סיכומי הרצאות במבוא לתורת המספרים
חורף 2018, הטכניון

הרצאותיו של פרופסור משה ברוך
סוכמו על ידי אלעד צורני

נפת להמר.

עדכון אחרון 26 בדצמבר 2018

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
1.6 קונגרואנציות ב־$\mathbb{Z}$ 8
1.6.1 המשוואה $ax \equiv b \pmod{m}$ 9
1.6.2 הפיכים ב־$\mathbb{Z}/m\mathbb{Z}$ 9
1.7 המשוואה $x^k = a$ בחבורה ציקלית 13
1.8 הרמה של פתרונות ממודולו p למודולו p^k 14

2 הדדיות ריבועית **16**
2.1 אלגוריתם מילר־רבין לבדיקת ראשוניות 20

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.

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

בקורס זה נניח כי כל החוגים הינם קומוטטיבים 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 $a\left(1-dc\right)=0$ 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. $k\left[X\right]$ פולינומים מעל שדה, עם $N\left(p(x)\right) = \deg\left(p\right)$.

הערה 1.2.10. חלוקה בחוג אוקלידי איננה יחידה. אם נדרוש גם $N(0) \leq N(r) < N\left(a\right)$ 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 $b \mid d$. גם $b = 1 \cdot b \in I$ לכן $b \mid d$.

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

$$\begin{aligned}\frac{a+bi}{c+di}&=\frac{x_1\left(c^2+d^2\right)+r_1+\left(x_2\left(c^2+d^2\right)+r_2\right)i}{c^2+d^2}\\&=x_1+x_2i+\frac{r_1+r_2i}{c^2+d^2}\end{aligned}$$

או לאחר כפל שני האגפים

$$a+bi=(x_1+x_2i)(c+di)+\frac{r_1+r_2i}{c^2+d^2}(c+di).$$

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־השיוויון 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 $a=q_1b+r_1$.
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.

$$\begin{aligned}91&=2\cdot35+21\\35&=1\cdot21+14\\21&=1\cdot14+7\\14&=2\cdot7+0\end{aligned}$$

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.

$$17=1\cdot25+(-8)$$
$$-19=-1\cdot25+6$$

נציב ב־1.2 ונקבל

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

נכפול ונקבל

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

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

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

מחלקים שוב $-4+6i=(-2i)(3-2i)+0$ 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 $N(a+bi)=a^2+b^2$ ראשוני ב־$\mathbb{N}$ אז $a+bi$ ראשוני ב־$\mathbb{Z}[i]$.*

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

$$13+13i=(2+3i)(2-3i)(1+i)$$

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

$$N(-1+18i)=1^2+18^2=325=5^2\cdot13.$$

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

$$(-1+18i)=(2+3i)(1+2i)(2-i)$$

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 $p\equiv3\pmod4$.

פתרון. נניח שיש מספר סופי של ראשוניים $p_1,\ldots,p_k\equiv3\pmod4$. 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 $q_i\equiv3\pmod4$ כי אחרת

$$N\equiv\prod_{i=1}^{m}q_i\equiv\prod_{i=1}^{m}1\equiv1\pmod4$$

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. $15=3\cdot 5=(-5)(-3)$ 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 $p_1 \mid p_2$. 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.

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

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 $z \in \{\pm 1, \pm i\}$ וכל אלו הפיכים כי $(-1)^2=i\cdot(-i)=1$. ∎

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. $p=(x+iy)(x-iy)$ פירוק 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 $p=x^2+y^2$.*

הוכחה. p אינו ראשוני ב־$\mathbb{Z}[i]$ לכן קיימים $z_1,z_2\in\mathbb{Z}[i]$ שאינם הפיכים עבורם $p=z_1z_2$. לכן

$$p^2=N(p)=N(z_1z_2)=N(z_1)N(z_2)$$

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 $p=x^2+y^2=N(z_1)$. ■

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 $\omega^2=-1-\omega=\bar{\omega}$. 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

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

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. *$\mathbb{Z}[\omega]$ חוג אוקלידי.*

הוכחה. נגדיר $N(z) := |z|^2$ ואז מתקיים

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

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

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

ואז

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

כנדרש. ∎

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

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

$$N(z) = N(a + b\omega) = (a + b\omega)(a + b(-1 - \omega)) = (a + b\omega)(a - b - b\omega) = 1.$$ ∎

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

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

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

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

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

מסקנה 1.5.14 *(האקסיומה השנייה של הנורמה בחוג אוקלידי). אם $z_1, z_2, z_3 \in \mathbb{Z}[\omega]$ שונים מאפס וגם $z_3 = z_1 z_2$ כאשר z_1, z_2 אינם הפיכים, אז $N(z_1) < N(z_3)$ ו־$N(z_2) < N(z_3)$.*

טענה 1.5.15. *יהי $p \in \mathbb{N}$ ראשוני. קיימים $a, b \in \mathbb{Z}$ כך ש־$p = a^2 - ab + b^2$ אם ורק אם $p = p + 0\omega$ אינו ראשוני ב־$\mathbb{Z}[\omega]$.*

הערה 1.5.16. הטענה מקבילה לטענה המתאימה ב־$\mathbb{Z}[i]$. ניתן לכתוב $p = a^2 + b^2$ אם ורק אם p אינו ראשוני ב־$\mathbb{Z}[i]$. ב־$\mathbb{Z}\left[2\sqrt{i}\right]$ הטענה המקבילה תתקיים עבור $p = a^2 + 2b^2$ עם הוכחה אנלוגית.

הוכחה. **כיוון ראשון:** נניח שקיימים $a, b \in \mathbb{Z}$ עבורם $p = a^2 - ab + b^2$. אז $p = (a + b\omega)(a - b - b\omega)$ פירוק של p ב־$\mathbb{Z}[\omega]$ כי $a + b\omega$ ו־$a - b - b\omega$ אינם הפיכים[3], לכן p איננו ראשוני ב־$\mathbb{Z}[\omega]$.

[3] כי לכל a, b כך שאחד מהאיברים הנ"ל שווה לאחד ההפיכים בחוג, נקבל כי $a^2 - ab + b^2$ אינו ראשוני ב־$\mathbb{Z}$

כיוון שני: נניח כי $p = p + 0\omega$ אינו ראשוני ב־$\mathbb{Z}[\omega]$. אז קיימים $z_1, z_2 \in \mathbb{Z}[\omega]$ שאינם הפיכים, כך שמתקיים $p = z_1 z_2$. אז $p^2 = N(p) = N(z_1) N(n_2)$ לכן $N(z_1) = N(z_2) = p$. אז אם $z_1 = a + b\omega$ נקבל $N(z_1) = a^2 - ab + b^2 = p$. ■

משפט 1.5.17 (descent). *יהי $p \in \mathbb{N}$ ראשוני. אם קיימים שלמים $a, b, c \neq 0$ עבורם $a^2 - ab + b^2 = cp$ כאשר $(c, p) = 1$ אז קיימים שלמים $x, y \in \mathbb{Z}$ עבורם $x^2 - xy + y^2 = p$.*

הוכחה. נניח שקיימים $a, b, c \in \mathbb{Z}$ כך שמתקיים $a^2 - ab + b^2$ כאשר $(c, p) = 1$. אז $(a + b\omega)(a - b - b\omega) = cp$. נניח בשלילה כי $p + 0\omega$ ראשוני ב־$\mathbb{Z}[\omega]$. אז $p \mid a + b\omega$ או $p \mid a - b - b\omega$. נניח כי $p \mid a - b - b\omega$ ואז קיימים $c, d \in \mathbb{Z}$ עבורם

$$p(c + d\omega) = a - b - b\omega$$
$$pc + pd\omega = a - b - b\omega.$$

מטענה קודמת, יש שיוויון בין החלקים החופשיים ובין המקדמים של ω. לכן

$$pc = a - b$$
$$pd = -b$$

ולכן $p \mid a - b, b$ כלומר $p \mid a$. לכן $a^2 - ab + b^2 = cp \mid p^2$ כאשר זאת סתירה כי $(c, p) = 1$. ■

מסקנה 1.5.18. *יהי $o \in \mathbb{N}$ ראשוני. קיימים $x, y \in \mathbb{Z}$ עבורם $x^2 - xy + y^2$, אם ורק אם יש פתרון למשוואה $a^2 - ab + b^2 \equiv 0 \pmod{p}$ עם $a, b \not\equiv 0 \pmod{p}$.*

הערה 1.5.19. יש מסקנה דומה (עם הוכחה שקולה) עבור $p = x^2 + 3y^2$ אם ורק אם יש פתרון $x^2 + 3y^2 \equiv 0 \pmod{p}$ עבור $x, y \not\equiv 0 \pmod{p}$.

1.6 קונגרואנציות ב־$\mathbb{Z}$

הרצאה 5 13 בנובמבר 2018

אם רוצים לפתור את אחת המשוואות הבאות

$$x^2 + y^2 \equiv 0 \pmod{p}$$
$$x^2 + 2y^2 \equiv 0 \pmod{p}$$
$$x^2 + 3y^12 \equiv 0 \pmod{p}$$
$$x^2 - xy + y^2 \equiv 0 \pmod{p}$$

רוצים להסתכל על המשוואות בקונגרואנציה.

