תרגיל 19

1. הוכח כי לכל m טבעי, k זוגי קיימים a, b שלמים וזרים ל-m כאלה ש- $k = a - b$.

פתרון. נגיד ש- $p_1, p_2, ..., p_n$ זו רשימה מלאה של כל המחלקים הראשוניים השונים של m. צריך בעצם למצוא b מודולו m עזה שגם b וגם $b + k$ זרים ל-m. אנחנו נוכיח שיש שארית r_j מודולו p_j שמקיימת גם r_j וגם $r_j + k$ לא מתחלקים ב-p_j . אז לפי משפט שאריות הסיני נוכל לבנות מספר b שנותן שאריות r_j מודולו p_j לכל j. אז גם b וגם $b + k$ לא יתחלק באף מחלק ראשוני של m.
ובכן, נשאר להוכיח טענה, שהיא בעצם אותה הטענה של השאלה אבל עבור $m = p$ ראשוני. עבור $p = 2$ זה קל מאוד: כל מספר אי-זוגי מתאים בתור b (וכאן אנחנו משתמשים בזוגיות של k).
עבור $p > 2$ יש שני מקרים:
אם k לא מתחלק ב-p, אז $a = 2k$, $b = k$, ושניהם לא מתחלקים ב-p.
אם k מתחלק ב-p, אז $a = 1 + k$, $b = 1$, ושניהם לא מתחלקים ב-p.

2. א. עבור איזה m, n המספר $3^m - 1$ מתחלק ב-2^n ?
ב. עבור איזה m, n המספר $2^m + 1$ מתחלק ב-3^n ?

פתרון. א. נניח כי s הוא מספר מינימלי כזה ש- $3^s = 1 \pmod{2^n}$. אז כל m שמתאים הוא כפולה של s. נניח בנוסף, כי $3^s \neq 1 \pmod{2^{n+1}}$, כלומר $3^s = 1 + (2k+1)2^n$ ונחפש t מינימלי שעבורו $3^t = 1 \pmod{2^{n+1}}$. הכפולה המינימלית של s אחרי s עצמו היא $2s$.
בואו ננסה: $3^{2s} = \left(1 + (2k+1)2^n\right)^2 = 1 + (2k+1)2^{n+1} + (2k+1)2^{2n}$.
לכן עבור $n > 1$, 3^{2s} היא חזקה מינימלית ששווה 1 מודולו 2^{n+1} , אבל היא לא שווה ל-1 מודולו . זה היה הצעד של אינדוקציה.
את הבסיס של אינדוקציה צריך לבדוק גם עבור $n = 1$ וגם עבור $n = 2$ (הרי המעבר עובד רק ל- $n > 1$).
ובכן, עבור $n = 1$, המספר $3^m - 1$ מתחלק ב-2 תמיד.
אבל עבור $m = 1$ המספר $3^m - 1$ לא מתחלק ב-4.
עבור $m = 2$ המספר $3^m - 1$ מתחלק גם ב-4 וגם ב-8 אבל לא ב-16. לכן לכל m זוגי $3^m - 1$ מתחלק גם ב-4 וגם ב-8.
לכן באינדוקציה עבור $n > 2$ המספר $m = 2^{n-2}$ הוא מינימלי שעבורו $3^m - 1$ מתחלק ב- 2^n , אבל הוא לא מתחלק ב- 2^{n+1} . לכן $3^m - 1$ מתחלק ב- 2^n עבור $n > 2$ אך ורק כאשר m מתחלק ב- 2^{n-2} .

