

פתרון תרגיל בית 9 בשדות ותורת גלואה 88-311 סמסטר א' תש"ף

שאלה 1 (חימום). יהי $m|n$. הוכיחו $x^m - 1 | x^n - 1$.

פתרון. נניח $n = dm$. ידוע לנו כי $x - 1 | x^d - 1$ שהרי

$$x^d - 1 = (x - 1)(x^{d-1} + x^{d-2} + \dots + x + 1)$$

נציב $x \mapsto x^m$ ונקבל את הדרוש:

$$x^n - 1 = x^{dm} - 1 = (x^m - 1)(x^{(d-1)m} + x^{(d-2)m} + \dots + x^m + 1)$$

שאלה 2. יהי $n > 1$ אי זוגי. הוכיחו שהפולינום הציקלוטומי מקיים $\Phi_{2n}(x) = \Phi_n(-x)$.

פתרון. יהי $-\rho_n$ שורש של $\Phi_n(-x)$, אז $(-\rho_n)^2 = (-1)^2 = 1$, ולכן הוא גם שורש של $\Phi_{2n}(x)$. בכיוון השני, יהי ρ_{2n} שורש של $\Phi_{2n}(x)$. אז $\rho_{2n} = e^{2\pi i k / 2n}$ עבור k זר ל- $2n$. לכן $(-\rho_{2n})^k = -e^{\pi i k} = 1$, ולכן ρ_{2n} הוא שורש של $\Phi_n(-x)$. כלומר ל- $\Phi_{2n}(x)$, $\Phi_n(-x)$ יש את אותם שורשים, שניהם אי פריקים מאותה מעלה (הרי $\varphi(2n) = \varphi(2)\varphi(n)$ כי n זר ל-2) ולכן הם שווים. במשוואה אחת ההוכחה היא

$$\Phi_{2n}(x) = \prod_{(k,2n)=1} (x - \rho_{2n}^k) = \prod_{(k,n)=1} (x + \rho_n^k) = (-1)^{\varphi(n)} \prod_{(k,n)=1} (-x - \rho_n^k) = (-1)^{\varphi(n)} \Phi_n(-x)$$

ורק צריך לוודא כי $\varphi(n)$ הוא זוגי. אבל זה נכון כי n אי זוגי, כי יש לו מחלק ראשוני אי זוגי p כלשהו וברור ש- $\varphi(p^k) = p^{k-1}(p-1)$ הוא זוגי.

שאלה 3. כתבו נוסחה קצרה לפולינום הציקלוטומי $\Phi_{2^n}(x)$.

פתרון. לפי נוסחת הנסיגה בכיתה נקבל

$$\Phi_{2^n}(x) = \frac{x^{2^n} - 1}{n-1} = \frac{x^{2^n} - 1}{x^{2^{n-1}} - 1} = x^{2^{n-1}} + 1$$

$$\prod_{k=0} \Phi_{2^k}(x)$$

שאלה 4. מצאו את כל הפולינומים הציקלוטומיים $\Phi_n(x)$ כך ש- $\deg \Phi_n(x) = 4$.

פתרון. נזכר ש- $\deg \Phi_n(x) = \varphi(n)$. אם ראשוני $p \geq 7$ מחלק את n , אז $n = p^k n'$ עבור $k \geq 1$ עם n' שזר ל- p ולכן

$$\varphi(n) = \varphi(p^k n') = \varphi(p^k) \varphi(n') = (p^k - p^{k-1}) \varphi(n') > 4$$

כי $4 < p^{k-1}(p-1)$ ו- $\varphi(n')$ טבעי. לכן מחפשים מספרים מהצורה $n = 2^a 3^b 5^c$ עם הדרישות $b, c < 2$ ו- $a < 4$. בדיקה זריזה אחר הפתרונות למשוואה $\varphi(n) = 4$ תגלה שהם רק 5, 8, 10, 12. הפולינומים המבוקשים הם:

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = x^4 + 1$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{12}(x) = x^4 - x^2 + 1$$

שאלה 5 (קצת קשה). יהי $n > 1$ טבעי, ונתבונן בפולינום הציקלוטומי $\Phi_n(x)$.

