פולינומים ציקלוטומים ומשפט זיגמונדי

אנחנו נדבר קצת על פולינומים ציקלוטומים, נגדיר אותם ונוכיח מספר תכונות שלהן ולאחר מכאן, חמושים בידע הדרוש, נוכיח את משפט זיגמונדי.

הפולינום המגניב הידוע הוא x^n-1 אבל לנו יהיה נוח לדבר על הגרסה ההומוגנית שלו a^n-b^n, הפולינום הזה מתאפס כאשר היחס הוא שורש יחידה מסדר n עד כדי זה שצריך להיזהר במה סדר אומר, פה הכוונה היא מספרים שבחזקת n הם אחד, אך טבעי והגיוני לדבר על השורשי יחידה שהם מסדר **בדיוק** n, לכן נגדיר:

$\Phi_n(x)$ זה הפולינום המתוקן שמתאפס פעם אחת על כל שורש יחידה מסדר בדיוק n, ו-$\Phi_n(a,b)$ זו ההומוגניזציה שלו, הם נקראים הפולינומים הציקלוטומים.

מספר דוגמאות לפולינומים ציקלוטומים:

$$\Phi_p(a,b)=\frac{a^p-b^p}{a-b}=a^{p-1}+a^{p-2}b+\ldots+ab^{p-2}+b^{p-1}$$

$$\Phi_{p^k}(a,b)=\frac{a^{p^k}-b^{p^k}}{a^{p^{k-1}}-b^{p^{k-1}}}=\Phi_p(a^{p^{k-1}},b^{p^{k-1}})$$

$$\Phi_6(a,b)=(a+\omega b)(a+\omega^2 b)=a^2-ab+b^2$$

נרשום מספר תכונות של פולינומים ציקלוטומים, ההוכחות ישירות מההגדרות ולכן נשאיר אותן לקרוא.

$$\deg(\Phi_n)=\phi(n)$$

$$a^n-b^n=\prod_{d|n}\Phi_d(a,b)$$

$$\Phi_n(a,b)=\prod_{d|n}(a^d-b^d)^{\mu(n/d)}$$

כאשר μ היא פונקציית מוביוס, שעבור מספרים שמתחלקים בריבוע מחזירה אפס ועובר מספרים שלא מתחלקים בריבוע מחזירה מינוס אחד בחזקת כמות המחלקים הראשוניים השונים של המספר.

נשים לב שבכל הדוגמאות שלנו הפולינומים הציקלוטומים יצאו עם מקדמים שלמים וזה אכן קורה תמיד ובשביל להוכיח זאת נצטרך להזכיר את הלמה של גאוס.

הלמה של גאוס אומרת שמכפלה של שני פולינומים פרימיטיביים היא פרימיטיבית. כאשר פולינומים פרימיטיביים הם פולינומים במקדמים שלמים ושאין ראשוני שמחלק את כל המקדמים שלהם.

ההוכחה ללמה של גאוס: נניח שמכפלה של שני פולינומים פרימיטיביים f,g היא לא פולינום פרימיטיבי, כלומר יש ראשוני p שמחלק את כל המקדמים של fg. נסתכל על המונום הכי קטן $a_i x^i$ ב-f שהמקדם שלו לא מתחלק ב-p ועל המונום הכי קטן $b_j x^j$ ב-g שהמקדם שלו לא מתחלק ב-p. אז המקדם של x^{i+j} ב-fg הוא

$$a_i b_j + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots$$

אבל מהנחת המינימליות כל האיברים בסכום חוץ מ-$a_i b_j$ מתחלקים ב-p אבל $a_i b_j$ לא מתחלק ב-p בסתירה לכך שכל המקדמים של fg מתחלקים ב-p.

מסכנה מגניבה מהלמה של גאוס היא שאם פולינום פרימיטיבי מתפרק לפולינומים במקדמים רציונליים אז הוא בעצם מתפרק לפולינומים במקדמים שלמים כי אם $f = g \cdot h$, כאשר f פרימיטיבי ו-g,h עם מקדמים רציונליים נוכל להכפיל את g במספר רציונלי כך שהוא יהפוך לפולינום פרימיטיבי g' (למה אפשר?) וכך גם את h נהפוך לפולינום פרימיטיבי h'. עכשיו קיבלנו ש-$f = g' \cdot h' = g \cdot h \cdot \frac{a}{b}$ כאשר a,b מספרים שלמים ולכן $b \cdot f = a \cdot g \cdot h$ אבל המחלק המשותף של כל המקדמים באגף ימין הוא a והמחלק המשותף של כל המקדמים באגף שמאל הוא b ולכן $a = b$ ולכן $f = g'h'$ כלומר f מתפרק מעל השלמים.

