תרגיל 7

1. מחלקים את כמספרים מ-1 עד 10 לשתי מחלקות, כך שמכפלת כל המספרים במחלקה ראשונה חלקי מכפלת כל המספרים במחלקה שנייה יהיה מספר שלם. מהו הערך המינימלי האפשרי של המנה?

תשובה. 7.

פתרון. למשל $\frac{7\cdot 10\cdot 9\cdot 2\cdot 4}{1\cdot 5\cdot 6\cdot 3\cdot 8}=7$. המספר 7 חייב להיות במונה, כי אם הוא במחנה השבר לא יהיה שלם.

2. הראו כי $n!=\prod_{i=1}^{n}\operatorname{lcm}\left\{1,2,...,\left\lfloor\frac{n}{i}\right\rfloor\right\}$.

פתרון. נרשום את אגף שמאל כמכפלה $1\cdot 2\cdot 3\cdot ...\cdot n$.

בכללי, נשאל את עצמינו באיזו חזקה מקסימלית מספר ראשוני p מופיע בפירוק לגורמים ראשוניים של מכפלה ארוכה כלשהי של מספרים טבעיים $a_1a_2\cdots a_n$. בהתחלה ניתן לספור כמה גורמים במכפלה זו מתחלקים ב-p, לאחר מכן צריך לספור כמה גורמים במכפלה זו מתחלקים ב-p^2 ולהוסיף את הכמות שלהם, אחרי זה לספור כמה גורמים מתחלקים ב-p^3 וכך הלאה.

לכן בשביל ששתי מכפלות תהיינה שוות, מספיק שלכל חזקה טבעית של ראשוני $q=p^k$ בכל מכפלה יש אותה כמות של גורמים שמתחלקים ב-q.

במכפלה של אגף שמאל $1\cdot 2\cdot 3\cdot ...\cdot n$ יש $\left\lfloor\frac{n}{q}\right\rfloor$ גורמים שמתחלקים ב-q.

לגבי המכפלה של אגף ימין. הגורם $\operatorname{lcm}\left\{1,2,...,\left\lfloor\frac{n}{i}\right\rfloor\right\}$ מתחלק ב-$q=p^k$ אם $q\le\left\lfloor\frac{n}{i}\right\rfloor$, ואם לא אז לא. כלומר כמות הגורמים המתחלקים ב-q היא כמות המספרים הטבעיים i עבורם $q\le\frac{n}{i}$ שזה כמות המספרי הטבעיים i עבורם $i\le\frac{n}{q}$ וזה שווה ל-$\left\lfloor\frac{n}{q}\right\rfloor$.

כלומר בשתי המכפלות מקבלים אותו דבר.

3. הראו כי $\prod_{k=1}^{n-1}\left(2^n-2^k\right)$ מתחלק ב-$n!$.

פתרון. נשתמש שוב בעיקרון שניסחנו בשאלה הקודמת: בשביל לבדוק האם מכפלה $\prod_{i=1}^{N} b_i$ מתחלקת ב-$\prod_{i=1}^{M} a_i$, מספיר לכל q שהוא חזקה של ראשוני לוודא שכמות ה-b_i שמתחלקים ב-q היא לפחות כמו כמות ה-a_i שמחלקים ב-q.

נתחיל מ-2. במכפלה $\prod_{k=1}^{n-1}\left(2^n-2^k\right)$ כל גורם מתחלק ב-2, לכן היא מתחלקת לפחות ב-2^{n-1}. אבל לפי העיקרון שהסברנו בשאלה הקודמת, החזקה שבה 2 מופיע ב-$n!$ הוא $\left\lfloor\frac{n}{2}\right\rfloor+\left\lfloor\frac{n}{4}\right\rfloor+\left\lfloor\frac{n}{8}\right\rfloor+...$ וזה קטן יותר מאשר הסכום האינסופי $\frac{n}{2}+\frac{n}{4}+\frac{n}{8}+...$ וזה n.

לכן נשאר לבדוק חזקות של מספרים ראשוניים אי-זוגיים.

אם $q=p^k$ כאשר p ראשוני אי-זוגי, אז כמות הגורמים ב-$n!$ שמתחלקים ב-q היא $s=\left\lfloor\frac{n}{q}\right\rfloor$. נעריך כמות הגורמים ב-$\prod_{k=1}^{n-1}\left(2^n-2^k\right)$ המתחלקים ב-q. חזקות של 2 זו סדרה מחזורית מודולו q, כי $2^{\varphi(q)}=1\left(\mathrm{mod}\ q\right)$. כלומר גודל המחזור m קטן מ-q. לכן גם $s\cdot m\le s\cdot\left(q-1\right)\le n-1$, הרי $s\cdot q\le n$. לכן במכפלה $\prod_{k=1}^{n-1}\left(2^n-2^k\right)$, המספר k עובר לפחות על s מחזורים של חזקות 2, ולכן יש לפחות s גורמים שמתחלקים ב-q גם ב-$\prod_{k=1}^{n-1}\left(2^n-2^k\right)$.

