תרגיל 7

1. רינה רושמת את כל הריבועים של מספרים טבעיים $1,4,9,16,25,...$. לאחר מכן היא רושמת הפרש של כל שני מספרים בשורה הקודמת. האם קיים מספר שמופיע ברשימה השנייה יותר מפעם אחת? האם קיים מספר שמופיע ברשימה השנייה 7 פעמים בדיוק?

פתרון. $a^2-b^2=(a-b)(a+b)$. כלומר מספר שמופיע ברשימה הוא מספר שאפשר להציג אותו כמכפלה של שני מספרים מסוג $m=a+b$ ו-$n=a-b$. זה אומר ש-m ו-n הם מספרים בעלי אותה זוגיות, וש-$m>n$. מצד שני, אם m ו-n הם מספרים בעלי אותה זוגיות שאחד מהם גדול מהשני, אז ניתן להציג אותם כ-$m=a+b$ ו-$n=a-b$, $a=\frac{m+n}{2}$ ו-$b=\frac{m-n}{2}$. לכן השאלה היא בעצם, האם קיים מספר שניתן להציג אותו כמכפלה של שני מספרים בעלי אותה זוגיות בדרכים שונות, ובפרט ב-7 דרכים שונות בדיוק.

למשל ניקח 3^{13}. אפשר להציגו בצורה 1×3^{13}, 3×3^{12}, $3^2\times 3^{11}$, . . . , $3^6\times 3^7$ ואלה כל ההצגות שקיימות. מש"ל.

2. האם קיימת סדרה אינסופית של מספרים טבעיים $a_1,a_2,a_3,...,a_n,...$ כך שלכל n הסכום $a_1^2+a_2^2+a_3^2+...+a_n^2$ הוא בהכרח ריבוע שלם?

פתרון. ננסה לבנות את הסדרה בשלבים. נרצה שיתקיים $a_1^2+a_2^2+a_3^2+...+a_n^2=b_n^2$, לכל n. אם כבר הצלחנו לבנות $n-1$ שלבים בסדרה ומחפשים איבר a_n שימשיך את הסדרה, בעצם נרצה שיתקיים $b_{n-1}^2+a_n^2=b_n^2$, כאשר המספר b_{n-1} כבר נתון, ואת המספרים הטבעיים a_n,b_n צריך עוד למצוא.

כלומר נרצה להציג מספר קיים בצורה $b_n^2-a_n^2$.

למשל אם $b_{n-1}^2=2k+1$ אי-זוגי גדול מ-1, אפשר לעשות זאת: $b_{n-1}^2=(k+1)^2-k^2$.

מכאן מקבלים תהליך שיוצר סדרה. אם $a_1=b_1=3$, אז $a_2=4,\ b_2=5$ ואז $a_3=13$ וכך הלאה: $...+84^2+\underbrace{\underbrace{3^2+4^2}_{5^2}+12^2}_{13^2}$ $_{85^2}$

צריכים להוכיח שהתהליך לא יעצור. על מנת שהתהליך ימשיך באותה צורה, צריך שבכל שלב נקבל b_n אי-וזגי. הגדרנו את b_n בתור $k+1$ כאשר $b_{n-1}^2=2k+1$, במילים אחרות $b_n=\frac{1}{2}\left(b_{n-1}^2+1\right)$, וצריך להראות שבאופן כזה עוברים ממספר אי-זוגי למספר אי-זוגי.

אבל אם $b_{n-1}=2\ell+1$, אז $b_{n-1}^2=4\ell^2+4\ell+1=4k+1$ ולכן

$$b_n=\tfrac{1}{2}\left(4k+1+1\right)=2k+1$$

מש"ל.

הערה. בעצם, כל מספר אי-זוגי שגדול מ-1 וכל מספר שמתחלק ב-4 וגדול מ-4 הוא הפרש של שני ריבועים שונים, ולכן אם מתחילים סדרה אם $a_1>2$ תמיד אפשר להמשיך את הסדרה בכל שלב.

3. האם קיימים מספרים שלמים חיוביים שונים m,n,s,t עבורם $\sqrt{m}+\sqrt[3]{n}=\sqrt{s}+\sqrt[3]{t}>2004$ ובנוסף גם $m+n=s+t$?

פתרון. במילים אחרות $\sqrt{m}-\sqrt{s}=\sqrt[3]{t}-\sqrt[3]{n}$ ובנוסף גם $m-s=t-n$. האגפים לא מתאפסים כי המספרים אמורים להיות שונים ולכן אפשר לחלק משוואה.