עכשיו גם ברור שהפולינומים הציקלוטומים הם פולינומים במקדמים שלמים כי מהנוסחה

$$\Phi_n(a,b) = \prod_{d|n} (a^d - b^d)^{\mu(n/d)}$$

ברור שהפולינום הציקלוטומי הינו במקדמים רציונלים, שהרי הוא מכפלה של פולינומים במקדמים שלמים ואחד חלקי פולינומים במקדמים שלמים ומהמסכנה מהלמה של גאוס נקבל שהוא בעצם במקדמים שלמים.

יכלנו גם להגיד ישירות ש- $a^n - b^n$ פרימיטיבי ולכן מתפרק לפולינומים במקדמים שלמים ולכן הפולינומים הציקלוטומים עם מקדמים שלמים.

עוד שתי נוסחאות שנצטרך:

אם $p \mid n$ אז:

$$\Phi_{p^k n}(a,b) = \Phi_n(a^{p^k}, b^{p^k})$$

ואם $p \nmid n$ אז:

$$\Phi_{p^k n}(a,b) = \frac{\Phi_n(a^{p^k}, b^{p^k})}{\Phi_n(a^{p^{k-1}}, b^{p^{k-1}})}$$

שוב נשאיר את ההוכחות לקרוא.

נוכיח שהפולינומים הציקלוטומים אי-פריקים (לא נשתמש בזה בהוכחה של זיגמונדי).

המקרה הקל הוא עבור $\Phi_p(x)$ נשים לב ש-

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1}$$

ומקריטריון אייזנשטיין זה אי-פריק.

כעט נוכיח את המקרה הכללי, נבחר שורש יחידה פרימיטיבי מסדר n, נסמן אותו ζ ונסתכל על הפולינום המינימלי שלו-פולינום עם מקדמים שלמים ודרגה מינימלית ש-ζ מאפס אותו, נסמן את הפולינום המינימלי f. נטען שאם p ראשוני הזר ל-n אז ζ^p מאפס את f.

נניח בשלילה ש-ζ^p לא מאפס את f. ζ הוא שורש של Φ_n ולכן $\Phi_n = f \cdot g$ אבל ζ^p גם הוא שורש של Φ_n ואם הוא לא שורש של f אז הוא שורש של g. נסמן את הפולינום המינימלי של ζ^p ב-h ואז נוכל לרשום ש- $g = h \cdot r$.

עכשיו קיבלנו ש- $\Phi_n(x^p) = f(x^p) \cdot h(x^p) \cdot r(x^p)$ אבל ζ הוא שורש של $h(x^p)$ ולכן f מחלק אותו ונרשום $h(x^p) = f(x) \cdot s(x)$ ועכשיו נקבל:

$$\Phi_n(x^p) = f(x^p) \cdot f(x) \cdot s(x) \cdot r(x^p)$$

נסתכל מודולו p

$$\Phi_n(x)^p = f(x)^{p+1} \cdot s(x) \cdot r(x)^p \; mod \; p$$

נבחר גורם אי-פריק של $f(x)$ מעל Z_p, הגורם האי פריק הזה חייב לחלק את $\Phi_n(x)$ ואף יותר מזה הוא חייב לחלק אותו פעמיים (כי באגף שמאל הוא בחזקה p ובאגף ימין הוא בחזקת $p + 1$).

טענה: השורשים של הפולינום הציקלוטומי מריבוי 1.

זה נובע מטענה כללית שאם פולינום זר לנגזרת שלו אז השורשים שלו מריבוי 1, שזו טענה ברור כי אם היה שורש מריבוי 2 אז הוא היה נשאר בנגזרת.

מהטענה קיבלנו סטירה כי מצאנו גורם שמחלק את הפולינום הציקלוטומי פעמיים ואמרנו שזה לא קורה.