הגדרה 1.6.1 יהיו $a, b, m \in \mathbb{Z}$ עם $m \neq 0$. נאמר כי $a \equiv b \pmod{m}$ אם $m \mid b - a$.

טענה 1.6.2. *$\equiv$ הוא יחס שקילות.*

סימון 1.6.3. אם $a \in \mathbb{Z}$ אז $\bar{a}$ מחלקת השקילות של a. מתקיים $\bar{a} = a + \mathbb{Z}m$.

טענה 1.6.4. *יש בדיוק m מחלקות שקילות, והן $\bar{0}, \bar{1}, \ldots, \overline{m-1}$.*

סימון 1.6.5. אוסף מחלקות השקילות יסומן $\mathbb{Z}/m\mathbb{Z}$.

הערה 1.6.6. $\mathbb{Z}/m\mathbb{Z}$ הוא חוג שנקרא חוג השאריות מוד m ביחס לפעולות חיבור וכפל המוגדרות על ידי

$$\bar{a} + \bar{b} := \overline{a + b}$$
$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}.$$

טענה 1.6.7. *$\mathbb{Z}/m\mathbb{Z}$ שדה אם ורק אם m ראשוני.*

הערה 1.6.8. אם $x \in \mathbb{Z}$ ופותר את המשוואה $ax \equiv b \pmod{m}$ אז כל איבר ב־$\bar{x}$ הוא פתרון. ההוכחה ישירה על ידי הצבה. כלומר, אנחנו מחפשים מחלקות שקילות שפותרות את המשוואה. באופן דומה, אם נחליף את a באיבר $a_1 \in \bar{a}$ נקבל את אותם הפתרונות למשוואה. כנ"ל עבור b. כלומר, אנו מחפשים פתרונות ב־$\mathbb{Z}/m\mathbb{Z}$ למשוואה $\bar{a}x = \bar{b}$. זה נכון לכל משוואה בקונגרואנציה.

1.6.1 המשוואה $ax \equiv b \pmod{m}$

דוגמה 1.6.9. נסתכל על המשוואה $6x \equiv 9 \pmod{15}$. נניח ש־$m > 0$ ונניח ש־$a, b \in \mathbb{Z}$ ו־$a \neq 0$. נסמן ב־$d = (a,m)$ ויהא $0 <$ $a' = \frac{a}{d}$ ו־$0 < m' = \frac{m}{d}$.

טענה 1.6.10. *למשוואה $ax \equiv b \pmod{m}$ יש פתרונות אם ורק אם $d \mid b$.*
אם $d \mid b$ יש בדיוק d פתרונות.
אם x_0 הוא פתרון, אז הפתרונות האחרים הם $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)\, m'$.

הוכחה. **כיוון ראשון:** נניח שיש פתרונות ויהי $x_0 \in \mathbb{Z}$ פתרון. אז $ax_0 \equiv b \pmod{m}$ ולכן קיים $y_0 \in \mathbb{Z}$ עבורו $ax_0 - b = my_0$. אז $ax_0 - my_0 = b$. נתון $d \mid m, a$ לכן $d \mid b$.

כיוון שני: נניח כי $d \mid b$. קיימים $x_0', y_0' \in \mathbb{Z}$ כך שמתקיים $ax_0' - my_0' = d$. יהי $c = \frac{b}{d}$ ואז $c \cdot d = b$. לכן $ax_0' - my_0' c = dc$. יהי $x_0 = x_0' c$ ואז $ax_0 - my_0' c = b$ ומתקיים $ax_0 \equiv b \pmod{m}$ כנדרש. ■

תרגיל 5. כל שני פתרונות נבדלים בכפולה של m'.

דוגמה 1.6.11. נחזור לדוגמה מלמעלה, $6x \equiv 9 \pmod{15}$. מתקיים $d =: 3 = (6, 15)$. כאן $b = 9$ ומתקיים $3 \mid 9$ כלומר $d \mid b$ לכן מהטענה יש פתרונות. אנו יודעים שיש 3 פתרונות מודולו 15. $m' = \frac{m}{d} = 5$ לכן $x_0 = 4, x_1 = 9, x_2 = 14$ הם כל הפתרונות.

מסקנה 1.6.12. *אם a, m זרים, יש בדיוק פתרון אחד למשוואה $ax \equiv b \pmod{m}$. אם $p = m$ ראשוני ו־$a \equiv 0 \pmod{p}$, למשוואה $ax \equiv b \pmod{p}$ יש פתרון יחיד.*

1.6.2 הפיכים ב־$\mathbb{Z}/m\mathbb{Z}$

$a \in \mathbb{Z}/m\mathbb{Z}$ הוא הפיך ב־$\mathbb{Z}/m\mathbb{Z}$ אם ורק אם יש $b \in \mathbb{Z}/m\mathbb{Z}$ כך שמתקיים $ab = 1$, כלומר יש פתרון למשוואה $ax \equiv 1 \pmod{m}$. לפי הטענה, למשוואה יש פתרון אם ורק אם $d = (a,m)$ מחלק את 1, כלומר $d = 1$, ולכן קיבלנו ש־$\bar{a}$ הפיך. לכן $(a,m) = 1$. לכן, יש לנו בדיוק $\varphi(m)$ הפיכים ב־$\mathbb{Z}/m\mathbb{Z}$, כאשר $\varphi(m)$ מספר השלמים הזרים ל־m בין 1 ל־$m-1$.

דוגמה 1.6.13. ב־$\mathbb{Z}/12\mathbb{Z}$ ההפיכים הם $\{1, 5, 7, 11\}$.

הגדרה 1.6.14. יהי R חוג עם יחידה ונסמן ב־R^* את חבורת ההפיכים. זו חבורה לגבי כפל.

דוגמה 1.6.15. $\#\left(\mathbb{Z}/12\mathbb{Z}\right)^* = 4$.

משפט 1.6.16 (Euler). *אם $(a,m) = 1$ אז $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

משפט 1.6.17 (פרמה הקטן). *אם p ראשוני וגם $p \nmid a$ אז $a^{p-1} \equiv 1 \pmod{p}$.*

נרצה להבין את $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$. האם חבורות אלו ציקליות? אם לא, מה המבנה שלהן כמכפלה ישרה של חבורות ציקליות?

דוגמה 1.6.18. כל האיברים מסדר 2 מודולו 12 הם $5, 7, 11$. לכן, החבורה איננה ציקלית (אין איבר מסדר 4) ולכן זאת חבורת קליין.

דוגמה 1.6.19 (משפט השאריות הסיני). $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

דוגמה 1.6.20. נסתכל על המשוואה $x^2 + y^2 \equiv 3 \pmod{35}$. אם x_0, y_0 פתרון אז $35 \mid \left(x_0^2 + y_0^2 - 3\right)$. לכן $5 \mid \left(x_0^2 + y_0^3 - 3\right)$ וגם $7 \mid \left(x_0^2 + y_0^3 - 3\right)$. לכן $x_0^2 + y_0^2 \equiv 3 \pmod{5}, \pmod{7}$. לכן

$$
\begin{aligned}
x_0 &\equiv 2 \pmod{5} & \qquad x_0 &\equiv 3 \pmod{7} \\
y_0 &\equiv 2 \pmod{5} & \qquad y_0 &\equiv 1 \pmod{7}
\end{aligned}
$$

ולכן $x = 17, y = 22$ יפתרו את המשוואה $x^2 + y^2 \equiv 3 \pmod{35}$.

למה 1.6.21. *אם $a_1, \ldots, a_k$ זרים ל־m אז $a_1 \cdot \ldots \cdot a_k$ זר ל־m.*

הוכחה. נציג שתי הוכחות.

1. נראה שאם $(a,m) = 1$ ו־$(b,m) = 1$ אז $(ab, m) = 1$. נוכיח בדרך השלילה. נניח כי $(ab, m) \neq 1$, אז יש ראשוני p כך ש־$p \mid m, ab$. לכן $p \mid a$ או $p \mid b$. אבל, זו סתירה לכך ש־$(a,m) = 1$ ו־$(b,m) = 1$.[4]
2. $a_1, \ldots, a_k$ זרים ל־m לכן הפיכים ב־$\mathbb{Z}/m\mathbb{Z}$. אז $\prod_{i=1}^{k} a_i$ הפיך ב־$\mathbb{Z}/m\mathbb{Z}$. אבל, איבר זה הפיך אם ורק אם הוא זר ל־m. ■

[4] ההוכחה הכללית באינדוקציה

משפט 1.6.22 (משפט השאריות הסיני). *יהיו $m_1, \ldots, m_k$ שלמים כך ש־$(m_i, m_j) = 1$ עבור $i \neq j$. יהיו $b_1, \ldots, b_k \in \mathbb{Z}$. יהי $m = \prod_{i=1}^{k} m_i$. נסתכל על המשוואות $x \equiv b_i \pmod{m_i}$ לכל $i \in [k]$. למשוואות אלו תמיד יש פתרון, וכל שני פתרונות נבדלים בכפולה של m.*

הוכחה. נוכיח באינדוקציה על k.

