משפט הריבועים של פרמה

מטרות

1. להכיר הרבה הוכחות למשפט הריבועים של פרמה
2. לגרות רצון להעמיק במתמטיקה מעניינת ומתקדמת יותר דרך ההוכחות

ראציונאל

1. הצגת הבעיה
2. מבוא – דוגמאות ודגשים מיוחדים על שדה מחלקי אפס ותחום שלמות, לפולינום מעל שדה יש לכל היותר דרגת הפולינום שורשים, קריטריון אוילר, אם p ראשוני מהצורה 4m+1 אז 1- הוא ריבוע
3. הוכחתו של לגרנז' – תבניות ריבועיות בשני משתנים, הדיסקרימיננטה של תבנית ריבועית, שקילות של תבניות ריבועיות, הוכחה שכל התבניות עם דיסקרימיננטה 1- שקולות, הוכחה של לגרנז'
4. משפט מינקובסקי, הוכחה באמצעות משפט מינקובסקי
5. מבוא לשלמים של גאוס –המרוכבים והפעולות עליהם, השלמים של גאוס, הנורמה והרדיוס, כפליות הנורמה, אלגוריתם אוקלידס, ראשוניים ומשפט היסודי של האריתמטיקה עבור השלמים של גאוס, הוכחה 2 של דדיקנד
6. אינבולוציה, הוכחה של צגייר

מהלך

הבעיה

היום אנחנו נתמודד עם הבעיה הבאה שהציג פרמה:

משפט הריבועים של פרמה

יהא p ראשוני. אזי $p=a^2+b^2$ עבור $a,b\in\mathbb{Z}$ כלשהם אם ורק אם $p\equiv 1 \bmod 4$ או $p=2$.

<u>דוגמאות</u>: 2=1+1, 5=1+4, 41=16+25 אבל ל- 3,7,43 אין הצגה כסכום של ריבועים.

הוכחת כיוון קל $\Leftarrow$

אם $p=a^2+b^2$ אז $p\equiv 0,1,2 \bmod 4$ (כי $a^2,b^2\equiv 0,1 \bmod 4$).

קבוצת דן של תשע"ו ראתה את הוכחתו המקורית של אוילר לעובדה הזאת בשיעור על "ירידה אינסופית" מסוף השנה. הנקודות המרכזיות בהוכחה ההיא מצורפות לתרגיל של השיעור הזה.

היום אנחנו נראה עוד כמה הוכחות למשפט הזה שדורשות ידע מתמטי עמוק יותר ששווה להכיר.

מבוא

אנחנו נצטרך כמה מושגים באלגברה מתקדמת וכמה משפטים בסיסיים כדי שתבינו את ההוכחות של היום. אז נתחיל בשדה, מחלקי אפס ותחום שלמות.

שדה

ההגדרה המדויקת של שדה מצורפת בנספח. הדבר החשוב שנדע על שדה זה שאלו אוסף של איברים עם חיבור וכפל שמקיימים את כל מה שהיינו מצפים מחיבור וכפל, בדגש על העובדה שלכל איבר שונה מ-0 יש הפכי.

דוגמאות:

המספרים הראציונאליים $\mathbb{Q}$, המספרים הממשיים $\mathbb{R}$, המספרים השלמים מודולו ראשוני p כלשהו $\mathbb{Z}/\langle p\rangle$, המספרים המרוכבים $\mathbb{C}$ (אליהם נחזור בקרוב).

המספרים השלמים $\mathbb{Z}$ אינם שדה מכיוון שלא לכל מספר שלם יש הפכי שהוא שלם (רק ל± 1 יש).

מחלקי אפס

יש עולמות של מספרים בהם שני מספרים ששונים מאפס, הכפל ביניהם הוא אפס. למספרים כאלו קוראים "מחלקי אפס".

דוגמא: $2,3 \neq 0 \bmod 6$ אבל $2\cdot 3 \equiv 0 \bmod 6$.

תרגיל: הוכיחו כי לא ייתכן כי למחלק אפס יש הפכי (ולכן בשדות אין מחלקי אפס).

