תרגיל 5

1. הראו שלא קיימים k,m שלמים חיוביים ו- p ראשוני עבורם $\sqrt[3]{k}+\sqrt[3]{m}=\sqrt[3]{p}$.

פתרון. נניח שקיימים. אז נעלה בשלישית: $k+m+3\cdot\sqrt[3]{km}\left(\sqrt[3]{k}+\sqrt[3]{m}\right)=p$,
אבל $\sqrt[3]{k}+\sqrt[3]{m}=p$ לכן $3\cdot\sqrt[3]{kmp}=p-k-m$.
לכן $\sqrt[3]{kmp}$ הוא מספר רציונאלי. אבל $0<k,m<p$ לכן k ו-m לא מתחלקים ב-p
לכן בפירוק לגורמים ראשוניים של kmp המספר p מופיע פעם אחד בלבד, כלומר $\sqrt[3]{kmp}$ אינו מספר רציונאלי. סתירה.

(אכן, לו היו מספרים שלמים a,b עבורם $\sqrt[3]{kmp}=\frac{a}{b}$, אז היה $kmp\cdot b^3=a^3$, ואז באגף שמאל בפירוק לגורמים ראשוניים p מופיעה בחזקה שלא מתחלקת ב-3, ובאגף ימין p מופיע בחזקה שכן מתחלקת ב-3, וזה נוגד את יחידות הפירוק של מספר לגורמים ראשוניים.)

2. איזה מספרים טבעיים n ניתן להציג כסכום של ארבעה מספרים שלמים חיוביים $n=a+b+c+d$, כך שמתקיים $ab=cd$?

תשובה. כל מספר פריק.
פתרון. נסמן ב-u את המחלק המשותף המרבי של a ו-c. אז $a=uv$, $c=uw$, כאשר v,w זרים, לכן $uvb=uwd$, לכן $vb=wd$, לכן d מתחלק ב-v, לכן $d=vt$, לכן $vb=vwt$, לכן $b=wt$.
נסכם מה שהראנו עד עכשיו: אם $ab=cd$, אז $a=uv$, $b=wt$, $c=uw$, $d=vt$.
לכן בשאלתנו $n=a+b+c+d=uv+uw+tv+tw=\left(u+t\right)\left(v+w\right)$.
לכן n בהכרח פריק.
מצד שני, אם n פריק, אז ניתן לרשום $n=km$ כאשר $k,m\geq 2$, לכן ניתן לרשום אותם בתור $k=u+t$, $m=v+w$ כאשר u,v,w,t שלמים חיוביים, לכן אם נגדיר 4 מספרים $a=uv$, $b=wt$, $c=uw$, $d=vt$ אז
$n=km=\left(u+t\right)\left(v+w\right)=uv+uw+tv+tw=a+b+c+d$.

3. הוכיחו שהמספרים הבאים אינם ראשוניים ללא שימוש במחשבון או מחיר ב:
א. 8027. **ב.** 104060509. **ג.** $512^3+675^3+720^3$. **ד.** 1280000401.

פתרון.
א. $8027=20^3+3^3=\left(20+3\right)\left(400-20\cdot 3+3^2\right)=23\cdot 349$.
כמובן, על נמת להבחין בדברים כאלה כדאי לזכור נוסחאות כפל מקוצר.

ב. נעשה בדיקת חלוקה במספרים ראשוניים קטנים באמצעות סימני חלוקה. 2, 3, 5, 11 לא מצליח. בדיקה ב-7 ו-13 נעשית באמצעות השיטה

$$abcdefghi = abc - def + ghi \pmod p .$$

במקרה שלנו המספר $553 = 613 - 60 = 509 + 60 - 104$, קל לבדוק שזה לא מתחלק ב-13 אבל כן מתחלק ב-7, הרי $56 = 7 \cdot 8$ והמספר שלנו הוא $7 \cdot (80 - 1) = 560 - 7$.

ובכן, המספר הארוך מתחלק ב-7.

הערה. הגורמים הראשוניים האחרים של המספר הם 1993 ו-7459 אבל זה יותר קל למצוא אם מחשב.

