תרגיל 8

1. מצאו את כל השלמים החיוביים n כך ש-n^2+2^n הוא ריבוע שלם.

תשובה. $n=6$.

פתרון. אם $n^2+2^n=m^2$ אז $2^n=m^2-n^2=(m-n)(m+n)$, לכן $m-n=2^k$, $m+n=2^\ell$ כאשר $\ell+k=n$. לגן $2n=2^\ell-2^k$. אם $2^\ell-2^k$ חיובי, אז $2^\ell-2^k\geq 2^{\ell-1}$.

מצד שני, $2\ell>\ell+k=n$. לכן $4\ell>2n$. לכן $4\ell\geq 2n=2^\ell-2^k\geq 2^{\ell-1}$.

מכאן אפשר להסיק כי $\ell\geq 2^{\ell-3}$. זה מוזר. עבור $\ell=6$ נקבל $6>8$ שזה כמובן שגוי. ככל שנגדיל את ℓ, האגף בשמאלי יוגדל ב-1, והימני פי 2 כלומר יותר מאשר ב-1. לכן הטענה הזו שגויה לכל $\ell\geq 6$. מכאן שלכל פתרון $\ell\geq 5$. בנוסף, היות ו-$k<\ell$, נקבל $\ell\geq 1$.

לכן צריך לבדוק מקרים $\ell=1,2,3,4,5$, ולבדוק בכל מקרה האם יש k קטן יותר, כך שמתקיים $2(\ell+k)=2^\ell-2^k$. אגף שמאלי מתחלק ב-2, אז גם הימני, לכן $k\geq 1$, ולכן $\ell\geq 2$.

לכן $\ell+k=2^{\ell-1}-2^{k-1}$.

אם $\ell=5$ נקבל $k+2^{k-1}=16-5=11$. עביר $k=4$ או יותר אגף שמאל הוא 12 או יותר וזה גדול מדי, עבור כל k קטן יותר זה קטן מדי.

אם $\ell=4$ נקבל $k+2^{k-1}=8-4=4$. זה אפשרי כאשר $k=2$ ורק אז.

אם $\ell=3$ נקבל $k+2^{k-1}=4-3=1$. זה בלתי אפשרי כי אגף שמאלי הוא לפחות 2.

אם $\ell=2$ נקבל $k+2^{k-1}=2-2=0$. זה בלתי אפשרי מאותה סיבה.

ובכן, יש פתרון יחיד, עבורו $\ell=4$, $k=2$, ואז $n=\ell+k=6$.

אכן, $2^6+6^2=64+36=10^2$.

2. מצאו את כל המספרים אי-זוגיים $n>1$, כך שלכל שני מחלקים זרים שלו a ו-b, גם $a+b-1$ הוא מחלק של n.

תשובה. $n=p^k$, כאשר p ראשוני אי-זוגי.

פתרון. נגיד ש-p הוא המחלק הראשוני הקטן ביותר שמחלק את n. אז ניתן לרשום $n=p^km$.

היות ו-p זר ל-m, לפי הנתון, $d=m+p-1$ הוא גם מחלק של n. אז d זר ל-m. אם לא, אז ל-m ול-$p-1$ יש מחלק משותף שקטן מ-p. אבל p הוא המחלק הכי קטן של n.

לכן d הוא מחלק של n שזר ל-m, לכן $d=p^u$.

אבל גם $e=d+p-1$ הוא מחלק של n, מצד שני $e=m+2p-2$. אז גם e זר ל-m, אחרת יש להם מחלק ראשוני משותף שהוא גם מחלק של $2(p-1)$ לכן הוא קטן מ-p אבל p הוא החלק הראשוני הקטן ביותר של n ולכן הוא גם קטן מכל מחלק ראשוני של m. אז גם e הוא מחלק של n שזר ל-m, ולכן גם $e=p^v$.

לכן $p-1=e-d=p^v-p^u=p^u\left(p^w-1\right)$. כלומר $u=0$, $w=1$. לכן $p=d=m+p-1$, לכן $m=1$. נותר לציין שעבור $m=1$ התנאי נכון באופן ריק: אם שני מחלקים זרים, אחד מהם שווה ל-1.

3. הראו כי $\binom{n}{1}+1973\cdot\binom{n}{3}+1973^2\cdot\binom{n}{5}+1973^3\cdot\binom{n}{7}+...$ מתחלק ב-2^{n-1}.

פתרון. נסמן $s_n=\binom{n}{1}+1973\cdot\binom{n}{3}+1973^2\cdot\binom{n}{5}+1973^3\cdot\binom{n}{7}+...$.

