\frac{1}{\alpha} + \frac{2}{\alpha} - \frac{3}{\alpha} = 0 (\mathrm{mod}\ p)$$

$$-\frac{1}{\alpha}\cdot\frac{2}{\alpha}\cdot\frac{3}{\alpha} = -\frac{6}{\alpha^3} = -\frac{6}{-6} = 1$$

לכן אלה מקיימים את המשוואות, מכיוון ש- p גדול מ- 5 קל לראות שאלו שאריות שונות, ובכך סיימנו.

3. א. הוכיחו שיש אינסוף ראשוניים p כך ש- $p+1$ מתחלק ב- 4.

ב. הוכיחו שיש אינסוף ראשוניים p כך ש- $p+1$ מתחלק ב- 5.

פתרון. א. נניח והטענה שגוייה, כלומר יש כמות סופית של ראשוניים כאלו, נניח והם $p_1, p_2, ..., p_k$, נסמן $P = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$ ונסתכל על המספר $4P - 1$.

הוא לא מתחלק באף p_i, ולכן מתחלק רק בראשוניים השווים לאחד מודולו 4, לפי המשפט היסודי של האריתמטיקה אפשר לרשום אותו כמכפלה של מספרים ראשוניים, ולכן הוא שווה לאחד מודולו 4, אך המספר הזה הוא -1 מודולו 4 בסתירה.

ב. נעשה דבר דומה, נניח בשלילה ש- $p_1, p_2, ..., p_k$ כל הראשוניים האלו, ונסמן $P = p_1 \cdot p_2 \cdot ... \cdot p_k$, ונסתכל על המספר $4P^2 - 5$, נניח q ראשוני המחלק את המספר הזה, אז מתקיים:

$$(2P)^2 = 5 (\mathrm{mod}\, q)$$

כלומר 5 שארית ריבועית מודולו q, נטען שמכאן נובע ש $q = \pm 1 (\mathrm{mod}\, 5)$, זוהי מסקנה מההדדיות הריבועית של גאוס, אך נראה את זה ישירות.

נניח בשלילה ש- $q = 3 (\mathrm{mod}\, 5)$, כלומר אפשר לרשום אותו כ- $q = 10k + 3$, נקרא לשאריות $1, 2, ..., 5k+1$ שאריות חיוביות, ולשאר שליליות, השאריות מתחלקות לזוגות של x ו- $-x$, שבכל זוג אחת השאריות חיוביות והשנייה שלילית, אם נכפיל את כל השאריות החיוביות ב- 5 נקבל שארית אחת מכל זוג, נבין מה החיוביות.

כאשר נכפיל את השאריות $1, 2, ..., k$ ב- 5 נקבל שאריות חיוביות.

כאשר נכפיל את השאריות $k+1, k+2, ...2k$ ב- 5 נקבל שאריות שליליות.

כאשר נכפיל את השאריות $2k+1, 2k+2, ..., 3k$ ב- 5 נקבל שאריות חיוביות.

כאשר נכפיל את השאריות $3k+1, 3k+2, ...4k, 4k+1$ ב- 5 נקבל שאריות שליליות.

כאשר נכפיל את השאריות $4k+2, 4k+3, ..., 5k+1$ ב- 5 נקבל שאריות חיוביות.

מכפלת השאריות שקיבלנו היא מצד אחד מכפלת השאריות $1, 2, ..., 5k+1$ כפול 5^{5k+1}, מצד שני מודולו q זה אותה המכפלה, רק עם שינוי סדר והשמת מינוס על כל שארית שיצאה שלילית, כמות השאריות שיצאו שליליות היא $2k+1$ ולכן קיבלנו ש:

$$5^{5k+1} = -1 (\mathrm{mod}\, q)$$

אך מצד שני אנו יודעים ש- $(2P)^2 = 5 (\mathrm{mod}\, q)$ ולכן קיבלנו:

$$(2P)^{q-1} = (2P)^{10k+2} = 5^{5k+1} = -1 (\mathrm{mod}\, q)$$

אך זה סותר את משפט פרמה שאומר ש- $(2P)^{q-1} = 1 (\mathrm{mod}\, q)$.

המקרה $q=2(\mathrm{mod}5)$ נעשה באותה שיטה.

