תורת המספרים

חומרת הנשת תרגילים (באמצע הקורס יצוין כמה בדיוק, יהין ואולב שמא בדרך להגיש)

ציון - (1.5 תרגילים + 0.9 מהחן, מהחן) ומה

מרק וויס - barakw@Post.tau.ac.il

פירוק לגורמים ראשוניים

מוטיבציה - להבדיר הראשוניים, ולהוכיח שכל מבני יתן לפרק למכפלה של ראשוניים בצורה יחידה.
כדי להוכיח נשאת, נדון בשאלה כללי יותר על חוגים.

הגדרה - $A \supseteq \mathbb{C}$ נקראת תחום אם: היחו מכילה את 0 ואת 1
סגורה תחת חיבור, חיסור, וכפל
* - יש הגדרה יותר מופשטת, אנחנו נסתפק בדוגמאות זה

דוגמאות - $\mathbb{Z}$ - שלמים
- $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$: "השלמים האוסטיניים"
- אם $\mathbb{Z} \ni \alpha$ שאינו ריבוע של מספר שלם, נסמן ב- $\sqrt{\alpha}$ את אחד השורשים של α, ונסמן $\mathbb{Z}[\sqrt{\alpha}] = \{a+b\sqrt{\alpha} \mid a,b \in \mathbb{Z}\}$ (הערה - כל הדגמה כאלה היו יחידה)

הגדרה - A חוג, $a \in A$ נקרא הפיך אם $a \neq 0$, $a^{-1} \in A$.
קבוצת כל ההפיכים ב- A תסומן ב- A^*. הערה - A^* סגור לכפל, מכיל ± 1, ושאר פעולות הוספיים

דוגמאות - ב- $\mathbb{Z}$ ההפיכים הם $\{\pm 1\}$
- $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$
הוכחה: יהי $a+bi \in \mathbb{Z}[i]^*$.
מהגדרה - $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} \in \mathbb{Z}[i]$
מסגרת $a\left(\frac{a-bi}{a^2+b^2}\right) = \frac{a^2}{a^2+b^2} - \frac{ab}{a^2+b^2} i \in \mathbb{Z}[i]$
אלג $\frac{a^2}{a^2+b^2} \in \mathbb{Z}$
נהמתקיים רק אם $a=0$ או $b=0$.
נגיב ונראה שנקבע בדיוק את מה שנקבע ($\pm 1, \pm i$)
- נשתכע עם החוג $\mathbb{Z}[\sqrt{2}]$.
נראה שכל המספרים $\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}, n(1+\sqrt{2})\}$ הפיכים ב- $\mathbb{Z}[\sqrt{2}]$
הוכחה: $1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^* \rightarrow 1 = 1-2 = (\sqrt{2}+1)(\sqrt{2}-1)$
(מסקירות שפע, נקבע $\{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^* \mid a,b \in \mathbb{Z}, n(1+\sqrt{2})\}$)

הגדרה - A חוג. יהיו $a,b \in A$. נאמר ש- a מחלק את b ($a \mid b$) אם קיים $c \in A$ כך ש- $ac = b$

טענה - לכל $a \in A$, $a \mid \pm 1$
- לכל $a \in A$, ולכל $0 \neq b \in A$, $a \mid ab$
- כל איבר מחלק את 0, ו- 0 מחלק רק את עצמו
- אם $a \mid b$, ו- $b \neq 0$ אז $|a| \leq |b|$
- אם $a \mid b$ ו- $b \mid c$ אז $a \mid c$
- אם $a \mid b$, $a \mid c$, אז $a \mid ub+vc$ $\forall u,v \in A$
- אם $a \mid b$ אז $ac \mid bc$ $\forall c \in A$

תזכורת - נגדרת שירות מהגדרה

Scanned by CamScanner

הגדרה - A חוג, $a,b\in A$. נאמר ש- b מחלק של a אם יש $c\in A$ כך ש- $a=bc$.
- $a\in A$ נקרא אי-פריק אם $a\neq 0$, $a\notin A^*$, וכל מחלק של a הוא חבר של a או של 1.
- $a\in A$ נקרא ראשוני אם $a\neq 0$, $a\notin A^*$, $a|ab \Rightarrow a|b$ או $a|a$ $\forall a,b\in A$
* נוכיח בהמשך שמתלקים מהגדרות של אי-פריק וראשוני שקולות (כמו ב-$\mathbb{Z}$), אבל לא בכלל

