תרגיל דיופנטי פתרון של השאלות האחרונות

7. מצאו את כל הראשוניים האי זוגיים p,q כך שקיים מספר טבעי $n \geq 2$ אשר עבורו מתקיים

$$\begin{cases} q^{n+2} \equiv 3^{n+2} (mod\ p^n) \\ p^{n+2} \equiv 3^{n+2} (mod\ q^n) \end{cases}$$

פתרון: אם $p = q$ אז שניהם שווים ל3.

אחרת p,q זרים ולכן $p^n q^n | p^{n+2} + q^{n+2} - 3^{n+2}$. נניח כי $p > q$

מתקיים $p^n q^n < 2p^{n+2}$ באופן שקול $q^n < 2p^2$ ולכן $q^{n-1} < p^2$.

מצד שני $q^{\frac{n(n-1)}{2}} < p^n \leq q^{n+2} - 3^{n+2} < q^{n+2}$

ולכן $n \leq 3$

אם $n = 2$ אז $p^2 | (q-3)(q+3)(q^2+9)$ נשים לב שאם p מחלק יותר מאחד מהגורמים אז הוא שווה ל3 ואז גם q שווה ל3. p^2 לא יכול לחלק את $q-3$ או את $q+3$ כי הוא גדול מ q. ולכן $p^2 | q^2 + 9$. בפרט $(q+2)^2 \leq p^2 \leq q^2 + 9$ וזה לא נכון ל$q \geq 3$.

ולכן $n = 3$.

אם אחד מהראשוניים הוא 5 אז $5^5 - 3^5 = 2 \cdot 11 \cdot 131$ מחלק בחזקה שלישית של מספר וזה לא נכון.

ולכן q לא יכול לחלק את $\frac{p^5 - 3^5}{p-3}$ וגם את $p-3$ ולכן אם $q | p-3$ אז $q^3 | p-3$ בפרט $q^3 < p$ אבל אנחנו יודעים כי $p^3 < q^5$ וזו סתירה.

ולכן $p^3 | q^4 + 3q^3 + 9q^2 + 27q + 81$.

הסדר של $\frac{p}{3}$ מודולו q מחלק את 5 אבל הוא לא 1. ולכן הוא שווה ל5. ולכן $5 | q-1$. מאותה סיבה $5 | p-1$. ולכן המספרים הראשוניים שלנו הם לפחות 11.

ולכן $q \geq 11$

$$p^3 \leq q^4 + 3q^3 + 9q^2 + 27q + 81 \leq q^4 \left(1 + \left(\frac{3}{11}\right)^1 + \left(\frac{3}{11}\right)^2 + \left(\frac{3}{11}\right)^3 + \left(\frac{3}{11}\right)^4\right) < 1.4q^4$$

$$\frac{p^5 + q^5 - 3^5}{p^3 q^3} < \frac{p^2}{q^3} + \frac{q^2}{p^3} < \frac{p^2}{\left(\frac{p^3}{1.4}\right)^{\frac{3}{4}}} + \frac{1}{p} = \frac{1.4^{\frac{3}{4}}}{p^{\frac{1}{4}}} + \frac{1}{p} < \left(\frac{1.4^3}{11}\right)^{\frac{1}{4}} + \frac{1}{11} < 1$$

ולכן קיבלנו סתירה.

8. הוכיחו כי למשוואה הבאה אין פתרונות ברציונליים $x-\frac{1}{x}+y-\frac{1}{y}=4$.

פתרון: נניח כי x,y חיוביים. אחרת נחליף את x ב $-\frac{1}{x}$. נסמן $x=\frac{a}{b},y=\frac{c}{d}$ שברים מצומצמים. אם a,b,c,d אי זוגיים אז $cd(a^2-b^2)+ab(c^2-d^2)=4abcd$ אגף ימין מתחלק ב 4 ולא ב8 ואילו אגף שמאל מתחלק ב8.

ולכן בה"כ המונה או המכנה של x זוגי. מספר z הוא מהצורה $y-\frac{1}{y}=z$ אם"ם z^2+4 הוא ריבוע.

ולכן $\left(4-x+\frac{1}{x}\right)^2+4$ ריבוע. אנחנו יודעים שמהכנה של השבר הוא ריבוע ולכן המונה שלו הוא גם ריבוע ולכן $(4ab-a^2+b^2)^2+4a^2b^2$ ריבוע שלם. a,b זרים, אחד מהם זוגי והשני אי זוגי ולכן יש לנו פה שלשה פיתגורית מצומצמת ולכן קיימים t,s זרים כך ש
$4ab-a^2+b^2=t^2-s^2$ וגם $ab=ts$.

קיימים u,v,p,q זרים בזוגות כך ש $a=up;b=vq;t=uq;s=vp$.

