משפט זיגמונדי ופולינומים ציקלוטומים

1. נסחו והוכיחו גרסה של משפט זיגמונדי עבור $a^n + b^n$.

פתרון: נבחר ראשוני p שמחלק את $a^{2n} - b^{2n}$ אבל לא מחלק חזקות קטנות יותר. אבל $a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n)$ ומהבחירה של p נקבל שהוא מחלק את $a^n + b^n$ אבל הוא לא מחלק את $a^k + b^k$ עבור k-ים שקטנים מ-n כי אז הוא היה מחלק את $a^{2k} - b^{2k}$ ובחרנו p שלא עושה את זה.

הוכחנו את זיגמונדי לחיבור ברוב המקרים, חוץ ממקרי המקצה שהתעלמנו מהם.

המקרה ש-$n = 1$ בזימונדי רגיל לא משפיע אצלינו.

המקרה ש-$n = 2$ ו-$a + b$ חזקת שתיים אצלינו הופך ל- $n = 1$ ו-$a + b$ חזקת שתיים, ואכן ברור שבמקרה הזה הטענה לא נכונה.

המקרה ש-$n = 6$ ו-$a = 2, b = 1$ הופך ל-$n = 3$ ו-$a = 2, b = 1$ ואכן $2^3 + 1^3 = 9$ לא מתחלק בדברים חדשים.

2. הוכיחו כי אף שלושה איברים בסדרה $a_n = 3^n - 2^n$ לא מהווים סדרה הנדסית.

פתרון: נניח בשלישה שקיימים $k > l > m$ כך ש-

$$a_l^2 = a_k \cdot a_m$$

לפי משפט זיגמונדי ל-a_l יש מחלק ראשוני שלא מחלקת את איברי הסדרה לפניו ולכן המשוואה $a_l^2 = a_k \cdot a_m$ לא יכולה להיות נכונה.

3. פתרו בשלמים חיוביים

$$(a+1)^m - 1 = a^n$$

פתרון: לפי משפט זיגמונדי $(a+1)^m - 1$ מתחלק בראשוני חדש ש-$(a+1) - 1 = a$ לא מתחלק בו ולכן $(a+1)^m - 1 \neq a^n$ אלה אם כן מתקיים אחד ממקרי הקצה של משפט זיגמונדי.

א. $m = 1$. לכן $a = a^n$ כלומר $a = 1$ או $n = 1$.

ב. $(a+1,1,m) = (2,1,6)$. במקרה הזה נקבל ש- $2^6 - 1 = 1^n$ וזה כמובן שטות.

ג. $m = 2$ ו- $a + 2$ זה חזקת 2. נסמן $a + 2 = 2^k$ונרשום את המשוואה מחדש:

$$(2^k - 1)^2 - 1 = (2^k - 2)^n$$

או באופן שקול $2^{k+1}(2^{k-1} - 1) = 2^n(2^{k-1} - 1)^n$ נצמצם את $2^{k-1} - 1$, הוא לא אפס כי אז $a = 2^k - 2 = 2(2^{k-1} - 1) = 0$, ונקבל ש-

$$2^{k+1} = 2^n(2^{k-1} - 1)^{n-1}$$

אבל $2^{k-1} - 1$ אי-זוגי או אפס ושתי האפשרויות לא הגיונית.

4. פתרו בשלמים חיוביים

$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

פתרון: נרשום את המשוואה עם פולינומים ציקלוטומים:

$$\Phi_7(x) = (y-1)\Phi_5(y)$$

נבחר ראשוני p המחלק את $\Phi_7(x)$ אז או ש- $p \equiv 1 \ mod \ 7$ או ש- $p = 7$.
אם $p = 7$ אז $(y-1)\Phi_5(y)$ מתחלק ב-7, כלומר או ש- $y \equiv 1 \ mod \ 7$ ואז

$$\Phi_5(y) = y^4 + y^3 + y^2 + y^1 + 1 \equiv 5 \; mod \; 7$$

וזה לא הגיוני כי זה אומר שיש ראשוני שמחלק את $\Phi_7(y)$ שהוא לא 7 ולא 1 מוד 7. לכן $7|\Phi_5(y)$ אבל 7 לא מחלק את 5 ולכן הסדר של y מודולו 7 זה 5 אבל אין מספרים כאלה.