ב. נניח כי s הוא המספר הטבעי הקטן ביותר שעבורו $2^s = \pm 1 \left(\mathrm{mod}\, 3^n\right)$. אז כאשר $m = ks$ נקבל $2^m = \pm 1 \left(\mathrm{mod}\, 3^n\right)$. עבור חזקות שלא מתחלקות ב-s זה לא מתקיים. אכן, אם $m = ks + r$ כאשר $0 < r < s$ ובכל זאת $2^m = \pm 1 \left(\mathrm{mod}\, 3^n\right)$ אבל הרי גם $2^{ks} = \pm 1 \left(\mathrm{mod}\, 3^n\right)$ לכן גם $2^r = \pm 1 \left(\mathrm{mod}\, 3^n\right)$ וזה נוגד את המינימליות של s.
כמובן, אם $2^s = -1 \left(\mathrm{mod}\, 3^n\right)$ אז הסימן בשוויון $2^m = \pm 1 \left(\mathrm{mod}\, 3^n\right)$ תלוי בזוגיות של k: הוא שלילי רק כאשר k אי-זוגי. אם $2^s = 1 \left(\mathrm{mod}\, 3^n\right)$ אז $2^m = -1 \left(\mathrm{mod}\, 3^n\right)$ לא פתיר.
נניח בנוסף כי $2^s = -1 \left(\mathrm{mod}\, 3^n\right)$ אבל $2^s \neq -1 \left(\mathrm{mod}\, 3^{n+1}\right)$. כלומר $2^s = 3^n q - 1$ כאשר q אינו מתחלק ב-3. כיצד מוצאים m מינימלי כזה ש-$2^m = -1 \left(\mathrm{mod}\, 3^{n+1}\right)$? כמובן, m כזה חייב לקיים גם $2^m = -1 \left(\mathrm{mod}\, 3^n\right)$ לכן הוא חייב להיות ks כאשר k אי-זוגי גדול מ-1. אז האופציה הקטנה ביותר שכדאי לנסות היא $k = 3$. ננסה:

$$2^{3s} = \left(3^n q - 1\right)^3 = 3^{3n} - 3^{2n+1} q + 3^{n+1} q^2 - 1 = 3^{n+1} Q - 1$$

כלומר כל אם $n > 0$, זה אכן $2^{3s} = -1 \left(\mathrm{mod}\, 3^{n+1}\right)$ אבל $2^{3s} \neq -1 \left(\mathrm{mod}\, 3^{n+2}\right)$.

בסיס של אינדוקציה: 1 הוא m מינימלי שעבורו $2^m = -1 \left(\mathrm{mod}\, 3\right)$ אבל עבורו גם $2^m \neq -1 \left(\mathrm{mod}\, 3^2\right)$. לכן לפי מה שראינו $m = 3^{n-1}$ הוא המספר הקטן ביותר כזה ש-$2^m = -1 \left(\mathrm{mod}\, 3^n\right)$ אבל עבורו גם $2^m \neq -1 \left(\mathrm{mod}\, 3^{n+1}\right)$.
לכן $2^m = -1 \left(\mathrm{mod}\, 3^n\right)$ אח ורק כאשר $m = 3^{n-1}\left(2k+1\right)$.

3. רשום את השבר העשרוני של 1/81 ללא שימוש במחשבון.

פתרון. לחזקות של 10 מודולו 9 יש מחזור של 1. לכן מודולו 81 ל-10 יש לא יותר מ-9 מצבים, כלומר המחזור של 10^k מודולו 81 הוא 9 לכל היותר. במילים אחרות קיים k שלא עולה על 9 כזה ש-$10^k = 1 \left(\mathrm{mod}\, 9\right)$. כלומר אם נחלק את 1 ב-81, אחרי k צעדים נקבל שארית 1 והתהליך של חלוקה יהפוך להיות מחזורי.
ובכן, המחזור של 1/81 הוא באורך 9 לכל היותר, והוא מתחיל ישר אחרי הנקודה העשרונית. עגב, לא קשה לראות כי $\frac{1}{9} = 0.111111111111111.... = \sum_{k=1}^{\infty} 10^{-k}$. אז מה שנשאר לנו לעשות זה להעלות את המספר הזה בריבוע עם דיוק של 10 ספרות אחרי הנקודה העשרונית: $\frac{1}{81} = \left(\frac{1}{9}\right)^2 = \sum_{k=1}^{\infty} 10^{-k} \cdot \sum_{m=1}^{\infty} 10^{-m} = \sum_{n=1}^{\infty} \frac{n}{10^{n+1}}$.
הזנב של הטור קטן מדי בשביל לתרום ל-9 ספרות הראשונות אחרי הנקודה:

$$\sum_{n=11}^{\infty}\frac{n}{10^{n+1}}=\frac{11}{10^{12}}+\frac{12}{10^{13}}+\frac{13}{10^{14}}+\frac{14}{10^{15}}+\ldots<\frac{11}{10^{12}}\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots+\frac{1}{2^n}+\ldots\right)=\frac{22}{10^{12}}$$

כלומר זה מספר קטן. עכשיו נחשב את הראש של הטור

$$\sum_{n=1}^{10}\frac{n+1}{10^n}=\frac{1}{10^2}+\frac{2}{10^3}+\frac{3}{10^4}+\frac{4}{10^5}+\frac{5}{10^6}+\frac{6}{10^7}+\frac{7}{10^8}+\frac{8}{10^9}+\frac{9}{10^{10}}+\frac{10}{10^{11}}$$

