תרגיל 12

1. מצאו את כל הזוגות של מספרים ראשוניים (p,q) כך ש-

$$p^3-q^5=(p+q)^2$$

פתרון: נניח ש- p,q לא מתחלקים ב-3, נטפל במקרה האחר בסוף.

נסתכל מודולו 3. לפי משפט הקטן של פרמה שהתנאי הוא:

$$p-q=(p+q)^2 \pmod 3$$

נשים לב שאם $p=q \pmod 3$ אז אגף שמאל מתחלק ב-3 אבל אגף ימין לא מתחלק ב-3 כי הנחנו ש-p ו-q לא מתחלקים ב-3.

אבל גם אם $p\neq q \pmod 3$, כלומר אחד מהם שווה ל- 1 מודולו 3 השני שווה ל-2 ולכן אגף ימין יהיה שווה ל-0 מודולו 3 אבל אגף שמאל לא.

קיבלנו סתירה בשני המקרים ולכן לפחות אחד משני הראשוניים מתחלק ב-3.

אם $p=3$ אז מקבלים:

$$0\le (p+q)^2=p^3-q^5=27-q^5$$

כלומר $q^5\le 27$ ולכן $q<2$ וזה בלתי אפשרי.

אם $q=3$ אז מהתנאי מקבלים ש-

$$p^3-p^2-6p-252=0$$

ולכן $$(p-7)(p^2+6p+36)=0$$

אבל $$p^2+6p+36>p^2+6p+9=(p+3)^2\ge 0$$

ולכן הפתרון היחיד הוא $p=7$.

נציב ונבדוק ש-$p=7,\ q=3$ באמת פתרון:

$$343-243=10^2.$$

2. נתון מספר טבעי n ותת קבוצה $\{a_1,a_2,...,a_k\}$ של הקבוצה $\{1,2,...,n\}$, $k>1$.

ידוע כי $n\,|\,a_i(a_{i+1}-1)$ לכל $i=1,2,\ldots,k-1$. הוכיחו כי n לא מחלק את $a_k(a_1-1)$.

פתרון: נניח בשלילה כי $n \mid a_k\left(a_1-1\right)$. נוח להניח שהאינדקסים מחזוריים $a_{j+k}=a_j$.

נשים לב כי $n \mid a_i\left(a_{i+1}-1\right)$ גורר ש-$a_i \equiv a_i a_{i+1}\left(\bmod n\right)$ לכל i ולכן

$$a_i \equiv a_i a_{i+1} \equiv a_i a_{i+1} a_{i+2} \equiv \cdots \equiv a_i a_{i+1} \cdot \ldots \cdot a_{i-1}\left(\bmod n\right)$$

לפיכך $a_i \equiv a_1 a_2 \cdot \ldots \cdot a_k\left(\bmod n\right)$ לכל i ולכן $a_1 \equiv a_2 \equiv \ldots \equiv a_k$ או במילים אחרות $n \mid a_1-a_2$ אבל $a_1, a_2 \le n$ וזו סתירה.

3. מצא את כל הפולינומים P, עם מקדמים שלמים כך ש-$n \mid P(2^n)$ לכל n טבעי.

פתרון: נבחר שני ראשוניים אי-זוגיים p,q. לפי המשפט הכי חשוב על פולינומים במקדמים שלמים $2^{pq}-2^q \mid P(2^{pq})-P(2^q)$. בנוסף, לפי משפט פרמה הקטן

$$2^{pq}=(2^q)^p=2^q \pmod p$$

ולכן

$$p \mid 2^{pq}-2^q$$

ואמרנו כבר כי

$$2^{pq}-2^q \mid P(2^{pq})-P(2^q)$$

ולכן

$$p \mid P(2^{pq})-P(2^q) \qquad (*)$$

אבל לפי הנתון $pq \mid P(2^{pq})$ ולכן $p \mid P(2^{pq})$, מזה ומ-$(*)$ נובע ש-$p \mid P(2^q)$ לכל שני ראשוניים אי זוגיים p ו-q. אבל לכל p גדול מספיק נקבל ש-p גדול מ-$P(2^q)$ ולכן $P(2^q)$ חייב להיות שווה ל-0, כלומר 2^q הוא שורש של הפולינומים לכל q ולכן לפולינום אינסוף שורשים ולכן הוא חייב להיות פולינום האפס.

