תרגיל 6

1. האם קיימים שני מספרים טבעיים c ו- d עבורם $c^3+d^4=19^{19}$?

רעיון של פתרון. נתבונן במשוואה זאת מודולו 13. למה דווקא מודולו 13?
מכיוון שאם $x\neq 0\pmod{13}$ אז $x^{12}=1\pmod{13}$, ולכן כל מספר מסוג $a=x^3$ שלא מתחלק ב-13 מקיים $a^4=1\pmod{13}$, וזה רק 4 אפשרויות (הרי לפולינום מדרגה 4 יש רק 4 שורשים). כמו כן, כל מספר מסוג $b=x^4$ שלא מתחלק מקיים $b^3=1\pmod{13}$, ולזה יש רק 3 אפשרויות (הרי לפולינום מדרגה 3 יש רק 3 שורשים).
לכן צפוי, שמודולו 13 נקבל מעט אפשרויות.

פתרון. ובכן, c^3 מודולו 13 יכול להיות $0,\ \pm 1^3=\pm 1,\ 2^3=8=-5$, וגם $(-2)^3=5$.
אלה 5 האפשרויות שקיימות: $0,\ \pm 1,\ \pm 5$.
d^3 מודולו 13 יכול להיות $0,\ 1,\ 2^4=16=3,\ 4^4=3^2=9$, ולא יתכן שיש אפשרויות נוספות כי זה כבר הכמות שצריכה להיות.
כל הסכומים האפשריים נרשום בטבלה:

	−5	−1	0	1	5
0	−5	−1	0	1	5
1	−4	0	1	2	6
3	−2	2	3	4	−4
−4	4	−5	−4	−3	1

כעת נחשב 19^{19} מודולו 13.

$$19^{19}=6^{19}=6^7=6\cdot\left(6^2\right)^3=$$
$$=6\cdot 36^3=6\cdot(-3)^3=6\cdot(-27)=$$
$$=6\cdot(-1)=-6\pmod{13}$$

וקל לראות שמספר זה לא מופיע בטבלה. לכן למשוואה אין פתרון בשלמים.

2. נבנה סדרה: $a_1=1$, ומכאן באמצעות כלל נסיגה: נסמן ב- c_n את ספרת היחידות של a_n ונגדיר $a_{n+1}=a_n+c_n$. הראו שכל חזרה של 4 מופיעה בסדרה (כלומר לכל k טבעי, קיים n טבעי, כך ש- $a_n=4^k$).

רעיון של פתרון. נסתכל על התהליך מודולו 20. מצד אחד זה מגדיר את הספרה האחרונה, ומצד שני אנחנו יודעים את חזקות 4 מודולו 20 (מכיוון ש- $4^k=0\pmod 4$, וגם $4^k=(-1)^k\pmod 5$, לכן $4^k=\pm 4\pmod{20}$), ומצד שלישי יש סיכוי טוב שהתהליך מחזורי ונוכל להבין לגמרי מה הולך (לא כמו במספרים טבעיים שיש אינסוף צעדים, ולא כמו שמסתכלים על שתי ספרות אחרונות שזה בטח ארוך).

פתרון. ננסה להריץ את התהליך מודולו 20. אז

$$1\to 2\to 4\to 8\to 16\to 22=2\pmod{20}$$

מרגע זה נמשיך לנוע במעגלים $2\to 4\to 8\to 16\to 2$. בכל מעגל כזה המספר גודל ב-20, לכן נעבור על כל המספרים שהם $\pm 4\pmod{20}$, וכל חזקות 4 הן כאלה (חוץ מ-1, אבל גם הוא מופיע בסדרה).

3. האם קיים n טבעי, עבורו המספר $5^{2n+3}+3^{n+3}\cdot 2^n$ ראשוני?

רעיון של פתרון. כנראה שזה בד"כ לא ראשוני, כי אנשים לא יודעים ליצור מספרים ראשוניים גדולים, אבל כן יכולים ליצור מספרים שמתחלקים במשהו. התרגיל עוצב כך, שהמספרים שיתקבלו לא יתחלקו ב-2, 3 ו-5. לכן צריך לחשוב על גורמים גדולים יותר.
ננסה להציב $n=0$, למרות שזה לא מספר ראשוני לפי הגדרה. אבל זה לא משנה: אם נוכיח שכל המספרים מתחלקים ב-p מסוים, אז זה מתחיל כבר ב-$n=0$, הרי הסדרה מחזורית מודולו p לכל $p>5$. אז נקבל מספר

$$5^3+3^3\cdot 2^0=125+27=152$$

כמובן שמספר זה מתחלק ב-2, אבל זה דווקא תכונה שלא תישמר. אבל אם נחלק את המספר הזה ב-2 מספר פעמים נקבל 76, ואז 38, ואז 19. לכן המספר מתחלק ב-19. יש תקווה שהתכונה הזאת תישמר, ואז יהיה פתרון פשוט לשאלה.

