

פתרון תרגיל בית 12 בשדות ותורת גלואה 88-311 סמסטר א' תשפ"ב

שאלה 1. מצאו כמה פולינומים מתוקנים אי פריקים יש ממעלה 4 מעל \mathbb{F}_3 .

פתרון. מכפלת הפולינומים האי פריקים ממעלה שמחלקת את 4, לפי טענה מהכיתה, היא

$$x^{3^4} - x = \Pi_1 \Pi_2 \Pi_4$$

כאשר Π_i היא מכפלת כל הפולינומים המתוקנים האי פריקים ממעלה i את $\Pi_1 = x^3 - x$ קל לפרק, והפולינומים ממעלה 1 הם $x, x-1, x-2$. כלומר יש 3 כאלו. מכפלת הפולינומים ממעלה שמחלקת את 2 היא $\Pi_2 = x^2 - x$, ולכן Π_2 היא ממעלה $3^2 - 3^1 = 6$. כלומר יש $\frac{6}{2} = 3$ פולינומים אי פריקים ממעלה 2. באותו אופן, המעלה של Π_4 היא $3^4 - 3 \cdot 2 - 3 \cdot 1 = 72$ (למעשה במקרה זה קצת יותר מהיר לחשב $3^4 - 3^2 = 72$). לכן יש $\frac{72}{4} = 18$ פולינומים מתוקנים אי פריקים ממעלה 4.

שאלה 2. יהי $f(x) \in \mathbb{F}_3[x]$ פולינום אי פריק ממעלה 3 והיה a שורש שלו (בשדה הפיצול). הוכיחו כי $a^{13} \in \mathbb{F}_3$.

פתרון. שדה הפיצול של $f(x)$ הוא השדה $\mathbb{F}_{3^3} = \mathbb{F}_{27}$. החבורה הכפלית של השדה היא חבורה ציקלית מסדר 26. בנוסף a הפיך (אחרת $a = 0 \in \mathbb{F}_3$ ויש לפולינום שורש ב- \mathbb{F}_3 , סתירה) ולפי משפט לגראנז' $a^{26} = 1$. לכן

$$a^{13} = \pm 1 \in \mathbb{F}_3$$

כי מעל שדה לפולינום $x^2 = 1$ יש לכל היותר 2 שורשים.

שאלה 3. 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 $8 \mid o(x)$. 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 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 $8 \mid |\mathbb{F}_q^*| = |\mathbb{F}_q| - 1 = p^n - 1$. 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, שהרי 33 אינו חזקה של מספר ראשוני.

כעת 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 $q = p^n \equiv 1 \pmod{8}$.

שאלה 4. 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 $\alpha^2, \alpha^{2^2}, \alpha^{2^3}$.

שאלה 5. 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 6. 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 שמקיים

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

פתרון.

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

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

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 $5779 | o(x)$. 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 $5779 | q - 1$, 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 $6|n$.

בהצלחה!