בסיס: אם יש משוואה אחת $x \equiv b_1 \pmod{m_1}$ אז $x = b_1$ פתרון.

צעד: נניח שיש x_1 שלם הפותר את $x_1 \equiv b_i \pmod{m_i}$ לכל $i \in [k-1]$. נרצה שגם $x_1 \equiv b_k \,(m_k)$, אבל זה לא בטוח. אם לא, נחליף את x_1. יהי $m' = \prod_{i=1}^{k-1} m_i$. נסתכל על $x_1 + ym'$ כאשר $y \in \mathbb{Z}$. נרצה $x_1 + ym' \equiv b_k \pmod{m_k}$. לכן נחפש את y המתאים, כלומר נפתור $m'y = b_k - x_1 \,(m_k)$. מתקיים $(m_i, m_j) = 1$ לכל $i \neq j$ ולכן לפי הלמה m' זר ל־m_k. אז $(m', m_k) = 1$ ולפי הטענה יש פתרון. ■

תרגיל 6. כל שני פתרונות נבדלים בכפולה של m.

נחזור לדוגמה ממקודם.

$$x^2 + y^2 \equiv 3 \pmod{35} \qquad x^2 + y^2 \equiv 3 \pmod{5} \qquad x^2 + y^2 \equiv 3 \pmod{7}$$

דוגמה 1.6.23. ראינו כי

$$x_0 \equiv 2 \pmod{5} \qquad x_0 \equiv 3 \pmod{7}$$
$$y_0 \equiv 2 \pmod{5} \qquad y_0 \equiv 1 \pmod{7}$$

ולפי משפט השאריות הסיני, יש פתרון משותף. $5, 7 \mid x^2 + y^2 - 3$ ו־$5, 7$ זרים לכן $35 \mid x^2 + y^2 - 3$ ונקבל $x^2 + y^2 \equiv 3 \pmod{35}$.

מסקנה 1.6.24. *כדי לפתור משוואה בקונגרואנציה מספיק לפתור את המשוואה מודולו חזקות של ראשוניים.*

הגדרה 1.6.25. נניח כי $R_1, \ldots, R_n$ חוגים, ונגדיר

$$\bigoplus_{i=1}^{n} R_i := \{(r_1, \ldots, r_n) \mid \forall i \colon r_i \in R_i\}$$

עם חיבור וכפל לפי רכיבים. זהו חוג ונקרא ***הסכום הישר של*** R_i.

דוגמה 1.6.26. נסתכל על $\mathbb{Z}/7\mathbb{Z}$. מתקיים

$$5^2 = 25 \equiv 4 \pmod{7} \quad 5^3 = 5 \cdot 4 \equiv 6 \pmod{7} \quad 5^4 = 5 \cdot 6 \equiv 2 \pmod{7} \quad 5^5 = 5 \cdot 2 \equiv 3 \pmod{7} \quad 5^6 \equiv 1 \pmod{7}$$

לכן 5 יוצר של $\mathbb{Z}/7\mathbb{Z}$.

למה 1.6.27. *יהי K שדה ויהי $p(x) \in K[x]$ מדרגה n. אז ל־p לכל היותר n שורשים שונים.*

הוכחה. נניח בשלילה שיש $n+1$ שורשים שונים. באינדוקציה נקבל $p(x) = c\prod_{i=1}^{n}(x - \alpha_i)$ ואז לאחר הצבת α_{n+1} שום גורם לא מתאפס, בסתירה. ■

הרצאה 7 21 באוקטובר 2018

הערה 1.6.28. הכיוון השני של משפט פרמה נכון. אם $n \mid a$ לא מתקיים $a^{n-1} \equiv 1 \pmod{n}$. אבל, יש מספרים עבור אם $(a, n) = 1$ אז $a^{n-1} \equiv 1$. מספרים אלו נקראים מספרי Carmichael.

מסקנה 1.6.29. *יהיו $p_1, p_2 \in k[x]$ מתוקנים מדרגה n. אם $p_1(\alpha_i) = p_2(\alpha_i)$ עבור n איברים שונים $\alpha_1, \ldots, \alpha_n \in k$ אז $p_1 = p_2$.*

הוכחה. נסתכל על הפולינום $p(x) = p_1(x) - p_2(x)$. אז ל־p דרגה לכל היותר $n-1$. מתקיים $p(\alpha_i) = p_1(\alpha_i) - p_2(\alpha_2) = 0$ לכן יש n שורשים שונים, אבל דרגתו $n-1$ לכן הינו פולינום האפס. ■

טענה 1.6.30. *יהי p ראשוני. אז $x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod{p}$*

הוכחה. יהיו $f(x) = x^{p-1} - 1$ ו־$g(x) = (x-1)(x-2)\ldots(x-(p-1))$. אז לכל $a \in \mathbb{Z}_p^*$ מתקיים $f(a) = 0$ ממשפט פרמה וגם $g(a) = 0$ ומהמסקנה $f = g$. ■

משפט 1.6.31 (Wilson). $(p-1)! \equiv -1 \pmod{p}$.

הוכחה. נציב $x = 0$ בטענה. ■

תרגיל 7. אם $n > 4$ פריק אז $(n-1)! \equiv 0 \pmod{n}$.

טענה 1.6.32. *יהי p ראשוני ו־$d \in \mathbb{N}$ עבורו $d \mid p-1$. אז לפולינום $x^d - 1$ בדיוק d שורשים שונים מודולו p.*

הוכחה. יהא $m=\frac{p-1}{d}$ ואז $p-1=dm$. נקבל
$$\frac{x^{p-1}-1}{x^d-1}=\frac{\left(x^d\right)^m-1}{x^d-1}.$$
יהי $y=x^d$. אז
$$\frac{y^m-1}{y-1}=1+y+\ldots+y^{m-1}$$
ולכן
$$\frac{prsx^{dm}-1}{x^d-1}=\overbrace{1+x^d+\ldots+x^{(m-1)d}}^{g(x)}$$
ולאחר העברת אגפים
$$x^{p-1}-1=\left(x^d-1\right)g(x).$$
לפי הטענה, לפולינום $x^{p-1}-1$ יש $p-1$ שורשים שונים, לכן לפולינום x^d-1 יש d שורשים שונים. ■

תהי G אבלית מסדר n. נניח שלכל מחלק $d\mid n$ יש בדיוק d איברים ב־G שמקיימים $x^d=e$. אז ידוע מחבורות כי G חבורה ציקלית.

משפט 1.6.33. *$\mathbb{Z}_p$ ציקלית לכל p ראשוני.*

הוכחה. הראינו שלכל $d\mid p-1$ יש בדיוק d פתרונות למשוואה x^d-1 כלומר $x^d=1$. ■

נוכיח שאם $p\neq 2$ ראשוני אז $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ ציקלית לכל k. נתחיל עם המקרה $k=2$.
נסתכל על החבורה $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$. ראינו כי זאת ציקלית, ולכן יש לה יוצר g. הסדר של g הוא $p-1$. מתקיים $\#\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*=p^2-p$. לכן אם $p\nmid a$ אז $a^{p^2-p}\equiv 1\left(\mathrm{mod}\ p^2\right)$. גם g מקיים $g^{p^2-p}=1\left(\mathrm{mod}\ p^2\right)$. יהי $d=o(g)$ הסדר ב־$\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$. אז $p^2\mid g^d-1$ ולכן $p\mid g^d-1$ כלומר $g^d\equiv 1\left(\mathrm{mod}\ p\right)$. לכן $p-1\mid d$. גם $d\mid(p-1)p$ ולכן $d=p-1$ או $d=(p-1)p$. אם $d=(p-1)p$ סיימנו. אחרת נגדיר $g_1=g+p$.

טענה 1.6.34. *יהי g יוצר של החבורה $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ עבורו $g^{p-1}\equiv 1\left(\mathrm{mod}\ p^2\right)$. אז $g_1=g+p$ יוצר של $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$. כלומר, $g_1^{p-1}\not\equiv 1\left(\mathrm{mod}\ p^2\right)$.*[5]

הוכחה.
$$\begin{aligned}
g_1^{p-1}&=(g+p)^{p-1}\\
&=\sum_{k=0}^{p-1}\binom{p-1}{k}g^{p-1-k}p^k\\
&\equiv g^{p-1}+(p-1)\,g^{p-2}p\left(\mathrm{mod}\ p^2\right)\\
&\equiv 1+(p-1)\,g^{p-2}p\left(\mathrm{mod}\ p^2\right)\\
&\neq 1\left(\mathrm{mod}\ p^2\right)
\end{aligned}$$
■

מהטענה הוכחנו כי $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ ציקלית עבור $k=2$. נוכיח באופן כללי.
ניקח g יוצר של $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$ ונראה שהוא יוצר של $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$. אז g יוצר גם של $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$. אז $g^{p-1}=1+ap$ עם $(a,p)=1$ (כי $o(g)=p^2-p>p-1$ מודולו p^2). ניקח איבר מהצורה $1+ap$ ונמצא את הסדר שלו ב־$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$.

