סיכומי הרצאות ותרגולים במבוא לתורת המספרים

חורף 2018, הטכניון

הרצאות ותרגולים של פרופסור משה ברוך

סוכמו על ידי אלעד צורני

עדכון אחרון 7 בנובמבר 2018

נפת להמר.

תוכן העניינים

1 מבוא **1**

1.1 רקע היסטורי . . . 1

1.2 חוגים וחוגים אוקלידיים . . . 1

1.2.1 חוגים כלליים . . . 1

1.2.2 חוגים אוקלידיים . . . 2

1.3 האלגוריתם של אוקלידס . . . 3

1.4 פירוק לראשוניים בחוג אוקלידי . . . 5

1.5 חוג השלמים הגאוסים $\mathbb{Z}[i]$ . . . 5

הקדמה

הבהרה

סיכומי הרצאות אלו אינם רשמיים ולכן אין כל הבטחה כי החומר המוקלד הינו בהתאמה כלשהי עם דרישות הקורס, או שהינו חסר טעויות. להיפך, ודאי ישנן טעויות בסיכום! אעריך אם הערות ותיקונים ישלחו אלי בכתובת דוא"ל tzorani.elad@gmail.com.
אלעד צורני.

ספרות מומלצת.

הספרות המומלצת עבור הקורס הינה כדלהלן.

Ireland and Rosen: A classical introduction to modern number theory

סילבוס

חוגים אוקלידיים, משפט השארית הסיני ושלמים גאוסים. שרשים פרימיטיביים, הדדיות ריבועית, סכומי גאוס, סכומי יעקובי. הדדיות מסדר שלוש, הדדיות מסדר ארבע, מספרים אלגבריים ושדות ריבועיים.
הסילבוס יכלול את הפרקים הבאים מספר הקורס: 1,34,5,6,8,9.

דרישות קדם

דרישת הקורס העיקרית הינה ידע של קורס מבוא בחבורות. נשתמש גם בידע מקורס בסיס בחוגים על חוגים אוקלידיים, ונניח את ההגדרות הבסיסיות. נחזור על נושא זה בתחילת הקורס.

ציון:

1. בוחן אמצע: 20% מגן.
2. שאלת תרגילי בית בבוחן 5% מגן.
3. שאלת תרגילי בית במבחן 5% מגן.
4. מבחן סופי.

פרק 1

מבוא

תורת המספרים נחלקת לשני תחומים עיקריים, תורת המספרים האלגברית ותורת המספרים האנליטית. אנו עוסקים בהקדמה לתורת המספרים האלגברית, ונדבר בקורס בין השאר על שדות מספרים אלגבריים. את תוצאות הקורס אפשר להכליל בתחום של תורת שדות מחלקה.

1.1 רקע היסטורי

הרצאה 1 24 באוקטובר 2018

בין שנת 1640 לשנת 1654, מתמטיקאי בשם פרמה[1] הסתכל על מספר שאלות בנוגע למספרים.

שאלה 1.1.1. אילו ראשונים p הם מהצורה

1. $x^2 + y^2$
2. $x^2 + 2y^2$
3. $x^2 + 3y^2$

כאשר $x, y \in \mathbb{Z}$?

פתרון. 1. פרמה ניסח את המשפט הבא

משפט 1.1.2. יהא p ראשוני אי־זוגי. קיימים שלמים x, y ש־$p = x^2 + y^2$ אם ורק אם $p \equiv 1 \pmod 4$.

2. נסו למצוא חוקיות לבד.

3. **משפט 1.1.3 (פרמה).** יהא $p \neq 3$ ראשוני. קיימים $x, y \in \mathbb{Z}$ כך ש־$p = x^2 + 3y^2$ אם ורק אם $p \equiv 1 \pmod 3$.

בין השנים 1729 ו־1772 אוילר[2] את שלושת המשפטים של פרמה. אוילר הוכיח את המשפטים בשני שלבים, הורדה descent והדדיות Reciprocity. אנחנו נשתמש בחוגים אוקלידיים עבור השלב הראשון, על מנת לפשט את ההוכחה.

1.2 חוגים וחוגים אוקלידיים

1.2.1 חוגים כלליים

ניתן מספר דוגמאות לחוגים.

דוגמאות.
- $\mathbb{Z}$
- $M_n(R)$ חוג מטריצות $n \times n$ מעל חוג R.
- חוג פולינומים $R[X]$ מעל חוג R.