תחום שלמות

שוב, הגדרה מדוייקת בנספח לתרגיל, מבחינתנו כל עולם שמקיים את כל התכונות של שדה חוץ מאולי הפכיים אבל שעדיין אין בו מחלקי אפס ייקרא תחום שלמות.

דוגמאות:

השלמים $\mathbb{Z}$, הפולינומים עם מקדמים ממשיים $\mathbb{R}[x]$, השלמים הגאוסיים $\mathbb{Z}[i]$.

שורשים של פולינומים מעל שדה

יהי F שדה ו- $p(x)=a_n x^n+\ldots+a_1 x+a_0$ פולינום מעל השדה F. אזי ל $p(x)$ יש לכל היותר n שורשים מעל השדה.

דוגמאות: מעל לממשיים או לראציונאליים לפולינום $p(x)=x^2-x$ יש רק שני שורשים – 0,1. אבל אם נחזור לדוגמא של $\mathbb{Z}/\langle 6\rangle$ ממקודם, שם יש לפולינום הזה 4 שורשים כי: $0^2-0\equiv 0 \bmod 6$, $1^2-1\equiv 0 \bmod 6$, $3^2-3\equiv 0 \bmod 6$, $4^2-4\equiv 0 \bmod 6$. זאת עוד דרך להראות כי $\mathbb{Z}/\langle 6\rangle$ אינו שדה.

הוכחה

תזכורת - ראינו בשיעור על פולינומים שנה שעברה כי $p(s)=0$ אם ורק אם $p(x)=(x-s)\cdot h(x)$ כאשר $\deg(h(x))=\deg(p(x))-1$.

כעת אפשר להוכיח באינדוקציה על הדרגה של הפולינום. אם $\deg(p(x))=1$ אז $p(x)=a(x-b)$ כאשר $a\neq 0$. אזי אם $x\neq b$ נובע כי $x-b\neq 0$ ולכן $a(x-b)\neq 0$ (כי בשדה אין מחלקי אפס). על כן ל$p(x)$ יש לכל היותר שורש אחד.

נניח נכונות לכל $\deg(p(x))<n$ ונוכיח ל- $\deg(p(x))=n$:

אם $p(s)=0$ אז לפי התזכורת $p(x)=(x-s)h(x)$. כעת $\deg(h(x))=\deg(p(x))-1=n-1$ ולפי הנחת האינדוקציה יש לכל היותר $n-1$ שורשים ל$h(x)$. אם $x_0\neq s$ וגם $h(x_0)\neq 0$ עבור $x_0\in F$ כלשהו

אז $p(x_0)=(x_0-s)h(x_0)\neq 0$ מכיוון שבשדה אין מחלקי אפס. לכן ל-$p(x)$ יש לכל היותר n שורשים וסיימנו.

מסקנה - קריטריון אוילר

יהיו $a,p\in\mathbb{Z}$ כך ש p ראשוני אי-זוגי ו-$\gcd(a,p)=1$. אזי $a^{\frac{p-1}{2}}\equiv\pm1\bmod p$ ול-a יש שורש מודולו p אם ורק אם $a^{\frac{p-1}{2}}\equiv1\bmod p$.

<u>דוגמאות:</u>

מודולו 7 יש לנו את הריבועים הבאים 0,1,2,4. נראה מה קורה כשלוקחים חזקה שלישית של אלו ששונים מ0: $1^3\equiv1\bmod 7, 2^3=8\equiv1\bmod 7, 4^3=64\equiv1\bmod 7$. אבל אם ניקח את 3 ונבדוק מה קורה כשלוקחים אותו בשלישית: $3^3=27\equiv-1\bmod 7$.

הוכחה

$a^{p-1}\equiv1\bmod p$ לפי משפט פרמה הקטן.

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv a^{p-1}-1\equiv0\bmod p.$$

מכיוון ש $\mathbb{Z}/\langle p\rangle$ שדה $a^{\frac{p-1}{2}}\equiv\pm1$.