טענה - יהי A חוג. אם $a\in A$ ראשוני אז a אי-פריק.
הוכחה: נניח ש-a ראשוני, ו-$a|$. צריך להוכיח ש-a חבר של 1 או של $a\in A^*$.
$a|$ קיים $b\in A$ כך ש- $ab=p \Rightarrow a|ab \Rightarrow a|p$ או $a|b$
במקרה ש-$a|p$ קיים $c\in A$ כך ש- $p=ac$
$a|b$ קיים $d\in A$ כך ש- $b=ad$ $\Rightarrow p=ab=a^2d \Rightarrow p\cdot d^{-1}=a^2\cdot d^{-1}=a$
a חבר של p, $d^{-1}\in A^*$
במקרה ש-$a|b$ קיים $c\in A$ כך ש- $b=pc$
$p=apc \Rightarrow apc=1 \Rightarrow a^{-1}=c \Rightarrow a$ הפיך

טענה - אם $A=\mathbb{Z}$, אזי כל $a\in A$ שונה מ-0,1 ואינו ב-A^*, אפשר לרשום במכפלה של אי-פריקים.

הוכחה - באינדוקציה על $|a|$, הטענה מתקיימת ב-$|a|=2$.
בסיס - $|a|=2 \Rightarrow a=\pm 2$ אי-פריק
מעבר - $|a|>2$, אם $|a|=2$ אז אפשר לרשום את a כמכפלת אי-פריקים
אחרת a פריק, אין מה להוכיח
$\Rightarrow a=bc \Rightarrow |a|=|b|\cdot|c| \Rightarrow |b|>1, |c|>1$
ובאופן דומה $|a|>|b|>1$
לפי הנחת האינדוקציה $b=b_1\cdot\ldots\cdot b_r$, b_i אי פריקים
$c=c_1\cdot\ldots\cdot c_s$, c_j אי פריקים
$a=b_1\cdot\ldots\cdot b_r c_1\cdot\ldots\cdot c_s$ מכפלה של אי-פריקים.

הגדרה - שני איברים שהפירוק שלהם כמכפלה של אי-פריקים הוא יחיד אם אפשר לרשום $a=a_1\cdot\ldots\cdot a_r$ כאשר a_i אי פריקים, ואם בכל שוויון מהצורה $a=b_1\cdot\ldots\cdot b_s$ ושלאחר שינוי סדר נקבל ש- a_i חבר של b_i, $r=s$.

טענה - נניח A חוג, בו כל מספר חלש מ-0 והפיכים אפשר לרשום כמכפלה של אי פריקים.
אזי הפירוק הוא יחיד $\Leftrightarrow$ כל אי-פריק ב-A הוא ראשוני

כעין ההוכחה - אינדוקציה על המינימלי של איברים אי פריקים, בהצגת a כמכפלת אי פריקים

$\Rightarrow$ יהי p אי-פריק, נוכיח ש-p ראשוני
נניח ש- $a,b\in A$ ו- $p|ab$, מלמ"ש $p|a$ או $p|b$
קיים $c\in A$ כך ש- $ab=pc$, נרשום את a,b,c כמכפלת אי פריקים:
$b=b_1\cdot\ldots\cdot b_k$, $a=a_1\cdot\ldots\cdot a_j$, $c=c_1\cdot\ldots\cdot c_i$
p (או a או b הפיכים, הטענה מיידית (מכפילים את שני האגפים בהופכי))
לפי הנחת האינדוקציה איבר ב-A כמכפלת אי-פריקים, קיים p' ש-$p|$ חבר של p, המופיע בפירוקו $a_1\cdot\ldots\cdot a_j\cdot b_1\cdot\ldots\cdot b_k$. למשל $a_1=p'$
$\Rightarrow$ וקיים $d\in A$ כך ש- $pd=p'$. אז:
$a=p'c=pdc \Rightarrow p|a$

Scanned by CamScanner

← אינדוקציה על האורך המינימלי של כתיבת a כמכפלה של ראשוניים.
כלומר - אינדוקציה על n, כך שקיימים $a_1 \dots a_n$ ראשוניים כך ש:
$a = a_1 \dots a_n$ ולכל הקיומים $a = a'_1 \dots a'_m$, $m \geq n$.