א. יהי $a \in \mathbb{Z}$ ויהי p ראשוני המחלק את $\Phi_n(a)$. הוכיחו כי $p|n$ או $p \equiv 1 \pmod{n}$.
 רמז: הפולינום $x^n - 1$ הוא ספרבילי מודולו p אם $p \nmid n$. מה הוא הסדר של $a \in U_p$?

ב. הסיקו מהסעיף הקודם שישנם אינסוף מספרים ראשוניים כך ש- $p \equiv 1 \pmod{n}$.

פתרון.

א. נניח כי $p \nmid n$. אז לנגזרת $(x^n - 1)' = nx^{n-1}$ אין גורם משותף עם $x^n - 1$ מודולו p . לכן $x^n - 1$ הוא פולינום ספרבילי ב- $\mathbb{F}_p[x]$. נזכר בנוסחה $x^n - 1 = \prod_{d|n} \Phi_d(x)$. ונציב בה a :

$$a^n - 1 = \prod_{d|n} \Phi_d(a) = \Phi_n(a) \cdot \prod_{d|n, d < n} \Phi_d(a) \equiv 0 \pmod{p}$$

כאשר השיוויון האחרון נכון לפי הנתון $p|\Phi_n(a)$. אבל כל השורשים של $x^n - 1$ שונים, ולכן $\Phi_n(a) = 0$ בשדה \mathbb{F}_p . כלומר $p \nmid \Phi_d(a)$ לכל $d|n$ כאשר $d < n$. כלומר a הוא שורש יחידה פרימיטיבי מסדר n ב- \mathbb{F}_p . לכן $n|p-1$, כדורש.

ב. מספיק להראות ש- $\Phi_n(a)$ הוא ראשוני אינסוף פעמים כאשר a שלם (לאו דווקא כל פעם). נניח בשלילה שזה לא נכון, ויש רק מספר סופי k של ראשוניים p_1, \dots, p_k . אז לכל $m \in \mathbb{Z}$ מתקיים כי

$$\gcd(\Phi_n(mp_1 \dots p_k), p_1 \dots p_k) = 1$$

כי $\Phi_n(mp_1 \dots p_k)$ מחלק את $(mp_1 \dots p_k)^n - 1$. לכן למספר $\Phi_n(mp_1 \dots p_k)$ יש גורם ראשוני שאינו בקבוצה $\{p_1, \dots, p_k\}$, כל עוד $|\Phi_n(mp_1 \dots p_k)| > 1$. אבל $\Phi_n(mp_1 \dots p_k)$ הוא פולינום לא קבוע במשתנה m , ולכן אפשר לבחור $m \in \mathbb{Z}$ כך שמתקיים תנאי זה. זו סתירה למקסימליות של k .
 בקורס תורת המספרים האלגבריים אולי תראו הכללה (או יותר) של סעיף זה לפיו יש אינסוף ראשוניים מן הצורה $b + kn$ כאשר b זר ל- n . בתרגיל הזה פתרנו את המקרה $b = 1$.

שאלה 6 (רשות). יהי n טבעי. בשאלה זו נראה הכללה לשאלות 2 ו-3 שתאפשר לחשב את הפולינום הציקלוטומי $\Phi_n(x)$ קצת יותר מהר.

א. יהי p ראשוני. הוכיחו שאם p זר ל- n , אז $\Phi_n(x^p) = \Phi_n(x) \Phi_{pn}(x)$. אחרת, אם $p|n$, הוכיחו כי $\Phi_{pn}(x) = \Phi_n(x^p)$.

ב. יהי r הרדיקל של n (כלומר מכפלת הראשוניים שמחלקים את n). הוכיחו שהפולינום הציקלוטומי מקיים $\Phi_n(x) = \Phi_r(x^{n/r})$.

שאלה 7 (רשות). כתבו תוכנה שבהינתן n טבעי מחשבת את הפולינום הציקלוטומי Φ_n . הדפיסו את $\Phi_1, \dots, \Phi_{100}$ ושערו השערה לגבי מקדמים של פולינומים ציקלוטומיים. חשבו את Φ_n עבור $n > 100$ ובדקו את השערתכם.

בהצלחה!