כעת, מכיוון שלפולינום $x^{\frac{p-1}{2}}-1$ יש לכל היותר $\frac{p-1}{2}$ שורשים ולכל מספר a שזר ל-p מתקיים $\left((\pm a)^2\right)^{\frac{p-1}{2}}=(\pm a)^{p-1}\equiv1\bmod p$ יש לפולינום הזה בדיוק $\frac{p-1}{2}$ שורשים ואלו הריבועים מודולו p.

טענה

אם $p\equiv1\bmod 4$ אז -1 הוא שארית ריבועית. כלומר, קיים $m\in\mathbb{Z}$ כך ש- $p\mid m^2+1$.

הוכחה

נסמן $p=4n+1$. אזי מקריטריון אוילר - $(-1)^{\frac{4n+1-1}{2}}=(-1)^{2n}=1$.

<u>דוגמאות:</u>

$2^2\equiv-1\bmod 5, 5^2\equiv-1\bmod 13, 9^2\equiv-1\bmod 41$.

הוכחה 1 - הוכחתו של לגרנז' – תבניות ריבועיות

נתחיל מכמה הגדרות עבור תבניות ריבועיות:

תבנית ריבועית

- מי שהיה בהרצאה של גיא בסמינר גמל ראה הגדרה יותר כללית לתבנית ריבועית. אנחנו נתמקד בהגדרה הבאה:

תבנית ריבועית בינארית שלמה תהיה פונקציה בשני משתנים $Q(x,y)=ax^2+2bxy+cy^2$ כך ש $a,b,c\in\mathbb{Z}$.

- לכל תבנית ריבועית נגדיר דיסקרימיננטה באופן הבא $\Delta(Q)=b^2-ac\in\mathbb{Z}$.
- אם $\Delta(Q)<0$ וגם $a>0$ נאמר כי התבנית חיובית.
- נאמר על מספר שלם $n\in\mathbb{Z}$ שהוא מיוצג על ידי $Q(x,y)$ אם קיימים $x_0,y_0\in\mathbb{Z}$ עבורם $Q(x_0,y_0)=n$.

<u>דוגמא</u>: $Q(x,y)=x^2+y^2$ היא תבנית ריבועית בינארית עם דיסקרימיננטה 1- שמייצגת את 2 כי $Q(1,1)=1^2+1^2=2$ אבל לא מייצגת אף מספר שלילי כי $x^2+y^2\geq 0$.

שקילות של תבניות

בשאלת בונוס על מטלה 1 של דן שנה שעברה ביקשתי מכם לומר מה התנאי על $a,b,c,d\in\mathbb{Z}$ כך שבהינתן ש$ax+by,cx+dy$ שלמים, מבטיח כי x,y שלמים? חלקכם שלחתם לי תשובות מדויקות והתשובה היא ש $ad-bc=\pm 1$.

תבניות שקולות

אם $Q(x,y),P(x,y)$ תבניות ריבועיות כך ש-$P(ax+by,cx+dy)=Q(x,y)$ עבור $a,b,c,d\in\mathbb{Z}$ שמקיימים $ad-bc=\pm 1$ נאמר כי התבניות שקולות.

<u>תרגיל:</u> לתבניות שקולות אותה דיסקרימיננטה והן מייצגות את אותם השלמים.

משפט

כל התבניות החיוביות עם דיסקרימיננטה 1- שקולות.

הוכחה

ניקח $Q(x,y)=ax^2+2bxy+cy^2$ חיובית עם דיסקרימיננטה 1-. כלומר $b^2-ac=-1,a>0$.

נשים לב שההחלפות $(x-y,y),(x,y-x),(x,-y)$ מקיימות את התנאי$ad-bc=\pm 1$. לכן אם נעשה את ההחלפות הללו ל-Q נשאר עם תבנית שקולה. באמצעות ההחלפה האחרונה אפשר לוודא כי $b\geq 0$ (אחרת נחליף ב $(x,-y)$ והוא יהפוך לחיובי)

מכיוון ש$b^2-ac=-1$ אז $ac>b^2$ ולכן $\frac{a+c}{2}\geq\sqrt{ac}>b$ וגם $c>0$. אם $a=c$ אז $b^2-a^2=-1$ והפתרון היחיד לדבר הזה הוא $a=1,b=0$. אחרת $a\neq c$ ואז או $a>b$ ו- $c\leq b$ או $c>b$ ו-$a\leq b$.