פתרון. נחשב מודולו 19. אם $n=k+1$

$$5^{2n+3}+3^{n+3}\cdot 2^n=5^2\cdot 5^{2k+3}+3\cdot 2\cdot 3^{k+3}\cdot 2^k=25\cdot 5^{2k+3}+6\cdot 3^{k+3}\cdot 2^k=$$
$$=6\cdot\left(5^{2k+3}+3^{k+3}\cdot 2^k\right)\ \left(\mathrm{mod}19\right)$$

לכן אם מספר אחד בסדרה מתחלק ב-19, אז גם המספר הבא וגם כל המספרים אחריו באינדוקציה. אבל המספר האפסי מתחלק ב-19. לכן כל המספרים מתחלקים ב-19 ואינם ראשוניים.

4. נתון מספר $k>1$ עבורו $p=6k+1$ ראשוני. נסמן $m=2^p-1$. הוכיחו כי $2^{m-1}-1$ מתחלק ב-$127m$.

פתרון. קל לבדוק שהמספר 127 ראשוני.
כאשר נתבונן ב-2^n מודולו 127, נוכל לשים לב כי $2^7=1\left(\mathrm{mod}127\right)$ ולכל m קטן יותר זה לא מתקיים. כל מספר ניתן להציג בצורה $n=7m+r$, כאשר $0\le r<7$. ואז רואים כי $2^n=2^{7m}\cdot 2^r=2^r\left(\mathrm{mod}7\right)$. זה שווה 1 רק כאשר $r=0$, כלומר כאשר n מתחלק ב-7. על מנת שהשאלה תהיה נכונה, $2^{m-1}-1$ חייב להתחלק ב-127, לכן $m-1$ חייב להתחלק ה-7.
קל לראות כי $m-1=2^p-2$ מתחלק ב-7 כאשר $2^{p-1}-1$ מתחלק ב-7, כלומר כאשר $p-1$ מתחלק ב-3, וזה כבר הובטח לנו: $p-1=6k$.

כמובן חייבים גם ש-$2^{m-1}-1=2^{2^p-2}-1$ יתחלק ב-m. אבל $2^p=1\left(\mathrm{mod}\,m\right)$, ולכן מספיק בשביל זה ש-$m-1=2^p-2$ יתחלק ב-p. אבל זה מתקבל מיידית ממשפט פרמה הקטן. למקרה ש-m ו-127 זרים זה מסיים.
אם m ו-127 לא זרים, אז $m=2^p-1$ מתחלק ב-127. הסדרה 2^n-1 מחזורית מודולו 127, וגודל המחזור הוא 7. לכן במקרה זה מתקבל ש-p מתחלק ב-7. אבל p ראשוני, ולכן p הוא 7. אבל נאמר כי $p=6k+1$ כאשר $k>1$, ובמקרה זה $k=1$.
כלומר המקרה האחר נפסל לפי תנאי השאלה.

הערה. בעצם אם לא היו פוסלים את 7 באופן מלאכותי, השאלה הייתה שגויה, מכיוון ש-$2^{2^7}-1$ לא מתחלק ב-7^2.

הערה נוספת. שאלה זו קשורה לשאלה: נשאל שאלה כללית: עבור אילו M ו-L טבעיים, המספר 2^M-1 מתחלק ב-q^L, למשל כאשר כאשר $q=127$. התשובה היא: אך ורק כאשר M מתחלק ב-$7\cdot q^{L-1}$. זה חלק מעיקרון כללי שנקראה הרמת אקספוננט, שעוזר לפתור הרבה שאלות מסוג זה. כאן אפשר לראות מספר שאלות וניסוח כללי:
http://taharut.org/imo/I5775/LiftingExp.pdf

5. נתונים מספרים טבעיים $K>L>M>N$ המקיימים
$$KM+LN=(K+L-M+N)(-K+L+M+N).$$
הראו כי $KL+MN$ פריק.