בקורס זה נניח כי כל החוגים הינם קומוטטיביים עם יחידה וללא מחלקי אפס (כלומר אם $ab = 0$ אז $a = 0$ או $b = 0$).

הגדרה 1.2.1. חוג עם התכונות הנ"ל נקרא **תחום שלמות**.

יהא R חוג ויהיו $a, b \in R$.

הגדרה 1.2.2. נאמר כי a **מחלק את** b אם קיים $d \in R$ עבורו $ad = b$. אם כן, נסמן $a \mid b$.

[1] Pierre de Fermat
[2] Leonhard Euler

הגדרה 1.2.3. a הפיך אם $a \mid 1$.

הגדרה 1.2.4. $0 \neq a$ שאינו הפיך הוא **ראשוני** ב־R אם $a \mid bc$ גורר $a \mid b$ או $a \mid c$.

הגדרה 1.2.5. $0 \neq a$ שאינו הפיך נקרא **אי־פריק** אם $a = bc$ גורר כי b הפיך או c הפיך.

הגדרה 1.2.6. $a \equiv b \pmod{c}$ אם $c \mid (b-a)$.

טענה 1.2.7. אם a ראשוני, הוא אי פריק.

הוכחה. יהי a ראשוני ונכתוב $a = bc$. אז $a \mid bc$. לכן $a \mid b$ או $a \mid c$. אם $a \mid b$ קיים d עבורו $b = ad$. אז $a = adc$. לכן $a(1-dc) = 0$ ולכן $dc = 1$. לכן c הפיך. אחרת, $a \mid c$ ונקבל באותו אופן כי b הפיך. ■

1.2.2 חוגים אוקלידיים

הגדרה 1.2.8. חוג R יקרא **חוג אוקלידי** אם קיימת פונקצייה $N \colon R \setminus \{0\} \to \mathbb{N}_0$ כך שמתקיימות שתי התכונות הבאות.

1. אם $a, b \in R$ שונים מאפס, קיימים $q, r \in R$ כך שמתקיים $r = 0$ או $N(r) < N(a)$ וגם $b = qa + r$.
2. אם $a \neq 0$ וגם $a = bc$ כאשר b, c אינם הפיכים, אז $N(c), N(b) < N(a)$.

הערה 1.2.9. התכונה השנייה בהגדרה איננה הכרחית.

דוגמאות.
1. $\mathbb{Z}$ עם $N(x) = |x|$.
2. $k[X]$ פולינומים מעל שדה, עם $N(p(x)) = \deg(p)$.

הערה 1.2.10. חלוקה בחוג אוקלידי איננה יחידה. אם נדרוש גם $N(0) \leq N(r) < N(a)$ נקבל כי החלוקה תהיה יחידה.

נניח בקורס כי $|r| \leq \frac{|a|}{2}$. אפשר לדרוש זאת במקרה $r \geq 0$ כי אם $b = qa + r$ נחליף את r ב־$r - a$. נקבל $b = (q+1)a + (r-a)$ ואז

$$|r-a| = |a-r| = |a| - |r| \leq |a| - \left|\frac{a}{2}\right| = \left|\frac{a}{2}\right| .$$

באופן דומה נוכיח עבור המקרה $r < 0$.

טענה 1.2.11. בחוג אוקלידי R, כל אידאל הינו ראשי. כלומר, אם $I \leq R$ אידאל, הוא מהצורה $I = (d) = dR = \{dr \mid r \in R\}$ עבור $d \in R$.

הוכחה. נמצא ב־I איבר d עם נורמה מינימלית (כתרגיל) ואז נראה $I = (d)$. ניקח איבר $a \in I$, נכתוב $a = qd + r$. אז $r = 0$ כי לא ייתכן $N(r) < N(d)$. ■

הרצאה 2 25 באוקטובר 2018

הגדרה 1.2.12. יהא R חוג ויהיו $a, b \in \mathrm{R} \setminus \{0\}$. d נקרא **מחלק משותף גדול ביותר של** a**ו־**b אם מתקיימות התכונות הבאות.

1. $d \mid a, b$
2. אם $d' \in R$ מקיים $d' \mid a, b$ אז $d' \mid d$.

טענה 1.2.13. יהא R חוג אוקלידי ויהיו $a, b \in R$ שונים מאפס אז קיים מחלק משותף גדול ביותר ל־a ו־b.

הוכחה. יהיו $a, b \in R \setminus \{0\}$ ויהא $I = \langle a, b \rangle$ האידאל הנוצר על ידי a ו-b. לפי הטענה, יש ל־I יוצר d, ונראה כי זהו ממג"ב (מחלק משותף גדול ביותר) של a, b.