הוכחנו שכל ראשוני שמחלק את אגף שמאל הוא 1 מוד 7 ולכן

$y - 1 \equiv 1 \; mod \; 7$ כלומר $y \equiv 2 \; mod \; 7$ ולכן

$$y^5 - 1 \equiv 2^5 - 1 = 31$$

ו-31 זה לא 1 מוד 7.

5. פתרו בשלמים חיוביים

$$(a+1)(a^2+a+1) \cdot \ldots \cdot (a^n + a^{n-1} + \ldots + 1) = a^m + a^{m-1} + \ldots + 1$$

פתרון: $n = m = 1$ זה פטרון טריוויאלי. חוץ מהפתרון הזה בברור צריך להתקיים ש-$m > n$. נרשום את המשוואה מחדש:

$$\frac{a^2-1}{a-1} \cdot \frac{a^3-1}{a-1} \cdot \ldots \cdot \frac{a^{n+1}-1}{a-1} = \frac{a^{m+1}-1}{a-1}$$

ואחרי שנכפיל במכנה נקבל:

$$(a^2-1) \cdot (a^3-1) \cdot \ldots \cdot (a^{n+1}-1) = (a^{m+1}-1)(a-1)^{n-1}$$

ממשפט זיגמונדי $a^{m+1} - 1$ מתחלק בראשוני שאף אחד מבין $a^k - 1$ לא מתחלק בהם (עבור $k < m$) ואז המשוואה שלנו לא הגיונית והפתרונות היחידים באים ממקרי קצה של זיגמונדי.

בגלל שאמרנו ש- $m > n$ אז $m + 1 \geq 3$ ולכן המקרה הרלוטני היחיד הוא ש- $m + 1 = 6$ ו- $a = 2$ ואז המשוואה תהפוך ל-

$$(2^2-1) \cdot (2^3-1) \cdot \ldots \cdot (2^{n+1}-1) = 63$$

וקל לראות שאין פתרון שעובד.

6. הוכיחו כי בסדרה ... 10001,100010001,1000100010001, אין מספרים ראשוניים.

פתרון: $100010001 \dots 0001$ זה כמובן שווה ל-

$1 + 10^4 + 10^8 + \ldots + 10^{4n}$ ואם $n + 1$ ראשוני אז זה פשוט להציב 10^4 בפולינום הציקלוטומי ה-$n + 1$. נשים לב שבעצם מספיק לנו לדבר רק על המקרה ש$n + 1$ ראשוני כי אם $m + 1 | n + 1$ אז גם

$$1 + 10^4 + 10^8 + \ldots + 10^{4m} | 1 + 10^4 + 10^8 + \ldots + 10^{4n}$$

כלומר אנחנו רוצים להוכיח ש-$\Phi_{n+1}(10^4)$ לא ראשוני.

טענה כללית: אם m, n זרים אז

$$\Phi_n(x^m) = \prod_{d|m} \Phi_{nd}(x)$$

הוכחה: נספור דרגות, הדרגה באגף שמאל היא $m \cdot \varphi(n)$ ובאגף ימין היא $\varphi(n) \cdot \sum \varphi(d) = \varphi(n) \cdot m$ ולכן הדרגות שוות ומספיק לבדוק שכל השורשים של אגף ימין הם גם השורשים של אגף שמאל.

השורשים של אגף ימין הם ω_{mn}^k כאשר k זר ל-n, וזה שורש פרימיטיבי מסדר $\frac{mn}{\gcd(k,m)}$ ולכן הוא שורש של $\Phi_{\frac{nm}{\gcd(k,m)}}$, כלומר כל שורש של אגף ימין הוא גם שורש של אגף שמאל והטענה הוכחה.

מהטענה נובע ש $\Phi_{n+1}(10^4) = \Phi_{n+1}(10) \cdot \Phi_{4n+4}(10)$ (זה נובע גם מנוסחאות יותר קלות שהיו במאמר אבל רצינו לטעון את הטענה הכללית כי היא שימושית ותעזור בעוד שאלות) כאשר $n + 1$ זר ל-4 כלומר המקרה היחיד שאנו צריכים לבדוק הוא $n + 1 = 2$ כלומר ש-10001 לא ראשוני אבל $10001 = 73 \cdot 137$ וניצחנו.

