<u>תרגילים על מקדמים בינומים מוכללים / אופיר גורודצקי</u>

הערות/הארות/שאלות/תיקונים ניתן לשלוח ל: bambaman1@gmail.com. מסמך זה לקוח מהבלוג oneand.wordpress.com.

<u>שאלה 1</u>

נסתכל על המקדמים הבינומים, המוגדרים באופן הבא לכל $n \geq k \geq 0$: $\binom{n}{k} := \frac{n!}{k!(n-k)!}$, כאשר $0! := 1$. הוכיחו שהמקדמים הם שלמים, בדרכים הבאות:

1. קומבינטוריקה - מצאו קבוצה שהמקדם $\binom{n}{k}$ סופר את איבריה.
2. ראשוניים - לכל ראשוני p הראו שמספר הפעמים ש־p מופיע במונה גדול/שווה ממספר הפעמים ש־p מופיע במכנה.
3. אינדוקציה - השתמשו בזהות פסקל, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (הוכיחו אותה אלגברית), כדי להוכיח את שלמות המקדמים באינדוקציה.

<u>הערה:</u> אפשר לנסח את שלמות המקדמים הבינומים באופן הבא: מכפלה של כל k מספרים טבעיים עוקבים מתחלקת במכפלה של k המספרים הטבעיים העוקבים הקטנים ביותר, שהיא $k!$.

המטרה בתרגיל זה היא להכליל את שתי ההוכחות האחרונות. למה הכוונה? עבור כל סדרה $\{a_n\}_{n\geq 1}$ של מספרים טבעיים, אפשר להגדיר פונקציית עצרת מתאימה: $0!_a := 1, n!_a := a_n a_{n-1} \cdots a_1$. בהינתן פונקציית עצרת, אפשר להגדיר מקדם בינומי שמתאים לסדרה: $\binom{n}{k}_a := \frac{n!_a}{k!_a(n-k)!_a}$. שאלה טבעית היא: מתי המקדמים הללו יוצאים שלמים?

<u>שאלה 2</u>

1. נסו לחקות את ההוכחה עם זהות פסקל. מפורשות: הראו שאם לכל $n \geq k \geq 0$ אפשר לרשום את a_n כקומבינציה לינארית עם מקדמים שלמים של a_k, a_{n-k}, אז $\binom{n}{k}_a$ תמיד שלם.
2. השתמשו באלגוריתם אוקלידס כדי לנסח תנאי זה בתור: $\forall i,j : \gcd(a_i, a_j) \mid a_{i+j}$.
3. הראו שאם מתקיים התנאי מסעיף 1 אז מתקיים גם $d \mid n \implies a_d \mid a_n$. הראו שתנאי זה לבדו לא מספיק לכך שהמקדמים הבינומים יהיו שלמים.
4. הראו שלכל c טבעי גדול מ־1, הסדרה $a_n = \binom{n+c-1}{c}$ נותנת מקדמים בינומים שלמים ($\binom{n}{k}_a \in \mathbb{Z}$) אבל היא לא מקיימת את התנאי של סעיף 2, ואפילו לא את של סעיף 3.

נרצה למצוא תנאי יותר פשוט מהתנאי $\gcd(a_i, a_j) \mid a_{i+j}$. נמצא כזה בשאלה הבאה.

<u>שאלה 3</u>

1. הראו שאם $\gcd(a_n, a_m) = a_{\gcd(n,m)}$ לכל n, m טבעיים, אז גם $\gcd(a_n, a_m) \mid a_{n+m}$ לכל n, m טבעיים, ובפרט המקדמים הבינומים $\binom{n}{k}_a$ יוצאים שלמים.
2. השתמשו באלגוריתם אוקלידס כדי לנסח תנאי זה בתור: $\forall n, m : \gcd(a_n, a_m) = \gcd(a_m, a_{n+m})$.