מחלק משותף: ניתן לכתוב $a = 1 \cdot a \in I$ לכן $d \mid b$. גם $b = 1 \cdot b \in I$ לכן $d \mid b$.

מקסימליות: אם $d' \mid b$ וגם $d' \mid b$. קיימים $x_1, y_1 \in R$ עבורם $d = x_1 a + y_1 b$. כעת $d' \mid a, b$ ולכן $d' \mid d$. ■

הגדרה 1.2.14. איברים $a, b \in R$ נקראים **חברים** אם קיים איבר הפיך $u \in R^{\times}$ עבורו $a = bu$.

הבחנה 1.2.15. חברות זה יחס שקילות.

טענה 1.2.16. יהיו $a, b \in \mathrm{R} \setminus \{0\}$ עם d, d' ממג"ב. אז d, d' חברים.

הוכחה. מהגדרת ממג"ב מתקיים $d \mid d'$ וגם $d' \mid d$. לכן יש x, y עבורם $d = xd'$ וגם $d' = yd$. נציב את השיוויון השני בראשון ונקבל $d = xyd$ לכן $xy = 1$ ונקבל כי x, y הפיכים. לכן d, d' חברים. ■

מסקנה 1.2.17. יהא d ממג"ב של $a, b \in \mathrm{R}$. קיימים $x, y \in R$ כך שמתקיים $d = xa + yb$.

מסקנה 1.2.18. נמצא ממג"ב אחד d' עבורו $(d) = \langle a, b\rangle$. d, d' חברים ולכן יוצרים את אותו האידאל $(d) = (d')$. לכן גם d' צירוף לינארי של a, b עם מקדמים ב־R.

דוגמה 1.2.19 (חוג השלמים הגאוסים). נגדיר $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

טענה 1.2.20. $\mathbb{Z}[i]$ חוג אוקלידי.

הוכחה. נזכיר כי בשלמים יש חלוקה עם שארית $b = qa + r$ עם התנאי $|r| \leq \frac{|a|}{2}$. נגדיר $N(a+bi) = a^2 + b^2 = |a+bi|^2$. יהיו $a + bi, c + di \in R$. נעשה חלוקה עם שארית ל־$a + bi, c + di$. מתקיים קודם כל

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i. \tag{1.1}$$

נחפש מספר ב־$\mathbb{Z}[i]$ קרוב ביותר למנה זאת. נעשה חלוקה עם שארית ב־$\mathbb{Z}$ במקום המקדמים במנה.

$$\begin{aligned} ac + bd &= x_1\left(c^2+d^2\right) + r_1 \\ bc - ad &= x_1\left(c^2+d^2\right) + r_2 \end{aligned}$$

כאשר $|r_i| \leq \frac{c^2+d^2}{2}$. נציב בנוסחה 1.1 ונקבל

$$\begin{aligned} \frac{a+bi}{c+di} &= \frac{x_1\left(c^2+d^2\right) + r_1 + \left(x_2\left(c^2+d^2\right)+r_2\right)i}{c^2+d^2} \\ &= x_1 + x_2 i + \frac{r_1 + r_2 i}{c^2+d^2} \end{aligned}$$

או לאחר כפל שני האגפים

$$a + bi = (x_1 + x_2 i)(c + di) + \frac{r_1 + r_2 i}{c^2+d^2}(c+di).$$

נטען כי זאת חלוקה עם שארית. יש להראות כי הביטוי $\frac{r_1+r_2i}{c^2+d^2}(c+di)$ שלם גאוסי וכי הנורמה שלו קטנה מזאת של $c + di$. אכן זהו שלם גאוסי כיוון שניתן לכתוב

$$\frac{r_1+r_2i}{c^2+d^2}(c+di) = a + bi - (x_1+x_2i)(c+di) \in \mathbb{Z}[i].$$

נשאיר את סיום ההוכחה כתרגיל. ■

תרגיל 1. הוכיחו את אי־השוויון הבא כדי לסיים את ההוכחה.

$$\left|\frac{(r_1+r_2)(c+di)}{c^2+d^2}\right|^2 < |c+di|^2$$

1.3 האלגוריתם של אוקלידס

תרגול 1
25 באוקטובר 2018

יהא R חוג אוקלידי ויהיו $a, b \in \mathrm{R} \setminus \{0\}$. האלגוריתם של אוקלידס מוצא ממג"ב של a ו־b.