אבל $\frac{8}{10^9}+\frac{9}{10^{10}}+\frac{10}{10^{11}}=\frac{8}{10^9}+\frac{9+1}{10^{10}}=\frac{9}{10^9}$ לכן הראש של הטור הוא

$$\sum_{n=1}^{10}\frac{n+1}{10^n}=\frac{1}{10^2}+\frac{2}{10^3}+\frac{3}{10^4}+\frac{4}{10^5}+\frac{5}{10^6}+\frac{6}{10^7}+\frac{7}{10^8}+\frac{9}{10^9}=0.012345679$$

ברור שהוספת זנב שקטן מ-$\frac{22}{10^{12}}$ לא יגע ב-9 ספרות הראשונות אחרי הנקודה של השבר, ומחזור של שבר לא עולה על 9, לכן השבר הוא

0.012345679012345679012345679012345679012345679012345679012345679...

או ברישום הקצר $0.\overline{(012345679)}$ כשהסוגריים מסמנות את הביטוי שחוזר על עצמו באופן מחזורי אינסוף פעמים.

הערה. הנה משהו נחמד:

81	=	81	× 1
972	=	81	× 12
9963	=	81	× 123
99954	=	81	× 1234
999945	=	81	× 12345
9999936	=	81	× 123456
99999927	=	81	× 1234567
999999918	=	81	× 12345678
9999999909	=	81	× 123456789

4. האם קיים N, שמתחלק בדיוק ב-2000 ראשוניים שונים, כזה ש-2^N+1 מתחלק ב-N?

פתרון. נניח ש-b אי-זוגי. אז $2^{ab}+1$ מתחלק ב-2^a+1.

טענה. עבור מספר k מספיק גדול $2^{3^k}+1$ מתחלק גם ב-3 וגם ב-1999 מספרים ראשוניים אי-זוגיים נוספים: $p_1, p_2, \ldots, p_{1999}$.

אם הטענה נכונה, אז ניקח $N=3^k\cdot p_1p_2\cdot\ldots\cdot p_{1999}$. אז 2^N+1 יתחלק ב-$2^{3^k}+1$ שהוא מתחלק ב-$p_1, p_2, \ldots, p_{1999}$ (לפי הטענה), וגם ב-3^k לפי שאלה 2ב'.
לכן 2^N+1 יתחלק ב-N. כלומר כל מה שצריך זה להוכיח את הטענה.

הוכחת הטענה. נסמן $a_k = 2^{3^k}+1$. כמובן שמחלקים ראשוניים שלו – אי-זוגיים.

$$a_{k+1} = \left(2^{3^k}\right)^3 + 1 = a_k\left(\left(2^{3^k}\right)^2 - 2^{3^k} + 1\right) = a_k\left(\left(a_k - 1\right)^2 - \left(a_k - 1\right) + 1\right) = a_k\left(a_k \cdot C + 3\right)$$

כבר ראינו כי a_k מתחלק בחזקה גבוהה של 3. לכן אפשר לרשום:

$$a_{k+1} = \left(2^{3^k}\right)^3 + 1 = 3a_k\left(\frac{a_k}{3} \cdot C + 1\right).$$

למספר $\frac{a_k}{3} \cdot C + 1$ יש מחלק ראשוני p_k, והוא כמובן לא מחלק של a_k. לכן ל-a_{k+1} יש את כל המחלקים הראשוניים של a_k ועוד מחלק ראשוני נוסף. לכן באינדוקציה ל-$2^{3^{2000}}+1$ יש לפחות 2000 מחלקים ראשוניים שונים, מש"ל.

5. מצא את כל המספרים הטבעיים N שעבורם 2^N+1 מתחלק ב-N^2.

תשובה. 2^3+1 מתחלק ב-1^2, גם 2^3+1 מתחלק ב-3^2 ואין דוגמאות אחרות.

פתרון. קודם כל ברור כי N אי-זוגי.

מפתרון של שאלה 2ב' ברור כי החזקה של 3 בפירוק של N היא 0 או 1.

יהיה p המחלק הראשוני הקטן ביותר שמחלק את N. יהיה s מספר מינימלי כזה ש-$2^s = -1 \pmod p$. ברור שגם N מקיים את זה, אבל ברור גם שהוא לא הכי קטן, כי מספר הכי קטן הוא קטן מ-p לפי משפט פרמה הקטן. ברור גם שסדר של 2 מודולו p הוא $2s$ (למה?). אז כל המספרים m שעבורם $2^m = -1 \pmod p$ אלה כפולות אי-זוגיות של s. לכן N הוא כופלה אי-זוגית של s. אבל כל הגורמים הראשוניים של N הם גדולים או שווים ל-p, בזמן של-s כל הגורמים הראשוניים קטנים מ-p. לכן אין ל-s גורמים ראשוניים, כלומר $s = 1$.