7. הוכיחו כי קיימים אינסוף שלמים חיוביים n כך שכל המחלקים הראשוניים של n^2+n+1 קטנים או שווים ל- $\sqrt{n}$.

פתרון: n^2+n+1 זה הפולינום הציקלוטומי השלישי ב-n. אנו מתעניינים בגורמים הראשוניים שלו ולכן נרצה להשתמש בנוסחה שהוכחנו בשאלה הקודמת, אם m,n זרים אז:

$$\Phi_n(x^m)=\prod_{d|m}\Phi_{nd}(x)$$

מכך נראה שאנו מתעניינים ב-n-ים מהצורה l^m כאשר m לא מתחלק ב-3, אכן במקרה זה נקבל

$$1+n+n^2=\prod_{d|m}\Phi_{3d}(l)$$

בנוסף נשים לב ש-

$$\Phi_{3d}(l)\le(l+1)^{\varphi(3d)}\le(l+1)^{\varphi(3m)}$$

כי $\Phi_{3d}(l)$ ממעלה $\varphi(3d)$ וכל אחד מהגורמים קטן או שווה ל-$l+1$.

כעט עבור l כלשהו נרצה למצוא m עבורו $(l+1)^{\varphi(3m)}\le l^{\frac{m}{2}}$ וזה יסיים.

נשים לב כי הביטוי $\frac{\varphi(m)}{m}$ יכול להיות קטן כרצוננו כלומר ניתן למצוא m עבורו $\varphi(3m)\ll 3m$. ועבור m כזה ו-l גדול מספיק נקבל ש-

$$(l+1)^{\varphi(3m)}<l^{\frac{m}{2}}$$

הערה: l גדול מספיק בשביל ש- $(l+1)^{\varphi(3m)}$ יהיה קטן מ- $l^{\frac{m}{2}}$ ולא $(l+1)^{\frac{m}{2}}$, זה לא באמת נחוץ אבל אפשר לבחור l גדול בשביל לא להתפסטן ממקרים קטנים.

8. נתון מספר ראשוני p הוכיחו כי קיימים אינסוף ראשוניים q שלכל n טבעי לא מחלקים את הביטוי $n^p - p$.

פתרון: נוכיח תחילה כי קיים q כמבוקש.

דבר ראשון נשים לב שאם קיים q כזה אז n^p לא יכול לקבל את כל הערכים מודולו q ולכן p צריך לחלק את הסדר של n מודולו q כלומר $p|q-1$.

כפי שהסברנו במאמר כל המחלקים הראשוניים של $\frac{p^p-1}{p-1}$ הם 1 מודולו p או p עצמו ולכן באופן כללי שיטה טובה להמציא ראשוניים שהם 1 מודולו p היא לבחור מחלק ראשוני של $\frac{p^p-1}{p-1}$.

כעת נניח ש-$q|\frac{p^p-1}{p-1}$ וש- $n^p \equiv p \ mod \ q$ ונראה מה התנאים על q.

נעלה את שני האגפים של $n^p \equiv p \ mod \ q$ בחזקת p ונקבל ש-

$$n^{p^2} \equiv p^p \equiv 1 \ mod \ q$$

קיבלנו שהסדר של n מודולו q מחלק את $\gcd(p^2, q-1)$ ולכן הוא $1, p$ או p^2 אם הוא 1 או p אז $p \equiv n^p \equiv 1 \ mod \ q$ ולכן $q|p-1$ אבל כבר אמרנו ש-$p|q-1$ וזו סתירה.

לכן בכדי להוכיח קיום של q כמבוקש מספיק להוכיח של- $\frac{p^p-1}{p-1}$ יש מחלק ראשוני q כך ש- $p^2 \nmid q-1$.

נשים לב ש- $\frac{p^p-1}{p-1} = p^{p-1}+\ldots+p^2+p+1 \equiv p+1 \ mod \ p^2$

ולכן לא יתכן שכל המחלקים של $\frac{p^p-1}{p-1}$ הם 1 מודולו p^2.