לסדרה שמקיימת את התנאי הנ"ל נקרא "סדרת GCD" (ידועה גם בתור "Strong Divisibiltiy Sequence"). הנה 2 תרגילים חמודים:

שאלה 4

1. תהי $\{a_n\}_{n\geq 1}$ סדרת GCD שכל איבריה שונים זה מזה. הוכיחו כי $d \mid n \implies a_d \mid a_n$.
2. תהי $\{a_n\}_{n\geq 1}$ סדרה של טבעיים המקיימת $\forall i \neq j : \gcd(a_i, a_j) = \gcd(i, j)$. הוכיחו ש־$\forall i : a_i = i$.

בתרגיל הבא נראה שהרבה מהתכונות של המקדמים הבינומים הרגילים בעצם אפשר להכליל:

שאלה 5

תהי $\{a_n\}_{n\geq 1}$ סדרת GCD.

1. הראו כי $\binom{n}{k}_a \frac{a_n}{a_{\gcd(n,k)}} \gcd(\binom{n}{k}_a, \binom{n-1}{k-1}_a) =$ ו־$\binom{n}{k}_a \frac{a_{n-k+1}}{a_{\gcd(n+1,k)}} \gcd(\binom{n}{k}_a, \binom{n}{k-1}_a) =$.
2. הסיקו כי $\binom{n}{k}_a \mid \frac{a_n}{a_{\gcd(n,k)}}$ ו־$\binom{n}{k}_a \mid \frac{a_{n-k+1}}{a_{\gcd(n+1,k)}}$. בפרט, $\binom{n}{k} \mid \frac{n}{\gcd(n,k)}$ ו־$\binom{n}{k} \mid \frac{n-k+1}{\gcd(n+1,k)}$. בפרט, מספר קטלן המוכלל $C_n = \frac{\binom{2n}{n}_a}{a_{n+1}}$ תמיד שלם.
3. נניח שבנוסף $\{a_n\}_{n\geq 1}$ היא סדרה עולה. הראו כי $\gcd(\binom{n}{i}_a, \binom{n}{j}_a) > 1$ תחת ההנחה הטבעית $0 < i, j < n$.
4. הכלילו את התוצאות, עם שינויים קלים, למקרה שהנתון היחיד על הסדרה $\{a_n\}_{n\geq 1}$ הוא שאיבריה טבעיים ושהמקדמים הבינומיים יוצאים שלמים.

כעת ניתן דוגמאות מעניינות לסדרות GCD. ודאו שהסדרות הבאות הן אכן סדרות GCD:

שאלה 6

1. $a_n = n$
2. $a_n = \frac{q^n-1}{q-1}$. המקדמים הבינומים המתקבלים נקראים מקדמים q־נומים. כאשר $q \to 1$, מקבלים את המקדמים הבינומים הרגילים.
3. $a_n = F_n$ (מספרי פיבונאצ'י ־ $F_1 = F_2 = 1, F_{n+1} = F_n + F_{n-1}$). ניתן להיעזר בזהות $F_{n+m} = F_nF_{m+1} + F_{n-1}F_m$ ($m = 1$ נותן את הרקורסיה הרגילה).
4. הראו ששלוש הדוגמאות האחרונות הן סדרות נסיגה מהצורה $a_{n+1} = Aa_n + Ba_{n-1}$, כאשר A, B שלמים זרים ותנאי ההתחלה הם $a_2 = A \cdot a_1$.
5. הראו שכל סדרת נסיגה כמו זו שבסעיף הקודם נותנת סדרת GCD. סדרה כזו נקראת "סדרת לוקאס" (תנאי ההתחלה חשובים מאוד).

הנה שתי דוגמאות יותר מוזרות לסדרות GCD:

שאלה 7

1. הראו שהסדרה $a_1 = 1, a_{n+1} = \lfloor e(a_n!) \rfloor$ היא סדרת GCD.
2. יהי f פולינום עם מקדמים שלמים. הראו שהסדרה $a_1 = f(0), a_{n+1} = f(a_n)$ היא סדרת GCD. שימו לב שחלק מהדוגמאות בשאלה 6 נכנסות תחת המקרה הזה.