אזי מתקיים $4uvpq=u^2p^2+u^2q^2-v^2q^2-v^2p^2=(u^2-v^2)(p^2+q^2)$

לא ייתכן שכולם אי זוגיים וגם לא ייתכן שיותר מאחד מהם זוגי. אם u זוגי אז למשוואה אין פתרון מודולו 4. בדומה עבור v ולכן בה"כ p זוגי. ולכן מתקיים

$$\begin{cases} p^2+q^2=uv \\ 4pq=u^2-v^2 \end{cases}$$

נחליף את u,v ב$\frac{u+v}{2},\frac{u-v}{2}$ ונקבל ש $uv=pq;p^2+q^2=u^2-v^2$. כאשר p,q זרים וגם u,v זרים.

נוכיח שלמערכת משוואות זו אין פתרון. נסתכל על הפתרון בו $uv=pq$ מינימלי. ונבנה פתרון עם מכפלה קטנה יותר.

קיימים m,n,k,r זרים בזוגות כך ש $u=mk;v=nr;p=mr;q=nk$

מתקיים $m^2r^2+n^2k^2=m^2k^2-n^2r^2$. לא ייתכן שכולם אי זוגיים. אם k זוגי והשאר אי זוגיים נקבל סתירה מודולו 4. אותו הדבר עבור m. ולכן בה"כ r זוגי

אז מתקיים $n^2(k^2+r^2)=m^2(k^2-r^2)$ ולכן

$$\begin{cases} n^2+r^2=k^2 \\ k^2+r^2=m^2 \end{cases}$$

מאיפיון של שלשות פיתגוריות נקבל 2 זוגות של מספרים זרים כאשר המכפלה של כל זוג היא $\frac{r}{2}$ והפרש ריבועים של אחד הוא k וסכום הריבועים של השני הוא גם k. קיבלנו פתרון שבו המכפלה היא $\frac{r}{2}<mnkr$.

פתרון של יואב אבידן וליאור ז'לזניאק (Железняк) האגדי: אחרי שמקבלים שמספיק לפתור את המערכת

$4ab - a^2 + b^2 = c^2 - d^2$ וגם $ab = cd$. כאשר $(a,b) = (c,d) = 1$.

נסמן $S = ab = cd$. עכשיו מתקיים $d = \frac{S}{c}; b = \frac{S}{a}$.

אנחנו מקבלים $4S = a^2 - \frac{S^2}{a^2} + c^2 - \frac{S^2}{c^2} = (a^2 + c^2)(1 - \frac{S^2}{a^2c^2})$

ולכן $ab < S$. באופן סימטרי $cd < S$. ולכן $abcd < S^2 = abcd$. סתירה.

9. יהיו $n \geq k^2 \geq 64$ מספרים טבעיים

א. הוכיחו כי קיים מספר ראשוני $p > k$ כך ש $p|\binom{n}{k}$.

ב. הוכיחו כי לא קיימים מספרים טבעיים $m, l \geq 2$ כך ש $\binom{n}{k} = m^l$.

פתרון: א. נניח בשלילה שכל הראשוניים שמחלקים את $\binom{n}{k}$ הם קטנים שווים לk . יהי p ראשוני שמחלק את k. ונניח כי $p^a \leq n < p^{a+1}$ הוא מקיים:

$$v_p\left(\binom{n}{k}\right) = \sum_{j=1}^{a} \left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n-k}{p^j} \right\rfloor - \left\lfloor \frac{k}{p^j} \right\rfloor$$

כל אחד מהגורמים בסכום הוא לכל היותר אחד ולכן $v_p\left(\binom{n}{k}\right) \leq a$ ולכן החזקה של p בפירוק של $\binom{n}{k}$ לגורמים ראשוניים קטנה או שווה לn ולכן $\binom{n}{k} \leq n^{\pi(k)}$.

אם $k \geq 8$ אז $\pi(k) \leq \frac{1}{2}k$ כי 9 לא ראשוני. מצד שני $\binom{n}{k} > \left(\frac{n}{k}\right)^k$ ולכן קיבלנו $\left(\frac{n}{k}\right)^k < n^{\frac{1}{2}k}$ בסתירה לכך ש $n \geq k^2$.

הוכחה לגרסה כללית של טענה זו ניתן למצוא במאמר של ארדש:

http://www.renyi.hu/~p_erdos/1934-01.pdf

ב.מסעיף א' קיים $p > k$ ראשוני כך ש $p|\binom{n}{k}$ ולכן $p^l|\binom{n}{k}$. $p > k$ ולכן קיים $0 \leq i \leq k-1$ כך ש $p^l|n-i$, בפרט $n \geq p^l > k^l \geq k^2$.

לכל $0 \leq i \leq k-1$ קיימים a_i, m_i כך ש $n - i = a_i m_i^l$ וa_i לא מתחלק באף חזקה p-ית.