נסמן $a=\sqrt{m}$, $b=\sqrt[3]{n}$, $c=\sqrt{s}$, $d=\sqrt[3]{t}$.

אז $a-c=d-b$ ובנוסף $a^2-c^2=d^3-b^3$ ולכן $a+c=b^2+bd+d^2$.

אם ניקח b,d כלשהם, יש לנו $a-c$ ו-$a+c$ ונוכל לחזר אותם אם המספרים הם באותה זוגיות. זה קורה אם bd זוגי, הרי הזוגיות של $b+d$ זהה לזוגיות של b^2+d^2. למשל אם ניקח $b=7$, $d=10$ אז $a+c=100+70+49=219$ וכן $a-c=3$ ולכן $a=111$, $c=108$ והמספרים במקור הם $111^2,7^3,108^2,10^3$.

כלומר 12321,343,11664,1000 וכולם שונים. כמובן יש גם דוגמאות אחרות רבות.

4. למספר חיובי שלם n לוקחים את 4 המחלקים הקטנים ביותר שלו $a<b<c<d$ (שגם הם שלמים חיוביים). מצאו את כל הערכים של n עבורם $n=a^2+b^2+c^2+d^2$.

תשובה. רק 130.

פתרון. ברור כי $a=1$. אם n אי-זוגי, כל המחלקים שלו אי-זוגיים, ואז n הוא סכום של 4 מספרים אי-זוגיים, ולכן n זוגי. לכן $b=2$.

מכאן $1+2^2+c^2+d^2$ זוגי, לכן c ו-d הן מזוגיות שונה: אחד מהם זוגי והשני אי-זוגי. מחלק אי-זוגי הכי קטן של n שהוא לא 1 הוא מספר ראשוני p. המחלק האחר שנמצא בין 4 מחלקים הקטנים ביותר חייב להיות זוגי, לכן הוא 4 או $2\cdot p$, תלוי אם n מתחלק ב-4 או לא. ובכן צריך לבדוק שני מקרים:

א. $n=1^2+2^2+p^2+4^2$, כאשר p ראשוני אי-זוגי של n, אבל מודולו 4 מקבלים $n=1+\left(2k+1\right)^2=2\left(\mathrm{mod}\,4\right)$ ולכן n לא מתחלק ב-4, בפרט 4 הוא לא אחד מ-

המחלקים הקטנים ביותר שלו כי הוא בכלל לא מחלק.

ב. $n=1^2+2^2+p^2+(2p)^2$ כאשר p מחלק ראשוני של n ולכן p מחלק של $1^2+2^2=5$ ולכן $p=5$.

במקרה זה $n=1^2+2^2+5^2+10^2=130=1\cdot 2\cdot 5\cdot 13$ ומחלקים הכי קטנים של מספר זה הם אכן 1, 2, 5 ו-10, לכן מספר זה מתאים.

5. מצאו מספר $100\le n\le 1997$ כך ש-2^n+2 מתחלק ב-n.

פתרון. בפירוק של n לגורמים ראשוניים 2 יכול להופיע בחזקה אפסית או ראשונה, כי 2^n+2 מתחלק ב-2 אבל לא ב-4. הגורמים הראשוניים האחרים חייבים להיות אי-זוגיים.

אם ניקח ראשוני אי-זוגי בודד p, אז 2^p+2 לא מתחלק ב-p מכיוון ש-$2^p+2=2+2=4\pmod p$, וגם $2^{2p}+2$ לא יתחלק ב-p מסיבה דומה. לכן ננסה למצוא את התשובה בצורה pq או $2pq$, כאשר p ו-q הם ראשוניים אי-זוגיים. כלומר נרצה ש-$2^{pq}+2$ או $2^{2pq}+2$ יתחלק ב-pq (כי הוא יתחלק ב-2 בכל מקרה).

ננסה $p=3$, כלומר $n=3q$ או $n=6q$. אם 2^n+2 מתחלק ב-3, אז n זוגי, כלומר $n=6q$. אבל נרצה שגם 2^n+2 יתחלק ב-q, כלומר $2^6+2=2^{q\cdot 6}+2=0\pmod q$, וזאת אומרת ש-$q$ מחלק את 66 כלומר q כנראה 11, אבל 66 מספר קטן מדי.

