5) פולינום מתוקן p ממעלה 3 במקדמים שלמים נקרא מגניב אם המספרים היחידים עבורם $p(n)$ ריבוע שלם הם 2017,2018 , ו- $p(2017), p(2018)$ הם אכן ריבועים שלמים.

א. מצאו פולינום מגניב.
ב. מצאו את כל הערכים האפשריים של $p(2018) \cdot p(2017)$ כאשר p פולינום מגניב.

פתרון: אפשר לעשות לפולינום הזה לינארית ואז נקבל פולינום מתוקן ממעלה 3 במקדמים שלמים כך ש $p(0), p(1)$ הם ריבועים ובשאר הערכים p הוא לא ריבוע.

א. נסתכל על $p(n) = n(n^2 - n + 1)$. נוכיח שזה פולינום מגניב. $p(0) = 0, p(1) = 1$ הם אכן ריבועים.

אם n שלילי $p(n)$ הוא שלילי ולכן לא ריבוע.

אם $n > 1$ הוא ריבוע וגם $p(n)$ הוא ריבוע אז גם $n^2 - n + 1$ הוא ריבוע. אבל $(n-1)^2 < n^2 - n + 1 < n^2$.

אם n לא ריבוע ו $\mathrm{p(n)}$ ריבוע אז קיים p ראשוני שמחלק את n כמות אי זוגית של פעמים. אז הוא חייב לחלק גם את $\mathrm{n^2} - n + 1$ כי אחרת הוא יחלק את $\mathrm{p(n)}$ כמות היא זוגית של פעמים. ולכן $\mathrm{p|1}$. סתירה

ב. נניח שp פולינום מגניב. נסמן $\mathrm{p(0) = a^2}$ ו $p(1) = b^2$.

נגדיר את הפולינומים הבאים: $q_1(n) = (a + (b-a)n)^2;\ q_2(n) = (a - (b+a)n)^2$

אז ל $i = 1,2$ מתקיים שעבור המשוואה $p(n) = q_i(n)$ 0,1 הם פתרונות. זו משוואה ממעלה שלישית ולכן יש לה פתרון שלם נוסף. אם הפתרון הזה שונה מ0,1 נקבל סתירה לכך ש p מגניב. כי בפתרון הזה p הוא ריבוע. ולכן 1 או 0 הם שורשים כפולים של המשוואה.

אם לשני ערכי i השורש הכפול הוא אותו שורש אז נקבל כי למשוואה $q_1(n) = q_2(n)$ יש שלושה שורשים. זו משוואה ממעלה 2 ולכן לכל n $q_1(n) = q_2(n)$. מהשוואת המקדם של n מקבלים כי $2a(b-a) = -2a(b+a)$ ולכן $\mathrm{ab} = 0$.

אחרת לכל i השורש הכפול הוא בנקודה שונה. ולכן בלי הגבלת הכלליות $p(n) - q_1(n) = n^3 - n^2$ וגם

$p(n) - q_2(n) = n^3 - 2n^2 + n$.

נחסר את 2 המשוואות ונקבל $q_1(n) - q_2(n) = -n^2 + n$ אבל לכל n $4|q_1(n) - q_2(n)$ סתירה. למשל עבור $n = 2$.

6) מצאו את כל הפונקציות $f: \mathbb{N} \to \mathbb{N}$, כך שלכל $x, y \in \mathbb{N}$ מתקיים:

א. $d\big(f(x)\big) = x$ כאשר $d(z)$ היא כמות המחלקים של המספר z.
ב. $f(xy) | (x-1)y^{xy-1}f(x)$

פתרון: נשים לב כי ל $f(2)$ יש 2 מחלקים ולכן הוא מספר ראשוני.

נתחיל למצוא את $f(p)$ כאשר $p \neq 2$ ראשוני. נציב $x = 2; y = p$ ונקבל $f(2p)|p^{2p-1}f(2)$. ל $2p$ יש $f(2p)$ מחלקים ולכן קיימים ראשוניים q, r כך ש $f(2p) = r^{2p-1}$ או $f(2p) = qr^{p-1}$ ולכן $f(2p) = p^{2p-1}$ או $f(2p) = f(2)p^{p-1}$

נציב $x = p; y = 2$ ונקבל כי $f(2p)|(p-1)2^{2p-1}f(p)$. אם $f(2p) = p^{2p-1}$ אז $p^{2p-1}|f(p)$ וזו סתירה כי ל $f(p)$ p מחלקים. ולכן $f(2p) = f(2)p^{p-1}$ ו- $f(2)p^{p-1}|(p-1)2^{2p-1}f(p)$ ולכן $f(p) = p^{p-1}$. ו $f(2)|(p-1)2^{2p-1}$. אם $f(2) \neq 2$ אז קיים מספר ראשוני שהוא לא 1 מודולו $f(2)$ ולכן בכל מקרה $f(2) = 2$.

חישבנו את $f(p)$ עכשיו נוכיח באינדוקציה כי אם הפירוק של מספר n לגורמים ראשוניים הוא $n = \prod_i p_i^{a_i}$ אז $f(n) = \prod_i p_i^{p_i^{a_i}-1}$.