4. מצאו את כל הפולינומים $P\left(x\right)$ עם מקדמים שלמים כך ש-$P\left(P\left(n\right)+n\right)$ ראשוני עבור אינסוף n-ים שלמים.

פתרון: לפי המשפט הכי חשוב על פולינומים עם מקדמים שלמים אנו מקבלים:

$$\left(P\left(n\right)+n\right)-n \mid P\left(P\left(n\right)+n\right)-P\left(n\right)$$

ולכן לפי טענה

$$P(n) \mid P(P(n)+n)-P(n)$$

כלומר $P(P(n)+n)=P(n)Q(n)$ עבור פולינום כלשהו Q וברור של-Q צריכים להיות מקדמים שלמים. אבל נתון ש- $P(P(n)+n)$ ראשוני עבור אינסוף ערכים של n ואם P לא קבוע אז למשוואה $P(x)=\pm 1$ יש מספר סופי של פתרונות ולכן למשוואה $Q(x)=\pm 1$ יש מספר אינסופי של פתרונות, ולכן Q פולינום קבוע. כלומר אנו מקבלים ש-

$$\deg(P(P(n)+n))=\deg(P(n))$$

ולכן הדרגה של P היא לכל היותר 1. נבדוק שני מקרים:

א. הדרגה של P זה 0 אז הפולינום קבוע וזה חייב להיות קבוע ראשוני ואז $P(P(n)+n)$ יהיה ראשוני עבור אינסוף n-ים שלמים.

ב. הדרגה של P שווה 1. נסמן $P(n)=an+b$ ואז

$$P(P(n)+n)=P((a+1)n+b)=a(a+1)n+ab+b=(a+1)(an+b)$$

בשביל שזה יהיה ראשוני עבור אינסוף n-ים $a+1$ צריך להיות שווה ± 1, אבל $a\neq 0$ כי הנחנו שהדרגה 1 ולכן $a=-2$. עכשיו מקבלים ש-$2n-b$ צריך להיות ראשוני ולכן b חייב להיות אי זוגי. ובכן קיבלנו שאם הפולינום ממעלה 1 אז $P(n)=-2n+b$ וזה מתאים לכל b אי-זוגי.

5. לכל פונקציה f נסמן $f^n(x)=f(f(f(\ldots f(x)\ldots)))$ הפעלה של הפונקציה n פעמים. נתון פולינום לא קבוע P עם מקדמים שלמים. הוכיחו כי לא קיימת פונקציה f מהטבעיים לטבעיים כך שכמות המספרים השלמים x עבורם $f^n(x)=f(x)$ שווה ל-$P(n)$ לכל $n\geq 1$.

פתרון: נבחר מספר טבעי ונתחיל להפעיל עליו את הפונקציה ונניח שלאחר מספר פעמים חזרנו למספר ההתחלתי. לכל המספרים שעברנו בהם נקרא מעגל ונסמן ב-a_n את כמות המעגלים הזרים באורך n.

נרשום את התנאי בשאלה בצורה הבאה:

$$P(n)=\sum_{d|n} d\cdot a_d$$

נזיז את הפולינום שלנו בקבוע ונדאג ש-a_1 יהיה שווה ל-0.

טענה 1: $P(0)=0$

הוכחת הטענה: לפי המשפט הכי חשוב על פולינומים במקדמים שלמים

$p\,|\,P(p)-P(0)$ כאשר p ראשוני (זה גם סתם טענה ברורה).

נשים לב כי $P(p)=a_1+pa_p$ כלומר $P(p)$ מתחלק ב-p ולכן כך גם $P(0)$ דהיינו

$P(0)$ מתחלק בכל ראשוני ולכן שווה ל-0.

טענה 2: $a_p=0$ לכל ראשוני p.