מקרה $n = 1$. a ראשוני. נניח ש- $a = a_1 \dots a_n$, a_i ראשוניים.
נוכיח ש- $n = 1$, $a = a_1$

$a = a_1 \cdot \underbrace{a_2 \dots a_n}_{b}$ ← $a \mid a_1 \dots a_n$. a ראשוני לכן ראשוני.

כלומר $a \mid a_1$. מאחר ש- a_1 ראשוני, a חבר של a_1, כלומר
יש $\varepsilon \in A^*$ כך ש- $a_1 = \varepsilon a$. אז $a = a\varepsilon b$.
אז $b\varepsilon = 1$ ← b הפוך. סתירה.

נניח שהאינדוקציה נכונה: כל $a \in A$ שיש לו n פירוקים $a_1 \dots a_n = a'_1 \dots a'_s$
n האורך המינימלי שלו מספיק את אי פרקים הבונים את a.

$a \mid a'_1 \dots a'_s$. a אי פריק ולכן הראשון. אז $a \mid a'_1$ או $a \mid a'_2 \dots a'_s$
אם $a \mid a'_1$ אז כמקודם a'_1 חבר של a. נצמצם ונמשיך בעזרת אינדוקציה.
אם $a \mid a'_2 \dots a'_s$, לכן, או ש- $a \mid a'_2$ וכך נמשיך כמו קודם,
או ש- $a \mid a'_3 \dots a'_s$. לבסוף מספר סופי שכזה, יהיה a'_j כך ש- $a \mid a'_j$

משפט - חלוקה עם שארית.
נתון $a, b \in \mathbb{Z}$, $a \neq 0$. אז יש $q \in \mathbb{Z}$, $0 \leq r < a$, $r \in \mathbb{Z}$ יחידים
כך ש: $b = aq + r$. (r נקראת השארית שמתקבלת בחלוקת b ב-a)

הוכחה - $x \in \mathbb{R}$. נסמן $L(x) = \max\{n \in \mathbb{Z} : n \leq x\}$ - הערך השלם של x
נסמן $q = L(\frac{b}{a})$. אז $q \in \mathbb{Z}$, $1 - \frac{b}{a} < q \leq \frac{b}{a}$
אז!
$b - a < aq \leq b$
נקח: $0 \leq r = b - aq < a$
יתכן כי: נניח ש- $b = aq_1 + r_1 = aq_2 + r_2$

נניח בשלילה $r_2 > r_1 \geq 0$. אז:
$r_2 - r_1 = aq_1 - aq_2$
$a \mid r_2 - r_1$

אבל $0 < r_2 - r_1 < a$. סתירה.

הגדרה - בהינתן $a, b \in \mathbb{Z}$. c יקרא **מחלק משותף** של a, b אם $c \mid a$ וגם $c \mid b$.
אוסף כל המחלקים המשותפים של a, b הוא קבוצה סופית.
המגדר הגדול ביותר בקבוצה זו נקרא המחלק המשותף הגדול ביותר: $\gcd(a,b)$
אם $\gcd(a,b) = 1$ נאמר ש- a, b **זרים**.

טענה - לכל $a, b \in \mathbb{Z}$, יש $k, l \in \mathbb{Z}$ כך ש- $\gcd(a,b) = ka + lb$

מסקנה - ב-$\mathbb{Z}$, כל אי פריק הוא ראשוני.

הוכחה - יהי p אי פריק ונניח $p \mid ab$, אך $p \nmid a$. צ"ל $p \mid b$.
$1 = \gcd(a,p) = ka + lp$ עבור $k, l \in \mathbb{Z}$
אז - $b = 1 \cdot b = (ka + lp)b = kab + lpb$
$p \mid lpb$ ← מתחלק ב-p

לכן $p \mid b$

נכיח את הטענה הנ"ל ב-2 דרכים שונות בעזרת הבאו

Scanned by CamScanner

טכניה שלכל $a,b\in\mathbb{Z}$ קיימים $k,l\in\mathbb{Z}$ כך ש- $\gcd(a,b)=ka+lb$

הוכחה 1 - נסמן $I=\{ka+lb \mid k,l\in\mathbb{Z}\}$

- נשים לב שהקבוצה סגורה לחיבור - $x,y\in I \to x+y\in I$

- וסגורה לכפל ב- $\mathbb{Z}$ - $x\in I,\ y\in\mathbb{Z} \to xy\in I$

(כלומר, I אידאל)