כעט נוכיח כי קיימים אינסוף ראשוניים המקיימים את התנאי.

במקום להסתכל על הביטוי $\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1}$ כמו קודם הביטוי הזה שווה ל-1 מודולו p, ואפשר לבחור a כך ש- $\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1} \not\equiv 1 \ mod \ p^2$ כי a^p יכול

להיות כל דבר מודולו p ולכן יהיה ראשוני q שמחלק את $\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1}$ שהוא לא 1 מודולו p^2.

כעת נניח ש-$q|\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1}$, שהוא לא 1 מודולו p^2 וש- $n^p \equiv p \ mod \ q$ ונראה מה התנאים על q.

הפעם נכפיל את שני האגפים ב-a^p ואז נעלה בחזקת p ונקבל ש-

$$(an)^{p^2} \equiv (pa^p)^p \equiv 1 \ mod \ q$$

קיבלנו שהסדר של an מודולו q מחלק את $\gcd(p^2, q-1)$ ולכן הוא 1 או p. בשני המקרים נקבל ש- $pa^p \equiv 1 \ mod \ q$ אבל אז

$$\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1} = (pa^p)^{p-1}+\ldots+1 \equiv p \ mod \ q$$

כלומר $q|p$ שזה לא הגיוני.

נשים לב שאנו יכולים לבחור את a כך שיתחלק בכל ה-q-ים שמצאנו עד כה ולכן הראשוני שנמצא עבור ה-a הזה יהיה זר לכל הראשוניים שמצאנו עד עכשיו (כי $\frac{(p\cdot a^p)^p-1}{p\cdot a^p-1}$ זר ל-a) ולכן זה יהיה ראשוני שלא מצאנו עד כה וכך נמצא אינסוף ראשוניים.

9. נתון פולינום מתוקן עם מקדמים שלמים שהשורשים המרוכבים שלו נמצאים במעגל היחידה. הוכיחו כי כל השורשים של הפולינום הם שורשי יחידה.

פתרון: נרשום את הפולינום שלנו בצורת מכפלה של גורמים לינאריים:

$$P(x) = (x-a_1)\cdot \ldots \cdot (x-a_d)$$

ונגדיר סדרה של פולינומים

$$P_n(x) = (x-a_1^n)\cdot \ldots \cdot (x-a_d^n)$$

נתבונן במקדם של x^m ב-$P_n(x)$. מצד אחד הוא חסום על ידי $\binom{d}{m}$ כי כל אחד מה-a-ים הוא לכל היותר 1. מצד שני הוא פולינום סימטרי אלמנטרי בשורשים של $P_n(x)$ כלומר פולינום סימטרי ב-$a_1, \ldots, a_d$ אבל כל

פולינום סימטרי ניתן לרשום כפולינום עם מקדמים שלמים בפולינומים סימטריים אלמנטריים. נשים לב שפולינומים סימטרי אלמנטרי ב-$a_1, \dots, a_d$ הוא מספר שלם כי זה מקדם של חזקת x כלשהי ב-$P(x)$ שהוא לפי הנתון פולינום במקדמים שלמים.

סך הכל קיבלנו שהמקדם של x^m ב-$P_n(x)$ הוא מספר שלם כי הוא פולינום עם מקדמים שלמים במספרים שלמים. אבל אמרנו שהוא גם חסום ולכן לכל ה-n-יש כמות סופית של אפשרויות למקדמים ולכן בכל סדרת ה-$P_n(x)$ יש כמות סופית של פולינומים.

נצטמצם ל-n-ים מהצורה $n = 2^k$, גם בסדרה הזו יש כמות סופית של פולינומים כלומר יש שתי חזקות שונות שנותנות את אותו פולינום:

$$P_{2^k}(x) = P_{2^{k+l}}(x)$$

כלומר המספרים $a_1^{2^{k+l}}, \dots, a_d^{2^{k+l}}$ הם פרמוטציה של $a_1^{2^k}, \dots, a_d^{2^k}$.
נפעיל את הפרמוטציה הזו r פעמים עד שנקבל את פרמוטציית הזהות ואז נקבל ש- $a_i^{2^k} = a_i^{2^{k\_lr}}$ כלומר a_i הוא 0 או שורש יחדה.