אם $a\leq b$ נפעיל את ההחלפה $(x-y,y)$ ואז נקבל

$$Q(x-y,y)=a(x-y)^2+2b(x-y)y+cy^2=ax^2+2(b-a)xy+(c+a-2b)y^2$$

ועדיין מתקיים $a,b-a,c+a-2b\geq 0$. נשים לב שהקטנו את ac ממש כי $c>c+a-2b$.

אם $c\leq b$ נפעיל את ההחלפה השנייה ונקבל דבר דומה כש a קטן ממש.

אזי כל עוד $a\neq c$ אפשר להקטין את הגדול מביניהם. התהליך הזה חייב להסתיים כי הצלחנו שכל האיברים יהיו אי-שליליים. על כן הוא יסתיים כאשר $a=c=1,b=0$ והראינו שכל תבנית ריבועית חיובית עם דיסקרימיננטה 1- שקולה ל-x^2+y^2.

מסקנה – משפט הריבועים של פרמה הוכחה 1

מכיוון שכל שתי תבניות שקולות מייצגות את אותם המספרים, מספיק להראות כי יש תבנית ריבועית חיובית עם דיסקרימיננטה 1- שמייצגת את p אם $p \equiv 1 \bmod 4$.

נזכר כי קיים $m \in \mathbb{Z}$ עבורו $p \mid m^2+1$ ולכן נביט בתבנית $Q(x,y) = px^2 + 2mxy + \frac{m^2+1}{p}y^2$.

היא חיובית כי $p > 0$ והדיסקרימיננטה שלה 1- כי $m^2 - p \cdot \frac{m^2+1}{p} = -1$.

אבל $Q(1,0) = p$ ולכן גם x^2+y^2 מייצגת את p.

הוכחה 2 – באמצעות למת מינקובסקי

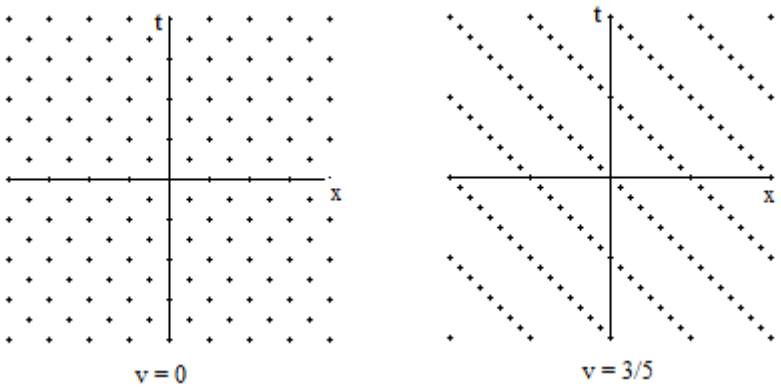
שריגים

לכל שני וקטורים בלתי תלויים $u, v \in \mathbb{R}^2$ במישור אפשר להגדיר את השריג שלהם:

$L = \{au + bv \mid a,b \in \mathbb{Z}\}$. נשים לב שזה מחלק את המישור למקבליות עם שטח $\det(u,v)$. נקרא לשטח הזה השטח היסודי של המקבילית.

<u>דוגמאות:</u>

השמאלי נוצר על ידי $u=(1,1), v=(1,-1)$ הימני נוצא על ידי $u=(-1,1), v=(8,0)$



אנו נשתמש במשפט מאד חשוב של מינקובסקי שאומר כך:

למת מינקובסקי

נתון שריג במישור עם שטח יסודי S. אזי אם ניקח קבוצה קמורה עם סימטריה ביחס ל $(0,0)$ ושטח גדול מ- $4S$ היא תכיל נקודת שריג שונה מ $(0,0)$.

הוכחה

נשתמש בהוכחה מהספר על משוואות פל - http://taharut.org/articles/Pell.pdf - עמודים 21-23.