למה 1.6.35. *יהי p ראשוני ו־$1\leq k\leq p-1$ שלם. אז $p\mid\binom{p}{k}$.*

הוכחה.
$$\binom{p}{k}=\frac{p!}{k!\,(p-k)!}$$
כאשר $p\nmid k!,(p-k)!$. לכן $p\mid\binom{p}{k}$. ■

למה 1.6.36. *אם $j\geq 1$ ואם $a\equiv b\left(\mathrm{mod}\ p^j\right)$ אז $a^p\equiv b^p\left(\mathrm{mod}\ p^{j+1}\right)$.*

---

[5] כי ראינו שהסדר של g_1 צריך להיות $p-1$ או $p\,(p-1)$

הוכחה. מתקיים
$$a = b + cp^j$$
עבור $c \in \mathbb{Z}$. כעת
$$\begin{aligned} a^p &= \left(b + cp^j\right)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} b^{p-k} \left(cp^j\right)^k \\ &\equiv b^p + pb^{p-1}cp^j \\ &\equiv b^p + b^{p-1}cp^{j+1} \\ &\equiv b^p \left(\bmod\ p^{j+1}\right) \end{aligned}$$
כנדרש. ■

מסקנה 1.6.37. *אם $j \geq 2$ ו־$p \neq 2$ ראשוני אז $\left(1 + ap\right)^{p^{j-2}} \equiv 1 + ap^{j-1} \left(\bmod\ p^j\right)$.*

הרצאה 8 28 בנובמבר 2018

טענה 1.6.38. *לכל $j \geq 3$ מתקיים $5^{2^{j-1}} \equiv 1 + 2^{j-1} \left(\bmod\ 2^j\right)$.*

הוכחה. תרגיל, באינדוקציה. ■

מסקנה 1.6.39. *הסדר של 5 ב־$\left(\mathbb{Z}/2\mathbb{Z}\right)^*$ הוא 2^{j-2}.*

הוכחה. $5^{2^{j-2}} \equiv 1 + 2^j \left(\bmod\ 2^{j+1}\right)$ לכן $5^{2^{j-2}} = 1 + 2^j + a2^{j+1}$. אז $5^{2^{j-2}} \equiv 1 \left(\bmod\ 2^j\right)$. מצד שני, $5^{2^{j-3}} \equiv 1 + 2^{j-1} \left(\bmod\ 2^j\right)$ ובפרט $5^{2^{j-3}} \not\equiv 1 \left(\bmod\ 2^j\right)$. ■

משפט 1.6.40. *אם $k \geq 3$ אז*
$$\left\{ \left(-1\right)^a 5^b \;\middle|\; \substack{a \in \{0,1\} \\ b \in \left\{1, \ldots, 2^{k-2}\right\}} \right\}$$
היא חתך של $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$.

הוכחה. נניח כי $\left(-1\right)^{a_1} 5^{b_1} \equiv \left(-1\right)^{a_2} 5^{b_2} \left(\bmod\ 2^k\right)$ כאשר $a_1, a_2 \in \{0,1\}$, $b_1, b_2 \in \left\{1, \ldots, 2^{k-2}\right\}$ ו־$k \geq 3$. אז
$$\left(-1\right)^{a_1} 5^{b_1} \equiv \left(-1\right)^{a_2} 5^{b_2} \left(\bmod\ 4\right)$$
ולכן
$$\left(-1\right)^{a_1} \equiv \left(-1\right)^{a_2} \left(\bmod\ 4\right)$$
כלומר $a_1 = a_2$.[6] קיבלנו $5^{b_1} \equiv 5^{b_2} \left(\bmod\ 2^k\right)$. הסדר של 5 הוא 2^{k-2} לפי המסקנה. לכן השיוויון שקיבלנו גורר $b_1 = b_2$. מתקיים $\#\left(\mathbb{Z}/2^k\mathbb{Z}\right) = 2^{k-1}$ לכן אלו כל האיברים וזה אכן חתך. ■

מסקנה 1.6.41. *תהא C_n חבורה ציקלית מסדר n. קיבלנו שאם $k \geq 3$ אז $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong C_2 \times C_{2^{k-2}}$.*

הערה 1.6.42. $C_n \times C_m$ ציקלית אם ורק אם (n, m) זרים.
יהי $m = \prod_{i=1}^{r} p_i^{k_i}$ פירוק לראשוניים של m, אז
$$\left(\mathbb{Z}/m\mathbb{Z}\right)^* = \left(\mathbb{Z}\Big/\left(\prod_{i=1}^{r} p_i^{k_i}\right)\mathbb{Z}\right)^* \underset{\mathrm{CRT}}{\cong} \prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{k_i}\right)^*$$

מסקנה 1.6.43. *$\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ ציקלית אם m הוא 2, 4, p^k או $2p^k$ עבור $p \neq 2$.*

נזכיר את הניסוח האחרון שלנו לשאלות של פרמה. עבור $a \in \mathbb{Z}$ המקיים $\gcd\left(a, p\right) = 1$, האם יש פתרון למשוואה $z^2 \equiv a \left(\bmod\ p\right)$? ראינו כי $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ציקלית ולכן נסתכל על משוואות מהצורה $g^2 = a$ בחבורות ציקליות.

משפט 1.6.44. *תהי G חבורה ציקלית מסדר n. יהי $a \in G$.*

1. *אם n אי־זוגי, קיים x יחיד ב־G עבורו $x^2 = a$*
2. *אם n זוגי, קיים x ב־G כך ש־$x^2 = a$ אם ורק אם $a^{\frac{n}{2}} = 1$ ובמקרה זה יש בדיוק 2 פתרונות.*

[6] כי לקחנו $a_1, a_2 \in \{0,1\}$

הוכחה. נסתכל על ההומומורפיזם

$$\Phi\colon G\to G$$
$$x\to x^2$$

(זה הומומורפיזם כי G אבלית.)

1. אם n אי־זוגי, אין איבר מסדר שתיים לכן הגרעין של Φ טריוואלי, לכן ההעתקה חח"ע ולכן על.
2. אם n זוגי אז $\#\ker\Phi=2$.[7] אז $\#\operatorname{Im}\Phi=\frac{\#G}{\#\ker\Phi}=\frac{n}{2}$.
אם קיים x עבורו $x^2=a$, נעלה את שני האגפים בחזקת $\frac{n}{2}$ ואז $a^{\frac{n}{2}}=1$. אם $a^{\frac{n}{2}}=1$ אז a פתרון של $x^{\frac{n}{2}}=1$ ויש בדיוק $\frac{n}{2}$ פתרונות כאלה שהם $\operatorname{Im}\Phi$: אם $y\in\operatorname{Im}\Phi$ קיים $x\in G$ עבורו $x^2=y$ ואז $y^{\frac{n}{2}}=x^n=1$. לכן $a\in\operatorname{Im}\Phi$. ■

הגדרה 1.6.45 יהי $a\in\mathbb{Z}$ ויהי $m\in\mathbb{N}$. a הוא ***שארית ריבועית*** מודולו m אם קיים $x\in\mathbb{Z}$ עבורו $x^2\equiv a\pmod m$.

מסקנה 1.6.46 *יהי $p\neq 2$ ראשוני ויהי $a\in\mathbb{Z}$ עבורו $\gcd(a,p)=1$. אז a הוא שארית ריבועית מודולו p אם ורק אם $a^{\frac{p-1}{2}}\equiv 1\pmod p$.*

הוכחה. $\#\left(\mathbb{Z}/p\mathbb{Z}\right)=p-1=:n$ זוגי לכן יש פתרון למשוואה $x^2\equiv a\pmod p$ אם ורק אם $a^{\frac{n}{2}}=a^{\frac{p-1}{2}}\equiv 1\pmod p$. ■

מסקנה 1.6.47 *יהי $p\neq 2$ ראשוני. -1 הוא שארית ריבועית מודולו p אם ורק אם $p\equiv 1\pmod 4$.*

הוכחה. -1 שארית ריבועית מודולו p אם ורק אם $(-1)^{\frac{p-1}{2}}\equiv 1\pmod p$ אם ורק אם $\frac{p-1}{2}$ זוגי אם ורק אם קיים $k\in\mathbb{Z}$ עבורו $p-1=4k$ אם ורק אם $p\equiv 1\pmod 4$. ■

הערה 1.6.48 לכל a, $a^{\frac{p-1}{2}}$ איבר מסדר 2 מודולו p לכן הינו ±1.

דוגמה 1.6.49

$$(-3)^{\frac{4}{2}}=9\equiv -1\pmod 5$$

לכן -3 אינו שארית ריבועית מודולו 5.

