

פתרון תרגיל בית 9 בשדות ותורת גלואה 88-311 סמסטר א' תשע"ט

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

פתרון. נניח $n = dm$. ידוע לנו כי $x^d - 1 | x^{dm} - 1$ 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. מצאו באילו שדות סופיים \mathbb{F}_q יש איבר x המקיים $x^4 = -1$. רמז: זו שאלה על החבורה הכפלית.

פתרון. נשים לב שאפס אינו מקיים את המשוואה, ולכן אנו מחפשים את הפתרון בחבורה הכפלית \mathbb{F}_q^* .

אם $x^4 = -1$ אז $x^8 = (-1)^2 = 1$, ולכן מתקיים $8 | o(x)$. מנגד, אם המאפיין של השדה איננו 2, אז $x^4 \neq 1$ כי $1 \neq -1$ לכן $4 \nmid o(x)$. במקרה זה בהכרח $o(x) = 8$. אם כן, נדרוש שב- \mathbb{F}_q^* יהיה איבר x מסדר 8, ואז הוא יקיים את המשוואה. מכיוון שסדר איבר מחלק את סדר החבורה (ממשפט לגראנז'), נסיק שהסדר של \mathbb{F}_q^* מתחלק ב-8, ואז מפני ש- \mathbb{F}_q^* ציקלית, אז גם קיים איבר מסדר 8.

בהתחשב בכך שסדרי השדות הסופיים האפשריים הם מהצורה p^n עבור p ראשוני, אנו מחפשים מקרים בהם $8 | p^n - 1 = |\mathbb{F}_q^*|$.

כלומר $p^n \equiv 1 \pmod{8}$. במקרה זה, פתרונות אפשריים הם השדות מסדרים: 9, 17, 25, 41. וכן הלאה. שימו לב שלא מופיע ברשימה 33 למרות ש- $33 \equiv 1 \pmod{8}$. הסיבה היא שאין שדה מסדר 33 כיוון ש-33 אינו חזקה של מספר ראשוני.

קעת נחזור ונטפל במקרה של מאפיין 2. במקרה זה מתקיים $1 = -1$, ולכן $x^4 = 1$. אכן האיבר 1 מקיים את השוויון ולכן שדה ממאפיין 2 עונה על הדרישה בתרגיל. לסיכום, השדות המבוקשים הם שדות ממאפיין 2 או מסדר $8 \equiv 1 \pmod{8}$.

שאלה 3. הפריכו שאם $F = \mathbb{F}_p[\alpha]$ שדה סופי, אז תמיד $F^* = \langle \alpha \rangle$.

רמז: כנראה מספיק לקחת $p = 2$. מי הם שאר השורשים של הפולינום המינימלי של α ?

פתרון. כמו ברמז, נבחר $p = 2$. נתבונן בפולינום $f(x) = x^4 + x^3 + x^2 + x + 1$ שאפשר לבדוק שהוא אי פריק. לכל שורש α של $f(x)$ נקבל ש- F/\mathbb{F}_2 היא הרחבה מממד 4 ולכן $F \cong \mathbb{F}_{16}$. מתקיים כי $F^* \cong \mathbb{Z}/15\mathbb{Z}$ לפי טענה שראינו בכיתה (למעשה כל חבורה מסדר 15 היא ציקלית). אבל α מאפס את $x^5 - 1$, ולכן הוא לא יוצר את F^* . אגב, שאר השורשים של הפולינום המינימלי של α הנמצאים במסלול תחת פורבניוס הם $\alpha^2, \alpha^4, \alpha^8$.

שאלה 4. בנו את השדה \mathbb{F}_{32} בלי לעבוד יותר מדי קשה: בכיתה מצאנו פולינומים אי פריקים f_1, f_2, f_3 ממעלה 1 או 2. הגדירו $g = f_1^2 f_2 f_3 + 1$.