הוכחה 2

נזכר כי מכיוון ש $p \equiv 1 \bmod 4$ קיים $m \in \mathbb{Z}$ כך ש $p \mid m^2+1$.

ניקח את השריג שנוצר על ידי הוקטורים $(p,0),(m,1)$. השטח היסודי של השריג הוא p. נביט במעגל עם רדיוס $\sqrt{2p}$ מסביב לראשית. הוא קמור ועם סימטריה ביחס ל-0, בנוסף הוא עם שטח $2p\pi > 4p$. על כן הוא מכיל נקודת שריג מהצורה $w = a(p,0)+b(m,1)$.

כעת $\|w\|^2 = (ap+bm)^2 + b^2 = a^2p^2 + 2apbm + \underbrace{b^2m^2+b^2}_{b^2(m^2+1)}$ ולכן $p \mid \|w\|^2$. מצד שני $\|w\|^2 < 2p$ לפי

זה שזאת נקודת שריג בתוך העיגול. אזי $(ap+bm)^2 + b^2 = \|w\|^2 = p$ וסיימנו.

הוכחה 3 – השלמים של גאוס והוכחה של דדיקנד

מרוכבים והשלמים של גאוס

להעמקה והשלמת פערים בהוכחות לגבי השלמים של גאוס אתם יכולים להשתמש בסיכום הבא - http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf

תחילה נזכר כי המרוכבים הם אוסף המספרים מהצורה $a+bi$ כש $a,b\in\mathbb{R}$ ו- $i^2=-1$.

$z+w=(a+bi)+(c+di)=(a+c)+(b+d)i$.

$zw=(a+bi)(c+di)=ac+adi+bci+bdi^2=(ac-bd)+(ad+bc)i$.

אפשר לסמן אותם במישור ולהתאים לכל מרוכב $a+bi$ את הנקודה (a,b).

נגדיר את האורך של המרוכב להיות המרחק של הנקודה מראשית הצירים כלומר $|a+bi|=\sqrt{a^2+b^2}$.

בנוסף לכל מספר מרוכב יש את הצמוד שלו $\overline{a+bi}=a-bi$. נשים לב כי

$z\cdot\bar{z}=(a+bi)(a-bi)=a^2+b^2=|z|^2$.

המרוכבים הם שדה. מציאת ההפכי דורשת כפל בצמוד. נשים לב כי אם $a+bi\neq 0$ אז $\frac{1}{a+bi}=\frac{a-bi}{a^2+b^2}$.

כעת, אנחנו נביט בשריג שחי בתוך המרוכבים ונוצר מ $1,i$, כלומר אוסף האיברים $a+bi$ עבורם $a,b\in\mathbb{Z}$. לאוסף הזה קוראים השלמים של גאוס ומסמנים אותו ב $\mathbb{Z}[i]$. החיבור והכפל שלהם זהה, אבל כמו בשלמים הרגילים אנו מאבדים את קיום ההופכי של כל האיברים שהם לא $\pm1,\pm i$.

נגדיר את הנורמה של איבר ב $\mathbb{Z}[i]$ בתור האורך של המרוכב בריבוע - $N(a+bi)=a^2+b^2$. **שימו לב שהנורמות הם מספרים טבעיים!**

טענה

$N(zw)=N(z)N(w)$ לכל שני שלמים של גאוס.

הוכחה

תרגיל.

השלמים של גאוס חולקים לא מעט תכונות עם השלמים הרגילים. התכונה הכי חשובה שלהם, אותה לא נוכיח אבל כן אתן את הדרך להוכחה שלה בתרגיל, היא שאפשר להגדיר בה מספרים ראשוניים וכל מספר הוא מכפלה יחידה של ראשוניים עד כפל ב $\pm1,\pm i$.

מיהו ראשוני? מה הדרך ההגיונית להגדיר ראשוני? איך מוכיחים דבר כזה?

אז ככה, קודם כל ברור מה זה אומר ש $z\,|\,w$ לשני שלמים של גאוס – אם קיים שלם שלישי של גאוס α עבורו $\alpha z = w$ - או לחילופין $\frac{w}{z} \in \mathbb{Z}[i]$.