דוגמה 1.6.50

$$(-3)^{\frac{6}{2}}=-27=-28+1\equiv 1\pmod 7$$

לכן -3 הינו שארית ריבועית מוולו 7.

דוגמה 1.6.51

$$(-3)^{\frac{11-1}{2}}=-3^5\equiv -1\pmod{11}$$

לכן -3 אינו שארית ריבועית מודולו 11.

1.7 המשוואה $x^k=a$ בחבורה ציקלית

משפט 1.7.1 *תהי G חבורה ציקלית מסדר n ויהי $a\in G$. נסתכל על המשוואה $x^k=a$.*

1. *אם $\gcd(k,n)=1$, קיים $x\in G$ יחידה עבורו $x^k=a$.*
2. *אם $k\mid n$ יהי $r=\frac{n}{k}$. קיים x ב־G כך ש־$x^k=a$ אם ורק אם $a^r=1$. אז יש בדיוק k פתרונות.*

הערה 1.7.2 כדי להוכיח את המשפט מסתכלים על ההומומרפיזם

$$\Phi\colon G\to G.\quad : x\to x^k$$

עשינו דבר דומה עבור $k=2$.

הוכחה. נציג הוכחה לחלק 2 של המשפט בלבד.
לכיוון אחד, נניח שקיים $x\in a$ עבורו $x^k=a$. אז

$$a^r=\left(x^k\right)^r=x^{k\frac{n}{d}}=x^{\frac{k}{d}n}=\left(x^{\frac{k}{d}}\right)^n=1.$$

להפך, נניח כי $a^r=1$ ונמצא $x\in G$ עבורו $x^k=a$. מההנחה, ומהסעיף הראשון, קיים $x\in G$ עבורו $x^d=a$. יש $\alpha,\beta\in\mathbb{Z}$ כך שמתקיים $\alpha k+\beta n=d$. אז

$$a=x^d=x^{\alpha k+\beta n}=\left(x^\alpha\right)^k\left(x^\beta\right)^n=\left(x^\alpha\right)^k$$

ולכן $a=y^k$ עבור $y=x^\alpha$. ■

דוגמה 1.7.4

[7] ראינו שבחבורה ציקלית למשוואה $x^d=1$ יש בדיוק d פתרונות לכל $d\mid n=\#G$

בהמשך נרצה להסתכל על המשוואות $x^3 \equiv a \pmod p$ ו־$x^4 \equiv a \pmod p$ כאשר $(a,p)=1$.

דוגמה 1.7.3 נסתכל על $k=3$ ועל $G=\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^*$.

1. אם $3 \nmid p-1$ מתקיים $(3,p-1)=1$ לכן $p \equiv 2 \pmod 3$ תמיד יש פתרון יחיד למשוואה $x3 \equiv a \pmod p$.
2. אם $3 \mid p-1$ אז $p \equiv 1 \pmod 3$. שליש מהאיברים הם חזקה שלישית כי $x^3 \equiv a \pmod p$ אם ורק אם $a^{\frac{p-1}{3}} \equiv 1 \pmod p$.

נסתכל על $x^4 \equiv a \pmod p$. נניח כי $p \not\equiv 2$ ואז $p-1$ זוגי. לכן $\gcd(4,p-1) \in \{2,4\}$. $p \equiv 1 \pmod 4$ אם ורק אם $4 \mid (p-1)$ ו־$p \equiv 3 \pmod 4$ אם ורק אם $2 \mid (p-1)$ ו־$4 \nmid (p-1)$. לכן לרבע מהאיברים יש שורש רביעי.

$$a^{\frac{p-1}{4}} \equiv 1 \pmod p \iff x^4 \equiv a \pmod p$$

1.8 הרמה של פתרונות ממודולו p למודולו p^k

טענה 1.8.1 *יהי* $p \neq 2$ *ראשוני ויהיו* a,k *זרים ל־*p. *אם יש פתרון למשוואה* $x^k \equiv a \pmod p$ *אז יש פתרון למשוואה* $x^k \equiv a \pmod{p^e}$ *לכל* $e \in \mathbb{N}_+$.

הוכחה. באינדוקציה על e.

בסיס: $e=1$ טריוויאלי.

צעד: נניח כי x_0 פתרון ל־$x^k \equiv a \pmod{p^e}$ ונמצא פתרון למשוואה $x^k \equiv a \left(\mathrm{mod}\ p^{e+1}\right)$. ניקח $x = x_0 + bp^e$. אז

$$.x^k = \left(x_0 + bp^e\right)^k = \sum_{i=0}^{k} x_0^i \left(bp^e\right)^{k-i} \equiv x_0^k + kx_0^{k-1}bp^e \left(\mathrm{mod}\ p^{e+1}\right)$$

ידוע מהגדרת x_0 כי $x_0^k = a + cp$ לכן

$$x^k \equiv a + cp^e + kx_0^{k-1}bp^e \left(\mathrm{mod}\ p^{e-1}\right) \equiv a + p^e\left(c + kx_0^{k-1}b\right) \left(\mathrm{mod}\ p^{e+1}\right)$$

ולכן צריך $c + \overbrace{kx_0^{k-1}}^{\alpha} \cdot \overbrace{b}^{y} \equiv 0 \pmod p$. כעת $\gcd(x_0,p)=1$ כי $x_0^k \equiv a \pmod{p^e}$ אבל a זר ל־p ולכן גם x_0. בנוסף, $\gcd(k,p)=1$ ולכן יש פתרון ל־$c + \alpha y \equiv 0 \pmod p$, כלומר, יש b עבורו $x = x_0 + b^e$, כנדרש. ∎

הרצאה 9 12 בדצמבר 2018

טענה 1.8.2 *יהי* a *אי־זוגי ויהי* $e \geq 3$. *למשוואה* $x^n \equiv 2 \pmod{2^e}$ *יש פתרון אם ורק אם מתקיים לפחות אחד התנאים הבאים.*

1. *n אי־זוגי*
2. *$a \equiv 1 \pmod 4$ ו־$a^{\frac{2^{e-2}}{d}} \equiv (2^e)$ כאשר $d = \gcd n, 2^{e-2}$*

הוכחה. *משתמשים במבנה של החבורה*

$$.\left(\mathbb{Z}/_{2^e\mathbb{Z}}\right)^* \cong C_2 \times C_{2^{e-2}}$$

∎

הגדרה 1.8.3 אם $\gcd(a,m)=1$ אז a ***שארית ריבועית מודולו*** m אם קיים $x \in \mathbb{Z}$ עבורו $x^2 \equiv a \pmod m$.

טענה 1.8.4 *יהי* $m = 2^e \prod_{i\in[k]} p_i^{e_i}$ *ונניח* $\gcd(a,m)=1$. *אז* a *שארית ריבועית מודולו* m *אם ורק אם מתקיימות שתי התכונות הבאות.*

1. *$a^{\frac{p_i-1}{2}} \equiv 1 \pmod{p_i}$ לכל $i \in [k]$.*
2. *אם $e=2$ אז $a \equiv 1 \pmod 4$. אם $e \geq 3$ אז $a \equiv 1 \pmod 8$.*

הוכחה. ממשפט השאריות הסיני, די לפתור $x^2 \equiv a \pmod{p_i}$ וגם $x^2 \equiv a \pmod{2^e}$.
נזכיר כי אם $\gcd(a,p)=1$ אז a שארית ריבועית מודולו p אם ורק אם $a^{\frac{p-1}{2}} \equiv 1$.
על מנת להמשיך את ההוכחה, ניעזר בהגדרה.
נסתכל כעת על p ראשוני אי־זוגי.

הגדרה 1.8.5 (סימן Legendre). יהיי $a \in \mathbb{Z}$ ויהי $p \neq 2 \in \mathbb{Z}$ ראשוני. נסמן $\left(\frac{a}{p}\right)$ ***סימן Legendre*** שערכו

- 1 אם a שארית ריבועית מודולו p
- -1 אם $\gcd(a,p)=1$ ו־a אינו שארית ריבועית מודולו p

- 0 אם $a \mid p$

משפט 1.8.6. *1.* $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3. אם $a \equiv b \pmod p$ אז $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

הוכחה. 1. אם a שארית ריבועית מודולו p ראינו $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ והגדרנו $\left(\frac{a}{p}\right) = 1$.

אם $a \mid p$ אז $a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod p$

אחרת, a אינו שארית ריבועית מודולו p ומהמשפט $c := a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. אז $c^2 = a^{p-1} \equiv 1 \pmod p$ לכן $c = -1$.[8] כלומר, $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$.

2. לפי הסעיף הקודם,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

3. לפי הסעיף הראשון,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod p.$$

■

סוף המשפט לא הוכח במהלך ההרצאות (ייתכן כי הינו מופיע ברשימות התרגולים). ■

[8] אנו מעל שדה, לכן יש שני פתרונות

פרק 2

הדדיות ריבועית

משפט 2.0.1 (הדדיות ריבועית). *יהיו p, q ראשוניים אי־זוגיים שונים.*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

מסקנה 2.0.2.