בהינתן סדרה או סדרות GCD, אפשר לייצר סדרות GCD חדשות באופן הבא:

שאלה 8

1. כפל בסקלר (או חלוקה בסקלר, אם כל האיברים מתחלקים בו), העלאה בחזקה.
2. אם $\{a_n\}_{n\geq 1}, \{b_n\}_{n\geq 1}$ הן שתי סדרות GCD, אפשר להרכיב אותן ולקבל את $\{a_{b_n}\}_{n\geq 1}$ שהיא שוב סדרת GCD.
3. אם $\{a_n\}_{n\geq 1}, \{b_n\}_{n\geq 1}$ הן שתי סדרות GCD, אז המכפלה שלהן איבר־איבר $\{a_n \cdot b_n\}_{n\geq 1}$ היא לאו דווקא סדרת GCD. עם זאת, אם קבוצת הגורמים הראשונים של $\{a_n\}_{n\geq 1}$ זרה לקבוצת הגורמים הראשונים של $\{b\}_{n\geq 1}$, המכפלה כן יוצאת סדרת GCD.
4. אם $\{a_n\}_{n\geq 1}$ סדרת GCD, ו־p ראשוני, אז $\{p^{v_p(a_n)}\}_{n\geq 1}$ היא סדרת GCD, כאשר $v_p(n)$ סופר כמה פעמים n מתחלק ב־p.

<u>הערה</u>: סדרת GCD מעניינת שמתקבלת מהרכבה היא הסדרה $a_n = x^{p^n} - x \mod p$. זו לא סדרה של מספרים אלא של פולינומים ב־$\mathbb{F}_p[x]$. היא מתקבלת מהרכבה של $x^{n+1} - x \mod p$ (סדרת פולינומים) עם $p^n - 1$ (סדרת מספרים). שדה הפיצול של a_n הוא $\mathbb{F}_{p^n}$. a_n שווה למכפלת כל הפולינומים האי־פריקים ממעלה המחלקת את n, ובהמשך נבין איך לחשב מתוכה את מכפלת כל הפולינומים האי־פריקים ממעלה n בדיוק.

כעת נגדיר סוג נוסף של סדרות, שיהיה קשור מאוד לסדרות GCD.

<u>הגדרה</u>: סדרה $\{a_n\}_{n\geq 1}$ של מספרים טבעיים נקראת "סדרה מתפרקת" אם קיימת סדרה $\{b_n\}_{n\geq 1}$ של מספרים טבעיים כך ש־$a_n = \prod_{d|n} b_d$ לכל n. הסדרה $\{b_n\}_{n\geq 1}$ היא יחידה ונקראת "החלק הפרימיטיבי של $\{a_n\}_{n\geq 1}$".

שאלה 9

הראו שאם $\{a_n\}_{n\geq 1}$ סדרה מתפרקת אז המקדמים הבינומים שלה, $\binom{n}{k}_a$, תמיד שלמים.

כעת נוכיח שכל סדרת GCD היא סדרה מתפרקת:

שאלה 10

1. תהי $\{a_n\}_{n\geq 1}$ סדרה של טבעיים. לכל חזקת ראשוני p^k נסמן ב־c_{p^k} את מיקום האיבר הראשון בסדרה שמתחלק בו (בהנחה שקיים). הראו ש־$\{a_n\}_{n\geq 1}$ סדרת GCD אמ"מ הקבוצה $\{n \in \mathbb{N} \text{ such that } p^k \mid a_n\}$ מכילה את כל הכפולות של c_{p^k} ורק אותן.
2. הוכיחו בעזרת 1 או בכל דרך אחרת, שאם $\{a_n\}_{n\geq 1}$ סדרת GCD אז היא סדרה מתפרקת.
3. הוכיחו יותר מכך: בסימונים של סעיף 1, הראו שאם $\{a_n\}_{n\geq 1}$ סדרת GCD אז החלק הפרימיטיבי שלה הוא $b_n = \prod_{p^k : c_{p^k} = n} p$.
4. הראו שהחלק הפרימיטיבי של סדרת GCD מקיים $\gcd(b_n, b_m) = 1 \implies n \nmid m, m \nmid n$, ושתנאי זה מספיק (והכרחי) לכך ש־$\prod_{d|n} b_d$ תהיה סדרת GCD.