אלגוריתם 1.3.1
1. נסמן $b = r_0$.
2. נכתוב $a = q_1 b + r_1$.
3. נחלק את r_{i-1} ב־r_i עם i מקסימלי. נכתוב $r_{i-1} = q_{i+1} r_i + r_{i+1}$.
נפסיק כשנקבל $r_{n+1} = 0$ ואז r_n הוא ממג"ב של a, b.

תרגיל 2. מצאו ממג"ב של 91 ו־35.

פתרון.

$$\begin{aligned} 91 &= 2\cdot 35 + 21 \\ 35 &= 1\cdot 21 + 14 \\ 21 &= 1\cdot 14 + 7 \\ 14 &= 2\cdot 7 + 0 \end{aligned}$$

לכן $\gcd(91, 35) = 7$.

תרגיל 3. מצאו את $\gcd\left(13+13i,-1+18i\right)$.

פתרון. נציג שני פתרונות.

1. נבצע חלוקה עם שארית. מתקיים

$$\frac{13+13i}{-1+18i}=\frac{17}{25}-\frac{19}{25}i \tag{1.2}$$

נבצע חלוקה עם שארית בשלמים.

$$\begin{aligned}17&=1\cdot 25+(-8)\\-19&=-1\cdot 25+6\end{aligned}$$

נציב ב־1.2 ונקבל

$$\frac{13+13i}{-1+18i}=\frac{28-8-25i+6i}{25}=1-i+\frac{-8+6i}{25}.$$

נכפול ונקבל

$$\begin{aligned}13+13i&=\left(1-i\right)\left(-1+18i\right)+\frac{-8+6i}{25}\left(-1+18i\right)\\&=\left(1-i\right)\left(-1+18i\right)+\left(-4-6i\right).\end{aligned}$$

כעת נחלק את $\left(-1+18i\right)$ בשארית $-4-6i$. יוצא

$$-1+18i=\left(-2-2i\right)\left(-4-6i\right)+3-2i.$$

מחלקים שוב $-4+6i=\left(-2i\right)\left(3-2i\right)+0$ ולכן $\gcd\left(13+13i,-1+18i\right)=3-2i$.

2. נזכיר טענה.

טענה 1.3.2. יהא $a+bi\in\mathbb{Z}[i]$. אם $N\left(a+bi\right)=a^2+b^2$ ראשוני ב־$\mathbb{N}$ אז $a+bi$ ראשוני ב־$\mathbb{Z}[i]$.

נפרק את $13+13i$ ואת $-1+18i$ למכפלות ראשוניים. מתקיים $13+13i=13\left(1+i\right)$ כאשר $N\left(1+i\right)=1^2+1^2=2$ ראשוני, לכן $1+i$ ראשוני. ניתן לכתוב $13=\left(2+3i\right)\left(2-3i\right)$ כאשר מהטענה זה פירוק לראשוניים. לכן

$$13+13i=\left(2+3i\right)\left(2-3i\right)\left(1+i\right)$$

פירוק לראשוניים.
נפרק את $-1+18i$. מתקיים

$$N\left(-1+18i\right)=1^2+18^2=325=5^2\cdot 13.$$

הנורמה אצלנו כפלית ולכן למחלקים נורמות בקבוצה $\left\{5,5^2,13\right\}$ (נפרט יותר בהרצאה). נחלק את $-1+18i$ ב־$2+3i$. יוצא

$$\left(-1+18i\right)=\left(2+3i\right)\left(1+2i\right)\left(2-i\right)$$

נקבל כי $2+3i$ הוא הגורם המשותף היחיד בפירוק לראשוניים עד־כדי חברות (לחברים יש אותה הנורמה) ולכן $\gcd\left(13+13i,-1+18i\right)=2+3i$.

משפט 1.3.3 (אוקלידס). יש אינסוף ראשוניים ב־$\mathbb{N}$.

הוכחה. נניח בשלילה שיש מספר סופי של ראשוניים $p_1,\ldots,p_k$ ונסמן $N=\left(\prod_{i=1}^k p_i\right)+1$. אם $p_i\in N$ אז $p_i\mid 1$ וזו סתירה לכך שיש ראשוני שמחלק את N. ■

תרגיל 4. יש ב־$\mathbb{N}$ אינסוף ראשוניים p שמקיימים $p\equiv 3 \pmod 4$.

