ספירת נקודות על יריעות מעל שדות סופיים, חישובי אינטגרלי קולמן ונקודות רציונליות

רקע

התחום של תורת המספרים החישובית מתפתח במהירות בשנים האחרונות. מטרת המחקר בתחום זה היא לפתח אלגוריתמים יעילים לפתרון של בעיות ולחישוב של פונקציות בתורת המספרים.

תורת המספרים החישובית קשורה קשר הדוק לתחום הקריפטוגרפיה ובעיות רבות בה מקורן בתחום זה. אחת הבעיות החשובות בתחום היא הבעיה של ספירת נקודות על יריעות מעל שדות סופיים.

הבעיה: נתונה מערכת משוואות פולינומיאלית במשתנים x_1 עד x_n :

$$f_i(x_1, \ldots, x_n) = 0, i = 1, \ldots, m$$

כאשר מקדמי המשוואות בשדה סופי נתון L. הבעיה היא למצוא את מספר פתרונות המשוואה בשדה L כלומר את מספר ה- nיות של ערכי L המקיימות את כל המשוואות.

האלגוריתם הנאיבי של מעבר על כל הפתרונות האפשריים אורך זמן שהוא פולינומיאלי בגודל השדה ובדרך כלל אינו מעשי לחלוטין.

למציאה מהירה של מספר הפתרונות חשיבות רבה במספר אלגוריתמים קריפטוגרפיים. אלגוריתמים אלו מנסים לנצל את אוסף הפתרונות של המשוואות להצפנה (לדוגמה, הצפנה בעזרת עקומים אליפטיים כנלמד בקורס "שיטות אריתמטיות בקריפטוגרפיה"). ידוע ששיטת ההצפנה תהיה חלשה אם מספר הנקודות מתחלק רק בראשוניים קטנים ולכן צעד הכרחי באלגוריתמים אלה הוא ספירת הנקודות ווידוא שמספר זה כולל גורם ראשוני גדול.

עבור משוואות מסוימות ידועים מספר אלגוריתמים יעילים לפתרון בעית ספירת הנקודות. עבור עקומים אליפטיים קיים האלגוריתם של Schoof משנת 1985 הנלמד בקורס "שיטות אריתמטיות בקריפטוגרפיה". עבור עקומים יותר כלליים קיים האלגוריתם של Kedlaya משנת 2001 ועבור יריעות כלשהן קיימים האלגוריתמים של Lauder.

האלגוריתמים של Kedlaya ו- Lauder מבשרים את כניסתן של שיטות מתמטיות מתקדמות מתחום הקוהומולוגיה ה- p-אדית לפתרון בעיות של ספירת נקודות. כבעיות מחקר הן גשר מצויין בין בעיות בעלות שמושים בשטח ההצפנה למחקר המצוי כיום בחזית המחקר התאורטי.

בעיה קלאסית אחרת בתורת המספרים היא מציאת פתרונות עם מקדמים רציונליים למשוואות פולינומיאליות. לדוגמה המשפט האחרון של פרמה הוא בעצם הקביעה ששני הפתרונות היחידים ברציונליים למשוואה $x^n + y^n = 1$ הם $(0, 1), (1, 0)$ כאשר $n > 2$.

לשיטות ה- p-אדיות לספירת נקודות קשר הדוק לבעיה של חישוב האינטגרלים של Coleman. אינטגרלים אלה, שהוגדרו בשנות השמונים, התגלו כמועילים ביותר במספר

בעיות תאורטיות בתורת המספרים. בפרט, מחקריו של M. Kim בעשור האחרון מצביעים על אפשרות להשתמש באינטגרלים אלה למציאת פתרונות רציונליים למשוואות פולינומיאליות.

למרות חשיבותם הרבה, לא היה בנמצא אלגוריתם אשר יוכל לחשב אינטגרלים אלה. פריצת הדרך היתה עבודת המוסמך של יגאל גוטניק באוניברסיטת בן-גוריון משנת 2005. בעבודתו הראה גוטניק ששינוי קל באלגוריתם של Kedlaya לספירת נקודות על עקומים היפראליפטיים נותן אלגוריתם לחישוב של אינטגרלי Coleman על אותם עקומים.

בעיות מחקר

א. הכללת האלגוריתם של גוטניק לעקומים לא מנווניים - האלגוריתם של Kedlaya הוכלל בשנת 2006 לאלגוריתם לספירת נקודות על עקומים המכונים לא מנווניים. כמעט כל עקום הוא לא מנוון. חלקו הראשון של המחקר הוא תכנות האלגוריתם המוכלל. חלקו השני הוא הכללה של האלגוריתם של גוטניק לחישוב אינטגרלי Coleman לעקומים לא מנווניים.

ב. שיטות דפורמציה לחישוב אינטגרלי Coleman - המילה האחרונה בתחום ספירת הנקודות הם אלגוריתמי הדפורמציה של Lauder המסוגלים לספור בעיקרון נקודות על כל יריעה אלגברית על ידי שינוי פרמטרי המשוואה לפרמטרים פשוטים וחקירת ההשתנות של מספר הפתרונות. חלקו הראשון של המחקר הוא תכנות אלגוריתמים אלה. החלק השני הוא יישום של שיטות דפורמציה לחישובם של אינטגרלי Coleman.

ג. שיטות לחישוב של אינטגרלי Coleman **חוזרים** - אלו הכללות של אינטגרלי Coleman והם אלו שיש להשתמש בהם בשימושים של השיטות של Kim למציאת פתרונות רציונליים למשוואות. השיטה לחישובם היא הכללה של השיטה של גוטניק. המחקר יתאר הכללה זו ויתכנת אותה.

ד. שיטות לחישובים מהירים של פוליולוגריתמים p-אדיים. פוליולוגריתמים p-אדיים הם מקרה מיוחד של אינטגרלי Coleman שיש להם חשיבות בחקר של השערות בחזית תחום הגאומטריה האריתמטית. אלגוריתם לחישובם פותח על ידי בשיתוף עם de Jeu אבל יש שורה ארוכה של שיפורים אפשריים שראוי לחקור. בפרט, המחקר יערב שאלות של חישוב נומרי מעל המספרים ה- p-אדיים, כמו קרובי Pade.

תוכנת Sage

המחקר יתבצע באמצעות תוכנת Sage. תוכנה זו היא העדכנית ביותר למחקר בתחומי תורת המספרים והגאומטריה האלגברית ומשלבת בתוכה את התוכנות שקדמו לה יחד עם ממשק משתמש גרפי ונוח במיוחד ותכנות בשפת Python. למעוניינים להמשיך במחקר בשטח המתמטיקה החישובית ידע בתוכנה זו נחוץ ביותר.

מלגות מוגדלות

מחקר זה נתמך על ידי מענק של הקרן הלאומית למדע. הדבר יאפשר הגדלת המילגות לחוקרים בפרוייקט.