4. מצאו את כל המספרים הטבעיים n שעבורם קיים a יחיד בתחום $0<a\le n!$ עבורו a^n+1 מתחלק ב-$n!$.

תשובה. n ראשוני.

פתרון. עבור $n=2$ המספר $a=1$ מתאים, והוא יחיד.

נניח כי $n>2$ וזוגי. אז נוכיח ש-a לא קיים. ברור כי $n!$ מתחלק ב-4, לכן גם $a^n+1=b^2+1$ מתחלק ב-4. אבל מספר מסוגם b^2+1 אף פעם לא מתחלק ב-4.

נשאר לדבר על המקרה של n אי-זוגי. במקרה זה $a=n!-1$ מתאים, והשאלה היא האם יש עוד דוגמה ל-a שמתאימה.

נניח כי הוא פריק: $n=p\cdot q$, כאשר p ראשוני הכי קטן שמחלק אותו. נוכיח שבמקרה זה $a=\frac{n!}{p}$ מתאים, כלומר a לא יחיד. אכן, $n!$ מתחלק ב-p^2 ולכן גם a^2 מתחלק ב-p ולכן,

$$a^n+1=\left(\frac{n!}{p}-1\right)^n+1=n\cdot\frac{n!}{p}-1+1=0\left(\mathrm{mod}\,n!\right)$$

נשאר המקרה ש-n ראשוני אי-זוגי.

במקרה זה נרשום $a^n+1=(a+1)\left(1-a+a^2-a^3+...+a^{n-1}\right)$. מספר זה מתחלק ב-$n!$.

ניקח מספר ראשוני $q<n$. יש שני מקרים $q\mid a+1$ או $q\nmid a+1$. נתחיל מהמקרה השני: אם $q\nmid a+1$, אז הסדר הכפלי של $-a$ מודולו q הוא n, לכן לפי המשפט הקטן של פרמה n מחלק את $q-1$, אזי n קטן או שווה מ-$q-1$ וקטן מ-q. אבל הנחנו הפוך.

לכן $q\mid a+1$, אבל צריך גם לבדוק באיזו חזקה q מחלק את a^n+1.
השאלה היא האם יתכן שגם $a+1$ וגם $1-a+a^2-a^3+...+a^{n-1}$ מתחלקים ב-q. אבל אז $a=-1\left(\mathrm{mod}\,q\right)$ ולכן גם

$$1-a+a^2-a^3+...+a^{n-1}=1+1+...+1=n\left(\mathrm{mod}\,q\right)$$

אבל n הוא מספר ראשוני שגדול מ-q. מכאן המסקנה כל הגורמים של המכפלה $1\cdot2\cdot...\cdot(n-1)$ שמחלקים את a^n+1 מחלקים גם את $a+1$.
לגבי n: מכיוון ש-n ראשוני, כשמשתמשים שוב במשפט פרמה הקטן, $a^n+1=a+1\left(\mathrm{mod}\,n\right)$, וכך רואים שאם a^n+1 מתחלק ב-n אז גם $a+1$ מתחלק ב-n.
ובכן, רואים כי $a+1$ מתחלק ב-$n!$. בהינתן $0<a\le n!$ זה מגדיר את a ביחידות.

5. הראו שהשאריות המתקבלות מהמספרים

$$\binom{2^n-1}{1},\binom{2^n-1}{3},\dots,\binom{2^n-1}{2^n-1}$$

כשמחלקים אותם ב-2^n, כולן שונות.

פתרון. נניח בשלילה שקיימים $x>y$ כך ש-

$$\binom{2^n-1}{x}-\binom{2^n-1}{y}\equiv 0\ mod\ 2^n$$

נוסיף ונחסר את הביטוי:

$$\binom{2^n-1}{x-1}+\binom{2^n-1}{x-2}+\dots+\binom{2^n-1}{y+1}$$

ונקבל ש-

$$(*)\qquad \binom{2^n}{x}-\binom{2^n}{x-1}+\binom{2^n}{x-2}+\dots-\binom{2^n}{y+1}\equiv 0\ mod\ 2^n$$

יש כאן הרבה חזקות שתיים ולכן נרצה להשתמש במשפט קומר, נזכיר את הניסוח שלו: כמות הפעמים ש-$\binom{n}{m}$ מתחלק ב-p שווה לכמות העברות בתרגיל חיבור $m+(n-m)$ בבסיס p.