פתרון. נניח שיש מספר סופי של ראשוניים $p_1,\ldots,p_k\equiv 3 \pmod 4$. ניקח $N=4\left(\prod_{i=1}^k p_i\right)-1$ ואז $p_i\nmid N$ לכל i. נפרק את N לראשוניים $N=\prod_{i=1}^m q_i$. אז קיים $q_i\equiv 3 \pmod 4$ כי אחרת

$$N\equiv\prod_{i=1}^m q_i\equiv\prod_{i=1}^m 1\equiv 1 \pmod 4$$

בסתירה. אבל $q_i\neq p_j$ לכל $j\in[k]$, בסתירה.

הגדרה 1.3.4. a,b **זרים** אם $\gcd(a,b)=1$.

משפט 1.3.5. נניח $\gcd(a,b)=1$ ויהא c מחלק משותף של a ו־b. אז $c \mid a,b$ ולכן $c \mid 1$, כלומר יש e עבורו $ce=1$ ולכן c הפיך.

טענה 1.3.6. $\gcd(a,b)=1$ אם ורק אם קיימים $x,y\in R$ עבורם $xa+yb=1$.

טענה 1.3.7. אם $\gcd(a,b)=1$, ראינו בהרצאה כי יש x,y כנדרש. להיפך, נניח שקיימים $x,y\in R$ כך שמתקיים $xa+yb=1$. אם $d \mid a,b$ אז $d \mid xa+yb=1$ לכן $d \mid 1$ ולכן 1 ממג"ב.

משפט 1.3.8. יהא R חוג אוקלידי. אם $p\in R$ הוא אי־פריק, אז p ראשוני.

הוכחה. נניח ש־p ראשוני אי־פריק ונוכיח כי הוא ראשוני. נניח ש־$p \mid ab$ וגם $p \nmid a$, ונראה $p \mid b$. נניח בשלילה ש־a,p אינם זרים ויהא $d \mid p,a$. קיים $c\in R$ עבורו $p=cd$. p אי־פריק, לכן c או d הפיכים. אם c הפיך, d חבר של p. אז $p \mid a$ בסתירה. אחרת, d הפיך ואז בבירור a,p זרים. כעת, יש $x,y\in R$ עבורם $xa+yp=1$. נכפול ונקבל $xab+ypb=b$ ומתקיים $p \mid ypb, xab$ כי $p \mid ab$. לכן $p \mid b$. ∎

1.4 פירוק לראשוניים בחוג אוקלידי

טענה 1.4.1. יהא R חוג אוקלידי ויהא $u\in R\setminus\{0\}$ כך ש־$N(u)=0$. אז $u\in R^\times$.

הוכחה. נחלק את 1 ב־u. מתקיים $1=qu+r$ כאשר $N(r)<0$ או $r=0$. אבל, לא ייתכן $N(r)<0$ לכן $r=0$ לכן $qr=1$ ולכן $r\in R^\perp$. ∎

טענה 1.4.2. יהי R חוג אוקלידי. נניח ש־$N(a)=1$ ו־$a\notin R^\perp$ אינו הפיך. אז a ראשוני.

הוכחה. נניח כי $a=bc$. נניח בשלילה ש־b,c שניהם אינם הפיכים. אז $N(b),N(c)<N(a)=1$. לכן $N(b)=N(c)=0$ ולכן b,c הפיכים, בסתירה. ∎

משפט 1.4.3. יהא R אוקלידי ויהא $a\in R\setminus\{0\}$ שאינו הפיך. אז קיימים ראשוניים (אי־פריקים) $p_1,\ldots,p_k\in R$ עבורם $a=p_1\cdot\ldots\cdot p_k$. כמו כן, אם קיימים ראשוניים $q_1,\ldots,q_m$ עבורם $a=q_1\cdot\ldots\cdot q_m$ אז $m=k$ ועד כדי שינוי סדר p_i חבר של q_i לכל i.

דוגמה 1.4.4. $(-3)(-5)=3\cdot 5=15$ אבל $-5,5$ חברים וגם $-3,3$ חברים.

הוכחה (עבור הקיום). נוכיח באינדוקציה על $N(a)$.

בסיס: אם $N(a)=0$, a הפיך ולכן הטענה נכונה באופן ריק. אם $N(a)=1$ ו־a אינו הפיך, הוא ראשוני.

צעד: אם a ראשוני (אי־פריק), סיימנו. אחרת קיימים $b,c\in R$ שאינם הפיכים המקיימים $a=bc$. אז $N(b),N(c)<N(a)$ ולכן מהנחת האינדוקציה קיימים פירוקים של b ושל c, שמכפלתם היא פירוק של a. ∎

טענה 1.4.5. יהיו $p_1,p_2\in R$ ראשוניים ונניח $p_2 \mid p_1$. אז p_1,p_2 חברים.