פתרון. נמצא פולינום אי פריק ממעלה 5 מעל \mathbb{F}_2 . בכיתה ראינו כי

$$f_1(x) = x \quad f_2(x) = x + 1 \quad f_3(x) = x^2 + x + 1$$

הם כל הפולינומים האי פריקים מעל \mathbb{F}_2 עד מעלה 2. נעזר ברמז ונגדיר

$$g(x) = f_1(x)^2 f_2(x) f_3(x) + 1 = x^2(x+1)(x^2+x+1) + 1 = x^5 + x^2 + 1$$

אז $g(x)$ לא מתחלק באף פולינום אי פריק ממעלה 1 או 2 (שהם הפולינומים לעיל). לכן $g(x)$ אי פריק ונסיק כי $\mathbb{F}_{32} \cong \mathbb{F}_2[x]/\langle g(x) \rangle$.

שאלה 5. רמז: המספרים 7 ו-5779 ראשוניים.

א. הוכיחו שקיים $x \in \mathbb{F}_q$ המקיים

$$\sum_{i=0}^{5778} x^i = 1 + x + \dots + x^{5778} = 0$$

אם ורק אם $q \equiv 0 \pmod{5779}$ או $q \equiv 1 \pmod{5779}$. רמז: קודם מצאו שורש של הפולינום $x^{5779} - 1$.

ב. (באופן דומה) מצאו עבור אילו מספרים טבעיים n השדה \mathbb{F}_{5^n} מכיל איבר x המקיים

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

פתרון.

א. לפי הרמז נשים לב כי $x = 1$ הוא שורש של הפולינום $x^{5779} - 1$. חלוקת פולינומים תניב

$$x^{5779} - 1 = (x - 1) \left(\sum_{i=0}^{5778} x^i \right)$$

ומכאן נפצל למקרים: אם $x = 1$ הוא שורש של הפולינום בשאלה, אז $5779 \cdot x = 0$ ולכן השדה ממאפיין 5779. אז בהכרח מתקיים $q \equiv 0 \pmod{5779}$ כי q יהיה חזקה של 5779. אחרת, אם $x \neq 1$ הוא שורש של הפולינום בשאלה, אז נקבל $x^{5779} = 1$. לכן $o(x) | 5779$. כלומר $o(x) = 1$ או $o(x) = 5779$. במקרה של $o(x) = 1$ כבר טיפלנו. מפני שידוע לנו לפי התרגיל בכיתה ש- $x^{q-1} = 1$, כמסקנה מלגראנז' עבור החבורה הכפלית \mathbb{F}_q^* , אז $q-1 | 5779$, ולכן $q \equiv 1 \pmod{5779}$. בכיוון השני, אם $q \equiv 0 \pmod{5779}$ נבחר $x = 1$. אם $q \equiv 1 \pmod{5779}$, ונניח כי α יוצר של \mathbb{F}_q^* , אז נבחר $x = \alpha^{(q-1)/5779}$. ודאו שאתם מבינים למה החזקה הזו של היוצר היא שורש של הפולינום בשאלה.

ב. עם הוכחה דומה לסעיף הקודם, השדות הסופיים שבהם קיים איבר שהוא שורש של הפולינום בשאלה הם שדות \mathbb{F}_q עבורם $q \equiv 0 \pmod{7}$ או $q \equiv 1 \pmod{7}$. מפני ש- $5 \in U_7$, אז אין n עבורו $5^n \equiv 0 \pmod{7}$. הסדר של 5 בחבורה U_7 הוא 6, ולכן כמסקנה ממשפט לגראנז' יתקיים $5^n \equiv 1 \pmod{7}$ אם ורק אם $6|n$.

שאלה 6. 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 $(\rho_{2n})^k = -e^{\pi i k} = 1$ והוא שורש של $\Phi_n(-x)$.

כלומר ל- $\Phi_n(-x)$, $\Phi_{2n}(x)$ 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, ולכן יש לו מחלק ראשוני אי זוגי p כלשהו וברור ש- $\varphi(p^k) = p^{k-1}(p-1)|\varphi(n)$ הוא זוגי.

שאלה 7. 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 8 (רשות). 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 $p \geq 7$ מחלק את n , אז $\varphi(n) > 4$. לכן מחפשים מספרים מהצורה $n = 2^a 3^b 5^c$ עם הדרישות $c < 2$, $b < 4$ ו- $a < 4$. בדיקה זריזה אחרי פתרונות המשוואה $\varphi(n) = 4$ 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 9 (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!