לדוגמא $\frac{5}{2+i} = 5 \cdot \frac{2-i}{2^2+1^2} = 2-i$ ולכן $(2+i)\,|\,5$.

מיהו מספר ראשוני? ניתן שתי הגדרות, אחת לאי-פריקות ואחת לראשוניות. צריך להוכיח שבמקרה של השלמים של גאוס ההגדרות שקולות:

1. שלם של גאוס α הוא אי-פריק אם השלמים היחידים שמחלקים אותו הם $\pm 1, \pm i, \pm \alpha, \pm i\alpha$.
2. שלם של גאוס α הוא ראשוני אם לכל $z, w \in \mathbb{Z}[i]$ עבורם $\alpha\,|\,zw$ מתקיים $\alpha\,|\,z$ או $\alpha\,|\,w$.

הטריק להוכיח שיש "פריקות יחידה" כמו המשפט היסודי של האריתמטיקה במקרה של השלמים של גאוס הוא להראות שיש מקבילה לאלגוריתם אוקלידס ולהשתמש בו להכל.

הוכחה 3

שוב, $p\,|\,m^2+1$ עבור $m \in \mathbb{Z}$ כלשהו.

אבל $m^2+1 = (m+i)(m-i)$ ו p לא מחלק את $m+i$ ולא את $m-i$. אז p לא ראשוני ולכן הוא פריק, כלומר יש שני מספרים שלמים של גאוס לא טריוויאלים שעבורם $\alpha\beta = p$. אבל $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$. כיוון ש α, β לא טריוויאלים אז $N(\alpha), N(\beta) > 1$. אז $N(\alpha) = p$. אבל זה אומר בדיוק ש-p סכום של ריבועים וסיימנו.

הוכחה 4 – אינבולוציה של צגייר

תחילה מה זאת אינבולוציה?

אינבולוציה תהיה פונקציה על קבוצה כלשהי שאחרי שתי הפעלות שלה מחזירה הכול למקום.

<u>דוגמאות:</u>

$f(x) = -x$, $f(z) = \overline{z}, z \in \mathbb{C}$, $f(x) = \frac{1}{x}, x \in \mathbb{R}^+$, כל שיקוף של המישור (דוגמה 2 היא מקרה פרטי), בין אוסף סופי של ילדים בכיתה ילדים מתחלקים לזוגות ומחליפים מקומות כל פעם שמוחאים כפיים, ועוד...

טענה

אם A קבוצה סופית, $f: A \to A$ אינבולוציה ו- $B = \{a \in A : f(a) = a\}$, אז $|B| \equiv |A| \bmod 2$.

<u>הוכחה:</u> תרגיל.

המשוואה של צגייר

בואו נביט על כל השלישיות (x, y, z) של מספרים שלמים חיוביים שפותרות את המשוואה $x^2 + 4yz = p$ כך ש $p \equiv 1 \bmod 4$ הוא הראשוני שאנו רוצים להראות שהוא סכום של ריבועים.

ודאי שאין אינסוף שלישיות כאלו כי $0 < x < \sqrt{p}, 0 < y < \frac{p}{4}, 0 < z < \frac{p}{4}$ ואלו מספרים שלמים.

כעת נגדיר שתי אינבולוציות על קבוצת הפתרונות של המשוואה הזאת:

<u>אינבולוציה ראשונה:</u> $f\left(x,y,z\right)=\left(x,z,y\right)$. היא ודאי שולחת כל פתרון לפתרון אחר כלשהו. נשים לב כי אם יש לאינבולוציה הזאת נקודת שבת זה מסיים את ההוכחה – נקבל פתרון מהצורה $\left(x,y,y\right)$ ואז $p=x^2+4y^2=x^2+\left(2y\right)^2$.

לכן מ.ל. כי יש נקודת שבת לאינבולוציה. מהטענה דלעיל אם יש כמות אי-זוגית של פתרונות סיימנו – חשבו למה.