ג. יש נוסחה שדומה לשאלה זאת:

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)\left(a^2 + b^2 + c^2 - ab - ac - bc\right) .$$

מה שיש לנו זה:

$$512^3 + 675^3 + 720^3 = \left(2^9\right)^3 + \left(5^2 \cdot 3^3\right)^3 + \left(3^2 \cdot 2^4 \cdot 5\right)^3$$

יש כאן רק 3 מחוברים, והסיבה לכך יכולה להיות ששני מחוברים התמזגו:

$a = 2^9, b = 5^2 3^3$, ואילו c דומה ל-$\pm\sqrt[3]{abc}$ ולכן קל לחבר בין c^3 ל-abc.

אז יהיה אפשר להפוך את שני המחוברים לאחד, ויהיה קשה להבחין בכך, שהיו שם בעצם שני מחוברים.

למשל אם $c = k2^3 \cdot 3^2 \cdot 5$ אז

$$c^3 - 3abc = k^3 2^9 3^6 5^3 - k2^{12} 3^6 5^3 = \left(k^2 - 2^3\right)k \cdot 2^9 \cdot 3^6 \cdot 5^3 \stackrel{?}{=} \left(2^4 \cdot 3^2 \cdot 5\right)^3 .$$

ובכן, צריך שיתקיים $\left(3k^2 - 8\right)k = 8$ וקל לנחש ש-$k = -2$ עושה את זה.

עד עכשיו דיברנו על כיצד למצוא את ההוכחה, כעת נכתוב את ההוכחה:

$$512^3 + 675^3 + 720^3 = \left(2^9\right)^3 + \left(5^2 \cdot 3^3\right)^3 + 2^3 \cdot \left(3^2 \cdot 2^3 \cdot 5\right)^3 =$$

$$= \left(2^9\right)^3 + \left(5^2 \cdot 3^3\right)^3 - \left(3^2 \cdot 2^4 \cdot 5\right)^3 + 3 \cdot 2^9 \cdot \left(5^2 \cdot 3^3\right) \cdot \left(3^2 \cdot 2^4 \cdot 5\right) =$$

$$= a^3 + b^3 - c^3 - 3abc = (a + b - c)\left(a^2 + b^2 + c^2 + ac + bc - ab\right) =$$

$$= (512 + 675 - 720) \cdot (...)$$

ד. $1280000401 = 2^7 \cdot 10^7 + 2^2 \cdot 10^2 + 1 = a^7 + a^2 + 1$, כאשר $a = 20$.

נשים לב שהפולינום $a^7 + a^2 + 1$ מתחלק בפולינום $a^2 + a + 1$.

אפשר לראות את זה בקלות מכך, ששני השורשים המרוכבים של $a^2 + a + 1$ מאפסים את $a^7 + a^2 + 1$, אבל ניתן גם לרשום במפורש:

$$a^7 + a^2 + 1 = a^7 - a^4 + a^4 - a + a^2 + a + 1 = \left(a^4 + a\right)\left(a^3 - 1\right) + a^2 + a + 1 =$$

$$= \left(\left(a^4 + a\right)(a - 1) + 1\right)\left(a^2 + a + 1\right) = \left(a^5 - a^4 + a^2 - a + 1\right)\left(a^2 + a + 1\right)$$

לכן המספר מתחלק ב-421.

4*. הוכיחו שלכל $k>2$ המספר $2^{2^{k-1}}-2^k-1$ אינו ראשוני.

פתרון. אנחנו ננסה למצוא ראשוני p, עבורו הנוסחה תקבל צורה $\frac{1}{2}+\frac{1}{2}-1$.
כלומר, נרצה שיתקיימו בו-זמנית משוואות:

$$\begin{cases} 2^{2^k}=1 \pmod p \\ 2^{k+1}=-1 \pmod p \end{cases}$$

ואז, אם נכפיל את המספר ב-2, נקבל $2^{2^k}-2^{k+1}-2=1-(-1)-2=0 \pmod p$. כול עוד $p\neq 2$, מקבלים שגם המספר הקודם מתחלק ב-p.

ובכן, שאיפה שלנו היא למצוא ראשוני p בו מתחלק $2^{k+1}+1$ וגם $2^{2^k}-1$.
נציג את $k+1$ כמכפלה של חזקת 2 ומספר אי-זוגי: $k+1=(2m+1)\cdot 2^\ell$.
ברור כי $\ell<k$, הרי $2^k>k+1>\ell+1$. כמובן, $\ell\geq 0$.