הוכחה. $p_2=p_1\cdot b$ עבור b כלשהו. כעת $p_2=p_1\cdot b$ ו־p_2 אי־פריק, לכן b הפיך. ∎

1.5 חוג השלמים הגאוסים $\mathbb{Z}[i]$

הערה 1.5.1. בחוג $\mathbb{Z}[i]$ הנורמה היא כפלית.

$$N(z_1z_2)=N(z_1)\,N(z_2)$$

כמו כן, אם $z=a+bi$ אז $N(z)=(a+bi)(a-bi)=z\cdot\bar{z}=|z|^2$. אם $z\in\mathbb{Z}[i]$ גם $\bar{z}\in\mathbb{Z}[i]$.

טענה 1.5.2. $z\in\mathbb{Z}[i]$ הפיך אם ורק אם $N(z)=1$.

הוכחה. אם z הפיך, יש $w\in\mathbb{Z}[i]$ עבורו $zw=1$. לכן $N(zw)=N(z)N(w)=1$ ולכן $N(z)=N(w)=1$ כי הנורמה מקבלת ערכים שלמים חיוביים.
לכיוון השני, $z\in\mathbb{Z}[i]$ מקיים $N(z)=1$ אם ורק אם $a^2+b^2=1$ עבור $z=a+bi$. לכן $z\in\{\pm1,\pm i\}$ וכל אלו הפיכים כי $1=(-1)^2=i\cdot(-i)$. ∎

טענה 1.5.3. יהא $p\in\mathbb{N}$ ראשוני ונניח שקיימים $x,y\in\mathbb{Z}$ עבורם $x^2+y^2=p$. אז p אינו ראשוני ב־$\mathbb{Z}[i]$.

הוכחה. $p=(x+iy)(x-iy)$ פרוק ב־$\mathbb{Z}[i]$ שאינו טריוויאלי כי

$$N(x+iy)=N(x-iy)=x^2+y^2=p\neq 1.$$ ∎

טענה 1.5.4. יהא $p \in \mathbb{N}$ ראשוני. אם $p \in \mathbb{Z}[i]$ אינו ראשוני, אז קיימים שלמים $x, y \in \mathbb{Z}$ עבורם $x^2 + y^2 = p$.

הוכחה. p אינו ראשוני ב־$\mathbb{Z}[i]$ לכן קיימים $z_1, z_2 \in \mathbb{Z}[i]$ שאינם הפיכים עבורם $p = z_1 z_2$. לכן

$$p^2 = N(p) = N(z_1 z_2) = N(z_1) N(z_2)$$

ולכן $N(z_i) \in \{1, p, p^2\}$ כי p ראשוני ב־$\mathbb{Z}$. אבל z_i אינם הפיכים לכן $N(z_i) = p$. נכתוב $z_1 = x + iy$ ואז $N(z_1) = x^2 + y^2 = p$.■

משפט 1.5.5 (אוילר 1729, הורדה). יהי $p \in \mathbb{N}$ ראשוני. אם קיימים $x, y, c \in \mathbb{Z}$ כך שמתקיים $\gcd(c, p) = 1$ וגם $x^2 + y^2 = cp$ אז קיימים $x_1, y_1 \in \mathbb{Z}$ עבורם $x_1^2 + y_1^2 = p$.

הוכחה. נניח ש־$x^2 + y^2 = cp$ עם $\gcd(c, p) = 1$. אז $(x + iy)(x - iy) = cp$. כלומר, מהטענה, צריך להוכיח ש־p אינו ראשוני ב־$\mathbb{Z}[i]$. נניח בשלילה שהוא כן ראשוני. ב־$\mathbb{Z}[i]$ מתקיים $p \mid (x + iy)(x - iy)$. לכן $p \mid (x + iy)$ או $p \mid (x - iy)$. בה"כ נניח $p \mid (x + iy)$. אז קיימים $n, m \in \mathbb{Z}$ עבורם $x + iy = p(n + mi) = pn + pmi$. אז $p \mid x, y$ ב־$\mathbb{Z}$. אז $p^2 \mid x^2 + y^2 = cp$ בסתירה לכך ש־$\gcd(c, p) = 1$. ■

מסקנה 1.5.6. יהי $p \in \mathbb{N}$ ראשוני. אז קיימים $x_1, y_1 \in \mathbb{Z}$ עבורם $x_1^2 + y_1^2 = p$ אם ורק אם קיימים $x, y \in \mathbb{Z}$ עבורם $x^2 + y^2 \equiv 0 \pmod{p}$ וגם $x, y \not\equiv 0 \pmod{p}$.

