תרגול מס' 1

3 בנובמבר 2012

1 מערכת המספרים השלמים

בשיעור הקרוב אנו נעסוק בקבוצת המספרים השלמים $\mathbb{Z}$ עם הפעולות $(+)$ ו $(\cdot)$, ויחס סדר $(<)$ או $(\leq)$. כל התכונות הרגילות והידועות של השלמים מתקיימות: חוק הקיבוץ (אסוציאטיביות), חוק החילוף, חוק הפילוג (דיסטריביוטיביות) וכן הלאה. נעבור לפתח כמה תכונות ומשפטים שיהיו כלים חיוניים להמשך הקורס.

הגדרה 1.1 קבוצת המספרים הטבעיים $\mathbb{N}$ היא $\{z \in \mathbb{Z} : 0 \leq z\}$.

נעבור לדון בכמה תכונות.

1.1 עקרון הסדר הטוב

משפט 1.2 עקרון הסדר הטוב: לכל תת־קבוצה לא ריקה של מספרים טבעיים קיים איבר מינימלי (או איבר ראשון).

מעקרון הסדר הטוב נובע משפט האינדוקציה המוכר לכם מהקורס במתמטיקה בדידה ומבית־הספר התיכון.

משפט 1.3 אינדוקציה על הטבעיים: תהי $A \subseteq \mathbb{N}$ כך ש־$0 \in A$ וכן לכל $a \in \mathbb{N}$, אם $a \in A$, אז $a + 1 \in A$. אזי $A = \mathbb{N}$.

הוכחה: נניח בשלילה $A \neq \mathbb{N}$. אזי הקבוצה $\{n \in \mathbb{N} : n \notin A\}$ אינה ריקה. לפי עקרון הסדר הטוב קיים בה איבר ראשון, b. b הוא טבעי שונה מאפס, ולכן גם $b - 1$ הוא טבעי. אזי $b - 1 \in \mathrm{A}$, לכן לפי הנחת המשפט $A \ni b = 1 + (b - 1)$. סתירה. ■

1.2 יחס חלוקה

הגדרה 1.4 עבור $a, b \in \mathbb{Z}$ אנו אומרים ש־a מחלק את b ומסמנים $a|b$ אם קיים $c \in \mathbb{Z}$ כך שמתקיים $ac = b$.

דוגמא: 2 אינו מחלק את 5, אבל 17 מחלק את 34.

ניתן לבדוק שהיחס $|$ הינו סדר חלקי על $\mathbb{N}$. (שימו לב: הטענה הזו עוסקת בטבעיים ולא בשלמים! עבור השלמים יחס חילוק אינו יחס סדר).

תכונות:

1. $a|b \wedge a|c \implies a|(b+c)$
2. $a|b \wedge b|c \implies a|c$
3. $(a|b) \wedge (b \neq 0) \implies |a| \leq |b|$. עבור שלמים חיוביים, היחס $|$ הינו תת־יחס של $\leq$.

2 אוקלידיות ואלגוריתם אוקלידס

2.1 אוקלידיות

משפט 2.1 לכל $a,b \in \mathbb{Z}$ קיימים $q \in \mathbb{Z}$ ו־$r \in \mathbb{N}$ כך ש־$r < |b|$ ו־$a = bq + r$.

במילים אחרות, ניתן לבצע חילוק עם שארית. מצאו דוגמאות באופן עצמאי!

2.2 מחלק משותף מקסימלי (gcd).

הערה מתודית: בשיעור התרגיל אנו נעסוק ביחס החלוקה בין מספרים טבעיים בלבד. ניתן להרחיב בקלות את כל ההגדרות גם למקרה של השלמים. נפתח בהגדרה המקובלת.

הגדרה 2.2 יהיו $a,b \in \mathbb{N}$ (לא שניהם 0). אנו נאמר ש־d הוא המחלק המשותף המקסימלי שלהם ונסמן $d = \gcd(a,b)$ אם $d|a \wedge d|b$ ולכל $n > 0$ שמחלק את a ואת b, $n|d$. אם $a = b = 0$ אז נסמן $\gcd(0,0) = 0$.

כסימון, מקובל להשמיט את האותיות gcd לפני הסוגריים, ולכתוב בקיצור $d = (a,b)$. נביא הגדרה הנוספת. בהמשך נראה שהיא שקולה לראשונה.