נחזור לשאלה, P מתחלק בכל ראשוני שהוא -1 מודולו 5, ולכן אף ראשוני כזה לא מחלק את $4P^2-5$, כלומר כל הראשוניים שמחלקים אותו מקיימים $q=1(\mathrm{mod}5)$ מכאן נקבל לפי המשפט היסודי של האריתמטיקה ש-$4P^2-5=1(\mathrm{mod}5)$, אך קל לראות מהגדרה שהוא שווה ל--1 מודולו 5, בסתירה.

4. הראו שיש אינסוף שלשות (x,y,z) של מספרים רציונלים כך ש:

$$x^3+y^3+z^3=2$$

פתרון. נתחיל מלשים לב שעל ידי הכפלה בקבוע המשוואה שקולה למשוואה:

$$x^3+y^3+z^3=2w^3$$

נתחיל לחשב:

$$(x^2+x)^3=x^6+3x^5+3x^4+x^3$$

נרצה לצמצם חלק מהדברים, ולכן נוריד את אותו הביטוי עם מינוס איקס:

$$(x^2-x)^3=x^6-3x^5+3x^4-x^3$$

$$(x^2+x)^3-(x^2-x)^3=6x^5+2x^3$$

פה יש את $2x^3$ כמו שרצינו, יש רק להפטר מה-$6x^5$, אם הוא חזקה שלישית אנחנו אכן יכולים לעשות את זה, לכן נציב $x=6a^3$ ונקבל:

$$(36a^5)^3=6^6a^{15}=6\cdot(6a^3)^5=6x^5$$

סך הכל קיבלנו ש:

$$(36a^6+6a^3)^3+(6a^3-36a^6)^3+(-36a^5)^3=2\cdot(6a^3)^3$$

$$(1+6a^3)^3+(1-6a^3)^3+(-6a^2)^3=2$$

ואלו אינסוף פתרונות כרצוי.

5. נתון p ראשוני, מצאו עבור אלו a טבעיים:

$$p \mid 1^a + 2^a + 3^a + ... + (p-1)^a$$

פתרון. הטענה שגוייה אם ורק אם $p-1 \mid a$.

אם $p-1 \mid a$ אז לפי משפט פרמה כל הנסכמים הם 1 מודולו p , ולכן כל הסכום הינו -1 מודולו p , אחרת, ניקח מספר g שלא מתחלק ב p ובנוסף:

$$g^a \neq 1 (\text{mod } p)$$

קיים כזה מכיוון שאם בשלילה אין כזה, אז כל מספר שלא מתחלק ב- p מקיים $g^a = 1 (\text{mod } p)$, לפי פרמה הקטן, כולם גם יקיימו $g^{\gcd(a, p-1)} = 1 (\text{mod } p)$, אבל $\gcd(a, p-1) < p-1$, ולפולינום כמות השורשים חסומה בדרגה, בסתירה, ולכן קיים מספר כזה.

נסמן:

$$M = 1^a + 2^a + ... + (p-1)^a$$

ונכפיל ב- g^a , ונקבל:

$$g^a M = (g \cdot 1)^a + (g \cdot 2)^a + ... + (g \cdot (p-1))^a$$

אך מכיוון שהכפלה במספר שזר ל- p היא פעולה הפיכה מודולו p , נקבל שסכום זה הוא פשוט סידור מחדש של הסכום הקודם מודולו p , כלומר:

$$g^a M = M (\text{mod } p)$$

$$(g^a - 1) M = 0 (\text{mod } p)$$

אבל $g^a - 1$ אינו מתחלק ב- p לפי הבחירה שלו, ולכן M מתחלק ב- p וסיימנו.

6. לכל מספר טבעי $n > 1$, נסמן $P(n)$ הראשוני הגדול ביותר שמחלק את n . הוכיחו שיש אינסוף שלשות (a,b,c) של מספרים טבעיים כך ש:

$$P(a^2+1) = P(b^2+1) = P(c^2+1)$$

פתרון. נסמן $f(x) = P(x^2+1)$. נתחיל מלשים לב לנוסחא המגניבה הבאה:

$$(x^2+1) \cdot ((x+1)^2+1) = (x \cdot (x+1) + 1)^2 + 1$$

אכן, נפתח ונקבל:

$$(x^2+1)\cdot((x+1)^2+1)=x^2\cdot(x+1)^2+x^2+(x+1)^2+1=$$
$$=x^2\cdot(x+1)^2+2x\cdot(x+1)+1+1=(x\cdot(x+1)+1)^2+1$$

מכאן נקבל ש:

$$f(x\cdot(x+1)+1)=\max(f(x),f(x+1))$$

אם עבור x מסוים מתקיים $f(x)>f(x+1),f(x-1)$ אז נקבל:

$$f(x(x+1)+1)=f(x)=f(x(x-1)+1)$$

וזו שלישייה כמו שמבוקש, לכן נניח בשלילה שיש כמות סופית של x כאלו, כלומר עבור x גדול מספיק, אם $f(x-1)<f(x)$ אז $f(x)<f(x+1)$.