נוכיח כי אם i, j שונים אז $a_i \neq a_j$. נניח בשלילה כי $a_i = a_j$ אז בה"כ $m_i \geq m_j + 1$ ולכן

$$k > n - i - (n - j) = a_j\left(m_i^l - m_j^l\right) \geq a_j\left(\left(m_j + 1\right)^l - m_j^l\right) > a_j l m_j^{l-1} > \frac{2(n-k)}{m_j}$$

מצד שני $\frac{2(n-k)}{m_j} \geq n^{\frac{1}{2}}$ כי $2(n-k) > n \geq n^{\frac{1}{2}+\frac{1}{l}} \geq n^{\frac{1}{2}} m_j$. ולכן קיבלנו סתירה.

נראה כי $\{1, \dots, k\} = \{a_0, \dots, a_{k-1}\}$ כקבוצות.

הוכחנו כי כל הa שונים ולכן מספיק להוכיח שהמכפלה שלהם מחלקת את $k!$.

אנחנו יודעים כי $\prod_{i=0}^{k-1} a_i m_i^l = m^l k!$. נצמצם את כל הגורמים המשותפים של m ושל $\prod m_i$ ונקבל כי קיימים u, v זרים כך ש $(\prod_{i=0}^{k-1} a_i)u^l = v^l k!$.

נניח בשלילה כי $v \neq 1$ ונקבל סתירה.

ניקח $q|v$ ראשוני. $q \nmid u$ ולכן $q|\prod_{i=0}^{k-1} a_i$. נספור כמה פעמים q יכול לחלק את המכפלה. נשים לב ש q^l לא מחלק אף אחד מהגורמים שבמכפלה. עבור כל $1 \leq j \leq l-1$ נרצה לחסום את כמות הa_i אשר מתחלקים בq^j. לשם כך מספיק לחסום את כמות המספרים מבין $n-k+1, \dots, n$ אשר מתחלקים בq^j.

ויש לכל היותר $\left\lfloor \frac{k}{q^j} \right\rfloor + 1$ כאלו. ולכן q מחלק את $\prod_{i=0}^{k-1} a_i$ לכל היותר $\sum_{j=1}^{l-1} \left(\left\lfloor \frac{k}{q^j} \right\rfloor + 1 \right)$ פעמים. מצד שני הוא מחלק את $k!$ לפחות $\sum_{j=1}^{l-1} \left\lfloor \frac{k}{q^j} \right\rfloor$ פעמים. ולכן הוא מחלק את v^l לכל היותר $\sum_{j=1}^{l-1} \left(\left\lfloor \frac{k}{q^j} \right\rfloor + 1 - \left\lfloor \frac{k}{q^j} \right\rfloor \right)$ כלומר לכל היותר $l-1$ פעמים. אבל כמות הפעמים הזו אמורה להתחלק ב l ולכן היא שווה ל 0 . אבל הנחנו כי $q|v$. סתירה.

קיבלנו כי $\{1, \dots, k\} = \{a_0, \dots, a_{k-1}\}$.

$k \geq 4$ ולכן אם $l = 2$ כבר קיבלנו סתירה. כי קיים i כך ש $a_i = 4$ אבל a_i חסר ריבויים. לכן $l \geq 3$.

קיימים i_1, i_2, i_3 כך ש $n - i_1 = r_1^l \; ; \; n - i_2 = 2r_2^l \; ; \; n - i_3 = 4r_3^l$.

נבדוק שלא יכול להתקיים $(n - i_1)(n - i_3) = (n - i_2)^2$. אם זה מתקיים אז $r_1 r_3 = r_2^2$ נסמן $b = n - i_2$ וגם $n - i_1 = b + x \; ; n - i_3 = b - y$. אנו יודעים כי $|x|, |y| < k$.

מתקיים $b^2 = (b + x)(b - y)$ ולכן $xy = b(x + y)$. $x + y \neq 0$ ולכן $b \geq |xy|$ אבל

$b > n - k \geq (k-1)^2 \geq |xy|$ סתירה.

נניח כי $r_1 r_3 > r_2^2$.

$$4\left(r_1^l r_3^l - r^{2l}\right) \geq 4((r^2+1)^l - r^{2l}) > 4lr^{2l-2}$$

מצד שני האגף הכי שמאלי של האי שוויון שווה ל$(n - i_1)(n - i_3) - (n - i_2)^2$. וזה מקיים:

$(n - i_1)(n - i_3) - (n - i_2)^2 < n^2 - (n - k + 1)^2 < 2(k-1)n$.

ולכן קיבלנו כי $4lr^{2l} < 2(k-1)nr_2^2$ כלומר $l(n - i_2)^2 < 2(k-1)nr_2^2$.

ולכן $2(k-1)nr_2^2 > 3(n - k + 1)^2 > 2n^2$.

מכך נובע כי $(k-1)r_2^2 > n$

אבל $(k-1)r_2^2 \leq (k-1)n^{\frac{2}{l}} < kn^{\frac{2}{3}}$ ולכן $\mathrm{k} > n^{\frac{1}{3}}$. סתירה