כעת נגדיר את p בתור מחלק ראשוני של $2^{2^\ell}+1$. אז $2^{2^\ell}=-1 \pmod p$
אז $2^{2^k}=\left(2^{2^\ell}\right)^{2\cdot\ldots\cdot 2}=(-1)^{2\cdot\ldots\cdot 2}=1 \pmod p$.
וגם $2^{k+1}=\left(2^{2^\ell}\right)^{2m+1}=(-1)^{2m+1}=-1 \pmod p$.
מש"ל.
(כמובן, $p\leq 2^{k+1}+1<2^{2^k}-2^k+1$.)

5. הראו שלכל k טבעי ו-p ראשוני למספר $(kp)^p-1$ יש גורם ראשוני q עבורו $q-1$ מתחלק ב-p. הסיקו (ללא שימוש במשפט דיריכלה) שלכל p ראשוני קיימים אינסוף מספרים ראשוניים מהצורה $np+1$, כאשר n מספר טבעי.

פתרון. $(kp)^p-1=(kp-1)\left((kp)^{p-1}+(kp)^{p-2}+\ldots+(kp)^2+kp+1\right)$
נתבונן בראשוני q שהוא מחלק של $(kp)^{p-1}+(kp)^{p-2}+\ldots+(kp)^2+kp+1$.
אז מתקיים $(kp)^p=1 \pmod q$.

מצד שני, $kp\neq 1 \pmod q$.
אכן, לו היה מתקיים $kp=1 \pmod q$, אז היינו מקבלים לפי הגדרת q
$0=(kp)^{p-1}+(kp)^{p-2}+\ldots+(kp)^2+kp+1=1+1+\ldots+1=p \pmod q$.
כלומר p מתחלק ב-q, אבל אפילו kp לא מתחלק ב-q.

נשים לב גם כי $kp\neq 0 \pmod q$, אחר היינו מקבלים $0=0^p=1 \pmod q$.

ובכן, מודולו q קיים מספר kp שהסדר שלו הוא p. אבל סדר מודולו q זה תמיד מחלק של $q-1$. לכן $q-1$ מתחלק ב-p, שזה מסיים א החלק הראשון של השאלה.

נניח שיש מספר סופי של מספרים מהסוג $np+1$. נשום את כולם: $q_1,...,q_m$.
לפי החלק הראשון של השאלה, למספר $\left(q_1 \cdot q_2 \cdot ... \cdot q_m \cdot p\right)^p - 1$ יש מחלק ראשוני q, שהוא מהצורה $np+1$, וכמובן שהוא לא נמצא ברשימה $q_1,...,q_m$. סתירה להנחת הסופיות.

6*. הוכיחו כי כל ראשוני p, קיים ראשוני q עבורו לאף n טבעי $n^p - p$ לא מתחלק ב-q.

פתרון. נתבונן ב-q שהוא מחלק ראשוני של

$$\frac{p^p-1}{p-1} = p^{p-1} + p^{p-2} + ... + p^2 + p + 1 = N.$$

נשים לב כי $p^p = 1 \pmod q$, אבל $p \neq 1 \pmod q$, הרי אחרת

$$0 = p^{p-1} + p^{p-2} + ... + p^2 + p + 1 = 1+1+1+...+1 = p = 1 \pmod q.$$

כמו כן, ברור כי $p \neq q$, הרי N אנו מתחלק ב-p.
לכן הסדר של p מודולו q הוא p. לו היה n עבורו $n^p - p$ מתחלק ב-q, כלומר

$$n^p = p \pmod q$$
$$n^{p^2} = 1 \pmod q$$

אז הסדר של n מודולו q הוא p^2. לכן לפי משפט פרמה הקטן, $q-1$ מתחלק ב-p^2, כלומר $q = p^2 \cdot m + 1$. ובכן, אם נצליח לבחור q שהוא מחלק ראשוני של N שאינו $p^2 \cdot m + 1$, אז מש"ל. אם כל המחלקים הראשוניים של N הם מסוג $p^2 \cdot m + 1$, כלומר שווים ל-1 מודולו p^2, אז גם N שווה ל-1 מודולו p^2, והוא לא. סתירה.