נסמן גם $r=\sqrt{1973}$. אז $s_n=\dfrac{(1+r)^n-(1-r)^n}{2r}$. אם נסמן $1-r=b$, $1+r=a$, נוכל לרשום $s_n=\dfrac{a^n-b^n}{2r}$. אבל

$$a^n-b^n=(a+b)\left(a^{n-1}-b^{n-1}\right)+ab\left(a^{n-2}-b^{n-2}\right)=2\left(a^{n-1}-b^{n-1}\right)+1972\left(a^{n-2}-b^{n-2}\right)$$

ולכן $s_n=2s_{n-1}+1972s_{n-2}$. מכאן קל לפתור את השאלה באינדוקציה. מספרים s_0,s_1 שלמים, 1972 מתחלק ב-4, לכן אם s_{n-1} מתחלק ב-2^{n-2} ו-s_{n-2} מתחלק ב-2^{n-3} אז שני המחוברים בנוסחה $2s_{n-1}+1972s_{n-2}$ מתחלקים ב-2^{n-1}.

4. מספרים טבעיים x,y,z (כאשר $x>2,\quad y>1$) מקיימים $x^y+1=z^2$. כמות המחלקים הראשוניים השונים של x תסומן u, כמות המחלקים הראשוניים השונים שח y תסומן v. הראו כי $u\geq v+2$.

פתרון. מתקיים $x^y=(z-1)(z+1)$.

אם x אי-זוגי, אז $(z-1,z+1)=1$. במקרה זה $z-1=u^y$, $z+1=v^y$. אבל אז $v^y-u^y=2$, כאשר $y>1$, $v>u$, כאשר v,u אי-זוגיים לכן $v-u\geq 2$, ולכן

$$4=2\cdot 2\leq(v-u)\left(v^{y-1}+v^{y-2}u+...+u^{y-1}\right)=v^y-u^y=2.$$

נשארת האפשרות השנייה: x אי-זוגי. אז $\left(z-1,z+1\right)=2$ אחד מבין המספרים $z-1$, $z+1$ אינו מתחלק ב-4, והשני כן. לכן $A=2\alpha^y, B=2^{y-1}\beta^y$, כאשר α מספר אי-זוגי, והמספרים A,B הם המספרים $z\pm1$, וגם $AB=x^y$.

לכן $2=\left|2\alpha^y-2^{y-1}\beta^y\right|$, כלומר $\left|\alpha^y-2^{y-2}\beta^y\right|=1$, ולכן $\alpha^y\pm1=2^{y-2}\beta^y$.

אם $\alpha=1$ אז $A=2$ ואז $B=4$, ולכן $z=3$, ואז $x^y=8$ אבל נאמר במפורש ש-$y>1$, $x>2$.
מכיוון ש-α אי-זוגי, נקבל ש-$\alpha\geq3$.

נשים לב גם כי y אי-זוגי: אחרת $z^2-\left(x^t\right)^2=1$ וזה לא יתכן (אלה אם כן $x=0$).

טענה 1. נניח כי $a\geq2$, p ראשוני אי-זוגי. אז למספר a^p-1 יש לפחות מחלק ראשוני אחד, שהוא לא מחלק של $a-1$.

טענה 2. נניח כי $a\geq2$, p ראשוני אי-זוגי, ולא מתקיים $\left(a,p\right)=\left(2,3\right)$. אז למספר a^p+1 יש לפחות מחלק ראשוני אחד, שהוא לא מחלק של $a-1$.

טענה 3. נניח כי $\left|a\right|\geq2$, $\left(k,m\right)=1$, כאשר k,m מספרים טבעיים. אז $\left(a^k-1,a^m-1\right)=a-1$.

טענה 4. נניח כי $\left|a\right|\geq2$, $\left(k,m\right)=1$, כאשר k,m מספרים טבעיים אי-זוגיים.
אז $\left(a^k+1,a^m+1\right)=a+1$.

נוכיח את הטענות בסוף, אבל קודם נפתור את השאלה באמצעות הטענות. בשאלה מבקשים להוכיח שאם ל-y יש v מחלקים ראשוניים $p_1,p_2,...,p_v$ אז ל-x יש לפחות $v+2$ מחלקים ראשוניים.
מחלקים ראשוניים של x הם מחלקים ראשוניים של A ושל B, זה כולל את המחלקים הראשוניים של α וגם את מחלקים של $\alpha^y\pm1$ (שהם שונים). בין המחלקים של $\alpha^y\pm1$ יש מחלק ראשוני של אחד לפחות $\alpha\pm1$ (הרי $\alpha\pm1>1$), וכל לכל $i=1,2,...,v$ מחלק ראשוני נוסף q_i של $a^{p_i}\pm1$ (לפי טענה 1 או 2 בהתאם לסימן), שהם שונים זה מזה (לפי טענה 3 או 4 בהתאם לסימן). לכן יש לפחות $v+2$ מחלקים.