הוכחה. אם $p = x_1^2 + y_1^2$, נניח בה"כ $x_1, y_1 \geq 0$. אבל, p ראשוני ולכן $x_1, y_1 > 0$. כעת $0 < x_1, y_1 < p$ ולכן $x_1^2 + y_1^2 \equiv 0 \pmod{p}$ כאשר $x_1, y_1 \not\equiv 0 \pmod{p}$.
לכיוון השני, אם יש $x, y \in \mathbb{Z}$ עבורם $x^2 + y^2 \equiv 0 \pmod{p}$ וגם $x, y \not\equiv 0 \pmod{p}$, יש c עבורו $x^2 + y^2 = cp$. נניח בה"כ כי $0 < x, y < p$ ובעצם $-\frac{p}{2} < x, y < \frac{p}{2}$ כי ניתן להזיז ב־p. בפרט $x^2 + y^2 < 2 \cdot \frac{p^2}{4} = \frac{p^2}{2}$. כעת

$$x^2 + y^2 = cp$$

ולכן $1 \leq c < \frac{p}{2}$ ולכן $\gcd(c, p) = 1$. לכן מהשקילות יש $x_1, y_1 \in \mathbb{Z}$ עבורם $x_1^2 + x_2^2 = p$ כנדרש. ■

הרצאה 4 7 בנובמבר 2018

משפט 1.5.7 (אוילר). יהי $p \in \mathbb{N}$ ראשוני. אם קיימים $x, y, c \in \mathbb{Z}$ כך שמתקיים $\gcd(c, p) = 1$ וגם $x^2 + 2y^2 = cp$ אז קיימים $x_1, y_1 \in \mathbb{Z}$ עבורם $x_1^2 + 2y_1^2 = p$.

הוכחה. אותה הוכחה עבור משפט ההורדה של אוילר, כאשר נעבוד ב־$\mathbb{Z}\left[\sqrt{2}i\right]$. ■

משפט 1.5.8 (אוילר). יהי $p \in \mathbb{N}$ ראשוני. אם קיימים $x, y, c \in \mathbb{Z}$ כך שמתקיים $\gcd(c, p) = 1$ וגם $x^2 + 3y^2 = cp$ אז קיימים $x_1, y_1 \in \mathbb{Z}$ עבורם $x_1^2 + 3y_1^2 = p$.

מסקנה 1.5.9. עבור $k \in \{1, 2, 3\}$ יש פתרון למשוואה $x^2 + ky^2 \equiv 0 \pmod{p}$ עם $x, y \not\equiv 0 \pmod{p}$ אם ורק אם יש פתרון למשוואה $x^2 + ky^2 = p$.

עשינו רדוקציה למציאת ראשוניים מהצורות

$$x^2 + y^2$$
$$x^2 + 2y^2$$
$$x^2 + 3y^2$$

למציאת פתרונות $(a, b) \neq (0, 0)$ למשוואות

$$x^2 + y^2 \equiv 0 \pmod{p}$$
$$x^2 + 2y^2 \equiv 0 \pmod{p}$$
$$x^2 + 3y^2 \equiv 0 \pmod{p}.$$

עבור $k \in \{1, 2, 3\}$ מתקיים $x^2 + ky^2 \equiv 0 \pmod{p}$ אם ורק אם $x^2 = -ky^2$ אם ורק אם $\left(\frac{x}{y}\right)^2 = -k$. לכן הבעיה שקולה לבדיקת קיום שורש של $-k$ בשדה $\mathbb{F}_p$.

שאלה 1.5.10. עבור אילו p ראשוני ו־$a \in \mathbb{F}_p$, קיים $z \in \mathbb{F}_p$ עבורו $z^2 = a$?