1. *-1 שארית ריבועית מודולו p אם ורק אם $p \equiv 1 \pmod 4$.*
2. *2 שארית ריבועית מודולו p אם ורק אם $p \equiv \pm 1 \pmod 8$.*
3. *אם $p \equiv 1 \pmod 4$ או $q \equiv 1 \pmod 4$ אז $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.*
אם $p \equiv 3 \pmod 4$ או $q \equiv 3 \pmod 4$ אז $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

הוכחה (של המסקנה). 1. אם $p \equiv 1 \pmod 4$ אז $p = 4k+1$ ואז $\frac{p-1}{2} = 2k$ ואכן $(-1)^{2k} = 1$.
אם $p \equiv \pm 3 \pmod 4$ אז $p = 8k+1$ ואז

$$\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k \in \mathbb{Z}$$

אחרת $p \equiv \pm 3 \pmod 8$ ואז $(-1)^{\frac{p^2-1}{8}} \equiv -1$ ואז $(-1)^{\frac{p^2-1}{8}} \equiv 1$. ■

ראינו בעצם כי עבור $a \in [3]$ יש פתרונו ל־$p = x^2 + ay^2$ אם ורק אם $\left(\frac{-a}{p}\right) = 1$.

משפט 2.0.3 (אוילר). *יהי $p \neq 2$ ראשוני. קיימים $x, y \in \mathbb{Z}$ עבורם $p = x^2 + 2y^2$ אם ורק אם $p \in \{1, 3\} \pmod 8$.*

משפט 2.0.4 (אוילר). *יהי $p \neq 3$ ראשוני. קיימים $x, y \in \mathbb{Z}$ עבורם $p = x^2 + 3y^2$ אם ורק אם $p \equiv 1\ mod 3$.*

הוכחה. נכתוב

$$\begin{aligned}\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)\\ &= \left(\frac{p}{3}\right)\end{aligned}$$

■

דוגמה 2.0.5.

$$\left(\frac{17}{47}\right) = \left(\frac{47}{17}\right) = \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$$

דוגמה 2.0.6. אם $x^2+5y^2=p$ אז $\left(\frac{-5}{p}\right)=1$ כאשר $p\neq 5$. באותו אופן עבור n כללי

$$x^2+ny^2=p$$

ולכן $\left(\frac{-n}{p}\right)=1$. נרצה לדעת מתי $\left(\frac{-5}{p}\right)=1$. מתקיים מהדדיות

$$\left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{5}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot\left(\frac{p}{5}\right).$$

לכן $1,4$ ריבועים מודולו 5 ו־$2,3$ אינם ריבועים מודולו 5. עתה $\left(\frac{-5}{p}\right)=1$ אם ורק אם מתקיים אחד המשפטים הבאים.

1. גם $p\equiv 1 \pmod 4$ וגם $p\equiv \pm1 \pmod 5$.
2. גם $p\equiv 3 \pmod 4$ וגם $p\equiv \pm 2 \pmod 5$.

לכן, לפי משפט השאריות הסיני, $p\equiv 1,3,7,9 \pmod{20}$ ולכן קיבלנו כי $\left(\frac{-5}{p}\right)=1$ אם ורק אם $p=1,3,7,9$.

משפט 2.0.7 (לגרנג'). *יהי p ראשוני שונה מ־5. קיימים $x,y\in\mathbb{Z}$ כך ש־$p=x^2+5y^2$, אם ורק אם $p\equiv 1,9 \pmod{20}$.*

הערה 2.0.8. מהמשפט, אם 5 שארית ריבועית מודולו 5, לא בהכרח פתרון מהצורה $x^2+5y^2=p$.
עבור $p\equiv 3,7 \pmod{20}$, לא ניתן להציג את p באמצעות x^2+5y^2.
נחשוב מה הסיבה לכך. עבור $x^2+ay^2=p$ עבדנו עם $\mathbb{Z}\left[\sqrt{-a}\right]$ אבל כאשר $a=5$ החוג אינו אוקלידי ואפילו אינו PID.

הגדרה 2.0.9. יהי b אי־זוגי חיובי ויהי $a\in\mathbb{Z}$. נניח כי $b=p_1\cdot\ldots\cdot p_k$ פירוק לראשוניים, ונגדיר את ***סימן יעקובי***

$$\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_k}\right).$$

הערה 2.0.10. אם b ראשוני, סימן יעקובי וסימן לז'נדר מזדהים.

הערה 2.0.11.
- סימן יעקובי מוגדר היטב, כי בפירוק של b לא מופיע 2, וסימן לז'נדר מוגדר עבור $p\neq 2$.
- אם b אינו ראשוני, $\left(\frac{a}{b}\right)$ אינו בהכרח בודק אם a שארית ריבועית מודולו b.

דוגמה 2.0.12. מתקיים

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=1$$

2 אינו שארית ריבועית מודולו 3 או מודולו 5 לכן $\left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right)=1$, אבל 2 אינו שארית ריבועית מודולו 5 כי אינו שארית ריבועית מודולו $3,5$.

הערה 2.0.13. מה שטוב בסימן יעקובי הוא שלא צריך לפרק את המספרים כפי שראינו בדוגמה עם $\left(\frac{17}{47}\right)$. נרצה להראות שלסימן יעקובי אותן תכונות של סימן לג'נדר, ובפרט הדדיות.

טענה 2.0.14.
1.

$$\left(\frac{a_1a_2}{b}\right)=\left(\frac{a_1}{b}\right)\cdot\left(\frac{a_2}{b}\right)$$

2.

$$\left(\frac{a}{b_1b_2}\right)=\left(\frac{a}{b_1}\right)\cdot\left(\frac{a}{b_2}\right)$$

3. אם $a_1\equiv a_2 \pmod b$ אז

$$\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$$

הוכחה. 1.

$$\begin{aligned}\left(\frac{a_1a_2}{b}\right)&=\left(\frac{a_1a_2}{p_1\cdot\ldots\cdot p_k}\right)\\&=\left(\frac{a_1a_2}{p_1}\right)\cdot\ldots\cdot\left(\frac{a_1a_2}{p_k}\right)\\&=\left(\frac{a_1}{p_1}\right)\left(\frac{a_2}{p_1}\right)\cdot\ldots\cdot\left(\frac{a_1}{p_k}\right)\left(\frac{a_2}{p_k}\right)\\&=\left(\frac{a_1}{p_1\cdot\ldots\cdot p_k}\right)\cdot\left(\frac{a_2}{p_1\cdot\ldots\cdot p_k}\right)\\&=\left(\frac{a_1}{b}\right)\cdot\left(\frac{a_2}{b}\right)\end{aligned}$$

2. מיידי מההגדרה.
3. אם ■

למה 2.0.15. *יהיו r, s אי־זוגיים. אז*

1.

$$\frac{rs-1}{2}=\frac{r-1}{2}+\frac{s-1}{2} \pmod 2$$

2.

$$\frac{r^2s^2-1}{8}=\frac{r^2-1}{8}+\frac{s^2-1}{8} \pmod 2$$

הוכחה. 1.

$$\begin{aligned}(r-1)(s-1) &\equiv 0 \pmod 4\\ rs-r-s+1 &\equiv 0 \pmod 4\\ rs-1 &\equiv r-1+s-1 \pmod 4\\ \frac{rs-1}{2} &\equiv \frac{r-1}{2}+\frac{s-1}{2} \pmod 2\end{aligned}$$

2.

$$\begin{aligned}\left(r^2-1\right)\left(s^2-1\right) &\equiv 0 \pmod{16}\\ r^2s^2-1 &\equiv r^2-1+s^2-1 \pmod{16}\\ \frac{r^2s^2-1}{8} &\equiv \frac{r^2-1}{8}+\frac{s^2-1}{8} \pmod 2\end{aligned}$$

■

מסקנה 2.0.16. *יהיו $r_!, \ldots, r_k$ אי־זוגיים. אז*

1.

$$\sum_{i\in[k]}\frac{r_i-1}{2}\equiv\frac{r_1\cdot\ldots r_k-1}{2} \pmod 2$$

2.

$$\sum_{i\in[k]}\frac{r_i^2-1}{8}\equiv\frac{r_1^2\cdot\ldots r_k^2-1}{8} \pmod 2$$

הוכחה. נוכיח את הסעיף הראשון באינדוקציה.

$$\sum_{i\in[k-1]}\frac{r_i-1}{2}\equiv\frac{r_1\cdot\ldots r_{k-1}-1}{2} \pmod 2$$

נגדיר $a=r_1\cdot\ldots\cdot r_{k-1}$ ואז מלמה 2.0.15 סעיף 1 נקבל

$$\frac{a-1}{2}+\frac{r_k-1}{2}\equiv\frac{ar_k-1}{2}\equiv\frac{r_1\cdot\ldots r_k-1}{2} \pmod 2$$

כנדרש.