נניח כי p_1 הוא הראשוני הכי קטן שמחלק את n. נציב $x = p_1; y = \frac{n}{p_1}$ ונקבל כי $f(n)|(p_1 - 1)z$ כאשר כל הגורמים הראשוניים של z מחלקים את n. נניח בשלילה כי קיים גורם ראשוני $q|f(n)$ שלא מחלק את n. ל $f(n)$ יש n מחלקים ולכן גם $q^{p_1^{-1}}|f(n)$. אבל אז $q^{p_1-1}|p_1 - 1$ וזה לא יכול להיות. ולכן אם n חזקת ראשוני אז $f(n) = p_1^{p_1^{a}-a}$.

אחרת, לכל i נציב $x = p_i^{a_i}; y = \frac{n}{x}$ ונקבל כי $f(x)\left(\frac{n}{x}\right)^{n-1}|f(n)$ ולכן החזקה המקסימלית של p_i שיכולה לחלק את $f(n)$ היא $p_i^{p_i^{a_i}-1}$ ולכן $\prod_i p_i^{p_i^{a_i}-1}|f(n)$ אבל יש להם אותה כמות מחלקים ולכן הם שווים.

נשאר לבדוק שהפונקציה הזו עובדת. קודם כל ברור כי $d(f(x)) = x$. נניח כי $x, p^b||y$ $\mathrm{p}^{\mathrm{a}}||$. אז $\mathrm{p}^{p^{a+b}-1}||f(xy)$, ואילו את $p, \mathrm{y}^{\mathrm{xy}-1}$ מחלק לפחות $b(p^{a+b}-1)$ פעמים. ולכן אם b שונה מ-0 אז p מחלק את $\mathrm{y}^{\mathrm{xy}-1}$ לפחות אותה כמות פעמים שהוא מחלק את f(xy). אם $\mathrm{b} = 0$ אז p מחלק את $f(xy)$ ואת f(x) אותה כמות של פעמים. ולכן $\mathrm{f(xy)}|\mathrm{y}^{\mathrm{xy}-1}f(x)$. ולכן f עובדת.

7) הוכיחו כי לכל מספר טבעי n קיימת קבוצה S של מספרים שלמים בגודל n כך שלכל $a, b \in S$ המספרים היחידים מ S אשר $a - b$ מחלק הם a, b.

פתרון: נוכיח באינדוקציה. עבור $n = 2$ אפשר לקחת את הקבוצה $\{2,4\}$.

נניח כי יש לנו קבוצה $\{a_1, \dots, a_n\}$ שמקיימת את התנאי. נסמן $\mathrm{M} = \prod_{i=1}^{n} a_i$. נבחר מספר ראשוני $p > M^2 n$.

נגדיר $\mathrm{b_i} = Ma_i$ עבור $1 \leq i \leq n$. ו $b_{n+1} = b_n + p$. נוכיח כי קיים c כך שהקבוצה $\{b_1 + M^2c, \dots, b_n + M^2c, b_{n+1} + M^2c\}$ מקיימת את התנאי. נשים לב כי ההפרשים בין איברי הקבוצה לא תלויים ב c.

נשים לב כי לכל c, ולכל $1 \leq i, j, k \leq n$

$$b_i + M^2c - b_j - M^2c \big| b_k + M^2c \Leftrightarrow M(a_i - a_j) \big| Ma_k \Leftrightarrow a_i - a_j | a_k \Leftrightarrow k = i, j$$

ולכן הקבוצה מקיימת את התנאי לכל האיברים מלבד אולי האיבר האחרון. נראה שאפשר לבחור את c כך שהתנאי יתקיים גם עבור האיבר האחרון. לכל $i, j \leq n$ $b_i - b_j$ לא מחלק את $b_{n+1} + M^2c$. נניח שכן אז לכל מספר ראשוני שמחלק את $b_i - b_j$ הוא מחלק גם את M ולכן הוא מחלק את p. סתירה כי $\mathrm{p} > \mathrm{b_i} - b_j$.

נשים לב כי אם נבחר c כך ש- $M^2c \equiv -b_i \ (mod\ b_{n+1} - b_i)$ אז יתקיים לכל i:

$b_{n+1} - b_i | b_j + M^2c \Leftrightarrow b_{n+1} - b_i | b_j - b_i$. נשים לב כי $b_{n+1} - b_i, b_j - b_i$ זרים אם $j \neq i, n+1$. כי אם q ראשוני שמחלק את $b_j - b_i$ ואת $b_{n+1} - b_i$ עבור $j \neq n+1, i$ אז $q|M$ ולכן $q|p$, סתירה. ולכן הקבוצה תקיים את התנאי.

נשאר להראות שאפשר לבחור c כך שכל השקילויות שאנחנו רוצים יתקיימו, וזה נכון כי $b_{n+1} - b_i$ זר ל-M. ובנוסף לכל $i \neq j$ $b_{n+1} - b_i, b_{n+1} - b_j$ זרים. כי אם q ראשוני שמחלק את שניהם אז $q|b_i - b_j$ וראינו שלא קיים מספר ראשוני שמחלק את $b_j - b_i$ ואת $b_{n+1} - b_i$. ולכן ממשפט השאריות הסיני אפשר לבחור c שיקיים את השקילויות.