בחוג $\mathbb{Z}[i]$ לקחנו את $\mathbb{Z}$ והוספנו שורש יחידה מסדר 4. נסתכל על שורשי יחידה מסדר 3. יהא $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{3}i}{2}$ ואז $\omega^2 = \bar{\omega} = \frac{-1-\sqrt{3}i}{2}$. ω שורש של הפולינום הציקלוטומי $\Phi_3(x) := x^2 + x^2 + 1$. מכך נובע כי $\bar{\omega} = \omega^2 = -1 - \omega$. מתקיים $\mathbb{Z}[\omega] = (a + b\omega)\, a, b \in \mathbb{Z}$ כי הוספנו שורש של פולינום אי־פריק ממעלה 2 (לחלופין, הדבר נובע מכך ש־$\omega^2 = 1 - \omega$).
מתקיים

$$a + b\omega = a + b\left(\frac{-1 + \sqrt{3}i}{2}\right) = a - \frac{b}{2} + \frac{b\sqrt{3}i}{2} \qquad (1.3)$$

טענה 1.5.11. יהיו $a,b,c,d\in\mathbb{Z}$. אם $a+b\omega=c+d\omega$ אז $a=c,b=d$.

הוכחה. נובעת מ־1.3. ■

משפט 1.5.12. $\mathbb{Z}\left[\omega\right]$ חוג אוקלידי.

הוכחה. נגדיר $N\left(z\right):=\left|z\right|^{2}$ ואז מתקיים

$$\begin{aligned}N(z)&=|z|^{2}\\&=|a+b\omega|^{2}\\&=(a+b\omega)\left(a+b\bar{\omega}\right)\\&=(a+b\omega)\left(a+b\omega^{2}\right)\\&=a^{2}+ab\omega+ab\omega^{2}+b^{2}\\&=a^{2}+ab\omega+ab\left(-1-\omega\right)+b^{2}\\&=a^{2}-ab+b^{2}\end{aligned}.$$

קיבלנו $N\left(a+b\omega\right)=a^{2}-ab+b^{2}$. נראה קיום של חלוקה עם שארית. יהיו $z_1,z_2\in\mathbb{Z}\left[\omega\right]$ ונרצה לחלק עם שארית $z_1=qz_2+r$. נסמן $\tilde{q}=\frac{z_1}{z_2}\in\mathbb{C}$ וניקח q את הנקודה הקרובה ביותר ב־$\mathbb{Z}\left[\omega\right]$. אם $r=0$ סיימנו. אחרת: אם מרחק המרכז של משולש עם צלעות באורך 1 מהקודקוד הוא x אז $x^{2}=\left(\frac{1}{2}\right)^{2}+\left(1-x\right)^{2}$ ולכן $x=\frac{5}{8}$. אז

$$N\left(q-\tilde{q}\right)\leq\frac{25}{64}$$

ואז

$$N\left(r\right)=N\left(z_1-qz_2\right)=N\left(\tilde{q}z_2-qz_2\right)=N\left(\tilde{q}-q\right)N\left(z_2\right)\leq\frac{25}{64}N\left(z_2\right)<N\left(z_2\right)$$

כנדרש. ■

טענה 1.5.13. $z\in\mathbb{Z}\left[\omega\right]$ הפיך אם ורק אם $N\left(z\right)=1$.

הוכחה. נניח כי z הפיך. אז יש w עבורו $zw=1$. אז $N\left(zw\right)=N\left(1\right)=1$ ולכן $N\left(z\right)N\left(w\right)=1$. מתקיים $N(z),N(w)\in\mathbb{N}$ ולכן $N(z)=N(w)=1$.
להיפך, נניח כי $N\left(z\right)=1$. נכתוב $z=a+b\omega$. אז

$$N\left(z\right)=N\left(a+b\omega\right)=\left(a+b\omega\right)\left(a+b\left(-1-\omega\right)\right)=\left(a+b\omega\right)\left(a-b-b\omega\right)=1.$$ ■

נרצה כעת למצוא את כל ההפיכים בחוג $\mathbb{Z}\left[\omega\right]$, כלומר כל האיברים מנורמה 1. נניח $z=a+b\omega\in\mathbb{Z}\left[\omega\right]$ מנורמה 1. אז $N\left(z\right)=a^{2}-ab+b^{2}=1$ ואז

$$\begin{aligned}\left(a-\frac{b}{2}\right)^{2}+\frac{3}{4}b^{2}&=1\\4\left(a-\frac{b}{2}\right)^{2}+3b^{2}&=4\\\left(2a-b\right)^{2}+3b^{2}&=4\end{aligned}$$

ונקבל ע"י מעבר על כל האפשרויות את הפתרונות הבאים.

$$(a,b)\in\left\{\left(0,1\right),\left(0,-1\right),\left(1,0\right),\left(1,1\right),\left(-1,0\right),\left(-1,-1\right)\right\}$$

מתקיים $-1-\omega=\omega^{2}$ לכן ההפיכים הם $\left\{\pm1,\pm\omega,\pm\omega^{2}\right\}$.