<u>אינבולוציה שנייה:</u>
$$f\left(x,y,z\right)=\begin{cases}\left(x+2z,z,y-x-z\right), & \text{if } x<y-z\\ \left(2y-x,y,x-y+z\right), & \text{if } y-z<x<2y\\ \left(x-2y,x-y+z,y\right), & \text{if } x>2y\end{cases}$$

מה אנחנו צריכים להראות עכשיו?

א) שזאת אינבולוציה.
ב) שהיא שולחת פתרונות של המשוואה לפתרונות של המשוואה.
ג) שיש לה נקודת שבת יחידה מבין כל הפתרונות.

זה יוכיח כי יש כמות אי-זוגית של פתרונות ונסיים.

<u>אז נוכיח כי היא אינבולוציה:</u> $x,y,z\in\mathbb{Z}^+$

אם $x<y-z$, אנחנו מפעילים את אופציה 1, כלומר $\left(x+2z,z,y-x-z\right)=:\left(a,b,c\right)$ ו- $f\left(x,y,z\right)$ $a,b,c\in\mathbb{Z}^+$.

אזי $a=x+2z>2z=2b$ ולכן כשנפעיל שוב את f נצטרך להפעיל את אופציה 3 ונקבל:

$$f\left(f\left(x,y,z\right)\right)=f\left(a,b,c\right)=\left(a-2b,a-b+c,b\right)=\left(x+2z-2z,x+2z-z+y-x-z,z\right)=\left(x,y,z\right)$$

באופן דומה מראים גם להפעלה של קודם 3 (ואז 1) ולהפעלה כפולה של 2.

<u>שולחת פתרונות לפתרונות:</u>

$$\left(x+2z\right)^2+4z\left(y-x-z\right)=x^2+4xz+4z^2+4zy-4zx-4z^2=x^2+4yz$$

$$\left(2y-x\right)^2+4y\left(x-y+z\right)=4y^2-4yx+x^2+4yx-4y^2+4yz=x^2+4yz$$

$$\left(x-2y\right)^2+4\left(x-y+z\right)y=x^2-4xy+4y^2+4xy-4y^2+4yz=x^2+4yz$$

<u>נקודת שבת יחידה:</u>

פעולות 1 ו-3 מגדילות ממש או מקטינות ממש את הכניסה הראשונה ולכן לא ייתכן כי הפעלה שלהן מאפשרת נקודת שבת. פעולה 2 יכולה ליצור נקודת שבת:

$\left(2y-x,y,x-y+z\right)=\left(x,y,z\right)\Rightarrow x=y$.

אבל אז $p=x^2+4yz=x^2+4xz=x\left(x+4z\right)$. אזי $x\mid p$ אבל בטוח ש $0<x<p$ ולכן $x=1$.

לכן $p=1+4z$ ויש z יחיד שמקיים זאת. על כן השלישייה $\left(1,1,z\right)$ היא נקודת השבת היחידה והיא קיימת.

תרגול – משפט הריבועים של פרמה

1. <u>הוכחתו של אוילר</u>:
   א) הוכיחו כי אם a,b הם מספרים טבעיים שניתנים לייצוג כסכום של שני ריבועים אז גם ab סכום של שני ריבועים.
   <u>רמז</u>: נורמה של מכפלה של מספרים מרוכבים.
   ב) הוכיחו כי אם a סכום של שני ריבועים, p ראשוני שמחלק את a ו- p ניתן לייצוג כסכום של שני ריבועים אז $\frac{a}{p}$ ניתן לייצוג כסכום של שני ריבועים.
   ג) הוכיחו כי אם a סכום של שני ריבועים, b מחלק את a, ו- b אינו סכום של שני ריבועים אז ל- $\frac{a}{b}$ יש ראשוני שמחלק אותו שאינו סכום של שני ריבועים.
   ד) הוכיחו כי אם $\gcd(a,b)=1$ אז a^2+b^2 מתחלק רק בראשונים שהם סכום של ריבועים.
   ה) הוכיחו כי כל ראשוני מהצורה $p=4m+1$ ניתן להצגה כסכום של שני ריבועים.
2. בהינתן חוג $(A,+,\cdot,0,1)$ הוכיחו כי אם קיימים $0\neq a,b\in A$ כך ש $ab=0$ אז אין $c\in A$ כך ש $ca=1$.
3. יהיו $a,b,c,d\in\mathbb{Z}$. הוכיחו כי העובדה ש- $ax+by, cx+dy$ שלמים מבטיח כי x,y שלמים אם ורק אם $ad-bc=\pm1$.