ננסה $p=5$, כלומר $n=5q$ או $n=10q$. אם 2^n+2 מתחלק ב-5, אז $n=3\pmod 4$, כלומר $n=5q$, כאשר גם $q=3\pmod 4$. אבל נרצה שגם 2^n+2 יתחלק ב-q, כלומר $2^5+2=2^{q\cdot 5}+2=0\pmod q$. זאת אומרת ש-$q$ מחלק את 34 כלומר $q=17$ אבל אז לא מתקיים ש-$q=3\pmod 4$.

ננסה $p=7$, ונראה שאף פעם 2^n+2 לא מתחלק ב-7 לאף n.

לא נתייאש כי זה נוגד את ערך האלימות וננסה $p=11$. אז $n=11\cdot q$ או $n=22\cdot q$. בדיקה פשוטה מראה כי 2^n+2 מתחלק ב-11 אך ורק כאשר $n=6\pmod{10}$ ולכן n זוגי כלומר $n=22\cdot q$. דרישה נוספת היא $2^{22}+2=2^{q\cdot 22}+2=0\pmod q$, במילים אחרות $2^{21}=-1\pmod q$, כלומר כדאי שהסדר של 2 יהיה 42, כלומר נרצה לבדוק ראשוניים מהסוג $42m+1$ שהקטן מהם הוא 43.
כלומר השאלה היא האם מתקיימת הזהות $2^{21}=-1\pmod{43}$. דרך פשוטה לענות על השאלה הזו היא הדדיות ריבועית. אכן 43 הוא 3 מודולו 8, לכן 2 אינו ריבועי מודולו 43, לכן הזהות אכן מתקיימת. בנוסף $2\cdot 43=6\pmod{10}$.

לכן $2\cdot 11\cdot 43=946$ זה מספר שעובד.

הערה. ניתן לבדוק באמצעות מחשב כי 946 זו תשובה יחידה.

6. יהא p הוא ראשוני אי-זוגי. לכל a, נגדיר מספר $S_a = \frac{a}{1} + \frac{a^2}{2} + \frac{a^3}{3} + ... + \frac{a^{p-1}}{p-1}$.

נגיד ש-m ו-n הם מספרים שלמים זרים, המקיימים $S_3 + S_4 - 3S_2 = \frac{m}{n}$. הוכיחו כי m מתחלק ב-p.

פתרון. ניתן לדבר על שברים מודולו p. נגיד כי $\frac{x_1}{y_1} = \frac{x_2}{y_2} \pmod p$ אם לאחר העברת אגפים והחסרת שברים המונה $x_1y_2 - x_2y_1$ מתחלק ב-p. בשביל שהשברים יהיו מוגדרים חייבים לדרוש ש-y_1, y_2 לא יתחלקו ב-p, כי אסור לחלק ב-0 גם מודולו p.

ננסה לפתח נוסחה עבור S_a מודולו p. נשים לב כי $\binom{p}{k} = 0$ מודולו p לכל $0 < k < p$, וכן $\frac{1}{p} \cdot \binom{p}{k} = \frac{(p-1)(p-2)\cdot...\cdot(p-k+1)}{1\cdot 2\cdot...\cdot k} = \frac{(-1)^{k-1}}{k} \pmod p$.

מכאן

$$S_a = \sum_{k=1}^{p-1} \frac{a^k}{k} = -\sum_{k=1}^{p-1} \frac{(-a)^k (-1)^{k-1}}{k} = -\sum_{k=1}^{p-1} \frac{1}{p} \cdot \binom{p}{k} (-a)^k =$$

$$= \frac{1 + (-a)^p - \sum_{k=0}^{p} \binom{p}{k} (-a)^k}{p} = \frac{1 - a^p - (1-a)^p}{p} = \frac{1 + (a-1)^p - a^p}{p} \pmod p$$

כאן אומנם מחלקים ב-p, אבל המספר שמחלקים אותו הוא כפולה של p.

$$S_3 + S_4 - 3S_2 = \frac{1 + 2^p - 3^p + 1 + 3^p - 4^p - 3\left(1 + 1^p - 2^p\right)}{p} =$$

$$= \frac{1 + 1 - 3 - 3 + 2^p + 3\cdot 2^p - 4^p}{p} = -\frac{4 - 4\cdot 2^p + 4^p}{p} = -\frac{\left(2^p - 2\right)^2}{p} \pmod p$$

נשים לב כי $2^p - 2$ מתחלק ב-p, ולכן $\left(2^p - 2\right)^2$ מתחלק ב-p^2, ולכן

$$\frac{\left(2^p - 2\right)^2}{p} = 0 \pmod p.$$