כלומר $2^1 = -1 \pmod p$ במילים אחרות $2+1$ מתחלק ב-p כלומר $p = 3$. כבר אמרנו שחזקה של 3 בפירוק של N לא עולה על 1 לכן N מתחלק ב-3 אבל לא ב-9.

עכשיו ניקח את הגורם הראשוני הקטן ביותר של N חוץ מ-3, ונקרא לא q. אם 3 הוא הגורם הראשוני היחיד, אז $N = 3$ לכן נעבור לפתרונות נוספים.

ובכן, נסמן ב-r את המספר הטבעי המינימלי שפותר משוואה $2^r = -1 \pmod q$. מספר כזה קיים, גם N הוא כזה, אבל N הוא לא מינימלי כי הוא גדול מ-q. קל לראות שסדר של 2 מודולו q הוא $2r$, וש-N הוא כפולה אי-זוגית של r (בדומה למה שעשינו כאשר דיברנו על p). לכן הגורמים הראשוניים של r קטנים ממש מ-q, אבל ל-N יש רק גורם יחיד שקטן מ-q וזה 3, והוא מופיע ב-N רק פעם אחד. לכן r הוא מחלק של 3. לכן $2^3 = -1 \pmod q$, ולכן 2^3+1 מתחלק ב-q. אבל אין מספרים ראשוניים כאלה חוץ מ-3, לכן אין מחלקים ראשוניים נוספים.

6. הוכח כי לכל מספר p ראשוני קיים מספר ראשוני q כזה שלאף n טבעי $n^p - p$ לא מתחלק ב-q.

פתרון. עבור $p = 2$, ניקח $q = 3$, וזה יעבוד, כי ריבועים לא שווים ל-2 מודולו 3.
לכן נשאר לטפל במקרה של p אי-זוגי.

ניקח $N = 1 + p + p^2 + ... + p^{p-1} = \frac{p^p - 1}{p-1}$. בסכום שרשמנו יש מספר אי-זוגי (p) של מחוברים אי-זוגיים, לכן N אי-זוגי. מצד שני $N = 1 + p \neq 1 \pmod{p^2}$, לכן יש ל-$N$ מחלק ראשוני q שהוא לא 1 מודולו p^2. אנחנו נוכיח שלמספר q יש את התכונה הנדרשת.

p ו-q מספרים שונים – הרי N מתחלק ב-q אבל לא ב-p.
קל לראות גם ש-$p-1$ לא מתחלק ב-q. אחרת $p = 1 \pmod{q}$
ואז $0 = N = 1 + p + p^2 + ... + p^{p-1} = 1 + 1 + ... + 1 = p \pmod{q}$
ואז p מתחלק ב-q, אבל זה בלתי אפשרי כי הם שונים.
נניח כי $n^p - p$ מתחלק ב-q. במילים אחרות $\boxed{n^p = p \pmod{q}}$.

הראנו כי $p \neq 1 \pmod{q}$ לכן גם $n \neq 1 \pmod{q}$.
גם הראנו כי $p \neq 0 \pmod{q}$ לכן גם $n \neq 0 \pmod{q}$.
נעלה את שני האגפים של הזהות במסגרת בחזקה p.

$$n^{p^2} = p^p \pmod{q}$$

אבל $p^p = 1 \pmod{q}$ כי $p^p - 1$ מתחלק ב-q. לכן $n^{p^2} = 1 \pmod{q}$.
אבל גם $n^{q-1} = 1 \pmod{q}$. היות ו-$n \neq 1 \pmod{q}$, יוצא ש-p^2 לא זר ל-$q-1$: שניהם מתחלקים בסדר של n מודולו q, שאותו נסמן ב-d. ובכן, קיים $d > 1$ שגם $q-1$ וגם p^2 מתחלקים בו, ובנוסף $n^d = 1 \pmod{q}$.
אבל בחרנו את q כך ש-$q-1$ לא מתחלק ב-p^2. לכן $d = p$.
לכן $n^p = 1 \pmod{q}$. יחד עם זאת $n^p = p \pmod{q}$. אבל $p \neq 1 \pmod{q}$ וזה לא יתכן.