- יש $a,b\neq 0$, I מכילה חיובים, ו- I מכילה את a ואת b

נסמן - $c=\min\{x\in I \mid x>0\}$

נראה מיד כי $I=c\mathbb{Z}$

נסמן $d=\gcd(a,b)$, נראה ש- $c=d$

$x=ka+lb\in I$ שלם, $d\mid a$, $d\mid b$ $\to$ $d\mid x$

בפרט $d\mid c$ $\to$ $c\geq d$

מצד שני, $a\in I$ $\to$ $c\mid a$

ולפי $I=c\mathbb{Z}$ $b\in I$ $\to$ $c\mid b$ $\to$ $d\geq c$ $\to$ $c=d$

$I\supseteq c\mathbb{Z}$ $\leftarrow$ $\forall x\in\mathbb{Z}.\ cx\in I$ $\leftarrow$ $c\in I$

נקח $x\in I$, כדי להראות ש- x כפולה של c, נצטרך למצוא q,r מהצורה:
$x=cq+r$, $0\leq r<c$ $\leftarrow$ $r=x-cq\in I$ מהצורה לעיל

אז קיים $c\in\mathbb{Z}$ כך ש- $x=cq$, אז $r=0$

אז קיים $c\in\mathbb{Z}$ כך ש- $I\supseteq c\mathbb{Z}$.

ומהכלה דו כיוונית $I=c\mathbb{Z}$.

מסקנה - אם $d=\gcd(a,b)$ ו- n מתקיים משותף של a,b אז $n\mid d$

הוכחה - $d=ka+lb$. אם $n\mid a$ ו- $n\mid b$ אז $n\mid d$

הוכחה 2 - האלגוריתם האוקלידי למציאת $\gcd(a,b)$.

בה"כ $a>0$. נסמן $r_0=a, r_{-1}=b$. נבצע חלוקה עם שארית:

$$b=q_0a+r_1 = q_0r_0+r_1 \qquad a=r_0,\ r_1\geq 0,\ r_1<r_0$$

$$r_0=q_1r_1+r_2 \qquad r_1,r_2\geq 0$$

ממשיכים. בצעד ה- j: $r_{j-1}=q_jr_j+r_{j+1}$ $\qquad r_j,r_{j+1}\geq 0$

ממשיכים עד שמקבלים שארית 0. נסמן יש k שמתקיים $r_{k+1}=0$ ו- $r_k\neq 0$.

טענה - $r_k=\gcd(a,b)$

הוכחה - נכיח ש- $\gcd(r_{j-1},r_j)=\gcd(r_j,r_{j+1})$ $(0\leq j\leq k)$

ואז - $\gcd(a,b)=\gcd(r_1,0)=\dots=\gcd(r_k,r_{k+1})=\gcd(r_k,0)=r_k$

$r_{j-1}=q_jr_j+r_{j+1}$ $\hookrightarrow$ $r_{j+1}=r_{j-1}-q_jr_j$

Scanned by CamScanner

דוגמה לאלגוריתם אוקלידס:

המחלקים המשותפים: $\pm\{3, 5, 15\}$

$a = 270$, $b = -105$

$a = 270 = r_0$, $b = r_{-1} = -105$

$b = q_0 a + r_1$

$270 = 1 \cdot 165 + 105 \rightarrow r_0 = 270$, $r_1 = 165$

$165 = 1 \cdot 105 + 60 \rightarrow r_2 = 105$

$105 = 1 \cdot 60 + 45 \rightarrow r_3 = 60$

$60 = 1 \cdot 45 + 15 \rightarrow r_4 = 45$

$45 = 3 \cdot 15 + 0 \rightarrow 15 = gcd(270, -105)$

נוסח מטריציוני של אלגוריתם אוקלידס

צורת הנוסחא $r_{j+1} + r_j = q_j r_{j-1}$ אפשר לרשום:

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_j \end{bmatrix} \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix}$$

מטריצה הפיכה בשלמים.

Scanned by CamScanner