פתרון. נפתח סוגריים.
$$KM+LN=(N+L)^2-(K-M)^2$$
$$(K-M)^2+KM=(N+L)^2-LN$$
$$K^2-KM+M^2=N^2+NL+L^2$$
לכן
$$(KM+LN)(N^2+NL+L^2)=KM(N^2+NL+L^2)+LN(K^2-KM+M^2)$$
$$=KMN^2+KML^2+LNK^2+LNM^2=(KL+MN)(KN+LM)$$
קל לבדוק כי בהינתן $K>L>M>N>0$, מתקיים
$$KL+MN>KM+LN>KN+LM$$
אבל ראינו כי $(KL+MN)(KN+LM)$ מתחלק ב-$KM+LN$. לו $KL+MN$ היה ראשוני, $KN+LM$ היה חייב להתחלק ב-$KM+LN$, אבל הוא קטן ממנו.

6. פתרו את המשוואה $2^x3^y-5^z7^w=1$ במספרים שלמים.

תשובות. $(1,0,0,0)$, $(3,0,0,1)$, $(1,1,0,0)$, $(2,2,1,1)$

פתרון. קל לראות שהמספרים אינם שלילים (אחרת אגף שמאל לא שלם)
נסתכל מודול 5. כל עוד $z>0$,
$$2^x3^y=1\pmod 5$$
2 ו-3 הן שאריות לא ריבועיות מודולו 5. לכן $x+y$ בהכרח זוגי.
נסתכל גם מודולו 7. כל עוד $w>0$,
$$2^x3^y=1\pmod 7$$
הפעם 2 הוא שארית ריבועית, ו-3 לא. לכן y זוגי. לכן גם x זוגי.
נרשום $x=2a$, $y=2b$. אז
$$5^z7^w=\left(2^a3^b\right)^2-1=\left(2^a3^b-1\right)\left(2^a3^b+1\right)$$

שני הגורמים נבדלים ב-2. אם אחד מהם מתחלק ב-5 או ב-7, אז השני לא. לא יתכן שאחד הגורמים הוא 1 (כי אז השני הוא 3 או -1, ולא מכפלה של חזקת 5 וחזקת 7). קיבלנו

טענה 1. אם $z,w>0$ אז $5^z,7^w=2^a3^b\pm1$ כאשר $a=\frac{x}{2}$, $b=\frac{y}{2}$ שלמים.

בדיקה מודולו 2 נותנת רק ש-$x>0$, אבל בדיקה מודולו 8 במקרה $x\geq3$ נותנת

$$-5^z7^w=1\pmod8$$

מכאן קל לראות, ש-z זוגי (אחרת היינו מקבלים $\pm5=1\pmod8$), וגם ש-w אי-זוגי. בדיקה מודולו 3 מראה כי

$$-(-1)^z=1\pmod3$$

וזה אומר ש-z אי-זוגי.

כבר הגענו לסתירה. בעצם הגענו לסתירה בשתי בדיקות אחרונות, כאשר הנחנו ש-2^x3^y מתחלק ב-8 וב-3. לכן ניתן להניח כי $x<3$ או ש-$y=0$. קיבלנו

טענה 2. $y=0$ או $x\in\{1,2\}$. אם $y>0$ אז z אי-זוגי, ובמקרה $x\geq3$ אז z זוגי ו-w אי-זוגי.

נעשה חלוקה למקרים. באמצעות טענה 2.

(א) $y=0$

במקרה זה לפי טענה 1 מקבלים שאם $w,z>0$ אז $5^z,7^w=2^a\pm1$.

כמו כן, אם $w=0$ אז $5^z=2^x-1$, ואם $z=0$ אז $7^w=2^x-1$.

שלושה תת-מקרים אלה מכסים את כל המקרה, ולכן נרצה לחקור שאלות:

שאלה א1. מתי $5^z=2^x-1$?

שאלה א2. מתי $7^w=2^x-1$?

אם נענה על שאלות אלו, נוכל לקחת a במקום x ולסיים גם את תת-מקרה הראשון במקרה הנוכחי. מצד שני, חייבים לענות על שתי השאלות כי כל תשובה תיתן פתרון למשוואה המקורית.