במקרה שלנו המשפט אומר ש- $v_2\binom{2^n}{m}=n-k$ כאשר k זה $v_2(m)$ (או במילים אחרות כמות האפסים בסוף של m ברישום בינארי).

נבחר $y+1\le m\le x$ כך ש-$v_2(m)$ מקסימלי, כלומר $v_2\binom{2^n}{m}=z$ מינימלי, נוציא 2^z מחוץ לסוגריים ב-(*), ברור ש-$z<n$ ולכן מה שנשאר בסוגריים צריך להיות זוגי כלומר לא יתכן שהמינימום מתקבל רק פעם אחת. נניח שהמינים של $v_2\binom{2^n}{k}$ מתקבל ב-m,m' ולכן גם

$v_2(m)=v_2(m')$ אבל אז קיים $m<M<m'$ שעבורו

$v_2(M)>v_2(m)$ בסתירה לכך ש- $v_2(m)$ מקסימלי. הוכחנו שהמשוואה (*) לא הגיונית ולכן גם ההנחה שלנו לא הגיונית.

6. נתון פולינום ממעלה 2 לפחות, שכל מקדמיו הם מספרים שלמים חיוביים. הראו שקיים m חיובי שלם, עבורו $P(m!)$ אינו ראשוני.

פתרון. נבדוק מתי עבור p ראשוני מתקיים ש- $p|P((p-k)!)$. בשביל זה נבין את $(p-k)!$ מודולו p. אנחנו יודעים (לפי משפט וילסון) ש-$(p-1)! = -1 \; mod \; p$ ומה שחסר ל-$(p-k)!$ עד $(p-1)!$ זה את $(-1)^{k-1}(k-1)!$ ולכן עבור k זוגי אנחנו מקבלים

$$(p-k)!\,(k-1)! = 1 \; mod \; p$$

עכשיו נבין את $P((p-k)!)$:

$$(k-1)!^n \, P((p-k)!) =$$

$$= \sum_{i=0}^{n} a_i (k-1)^{n-i} \cdot [(p-k)!\,(k-1)!]^i = \sum_{i=0}^{n} a_i (k-1)!^{n-i} \; mod \; p$$

כאשר a_i הם המקדמים של הפולינום ו-n המעלה שלו.

נגדיר $Q(x) = a_n + a_{n-1}x + \ldots + a_0 x^n$, הוכחנו ש-$p|P((p-k)!)$ אם ורק אם $p|Q((k-1)!)$.

נשים לב ש- $Q((k-1)!)$ לא תלוי ב-p ולכן נוכל לבחור כל k שנרצה ואז לבחור ראשוני p שיחלק את $Q((k-1)!)$ ולכן הוא יחלק גם את

$P((p-k)!)$, אבל צריך לדאוג ש-p יהיה גדול מ-k.

בשביל זה נשים לב שעבור k גדול מספיק $Q((k-1)!)$ מתחלק ב-a_n, נסמן $Q((k-1)!) = a_n b_k$, בנוסף נבחין כי $b_k = 1 \; mod \frac{(k-1)!}{a_n}$ אבל $\frac{(k-1)!}{a_n}$ מתחלק בכל הראשוניים הקטנים מ-k (כי בחרנו k גדול) ולכן b_k מתחלק רק בראשוניים הגדולים מ-k (ברור ש-$b_k > 1$ כלומר לכל k (גדול) נבחר ראשוניים p המחלקים את b_k.

כעט נשאר לנו רק לבחור k כך ש-$P\big((p-k)!\big)$ יצא גדול מ-p וזה ינצח.

נבחר $k=(q-1)!$ עבור q ראשוני גדול, ברור שכל המספרים

$k+1, k+2, \dots, k+q-1$ פריקים ולכן $p \geq k+q$.

כעט נקבל: $P\big((p-k)!\big) > (p-k)! > k! + (p-k) > p$

אי השוויון הראשון נובע מכך שהמקדם המוביל של הפולינום חיובי ומכך שבחנו את k כך שההפרש בין p ל-k גדול כרצוננו.

הערה: השתמשנו רק בכך שהמקדם המוביל חיובי ולא הינו צריכים שכולם חיוביים. כמו כן השאלה נכונה גם עבור פולינומים לינאריים, הפתרון עובד עבור כל פולינום לינארי חוץ מ-$P(x) = x + a_0$ אבל המקרה הזה קל ונשאיר אותו בתור תרגיל לקורא.