הגדרה 2.3 יהיו $a,b \in \mathbb{N}$ (לא שניהם 0). אנו נאמר ש־d הוא המחלק המשותף המקסימלי שלהם ונסמן $d = (a,b)$ אם $d|a \wedge d|b$ ולכל $n > 0$ שמחלק את a ואת b, $n \leq d$. אם $a = b = 0$ אז נסמן $(0,0) = 0$.

נעבור להוכיח משפט שממנו נסיק את השקילות של ההגדרות, ונקבל דרך מאד נוחה לתאר את המחלק המשותף המקסימלי.

משפט 2.4 יהיו $a,b \in \mathbb{N}$ כך שלא שניהם אפס. תהי

$$D := \{n \in \mathbb{N} : n > 0 \wedge \exists \alpha, \beta \in \mathbb{Z}, n = \alpha a + \beta b\}$$

זו קבוצה סדורה היטב לא ריקה. נתבונן באיבר המינימלי $d \in D$. אזי $d = (a,b)$. המשפט נכון עבור שתי ההגדרות שראינו לעיל.

הוכחה: ראשית נוכיח ש $d|a \wedge d|b$. לפי משפט 2.1 קיים $0 \leq r < d$ וקיים $q \in \mathbb{Z}$ כך ש $a = dq + r$. מכיוון ש $d \in D$, קיימים α, β כך ש $\alpha a + \beta b = d$. נציב את הביטוי במקום d ונקבל $a = (\alpha a + \beta b)q + r$. לאחר העברת אגפים, נקבל $r = (1 - \alpha q)\,a - \beta q b$. אם כן r הוא צירוף לינארי של a,b. לפיכך אם $r > 0$ אז $r \in D$. אבל $r < d$ שהוא האיבר המינימלי של D, וזו סתירה. לפיכך $r = 0$ וכך $a = dq$. כלומר $d|a$. באופן דומה מראים ש־$d|b$. בזאת הראנו כי מתקיים התנאי הראשון של ההגדרה, הן בהגדרה 2.2 והן בהגדרה 2.3.

עכשיו נראה כי גם התנאי השני בהגדרות מתקיים. יהי n המחלק את a ואת b. אזי מתקיים:

$$n|a \wedge n|b \implies n|\alpha a \wedge n|\beta b \implies n|(\alpha a + \beta b) = d$$

מצאנו כאן כי $n|d$, ובכך הראנו כי מתקיים גם התנאי השני בהגדרה 2.2. מתכונות יחס החלוקה שהבאנו לעיל נובע שאכן $n \le d$ והראנו את קיום התנאי השני גם עבור הגדרה 2.3. לפיכך $d = (a,b)$. ■

הערה 2.5 שימו לב כי במשפט זה הוכחנו קיום (a,b) לפי כל אחת מן ההגדרות, וממילא הוכחנו כי הן שקולות. כמו כן קיבלנו אפיון פשוט של (a,b): (a,b) הינו צירוף לינארי (מעל $\mathbb{Z}$) של a ושל b, המינימלי מבין הצירופים שהם חיוביים.

מסקנה 2.6 הגדרה 2.2 והגדרה 2.3 שקולות.

תרגיל: נניח שעבור המספרים $n_1, ..., n_t$, המחלק המשותף המקסימלי הוא d. הוכח שקיימים $\alpha_1, ..., \alpha_t$ שלמים כך ש-$\alpha_1 n_1 + ... + \alpha_t n_t = d$.

הוכחה: באינדוקציה על t. ■

2.3 האלגוריתם של אוקלידס

בסעיף זה אנו נראה דרך יעילה למציאת $d = (a,b)$ ומציאת המקדמים של a ושל b בביטוי $d = \alpha a + \beta b$.

למה 2.7 אם $a = bq + r$, אזי $(a,b) = (b,r)$.

הוכחה: יהי d שמחלק את a ואת b. אזי הוא מחלק כל צירוף שלהם ובפרט את r. באופן דומה, כל d שמלחק את r ואת b, מחלק כל צירוף שלהם ופרט את a. לכן קבוצת המחלקים של a ושל b שוה לקבוצת המחלקים של b ושל r. לכן $(a,b) = (b,r)$. ■

למה 2.8 עבור $a \neq 0$ מתקיים $(a,0) = |a|$.

