סמינר בתורת המספרים – תרגיל 3

חלק א:

1. עבור השדה Z/5Z[x]/x^2+X+1 , נגדיר את G להיות התת חבורה הכפלית של איברים שונים מאפס בשדה.
   א. כמה איברים יש מכל סדר d, כאשר d=1,2,,,,,|G|. (אין צורך לחשב איבר איבר; ניתן להשתמש בזהות שהוכחנו בכיתה).
   ב. מצא לפחות יוצר אחד לG.

חלק ב:

אנחנו תמיד עובדים עם פולינומים מעל שדה סופי F בעל q איברים שזה חזקה של ראשוני p.
נסמן A=F[X], לפולינום P: B=A/PA. *B החבורה הכפלית של B.

1)

בדוגמא בהרצאה ראינו שאם המשוואה $Y^2 \equiv b(\mathrm{mod}\, P)$ פתירה אז b אינו שורש פרימיטיבי של *B.

להפריך את הכיוון השני עבור P(x)=x, q=7 כלומר:

למצוא b ב-*B פולינום שאינו שורש פרימיטיבי של *B כך שעבורו המשוואה $Y^2 \equiv b(\mathrm{mod}\, P)$ אינה פתירה. כאשר F שדה בגודל 7, P(x)=x.

2)

באותה שיטה כמו בדוגמא השנייה בהרצאה (**כלומר ללא שימוש בכך שלפולינום $x^2=1$ יש שני שורשים בדיוק בשדה**) עבור F כך ש-q=5 , $P(x)=X^2+X+1$ מעל F.

תוכיחו ש-P אי פריק מעל F ותמצאו לאילו b המשוואה $Y^{12} \equiv b(\mathrm{mod}\, P)$ פתירה.