הוכחת הטענה: נשים לב כי לכל זוג ראשוניים p,q

$$P(pq)=a_1+pa_p+qa_q+pqa_{pq}=pa_p \pmod q$$

אבל שוב לפי המשפט הכי חשוב על פולינומים עם מקדמים שלמים

$P(pq)-P(0)=P(pq)$ מתחלק ב-pq ובפרט מתחלק ב-q אבל p ו-q זרים ולכן

a_p מתחלק ב-q אבל זה נכון לכל ראשוני q ששונה מ-p ולכן $a_p=0$.

מטענה 2 נובע כי $P(p)=a_1+pa_p=0$, לפיכך לפולינום אינסוף שורשים ולכן הוא

זהותית שווה ל-0 בסתירה לכך שהפולינום לא קבוע.

6. הוכיחו כי קיימים אינסוף זוגות (m,n) של מספרים טבעיים כך שמתקיים:

$m+n\,|\,(m!)^n+(n!)^m+1$.

פתרון: נבקש ש-$m+n$ יהיה ראשוני ונסמן $m=p-n$, כאשר p ראשוני.

נחשב את $m!$ מודולו p:

$$m!=(p-n)!=\frac{(p-1)!}{(p-n+1)\cdot\ldots\cdot(p-2)(p-1)}=\frac{-1}{(-n+1)\cdot\ldots\cdot(-2)(-1)}=$$

$$=\frac{-1}{(-1)^{n-1}(n-1)!}=\frac{n}{(-1)^n\cdot n!} \pmod p$$

נניח ש- n זוגי ולכן ה- $(-1)^n$ יצטמצם והתנאי המקורי יהפוך ל-

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

קיבלנו תנאי שלא תלוי ב- m ולכן p לא תלוי ב- n. כלומר מספיק למצוא אינסוף n-ים עבורם קיים מספר ראשוני p שמחלק את $n^n+n!+n!^n$, ובנוסף $p>n$ כי כל הראשוניים שמחלקים את המכנה $n!^n$ בהכרח קטנים מ- n.

נוכיח שכל ה- n-ים מהצורה $n=2q$, עבור ראשוני q, מקיימים את התנאי.

נסמן $X=(2q)^{2q}+(2q)!+(2q)!^{2q}$.

נשים לב שכל המחלקים הראשוניים של X הקטנים מ- $2q$ הם $2,q$ כיוון שאם r ראשוני הקטן מ- $2q$ אז הוא בברור מחלק את $(2q)!$ וכך גם את $(2q)!^{2q}$ ועל כן בכדי ש- r יחלק את X הוא צריך לחלק את $(2q)^{2q}$ כלומר r צריך לחלק את $2q$ ולפיכך r שווה ל-2 או ל- q.

המטרה שלנו כעת היא להוכיח כי 2 ו- q לא יכולים לחלק את X הרבה פעמים ולכן חייב להיות לו מחלק הגדול מ- $2q$.

נחשב את $v_q(X)$.

קל לראות כי $v_q\left((2q)^{2q}\right)=2q$, $v_q\left((2q)!\right)=2$, $v_q\left((2q)!^{2q}\right)=4q$ ולכן

$$v_q(X)=\min\left(v_q\left((2q)^{2q}\right),v_q\left((2q)!\right),v_q\left((2q)!^{2q}\right)\right)=2$$

עכשיו נחשב את $v_2(X)$. תחילה נעריך את $v_2\left((2q)!\right)$:

$$v_2\left((2q)!\right)=\left\lfloor\frac{2q}{2}\right\rfloor+\left\lfloor\frac{2q}{4}\right\rfloor+\left\lfloor\frac{2q}{8}\right\rfloor+\ldots<\frac{2q}{2}+\frac{2q}{4}+\frac{2q}{8}+\ldots=2q$$

אבל $v_2\left((2q)^{2q}\right)=2q$ וברור שגם $v_2\left((2q)!^{2q}\right)<v_2\left((2q)!\right)$ ולכן

$v_2(X)=v_2\left((2q)!\right)<2q$.

אבל $X>(2q)^{2q}>2^{2q}\cdot q^2$ ולכן ל- X יש מחלק ראשוני שגדול מ- $2q$.