עבודה בקורס אלגברה מתקדמת
83-804 סמסטר א' תשפ"א

בחרו שפת תכנות שבה אתם שולטים וענו על החלקים הבאים. כמה הערות כלליות לכל שאלות התכנות:

- הוסיפו קוד בדיקות, כך שכל פונקציה או מתודה תבדק לפחות בכמה מקרים שלא מופיעים בשאלות. זה המקום לבדוק את המימוש שלכם גם ידנית.
- הקוד לא חייב להיות מהיר, אבל גם אין צורך לחוסר יעילות משווע.
- כתבו תיעוד ברור.
- כמו לרוב התוכנות, כדאי להשתמש במערכת לניהול גרסאות כמו Git או Mercurial.

כל אחד יקבל מספר ראשוני p עבורו הוא יבדוק את כלל הפונקציות. כדאי לנסות גם עבור $p = 7$ או ראשוני קטן אחר עבורו אפשר לבדוק ידנית. נתבונן בשדה $\mathbb{F}_p$.

א. ממשו מחלקה (או אובייקט דומה בשפה שבחרתם) הממשת איבר בשדה $\mathbb{F}_p$. ממשו לכל איבר מתודות לארבע פעולות חשבון, מתודה לחישוב הסדר החיבורי ומתודה לחישוב הסדר הכפלי.
אם השפה שבחרתם תומכת ב-operator overloading ממשו איתם את ארבע פעולות חשבון. הקפידו להעלות חריגה (Exception) או להחזיר קוד שגיאה בחלוקה באפס.

ב. ממשו בשיטת חישוב חזקה בעזרת ריבועים את פעולת החזקה במספר שלם בשדה $\mathbb{F}_p$.

ג. הראשוני שקיבלתם הוא "בטוח" במובן שגם $q = \frac{p-1}{2}$ הוא ראשוני. הוכיחו שבחבורה הכפלית $\mathbb{F}_p^*$ עבור ראשוני "בטוח" הסדר של האיברים הוא בהכרח אחד מארבעה מספרים בלבד. ממשו מחדש את פונקציית הסדר הכפלי שתהיה הרבה יותר יעילה.

ד. מצאו שני איברים $a, b \in \mathbb{F}_p$ שאינם אפס או אחד עבורם $4a^3 + 27b^2 \not\equiv 0 \pmod p$.

ה. ממשו מחלקה (או אובייקט דומה בשפה שבחרתם) הממשת את החבורה $C(\mathbb{F}_p)$ כאשר C הוא העקום האליפטי הפרוייקטיבי

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

הוסיפו מתודות לחישוב סדר החבורה ולהחזרת איבר היחידה. באופן דומה נתבונן בעקום

$$C_{\text{aff}}(\mathbb{F}_p) = y^2 - x^3 - ax - b$$

שהוא העקום האפיני המתקבל על ידי הורדת הנקודה $\mathcal{O} = (0 : 1 : 0)$ מ-$C(\mathbb{F}_p)$. הוסיפו מתודה להחזרת כל נקודות החבורה $C_{\text{aff}}(\mathbb{F}_p)$ התומכות בנקודות של $C(\mathbb{F}_p)$. הוסיפו קוד לבדיקה שחסם הסה מתקיים.

ו. ממשו מחלקה (או אובייקט דומה בשפה שבחרתם) הממשת נקודה $P \in C_{\text{aff}}(\mathbb{F}_p)$. הוסיפו מתודה להחזרת הנקודה ההופכית $-P$, מתודה לחישוב הסדר של נקודה $P \in C_{\text{aff}}(\mathbb{F}_p)$, הדפסת איברי $\langle P \rangle$ וחישוב יעיל של nP לכל $n \in \mathbb{Z}$ (למשל עם השיטה לחישוב חזקה בעזרת ריבועים). הוסיפו מתודה המקבלת נקודה $Q \in C_{\text{aff}}(\mathbb{F}_p)$ ומחזירה את הסכום $P + Q$.

בהצלחה!