הוכחה הינה תרגיל פשוט, שכדאי לעשות אותו על מנת לוודא שמבינים את כל ההגדרות.

אלגוריתם: האלגוריתם של אוקלידס

1. אם $a = b = 0$ אזי (a,b) אינו מוגדר.
2. אחרת, בצע חילוק עם שארית על מנת לקבל $a = bq + r$.
3. אם $r = 0$ אזי $(a,b) = b$.
4. אחרת $a = b, b = r$ וחזור לשורה 2.

שימו לב, אם אנו זוכרים את כל ההצבות בכל צעד של האלגוריתם, אנו יכולים לצעוד אחורנית, מסופו לראשיתו, ולקבל גם את המקדמים של הצירוף הלינארי.

דוגמא: מצאו את $(77,21)$, ובטאו אותו כצירוף לינארי של 77 ושל 21.

פתרון:

1. $77 = 21 \cdot 3 + 14$
2. $21 = 14 + 7$
3. $14 = 7 \cdot 2$

לכן $7 = (77, 21)$. נמצא את המקדמים:

$$7 = 21 - 14 \overset{14=77-21\cdot 3}{\Longrightarrow} 7 = 21 - (77 - 21 \cdot 3) = (-1) \cdot 77 + 4 \cdot 21$$

קיבלנו את 7 כצירוף של 77 ו 21 .

הערה 2.9 המקדמים α, β בביטוי $d = \alpha a + \beta b$ אינם יחידים. קיימת טעות טיפשית אבל נפוצה: $d = \alpha a + \beta b$ עבור מקדמים α, β כלשהם ולכן מהווה (a, b). הטעות היא שאנו דרשנו צירוף מינימלי במשפט 2.4. gcd מוגדר לכל זוג של מספרים שלמים (לאו דווקא חיוביים) באופן הבא: $(a, b) := (|a|, |b|)$.

תרגיל: הראה שלכל n, $(4n+3, 7n+5) = 1$.

פתרון: נשתמש באלגוריתם אוקלידס.

1. $7n + 5 = 1 \cdot (4n + 3) + (3n + 2)$
2. $4n + 3 = 1 \cdot (3n + 2) + (n + 1)$
3. $3n + 2 = 2 \cdot (n + 1) + n$
4. $n + 1 = 1 \cdot n + 1$
5. $n = 1 \cdot n$

לכן $1 = (4n+3, 7n+5)$. נבטא את 1 כצירוף שלהם. נתחיל בצעד 4 (תמיד מדלגים על הצעד האחרון). נבודד את n מצעד 3, את $n+1$ מצעד 2, ואת $3n+2$ מצעד 1. נציב זאת לפי הסדר:

$$\begin{aligned}
1 &\overset{(4)}{=} (n+1) - n \\
&\overset{(3)}{=} (n+1) - ((3n+2) - 2 \cdot (n+1)) = 3 \cdot (n+1) - (3n+2) \\
&\overset{(2)}{=} 3 \cdot ((4n+3) - (3n+2)) - (3n+2) = 3 \cdot (4n+3) - 4 \cdot (3n+2) \\
&\overset{(1)}{=} 3 \cdot (4n+3) - 4 \cdot ((7n+5) - (4n+3)) = 7 \cdot (4n+3) - 4 \cdot (7n+5)
\end{aligned}$$

בסיכום קיבלנו $1 = 7 \cdot (4n+3) - 4 \cdot (7n+5)$.

2.4 מספרים זרים

הגדרה 2.10 אנו אומרים על זוג מספרים n ו־m שהם זרים אם $(n,m)=1$.

תרגיל: יהיו $n,m\in\mathbb{Z}$. נסמן $d=(n,m)$. אזי קיימים n',m' זרים כך ש $n=dn'$ וכן $m=dm'$.

פתרון: נסמן $m'=\frac{m}{d},n'=\frac{n}{d}$. אלו מספרים שלמים (הוכיחו!). יהיו $\alpha,\beta\in\mathbb{Z}$ כך ש $\alpha n+\beta m=d$. הצבה תגלה ש $\alpha n'+\beta m'=1$. לכן m' ו־n' זרים.

טענה 2.11 אם a ו־b זרים, וכן $a|bc$ אזי $a|c$.