תשובה אחת היא $x=1$ ואז $z=w=0$. אם $x>1$, אז בשאלה א1 2^x-1 רואים ש-x מתחלק ב-5. זה קורה כאשר x מתחלק ב-4. אבל $2^{4t}-1=\left(2^{2t}-1\right)\left(2^{2t}+1\right)$, והרי לא יתכן ששני הגורמים באגף ימין הם חזקות של 5, הרי ההבדל בינם הוא 2.

אם $x>1$ ו-$7^w=2^x-1$, אז 2^x-1 מתחלק ב-7, ואז x מתחלק ב-3. כאשר $x=3$ זה באמת נותן תשובה. אם $x>3$ אז $x=3t$, ואז $2^{3t}-1=\left(2^t-1\right)\left(2^{2t}+2^t+1\right)$. לא יתכן ששני הגורמים באגף ימין מתחלקים ב-7: אם $2^t=1\pmod7$ אז נקבל

$$2^{2t}+2^t+1=3\pmod7.$$

ובכן, קיבלנו שתי תשובות: $2^x-1=1$ ו-$2^x-1=7$. מזה מקבלים שני פתרונות למשוואה המקורית (שתי התשובות הראשונות ברשימת תשובות), אבל לא מקבלים אף מקרה שבו גם 2^x+1 הוא חזקה של 5 או 7, לכן לא מקבלים פתרון בתת-מקרה ראשון.

(ב) $x=1$ כאשר $y>0$

שוב, נעשה חלוקה לתת-מקרים בעזרת טענה 1. המקרה $z,w>0$ נפסל מראש כי במקרה זה x חייב להיות זוגי, ובמקרה הנוכחי x אי-זוגי. לכן z או w שווה 0. מקבלים כי $2\cdot 3^y-1$ הוא חזקה של 5 או של 7. חזקה של 7 לא יכול להיות מהסתכלות מודולו 3, לכן נשאר לפתור משוואה

$$2\cdot 3^y=5^z+1$$

דוגמה מתבקשת היא $y=1$, וזה נותן את התשובה השלישית ברשימת תשובות.

אם $y>1$ אז z בהכרח אי-זוגי (מבדיקה מודולו 3). מהתבוננות מודולו 9 רואים כי z מתחלק ב-3. אז נרשום $z=3t$ ונפרק לגורמים:

$$2\cdot 3^y=5^{3t}+1=\left(5^t+1\right)\left(25^t+5^t+1\right)$$

אבל 5^t+1 זוגי, לכן גם הוא פעמיים חזקה של 3. לכן אם $z>1$ פתרון, אז גם $\frac{z}{3}$ פתרון.

לכן כל פתרון z נוכל לחלק ב-3 מספר פעמים, ונקבל פתרונות כל הזמן, עד שנגיע ל-1. לכן נוכל לקבל כל פתרון כאשר ניקח את 1 ונכפיל אותו ב-3 מספר פעמים, וכל המספרים שנעבור באמצע הם פתרונות. אבל כבר ניסיון ראשון $z=3$ נותן $5^3+1=126$ וזה לא פעמיים חזקת 3. לכן אין תשובות נוספות במקרה זה.

(ג) $x=2$ כאשר $y>0$. נזכיר כי z אי-זוגי לפי טענה 2.

שוב נעשה חלוקה לתת-מקרים בעזרת טענה 1. לא יתכן ש-$z=0$ (הרי הוא אי-זוגי), אבל יתכן כי $w=0$, ואם לא אז $5^z,7^w=2^a3^b\pm 1$, כאשר $a=\frac{x}{2}$, $b=\frac{y}{2}$.

בתת-מקרה ראשון נקבל: $4\cdot 3^y=5^z+1$.

בתת-מקרה שני נקבל: $5^z,7^w=2\cdot 3^b\pm 1$

לגבי תת-מקרה שני: את המשוואה $5^z,7^w=2\cdot 3^b-1$ פתרנו כאשר ניתחנו מקרה (ב) (אם y במקום b), והיה שם פתרון אחד בלבד $b=1$. לכן

$$5\cdot 7=\left(2\cdot 3-1\right)\left(2\cdot 3+1\right)=2^2 3^2-1$$

וזה נותן פתרון רביעי ברשימת תשובות, אבל אין פתרונות נוספים במקרה זה.

נשאר תת-מקרה ראשון: $4\cdot 3^y=5^z+1$. בדיקה מודולו 4 מחסלת אותו:

$$0=1^z+1\left(\mathrm{mod}\,4\right).$$

בתת-מקרה זה אין אף תשובה.