סך הכל הוכחנו שאם n זר ל-p ו-ζ שורש של Φ_n ו-$f(x)$ זה הפולינום המינימלי של ζ אז גם ζ^p הוא שורש של f. נבחר את ζ להיות $\omega_n = e^{\frac{2\pi i}{n}}$ אז הפולינום המינימלי של ω_n מתאפס ב-ω_n^p לכל p שזר ל-n ואז אפשר לבחור ראשוני אחר q שזר ל-n ואז גם ω_n^{pq} מאפס את הפולינום המינימלי ואז באינדוקציה נקבל ש-ω_n^m מאפס את הפולינום המינימלי לכל m שזר ל-n אבל אלו כל השורשים של Φ_n ולכן הוא בעצם הפולינום המינימלי של ω_n ולכן הוא אי-פריק.

עכשיו נדבר קצת על מחלקים ראשוניים של הפולינומים הציקלוטומים, אם p ראשוני המחלק את $\Phi_n(a,b)$ אז בפרט הוא מחלק את a^n-b^n ולכן אם a,b זרים אז $p|n$ $ord_p\left(\frac{a}{b}\right)$.

נשים לב שאם הסדר הוא בדיוק n אז בגלל שהסדר מחלק את $p-1$ נקבל ש-p זה 1 מודולו n. בנוסף נשים לב שאם $p|\Phi_n(a,b)$ ו-$p|n$ אז $p|\Phi_{\frac{n}{p}}(a,b)$ ולכן אפשר להניח ש-$p|\Phi_n(a,b)$ אבל p לא מחלק את n ואז טענן שהסדר של $\frac{a}{b}$ צריך להיות בדיוק n. אכן נניח כי הסדר הוא $k<n$ אז p מחלק את a^k-b^k ולכן מחלק פולינום ציקלוטומי נוסף ולכן p מחלק את x^n-1 פעמיים אבל הנגזרת של x^n-1 מודולו p לא מתחלק ב-p (בהנחה ש-n ו-p זרים) וזו סתירה.

שני הדברים האחרונים שנשאר לפני שנתחיל להוכיח את משפט זיגמונדי, זה התכונה הבסיסית הבאה:

$$(a^n-b^n,a^m-b^m)=a^{(n,m)}-b^{(n,m)}$$

בהנחה ש- a,b זרים, למי שלא מכיר זה תרגיל נחמד.

וחסמים טריוואלים על הגודל של פולינום ציקלוטומי עבור מספרים חיוביים:

$$\left|a-b\right|^{\phi(n)}\le\left|\Phi_n(a,b)\right|\le\left|a+b\right|^{\phi(n)}$$

אלה ברורים מהפירוק למכפלה לגורמים לינארים, והעובדה שכל השורשים מנורמה 1.

המשפט!

משפט זיגמוני מדבר על הביטוי $a^n - b^n$ ואומר שהוא מתחלק בהרבה ראשוניים שונים. כלומר שכאשר מגדילים את n כל פעם יש ראשוני חדש שמחלק את הביטוי, כלומר ראשוני שלא מחלק את $a^k - b^k$ עבור $k < n$.

נעבור להוכחה.

נניח p ראשוני טוב, כלומר מחלק את $a^n - b^n$ אבל לא את $a^k - b^k$ עבור $k|n$ (לפי התרגיל זה אותו דבר כמו $k < n$).

לפי הנוסחא הבסיסית על פולינומים ציקלוטומים, נקבל ש-P מחלק גם את $\Phi_n(a,b)$.

נרצה להבין עד כמה הכיוון ההפוך נכון, נניח $p|\Phi_n(a,b)$ אך גם $p|a^k - b^k$ עבור $k|n$, מכאן והנוסחה הבסיסית של הפולינומים הציקלוטומים (פעמיים) נקבל:

$$p \mid \frac{a^n - b^n}{a^k - b^k}$$

אבל מהרמת אקספוננט נקבל שזה שקול לכך ש- $p|\frac{n}{k}|n$, לכן נרשום $n = \mathrm{p}^\alpha q$, לפי הנוסחאות שלנו:

$$p \mid \Phi_n(a,b) \mid \Phi_q(a^{p^\alpha}, b^{p^\alpha})$$

לכן לפי פרמה $p|\Phi_q(a,\mathrm{b})$, בנוסף $p \equiv 1\ (\mathrm{q})$, ולכן הוא הראשוני הכי גדול שמחלק את n, (בפרט יש לכל היותר ראשוני אחד כזה).