שאלה 11

1. מצאו את החלק הפרימיטיבי של כל הסדרות בשאלה 6. אתם יכולים להשתמש בפולינומים ציקלוטומים כדי להביע אותו.
2. הראו שהחלק הפרימיטיבי של הסדרה $x^{p^n} - x \mod p$ מההערה שווה למכפלת כל הפולינומים האי־פריקים ממעלה n בדיוק ב־$\mathbb{F}_p[x]$. בפרט, מצאו כמה פולינומים כאלו יש.

שאלה 12

1. הראו שכל סדרה מהצורה $g_n^{(N,c)} = \begin{cases} 1 & n \nmid N \\ c & n \mid N \end{cases}$ היא סדרת GCD ‏(N, c פרמטרים טבעיים). זו הדוגמא הפשוטה ביותר לסדרות GCD, ובסעיף הבא נראה שסדרות אלו מהוות מעין בסיס כפלי לסדרות GCD.
2. הראו שכל סדרת GCD ‏$\{a_n\}_{n\geq 1}$ עם חלק פרימיטיבי $\{b_n\}_{n\geq 1}$ אפשר להביע בתור $a_n = \prod_{N\geq 1} g_n^{(N,b_N)}$.
הראו שאין יצוגים מהצורה $a_n = \prod_{N\geq 1} g_n^{(N,c_N)}$ מלבד יצוג זה.

שאלה 13

נסתכל על סדרת ה־GCD הבאה: $a_n = a^n - 1, a > 2$.

1. נסמן ב־q את הגורם הראשוני הכי גדול של n. הראו שהחלק הפרימטיבי של $\{a_n\}_{n\geq 1}$ מקיים: $b_n \geq a^{q-2}$ (דורש מניפולציה על פולינומים ציקלוטומים).
2. הראו שאם $p \mid b_n$ ו־p ראשוני שמחלק איבר קודם בסדרה ($\exists d < n, p \mid b_d$), אז בהכרח p שווה לגורם הראשוני הכי גדול של n ומופיע בריבוי 1 בדיוק (דורש קצת תורת מספרים).
3. הסיקו שלכל $n > 2$ קיים ראשוני p כך ש־$p \mid a_n$ ו־p לא מחלק את האיברים הקודמים: $\forall d < n : p \nmid a_d$.
במילים אחרות, לכל $n > 2$ קיים ראשוני p כך שהסדר הכפלי של a מודולו p שווה בדיוק n. (מקרה פרטי של משפט Zsigmondy).
4. הוכיחו טענה דומה עבור סדרת פיבונאצ'י $a_n = F_n$. ספציפית, סעיפים 1 עד 3 הופכים לטענות הבאות:
   (א) $b_n \geq (\frac{2}{5})(\frac{3}{2})^{\phi(n)}$.
   (ב) עבור $n > 6$ מתקיים: אם $p \mid b_n$ ו־p ראשוני שמחלק גם איבר קודם בסדרה אז $p \mid n$ והוא מופיע בריבוי 1 בדיוק.
   (ג) כך ניתן להוכיח שאם $n > 12$ אז קיים ראשוני p כך ש־$p \mid F_n$ ו־p לא מחלק את $\{F_i\}_{i<n}$ (מקרה פרטי של משפט Carmichael).

שאלה 14 ־ שאלת מחקר פתוחה

מצאנו בינתיים 2 קריטריונים לכך שהמקדמים הבינומים של סדרה יהיו שלמים: בשאלה 9 ראינו שמספיק ש־$\{a_n\}_{n\geq 1}$ תהיה סדרה מתפרקת (מכיל את המקרה של סדרות GCD), ובשאלה 2 ראינו שמספיק ש־$\gcd(a_n, a_m) \mid a_{n+m}$ לכל n, m. האם יש עוד קריטריונים מעניינים?