4. יש גן בצורת עיגול עם רדיוס של קילומטר אחד. בגן יש עצים שמושתלים בקודקודים של רשת ריבועית עם צלע של מטר אחד (כולל הקודקודים שנמצאים על הקצה של הגן). אם מרחק מקודקוד של הרשת עד קצה של הגן קטן מרדיוס של עץ מסויים, אז העץ חורג מגבולות הגן. הקודקוד היחיד של הרשת בו אין עץ זה מרכז של הגן. רדיוס של כל עץ שווה למילימטר אחד. הוכח שתצפית ממרכז הגן חסומה לגמרי, כלומר, כל קרן שיוצאת משם חותך גזע איזשהו.

5*. יהיו $a,\ b,\ c$ – מספרים שלמים, ונתון בנוסף כי $a>0,\ ac-b^2=1$. הוכח כי למשוואה $ax^2+2bxy+cy^2=1$ יש פתרון שלם.

את שאלה 5 פתרו בשתי דרכים – באמצעות למת מינקובסקי ובאמצעות שקילות של תבניות ריבועיות.

6. הוכיחו כי לתבניות שקולות אותה דיסקרימיננטה והן מייצגות את אותם השלמים.
7. הוכיחו כי הנורמה היא כפלית - $N(zw)=N(z)N(w)$ לכל שני שלמים של גאוס.

נספחים

שדה

שדה הוא קבוצה F שבה יש שני איברים מיוחדים שונים שנקראים $0_F, 1_F$ ושתי פעולות בינאריות $+: F \times F \to F$, $\cdot: F \times F \to F$ כך שמתקיימים התנאים הבאים:

<u>תנאים על החיבור:</u>

1. אסוציאטיביות: לכל $x, y, z \in F$ מתקיים $x + (y + z) = (x + y) + z$.
2. ניטרלי לחיבור: לכל $x \in F$ מתקיים $x + 0 = 0 + x = x$.
3. קיום נגדי: לכל $x \in F$ קיים $(-x) \in F$ כך ש- $x + (-x) = (-x) + x = 0$.
4. קומוטטיביות (חילופיות): לכל $x, y \in F$ מתקיים $x + y = y + x$.

<u>תנאים על הכפל:</u>

1. אסוציאטיביות: לכל $x, y, z \in F$ מתקיים $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
2. ניטרלי לכפל: לכל $x \in F$ מתקיים $x \cdot 1 = 1 \cdot x = x$.
3. קיום הפכי: לכל $0 \neq x \in F$ קיים $x^{-1} \in F$ כך ש- $x \cdot x^{-1} = x^{-1} \cdot x = 1$.
4. קומוטטיביות (חילופיות): לכל $x, y \in F$ מתקיים $x \cdot y = y \cdot x$.

<u>תנאים משולבים:</u>

1. דיסטריביוטיביות (פילוג/הוצאת גורם משותף): לכל $x, y, z \in F$ מתקיים $x(y + z) = xy + xz$.

תחום שלמות עם יחידה

אם כל התנאים של שדה מתקיימים חוץ מתנאי 3 של כפל וגם מתקיים כי:

1. אין מחלקי אפס: לכל $0 \neq x, y \in F$ מתקיים $x \cdot y \neq 0$.

אז זהו תחום שלמות.

בעצם שדה הוא תחום שלמות שמקיים את תנאי 3 של כפל.

חוג

אם כל התנאים של שדה מתקיימים חוץ מאולי תנאים 2-4 של כפל (ואז מרחיבים את הדיסטריביוטיביות להיות משני הצדדים) אז נאמר כי המבנה הוא חוג. אתם צריכים זאת לשאלה 2 מהתרגול.