בשביל להשלים את הפתרון, נוכיח את הטענות:

הוכחת טענה 1. המספר מתפרק לשני גורמים $a^p-1=\left(a-1\right)\left(a^{p-1}+...+a^2+a+1\right)$. כל מחלק של $a^{p-1}+...+a^2+a+1$ שהוא גם מחלק של $a-1$ הוא בהכרח מחלק של p, היות ו-

$$a^{p-1}+...+a^2+a+1=1^{p-1}+...+1^2+1+1=p\left(\mathrm{mod}\ a-1\right)$$

לכן המקרה היחיד שיש לדון בו זה $p\left|a-1\right.$. במקרה זה, $a=p\cdot c+1$ ולכן

$$a^p-1=\left(p\cdot c+1\right)^p-1=\left(pc\right)^3\cdot M+\left(pc\right)^2\binom{p}{2}+p^2c+1-1=p^2c\cdot\left(1+pN\right)$$

כלומר $a^{p-1}+...+a^2+a+1=\frac{a^p-1}{a-1}=p\cdot\left(1+pN\right)$, כלומר מספר זה מתחלק ב-$p$ ולא ב-p^2.
אבל $a>1$ וסכום של p מחוברים שהם חזקות של a בהכרח גדול מ-p, לכן יש גם עוד מחלק ראשוני שהוא לא p והוא לא מחלק של $a-1$.

הוכחת טענה 2. המספר המפרק לגורמים $\left(a+1\right)\left(a^{p-1}-a^{p-2}+...+a^2-a+1\right)$ הוא a^p+1.

$$a^{p-1}-a^{p-2}+...+a^2-a+1=\left(-1\right)^{p-1}-\left(-1\right)^{p-2}+...+\left(-1\right)^2-\left(-1\right)+1=$$
$$=\underbrace{1+...+1}_{p}=p\left(\mathrm{mod}\ a-1\right)$$

לכן אם יש מחלק ראשוני משותף ל-$a+1$ ול-$a^{p-1}-a^{p-2}+...+a^2-a+1$, אז זה p. אם נוכיח ש-$a^{p-1}-a^{p-2}+...+a^2-a+1$ אינו מתחלק ב-p^2 וקל לראות כי

$$a^{p-1}-a^{p-2}+...+a^2-a+1=\left(a-1\right)a^{p-2}+...+\left(a-1\right)a+1\geq 2+...+2+1=p$$

שוויון מתקיים רק אם $a=2$ (רק אז $a-1=1$), ורק כאשר $p=3$ (אחרת $a^{p-2}>2$), וזה המקרה היחיד שטענה לא מטפלת בו. לכן הגורם גדול ממש מ-p, ואם הוא לא מתחלק ב-p^2 אז יש עוד גורם ראשוני שלא משתתף ב-$a+1$.

ההוכחה שזה לא מתחלק ב-p^2 זהה בדיוק להוכחה בטענה ראשונה. אכן אם מחליפים סימן ל-a, בדיוק מגיעים לטענה 1. ובעצם סימן של a לא משפיע על תכונות התחלקות (גם אם הוא משפיע על אי-שוויונים), אז אפשר לא לחזור על ההוכחה.

הוכח טענה 3. נניח כי $k<m$. אז

$$\left(a^k-1,a^m-1\right)=\left(a^k-1,a^m-1-a^{m-k}\left(a^k-1\right)\right)=\left(a^k-1,a^{m-k}-1\right)$$

לכן אפשר להחליף זוג k,m בזוג $k,m-k$. תהליך שבו עושים כל פעם החלפות מסוג זה הוא בעצם אלגוריתם אוקלידוס. לכן בסוף נקבל $\left(a^k-1,a^m-1\right)=a^d-1$ כאשר $d=\left(k,m\right)$. כמקרה פרטי, אם $\left(m,k\right)=1$ אש $d=1$.

הוכחת טענה 4. מחליפים סימן ל-a ומגיעים לטענה 3.

הערה. בעצם בשיטה דומה אפשר לחזר את טענת הבעיה: אם y הוא מכפלת v גורמים שגדולים מ-1, אז ל-x יש לפחות $v+2$ גורמים ראשוניים שונים.

5. הראו שלכל מספר חיובי שלם n קיים מספר טבעי m עבורו 2^m+m מתחלק ב-n.

פתרון. נוכיח באינדוקציה על n שקיים m גדול כרצוננו עבורו $2^m=-m\left(\mathrm{mod}\,n\right)$ מתחלק ב-n.
עבור $n=1$ זה ברור לקיפוד, נניח ש-$n>1$.