עכשיו נרצה לחסום את כמה פעמים שהראשוני הזה מחלק את $\Phi_n(a,\mathrm{b})$.

לפי מה שראינו, אם $p|a^d - b^d$ אז $q|d$. לכן אם נסתכל על הנוסחה שלנו:

$$\Phi_n(a,b) = \prod_{d|n} (a^d - b^d)^{\mu(n/d)}$$

יש רק שני מוכפלים המתחלקים ב-p, כלומר:

$$v_p(\Phi_n(a,b)) = v_p(a^n - b^n) - v_p(a^{\frac{n}{p}} - b^{\frac{n}{p}})$$

אם $p \neq 2$ מהרמת אקספוננט נקבל ש:

$$v_p(\Phi_n(a,b)) = 1$$

שזה מעולה! אם $p = 2$ נקבל ש-$n = 2^\alpha$, אז:

$$\Phi_n(a,b) = a^{\frac{n}{2}} + b^{\frac{n}{2}}$$

אם $n > 2$ זה סכום שני ריבועים, ולכן לא יכול להתחלק ב-4, אם אכן $n = 2$ ו-$a + b$ מתחלק בראשוני שאינו 2 אז מצאנו ראשוני טוב וסיימנו, לכן המקרה הבעייתי היחיד הוא כרגע הוא כאשר $n = 2, a + b = 2^k$, וזה מקרה שהוא פשוט אינו נכון.

לכן נוכל להניח ש-$v_p\big(\Phi_n(a,b)\big) = 1$, וזה נראה מאוד מבטיח כי זה מאוד קטן.

כל מה שנשאר לנו כדי לסיים הוא לחסום את $\Phi_n(a,b)$ מלמטה.

אם אין לו את המחלק הראשוני המוזר, מספיק להראות שהוא גדול מאחד (בערך מוחלט) לפי האי-שיוויון שהיה לנו (שימו לב שיש בו שיוויון רק כאשר $(n = 1, a - b = 1$

אם יש ראשוני כזה p אז $n = p^\alpha q$ ויש להראות ש- $\Phi_n(a,b) > p$.

אם $\alpha > 1$ אז נקבל:

$$\Phi_n(a,b) = \Phi_{\frac{n}{p}}(a^p, b^p) \geq a^p - b^p \geq (b+1)^p - b^p > p$$

לכן נשאר עם המקרה $n = pq$.

אם $a - b > 1$ נקבל:

$$\Phi_n(a,b) \geq (a-b)^{\phi(n)} \geq 2^{p-1} \geq p$$

ושיוויון רק כאשר $n=1$ וסיימנו.

לכן נשאר המקרה $a=b+1$, אז:

$$\Phi_n(a,b)=\frac{\Phi_q(a^p,b^p)}{\Phi_q(a,b)}\geq\frac{(a^p-b^p)^{\phi(q)}}{(a+b)^{\phi(q)}}$$

$$\frac{a^p-b^p}{a+b}=\frac{(b+1)^p-b^p}{2b+1}\geq\frac{(2^p-1)b}{2b+1}\geq\frac{2^p-1}{3}\geq 1$$

עבור $p\geq 5$ זה כבר גדול מ p, אם $p=2$ אז חייב להיות ש-$n=2$ ואז זה טריוואלי, ולבסוף אם $p=3$ אז $n=3,6$ במקרה הראשון נקבל שהסדרה היא:

$$1,a+b,a^2+ab+b^2$$

וכל מחלק של האיבר השלישי יהיה ראשוני טוב.

במקרה האחרון נקבל ש-

$$\Phi_6(a,b)=a^2-ab+b^2=b^2+b+1$$

ולכן המקרה היחיד הבעייתי הוא $b=1$ ואז $a=2$, ומעבר לזה, סיימנו!

לסיכום, לכל איבר בסדרה a^n-b^n כאשר $a>b>0$ זרים, יש ראשוני חדש המחלק אותו, חוץ משלושת המקרים הבאים:

- $n=1,a-b=1$
- $n=2,a+b=2^k$
- $n=6,a=2,b=1$

וזה משפט זיגמונדי!!! כל הכבוד!