תרגיל פולינומים אי פריקים

תזכורת

1. קריטריון אייזנשטיין – אם $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ פולינום כך שp מחלק את כל המקדמים חוץ מהמוביל ו$p^2 \nmid a_0$ אז f אי פריק
2. הלמה של גאוס – פולינום בשלמים פריק ב$\mathbb{Q}$ אם"ם הוא פריק ב$\mathbb{Z}$
3. יש gcd לפולינומים מתוקנים עם מקדמים שלמים והוא פולינום מתוקן עם מקדמים שלמים

תרגילים

1. יהי f פולינום אי פריק, הוכח שאין לו שורשים כפולים

פתרון: יש לו GCD עם הנגזרת שלו

2. הוכח שהפולינום $x^4 + 6x^2 + 1$ פריק מודולו כל ראשוני, אבל לא פריק

פתרון:
נתחיל מאי פריקות, אין לו שורש ולכן אם הוא מתפרק אז זה לשני פולינומים ממעלה 2, ואז הם מתוקנים והמקדם התחתון ± 1, לפי המקדם השני קל להסיק שהוא מהצורה $(x^2 + ax \pm 1)(x^2 - ax \pm 1)$ המקדם של x^2 הוא $\pm 2 - a^2$ שלא יכול להיות 6.
אבל מספיק להראות שמודולו כל ראשוני יש פתרון.
יש פירוק מהצורה הנ"ל אם $a^2 = -6 \pm 2$ כלומר לפחות אחד מ$-4, -8$ הוא שארית ריבועית. קל לראות שזה קורה אם"ם $p \neq 7 (mod\ 8)$.
מצד שני, אפשר לנסות לפתור את המשוואה הריבועית בx^2, הדיסקרמיננטה היא 32 והיא שארית ריבועית כש $p = 7 (mod\ 8)$

3. יהי p ראשוני, הוכח שהפולינום $f = x^{p-1} + 2x^{p-2} + 3x^{p-3} + \cdots + p$ אי פריק.

פתרון:
אפשר להראות ש$f = \frac{x^{p+1} - (p+1)x + p}{(x-1)^2}$ ואז אם נסתכל על $f(x+1)$ אז מודולו p מקבלים $x^{p-1} + x^{p-2}$ ולכן אם יש פירוק אז מודולו p הוא מהצורה $x^k, (x+1)x^{p-1-k}$. המקדם החופשי הוא $\frac{p(p+1)}{2}$ ולכן לא מתחלק בp^2 ולכן כמו באייזנשטיין $p - 1 - k = 0$ אבל אז אחד הגורמים הוא לינארי, כלומר יש שורש שמתחלק בp שהוא בפרט שורש של $x^{p+1} - (p+1)x + p$, וקל לראות שאין לו שורש שלם.

4. יהי f פולינום אי פריק מתוקן עם מקדמים שלמים, נניח כי $|f(0)|$ לא ריבוע, הוכח ש$f(x^2)$ אי פריק.

פתרון:

השורשים של $f(x^2)$ באים בזוגות $\alpha, -\alpha$ (אין 0).

נסתכל על g גורם אי פריק של $f(x^2)$, ונסתכל על ה$\gcd(g(x), g(-x))$ g אי פריק ולכן זה או 1 או g, אם זה g זה אומר שכל שורש מופיע עם הזוג שלו ולכן זה פולינום בx^2 כלומר f פריק.

אחרת הבנו שבכל גורם אי פריק מופיע רק אחד מכל זוג שורשים וזה אומר שהגורמים מתחלקים לזוגות $g(x), g(-x)$ אבל אז המקדם החופשי הוא ריבוע.

5. יהי f פולינום אי פריק עם מקדמים שלמים לא לינארי, נניח שיש לf שני שורשים שמכפלתם 1, אז f ממעלה זוגית.

פתרון:

נסתכל על $x^d f\left(\frac{1}{x}\right)$, שהוא הפולינום שבו אנחנו הופכים את סדר המקדמים, יש לו שורש משותף עם f ולכן אם נעשה gcd מעל $\mathbb{Q}[x]$ אז נקבל פולינום שמחלק את f ב$\mathbb{Q}[x]$ ולכן מהלמה של גאוס גם מעל $\mathbb{Z}[x]$ ולכן הם שווים, אבל אז כל השורשים באים בזוגות, אולי חוץ מ± 1 אבל הם לא שורשים כי f אי פריק

6. האם יש סדרה $a_0, a_1, a_2 \ldots \in \mathbb{Z}$ של מספרים זרים כך שלכל n, הפולינום $\sum_{i=0}^{n} a_i x^i$ הוא אי פריק?

פתרון:

כן! אם נבחר a_n להיות ראשוני שגדול מסכום כל הקודמים, אז כל השורשים קטנים בערך מוחלט מאחד (כי אחרת החלק המוביל גדול מדי). ומצד שני אם הפולינום מתפרק, אז אחד הגורמים מתוקן ואז מכפלת השורשים שלו שלמה ולכן גדולה שווה ל1 (0 לא יהיה שורש).

7. הוכח ש$(x^2 + x)^{2^n} + 1$ אי פריק.

פתרון:

הפולינום שווה ל$(x^2 + x + 1 - 1)^{2^n} + 1$ ממשפט לוקאס, מודולו 2 הפולינום שווה ל $(x^2 + x + 1)^{2^n}$. הפולינום $x^2 + x + 1$ הוא אי פריק מודולו 2 ולכן אם הפולינום מתפרק הוא מתפרק לגורמים מהצורה $(x^2 + x + 1)^k$ מודולו 2, לכן נקבל משוואה מהצורה:

$(x^2 + x +$

מלוקאס נקבל מודולו 4:

$(x^2 + x +$

כלומר מודולו 2:

$(x^2$

אבל אגף ימין מתחלק ב x^2+x+1 ואגף שמאל לא, אז $k=0$ אבל בגלל שהפולינום מתוקן זה גורר שאחד הגורמים קבוע.