את הסעיף השני נוכיח באותו אופן. ■

משפט 2.0.17. *יהי b שלם חיובי ואי־זוגי.*

1.

$$\left(\frac{-1}{b}\right)=(-1)^{\frac{b-1}{2}}$$

2.

$$\left(\frac{2}{b}\right)=(-1)^{\frac{b^2-1}{8}}$$

3. *אם* $a\neq 1$ *אי זוגי ו־*$(a,b)=1$ *אז*

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

הוכחה. 1.

$$\begin{aligned}\left(\frac{-1}{b}\right)&=\left(\frac{-1}{p_1}\right)\cdot\ldots\left(\frac{-1}{p_k}\right)\\&=(-1)^{\frac{p_1-1}{2}+\ldots+\frac{p_k-1}{2}}\\&\underset{\text{previous lemma}}{=}(-1)^{\frac{p_1\cdot\ldots\cdot p_k-1}{2}}\\&=(-1)^{\frac{b-1}{2}}\end{aligned}$$

2. באותה דרך כמו הסעיף הקודם.

3. נכתוב $a=q_1\cdot\ldots\cdot q_m$. מתקיים

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)&=\prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\\&=\prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\\&=(-1)^{\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\\&=(-1)^{\left(\sum_{i\in[k]}\frac{p_i-1}{2}\right)\left(\sum_{j\in[m]}\frac{q_j-1}{2}\right)}\\&\underset{\text{from corollary}}{=}(-1)^{\frac{p_1\cdot\ldots\cdot p_k-1}{2}\cdot\frac{q_1\cdot\ldots\cdot q_m-1}{2}}\\&=(-1)^{\frac{b-1}{2}\cdot\frac{a-1}{2}}\end{aligned}$$

■

דוגמה 2.0.18. נרצה לחשב את $\left(\frac{1001}{9907}\right)$.
דרך אחת היא פירוק $1001=7\cdot 11\cdot 13$ ואז חישוב כמכפלת סימני לג'נדר.
דרך נוספת היא עם סימן יעקובי.

$$\begin{aligned}\left(\frac{1001}{9907}\right)&=\left(\frac{9907}{1001}\right)\\&=\left(\frac{898}{1001}\right)=\left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right)\\&=(-1)^{\frac{1001^2-1}{8}}\left(\frac{449}{1001}\right)=\left(\frac{1001}{449}\right)\\&=\left(\frac{103}{449}\right)=\left(\frac{449}{103}\right)\\&=\left(\frac{37}{103}\right)=\left(\frac{103}{37}\right)\\&=\left(\frac{29}{37}\right)=\left(\frac{37}{29}\right)\\&=\left(\frac{8}{29}\right)=\left(\frac{4}{29}\right)\cdot\left(\frac{2}{29}\right)\\&=\left(\frac{2}{29}\right)\qquad=-1\end{aligned}$$

2.1 אלגוריתם מילר־רבין לבדיקת ראשוניות

יהי n שלם אי־זוגי. נרצה לדעת האם n ראשוני.
בעזרת אלגוריתם מילר־רבין ניתן לבדוק בהסתברות גבוהה האם מספר הינו ראשוני.
הרעיון הראשון הוא להשתמש במשפט פרמה. נגריל $1 < a < n-1$. אם $a^{n-1} \not\equiv 1 \pmod n$ אז n לא ראשוני. אז a נקרא "עד" לכך ש־n אינו ראשוני. אחרת, a איננו עד, אבל ייתכן עדיין כי n אינו ראשוני. ניקח $b \neq a$ ונבדוק האם $b^{n-1} \equiv 1$.
לרעיון זה יש בעיה, כי אם n מספר Carmichael אז אינו ראשוני אבל $a^{n-1} \equiv 1 \pmod n$ לכל a עבורו $\gcd(a,n)=1$.
כדי לתקן זה, נוסיף עוד עדים. אם $x^2 \equiv 1 \pmod n$ כאשר $x \not\equiv \pm 1 \pmod n$ אז n אינו ראשוני. כדי לבדוק זאת, אם n אי־זוגי ניתן לכתוב $n-1 = 2^d m$ כאשר m אי־זוגי. אז נכתוב $a^{n-1} = \left(\left((a^m)^2\right)^{\cdot^{\cdot^{\cdot}}}\right)^2$. אם קיבלנו בשלב מסוים 1 ובשלב לפניו לא קיבלנו ± 1, אז a הוא עד.

אלגוריתם 2.1.1. נתון n אי־זוגי.

1. נפרק $n-1 = 2^d m$ עבור m אי־זוגי.
2. נבחר a בין 2 ל־$n-1$ באופן אקראי.
3. נחשב $a^m \pmod n$. אם $a^m \equiv \pm 1 \pmod n$ נסיים ונחזיר כי n חשוד להיות ראשוני.
4. אם $a^m \not\equiv \pm 1 \pmod n$, נרשום $a^m \equiv b_0 \pmod n$ ונסתכל על הסדרה

   $b_0, b_1 = b_0^2, \ldots, b_{d-1} = b_{d-2}^2$.

   אם בשלב ה־ j כלשהו $b_j \equiv -11 \pmod n$, נחזיר כי n ראשוני. אחרת הוא בוודאות אינו ראשוני.

הערה 2.1.2. נרצה לחשב את a^m בצורה יעילה. נכתוב $2^\ell \le m < 2^{\ell+1}$ ונחשב $a^2, \ldots, a^{2^\ell}$ מודולו n. אז נכתוב את a^m כמכפלה של החזקות מלמעלה.

משפט 2.1.3. *אם $n > 9$ וקיבלנו בתהליך מילר־רבין ש־n ראשוני אז יש סיכוי של פחות מ־ $\frac{1}{2}$ ש־n אינו ראשוני.*

הערה 2.1.4. סיבוכיות האלגוריתם היא $\Theta\left((\log n)^3\right)$.

הערה 2.1.5. אם נחזור על התהליך עשר פעמים, נקבל שהסיכוי ש־n אינו ראשוני הוא $\frac{1}{1000000} \sim \left(\frac{1}{4}\right)^{10}$.

משפט 2.1.6. *יהי $a \in \mathbb{N}$ שלם שאינו ריבוע. יש אינסוף ראשוניים p עבורם a אינו שארית ריבועית.*

למה 2.1.7. *נכתוב $a = b^2 a'$. אם יש אינסוף ראשוניים p עבורם a' אינו שארית ריבועית, אז יש אינסוף ראשוניים עבורם a אינו שארית ריבועית.*

הוכחה. כתרגיל. ■

הוכחה (משפט). נכתוב $a' = 2^\alpha \prod_{i\in[n]} q_i$ כאשר $\alpha \in \{0,1\}$ ו־q_i ראשוניים.

מקרה א': $n \ge 1$. יהיו $\{\ell_i\}_{i\in[k]}$ ראשוניים אי־זוגיים ושונים מכל ה־q_i. נמצא פתרון למשוואות

$$\begin{aligned} \forall i \in [k] \colon x &\equiv 1 \pmod{\ell_i} \\ \forall i \in [n-1] \colon x &\equiv 1 \pmod{q_j} \\ x &\equiv s \pmod{q_n} \\ x &\equiv 1 \pmod 8 \end{aligned}$$

ולפי משפט השאריות הסיני, יש פתרון b. נחשב את $\left(\frac{a'}{b}\right)$. נכתוב $b = \prod_{i\in[m]} p_i$. אז

$$\left(\frac{a'}{b}\right) = \left(\frac{2^\alpha}{b}\right) \prod_{i\in[n]} \left(\frac{a_i}{b}\right) = \prod_{i\in[m]} \left(\frac{a'}{p_i}\right).$$

נחשב את $\left(\frac{a'}{b}\right)$ לפי הביטוי השמאלי. כיוון ש־$b \equiv 1 \pmod 8$, לפי משפט 1 $\left(\frac{2}{b}\right) = 1$. לכן לפי משפט $\left(\frac{q_1}{b}\right) = \left(\frac{b}{q_1}\right)$. אבל, b פתרון של $x \equiv 1 \pmod{q_1}$, לכן $\left(\frac{q_1}{b}\right) = \left(\frac{b}{q_1}\right) = \left(\frac{1}{q_1}\right) = 1$. באותו אופן לכל $i \in [n-1]$, ועבור n נקבל

$$\left(\frac{q_n}{b}\right) = \left(\frac{b}{q_n}\right) = \left(\frac{s}{q_n}\right) = -1$$

אם נבחר s שאינו שארית ריבועית מודולו q_n. לכן קיבלנו

$$-1 = \left(\frac{a'}{b}\right) = \prod_{i\in[m]} \left(\frac{a'}{p_i}\right)$$

ולכן קיים p_i עבורו $\left(\frac{a'}{p_i}\right) = -1$. כלומר, a' אינו שארית ריבועית מודולו p_i. נניח בשלילה שיש מספר סופי של ראשוניים $\{\ell_i\}_{i\in[k]}$ שבהם a' אינו שארית ריבועית, ומקבלים ראשוני חדש p_i שאינו שארית ריבועית, בסתירה. לכן יש אינסוף ראשוניים שבהם a' אינו שארית ריבועית. ■

הגדרה 2.1.8. $\alpha \in \mathbb{C}$ נקרא מספר אלגברי אם קיים פולינום $q(x) \in \mathbb{Q}[x]$ שונה מאפס עבורו $q(\alpha) = 0$.