מכיוון שהפונקציה לא יכולה תמיד לקטון כי היא שלמה וחיובית, מתישהו תהיה עלייה, ולכן משם הפונקציה תהיה מונוטונית, אבל אז:

$$f(x(x+1)+1)=f(x+1)<f(x+2)<....<f(x(x+1))<f(x(x+1)+1)$$

בסתירה.

פתרון נוסף. נחפש זוגות מספרים (a,b) כך ש-$a^2+1=2(b^2+1)$, במקרה הזה באופן די ברור $f(a)=f(b)$ שזו התקדמות טובה, נראה שאפשר למצוא אינסוף זוגות כאלה.

אנחנו רוצים למצוא פתרונות למשוואה:

$$a^2-2b^2=1$$

כדי לעשות את זה נשים לב ש-$(3,2)$ הוא פתרון, בנוסף יש נוסחא מגניבה:

$$(a^2-2b^2)(c^2-2d^2)=(ac+2bd)^2-2(ad+bc)^2$$

ובפרט, אם (a,b) פתרון למשוואה, אז:

$$(3a+4b)^2-2(2a+3b)^2=(a^2-2b^2)(3^2-2\cdot2^2)=1$$

ולכן אפשר למצוא אינסוף פתרונות כאלו, ואפילו אפשר לרשום להם נוסחא:

$$a=\sum_{0\le 2k\le n}\binom{n}{2k}\cdot 2^k\cdot 2^{2k}\cdot 3^{n-2k}$$
$$b=\sum_{0\le 2k+1\le n}\binom{n}{2k+1}\cdot 2^k\cdot 2^{2k+1}\cdot 3^{n-2k-1}$$

ועבור כל n זהו זוג פתרונות.

נחזור לשאלה, מצאנו ש $f(a)=f(b)=p$, יש למצוא מספר שלישי, נגדיר a' להיות שקול ל- a מודולו p ובנוסף $1\le a'<p$, ונטען ש- $f(a')=f(p-a')=p$, בתור התחלה מהגדרה:

$$p\mid a'^2+1,(p-a')^2+1$$

מכיוון שהוא מחלק את a^2+1, מצד שני, מתקיים:

$$a'^2+1,(p-a')^2+1\le(p-1)^2+1=p^2-2p+2<p^2$$

ולכן כל המחלקים האחרים שלהם חייבים להיות קטנים מ- p .

מצאנו 4 מספרים ש- f שווה עליהם, אבל אולי חלקם אותו דבר, המקרה היחיד הבעייתי הוא אם $\{a,b\}=\{a',p-a'\}$, במקרה זה נקבל ש- $a+b=p$, לכן אם נראה שזה לא יכול לקרות אינסוף פעמים, נסיים.

נשתמש בנוסחאות, נזכור טענה שמקדם בינומי $\binom{5^r}{k}$ תמיד מתחלק ב- 5 חוץ מב- $k=0,5^r$, לכן $a+b$ עבור $n=5^r$ מודולו 5 יוצא:

$$3^n+2^{\frac{n-1}{2}}\cdot 2^n$$

אם $\frac{n-1}{2}$ מתחלק ב-4 אז $2^{\frac{n-1}{2}}=1(\mathrm{mod}\,5)$, ולכן מודולו 5 נקבל:

$$a+b=3^n+2^{\frac{n-1}{2}}\cdot 2^n=3^n+(-3)^n=0(\mathrm{mod}\,5)$$

כי n אי-זוגי, $\frac{n-1}{2}$ מתחלק ב-4 כאשר r זוגי, וזה קורה אינסוף פעמים.

סך הכל קיבלנו שיש אינסוף פעמים שבהם $a+b$ מתחלק ב-5, ולכן לא יכול להיות שווה לראשוני, ולכן מצאנו אינסוף שלישיות.