סדרה של חזקות 2 מודולו n היא סדרה מחזורית, והמחזור הוא מחלק של $\varphi(n)$.
נתבונן במספרים m מסוג $m=-2^k\left(\mathrm{mod}\ m\cdot\varphi(m)\right)$, כאשר k גדול מספיק.
לכן אם $x=y\left(\mathrm{mod}\varphi(n)\right)$, והמספרים x,y גדולים מספיק, אז הנוסחה $2^m=-m\left(\mathrm{mod}\,n\right)$ שקולה לנוסחה $2^m=2^k\left(\mathrm{mod}\,n\right)$, וזה מתקיים אם $m=k\left(\mathrm{mod}\,\varphi(n)\right)$, כאשר k,m גדולים מספיק, כלומר כאשר $k=-2^k\left(\mathrm{mod}\,\varphi(n)\right)$. אבל זה קיים לפי הנחת האינדוקציה, הרי $\varphi(n)<n$.

6. בהינתן מספר ראשוני p, מצאו את כל המספרים הטבעיים m עבורם קיימים אינסוף ראשוניים q כך ש-q לא מחלק אף מספר מהצורה n^p-p^m כאשר n טבעי.

תשובה. $p\nmid m$

פתרון. אם $p\mid m$ אז $m=k\cdot p$ ואז $n^p-p^m=n^p-\left(p^k\right)^p=\left(n-p^k\right)\cdot(\ldots)$, והרי כל מספר ראשוני מספיק גדול הוא $n-p^k$, לכן יש רק מספר סופי של q מסוג זה.
נעבור למקרה $p\nmid m$. אנחנו נרצה להוכיח כי קיימים אינסוף q עבורם אין אף n שפותר משוואה $n^p=p^m\left(\mathrm{mod}\,q\right)$.
קודם נפשט את המשוואה. כמובן אפשר להניח כי $p\neq q$ (גם כי $p=q$ זו רק דוגמה אחת וצריך אינסוף דוגמאות, וגם כי $p=q$ לא עובד). היות ו-$(m,p)=1$ קיים w כך ש-$mw=ps+1$, ואז אם נעלה את שני האגפים בחזקה w נקבל $n^{wp}=p^{sp}\cdot p\left(\mathrm{mod}\,q\right)$. אם ניקח $\tilde{n}=\frac{n^w}{p^s}$ נקבל משוואה $\tilde{n}^p=p\left(\mathrm{mod}\,q\right)$.

לכן מספיק למצוא אינסוף q עבורם אין פתרון ל-$n^p=p\left(\mathrm{mod}\,q\right)$.

נסמן $Q(x)=x^{p-1}+x^{p-2}+\ldots+1=\frac{x^p-1}{x-1}$.

נבחר k שזר ל-p. נתבונן ב-$Q\left(k^p p\right)$. אז $Q\left(k^p p\right)=1+k^p p\neq 1\left(\mathrm{mod}\,p^2\right)$.

לכן קיים q ראשוני שמחלק את $Q\left(k^p p\right)$ כך ש- $q \neq 1 \left(\mathrm{mod}\ p^2\right)$.

כל מחלק של $Q(x)$ הוא גם מחלק של $x^p - 1$, אבל אם הוא מחלק גם את $x-1$ אז הוא בהכרח מחלק את p, הרי $Q(x) = x^{p-1} + x^{p-2} + \ldots + 1 = \underbrace{1+1+\ldots+1}_{p} = p \left(\mathrm{mod}\ x-1\right)$.

לכן $q \mid \left(k^p p\right)^p - 1$, אבל $q \nmid k^p p - 1$.

נניח בשלילה ש- $p = n^p \left(\mathrm{mod} q\right)$. אז $\left(nk\right)^p = k^p x \neq 1 \left(\mathrm{mod}\ q\right)$.

מצד שני $\left(nk\right)^{p^2} = \left(k^p x\right)^p = 1 \left(\mathrm{mod}\ q\right)$. לכן הסדר הכפלי של nk מודולו q הוא p^2. לכן לפי משפט פרמה הקטן, $p^2 \mid q-1$. אבל בחרנו ש- $q \neq 1 \left(\mathrm{mod}\ p^2\right)$.

נותר להראות, שיש אינסוף מספרים ראשוניים q מסוג זה. בשיטה שתיארנו, q נבחר להיות מחלק של $Q\left(k^p p\right)$, שהוא זר ל- k ול- p כאשר k מספר כלשהו שזר ל- p.

נניח שמצאונו רק M מספרים מסוג זה: $q_1, q_2, q_3, \ldots, q_M$. בבנייה הבאה ניקח $k = q_1 q_2 \cdot \ldots \cdot q_m$, זה יבטיח שהמספר q החדש שונה מכל המספרים שבחרנו קודם ומקיים את התנאים.