הגדרה 2.1.9. $\alpha \in \mathbb{C}$ נקרא שלם אלגברי אם קיים פולינום מתוקן $q(x) \in \mathbb{Z}[x]$ עבורו $q(\alpha) = 0$.

טענה 2.1.10. *יהי $\alpha \in \mathbb{C}$ ויהי $p(x) \in \mathbb{Q}[x]$ פולינום אי־פריק. נניח כי $p(\alpha) = 0$. יהי $m(x) \in \mathbb{Q}[x]$ פולינום עבורו $m(\alpha) = 0$. אז $(x) \mid m(x)$.*

טענה 2.1.11. *אם $r \in \mathbb{Q}$ שלם אלגברי אז $r \in \mathbb{Z}$.*

טענה 2.1.12. *יהי $\alpha \in CC$ מספר אלגברי. אז יש פולינום אי־פריק מתוקן **יחיד** $p(x) \in \mathbb{Q}[x]$ עבורו $p(\alpha) = 0$.*

הגדרה 2.1.13. הפולינום היחיד מהמסקנה הנ"ל נקרא הפולינום המינימלי של α.

למה 2.1.14 (גאוס). *יהי $p(x) \in \mathbb{Z}[x]$ פולינום מתוקן ונניח כי $p(x) = q_1(x) q_2(x)$ כאשר $q_1(x), q_2(x) \in \mathbb{Q}[x]$ פולינומים מתוקנים. אז $q_1(x), q_2(x) \in \mathbb{Z}[x]$.*

טענה 2.1.15. *יהי $\alpha \in \mathbb{C}$ מספר אלגברי. אז α שלם אלגברי אם ורק אם הפולינום המינימלי $p_\alpha(x)$ שלו ב־$\mathbb{Z}[x]$.*

הוכחה. אם הפולינום המינימלי עם מקדמים שלמים, ברור כי α שלם אלגברי.
נניח ש־α שלם אלגברי, ונוכיח שהפולינום המינימלי שלו עם מקדמים שלמים.
אם α שלם אלגברי, קיים $m(x) \in \mathbb{Z}[x]$ מתוקן עבורו $m(\alpha) = 0$. לפי הטענה, $p_\alpha(x) \mid m(x)$, כלומר $m(x) = p_\alpha(x) q(x) \in \mathbb{Z}[x]$ ולפי הלמה של גאוס $p_\alpha(x) \in \mathbb{Z}[x]$. ■

דוגמה 2.1.16. $\mathbb{Q}[i]$ שדה בו כל המספרים אלגבריים. זה נובע מהלמה הבאה.

למה 2.1.17. *יהיו $r_1, r_1 \in \mathbb{Q}$, אז $x = r_1 + r_2 i$ מספר אלגברי.*

הוכחה. מתקיים

$$x^2 = r_1^2 - r_2^2 + 2r_1 r_2 i$$

וגם

$$\begin{aligned} x^2 - 2r_1 x &= r_1^2 - r_2^2 + 2r_1 r_2 i - 2r_1^2 - 2r_1 r_2 i \\ &= -r_1^2 - r_2^2 \end{aligned}$$

וקיבלנו שהפולינום

$$x^2 - 2r_1 x + r_1^2 + r_2^2$$

ב־$\mathbb{Q}[x]$ מאפס את $r_1 + r_2 i$. ■

דוגמה 2.1.18. נרצה למצוא את השלמים האלגבריים ב־$\mathbb{Q}[i]$. אם $r_2 = 0$ אז $x \in \mathbb{Q}$ שלם אלגברי. אחרת, $r_1 + r_2 i \notin \mathbb{Q}$ לכן הפולינום המינימלי שלו אינו מדרגה 1.

$$p_1(x) = x^2 - 2r_1 x + r_1^2 + r_2^2$$

לפי המשפט, $r_1 + r_2 i$ שלם אלגברי אם ורק אם $p_1(x) \in \mathbb{Z}[x]$. לכן הדרישה היא $-2r_1 \in \mathbb{Z}$ וגם $r_1^2 + r_2^2 \in \mathbb{Z}$. אז ניתן לכתוב $r_1 = \frac{m}{2}$ כאשר $m \in \mathbb{Z}$. נכתוב $r_2 = \frac{c}{d}$ שבר מצומצם. אז

$$r_1^2 + r_2^2 = \frac{m^2}{4} + \frac{c^2}{d^2} = \frac{d^2 m^2 + 4c^2}{4d^2} \in \mathbb{Z}$$

ואז

$$4d^2 \mid d^2 m^2 + 4c^2.$$

כלומר

$$d^2 \mid d^2 m^2 + 4c^2$$

ואז

$$d^2 \mid 4c^2$$

ואז $d^2 \mid 4$ ונקבל $d \in \{\pm 1, \pm 2\}$. לכן נכתוב $r_2 = \frac{c_1}{2}$ כאשר c_1 יכול להיות זוגי. נכתוב

$$r_1^2 + r_2^2 = \frac{m^2 + c_1^2}{4} \in \mathbb{Z}$$

כלומר $4 \mid m^2 + c_1^2$. אם m, c_1 אי–זוגיים, אז $m^2 + c_1^2 \equiv 2 \pmod 4$ בסתירה! אחרת m, c_1 זוגיים ולכן $r_1, r_2 \in \mathbb{Z}$.

טענה 2.1.19. *$\mathbb{Q}[\omega]$ הוא שדה בו כל האיברים הם מספרים אלגבריים. השלמים האלגבריים בתוך $\mathbb{Q}[\omega]$ הם $\mathbb{Z}[\omega]$.*

הוכחה. נכתוב $\alpha = r_1 + r_2\omega$. נחשב.

$$\begin{aligned}(x-\alpha)(x-\bar{\alpha}) &= (x-(r_1+r_2\omega))(x-(r_1+r_2\bar{\omega})) \\ &= (x-(r_1+r_2\omega))\left(x-\left(r_1+r_2\omega^2\right)\right) \\ &= x^2+\left(-2r_1-r_2\omega-r_2\omega^2\right)x+r_1^2-r_1r_2+r_2^2 \\ &= x^2+\left(-2r_1-r_2\left(\omega+\omega^2\right)\right)x+r_1^2-r_1r_2+r_2^2 \\ &= x^2+(-2r_1+r_2)x+r_1^2-r_1r_2+r_2^2 \in \mathbb{Q}[x]\end{aligned}$$

לכן α מספר אלגברי. אז $r_1 + r_2\omega$ שלם אלגברי אם ורק אם $r_1^2 - r_1r_2 + r_2^2 \in \mathbb{Z}$ וגם $-2r_1 + r_2 \in \mathbb{Z}$. במקרה זה

$$(r_2-2r_1)^2+3r_2^2 = 4\left(r_1^2+r_1r_2+r_2^2\right) \in \mathbb{Z}$$

ואז $3r_2^2 \in \mathbb{Z}$ ולכן $r_2 \in \mathbb{Z}$. נתון $-2r_1 + r_2 \in \mathbb{Z}$ לכן $-2r_1 \in \mathbb{Z}$ ונכתוב $r_1 = \frac{m}{2}$. אז

$$r_1(r_1-r_2) = \frac{m^2}{4} - \frac{mr_2}{2} \in \mathbb{Z}$$

ואפשר לקבל מכאן כי $r_1 \in \mathbb{Z}$. ■

טענה 2.1.20. *יהי α מספר אלגברי. אז $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.*

הוכחה. יהי $p(x) \in \mathbb{Q}[x]$ שאינו מתאפס ב־α, ונראה כי $\frac{1}{p(\alpha)} \in \mathbb{Q}[\alpha]$.
$p_\alpha(x)$ איננו פריק. מתקיים

$$\gcd(p(x), p_\alpha(x)) = 1 .$$

אז קיימים פולינומים $a(x), b(x) \in \mathbb{Q}[x]$ עבורם

$$a(x)p(x)b(x)p_\alpha(x) = 1$$

ולאחר הצבה נקבל $a(\alpha)p(\alpha) = 1$ כלומר $b(\alpha) = \frac{1}{p(\alpha)}$. ■

טענה 2.1.21. *יהי α אלגברי עם פולינום מינימלי מדרגה n. אז*

$$[\mathbb{Q}[\alpha]:\mathbb{Q}] = n$$

ובסיס ההרחבה הוא $1, \alpha, \ldots, \alpha^{n-1}$.

הוכחה. אם הוקטורים תלויים לינארית, נקבל פולינום שונה מאפס ממעלה קטנה מ־n המאפס את α. ע"י בידוד α^n מהמשוואה מקבלים כי α^n בשדה, ובאופן דומה אפשר להראות שהקבוצה פורשת. ■