הוכחה: $c=c\cdot 1=c\cdot(\alpha a+\beta b)=\alpha ca+\beta bc$. מכיוון ש a מחלק כל מחובר בסכום, a מחלק את כל הביטוי, כלומר את c. ■

2.5 הכפולה המשותפת המינילית (lcm).

הגדרה 2.12 יהיו n,m מספרים שלמים. אזי הכפולה המשותפת המינימלית (lcm) שלהם מוגדרת כמספר הטבעי הקטן ביותר שמתחלק בשניהם. אנו מסמנים $[n,m]:=\mathrm{lcm}\,(n,m)$.

טענה 2.13 יהיו n,m מספרים טבעיים. אזי $[n,m](n,m)=nm$.

הוכחה: נסמן $(n,m)=d$. לפי התרגיל בסעיף 2.4, קיימים m',n' זרים כך ש $n=n'd$, $m=m'd$. אנו נראה ש $[n,m]=dn'm'$. ברור, ש $m\mid dn'm', n\mid dn'm'$. אנו נוכיח שלכל $p\neq 0$ שמתחלק ב־m וב־n, $dn'm'\leq p$. נניח, מספר כלשהו $p\neq 0$ שמתחלק ב־n וב־m. אזי, ניתן לבטא אותו בשני אופנים $p=\alpha m=\beta n$. נציב את הביטויים עבור n ו־m, ונקבל $\alpha dm'=\beta dn'$. נחלק את שני האגפים ב־d, ונקבל $\alpha m'=\beta n'$. על פי טענה 2.11 $\alpha\mid n'$ ולכן $m'n'\leq m'\alpha$. לכן $n'dm'\leq\alpha dm'=p$. ■

3 מספרים ראשוניים ופירוק לגורמים

3.1 מספרים ראשוניים ומספרים אי פריקים

הגדרה 3.1 מספר שלם $0\neq a\in\mathbb{Z}$ הוא ראשוני, אם לכל b ו־c המקיימים $a=bc$, מתקיים b הפיך או c הפיך.

בהקשר של המספרים השלמים, ניתן לנסח את ההגדרה גם כך: מספר שלם a הוא ראשוני אם אין לו מחלקים חיוביים מלבד $|a|$ עצמו ו־1. הספרים השלמים הם דוגמא לתחום שלמות, עליהם נלמד בהמשך הקורס. בתחומי שלמות מבחינים בין המושגים אי־פריק וראשוני. ההגדרה שלעיל מתאימה למושג אי־פריק. בטענה 3.3 נוכיח כי גם תכונת הראשוניות מתקיימת.

דוגמא: 2 הוא מספר ראשוני.

טענה 3.2 אם p ראשוני אזי לכל n, מתקיימת לפחות אחת מהשתיים: $p|n$, או $(p,n)=1$.

הוכחה: נניח $(p,n)=d\neq 1$. בפרט $d|p$ וקיים q כך ש־$dq=p$. p ראשוני, d לא הפיך, ולכן q הפיך, $d=pq^{-1}$. בנוסף, $d|n$ וקיים m כך ש־$dm=n$. ביחד נקבל $n=dm=pq^{-1}m$, וכך $p|n$ כמבוקש. ■

טענה 3.3 (אי־פריקות גוררת ראשוניות) אם p הוא ראשוני, אזי לכל b ו־c המקיימים $p|bc$, מתקיים גם $p|b$ או $p|c$.

הוכחה: נניח ש־p הוא ראשוני. יהיו b ו־c, כך ש $p \mid bc$. אם p ו־b זרים, אזי p מחלק את c על פי טענה 2.11. אחרת p מחלק את b על פי הטענה 3.2. ■

3.2 פירוק לגורמים

טענה 3.4 כל מספר טבעי, אפשר להציג כמכפלה של ראשוניים.

הוכחה: נוכיח את המשפט באינדוקציה. עבור $n = 1, 2$ הטענה נכונה. נניח שהטענה נכונה לכל $1 < m < n$. אנו נוכיח שהטענה אף ל n. אם n ראשוני, הטענה נכונה. אחרת n פריק, לכן קיימים $a, b < n$, כך ש $n = ab$. לפי הנחת האינדוקציה, a ניתן להציג כמכפלה של מספרים ראשוניים ו־b ניתן להציג כמכפלה של מספרים ראשוניים. לכן n אף הוא מכפלה של מספרים ראשוניים. ■

טענה 3.5 הפירוק של מספר טבעי לגורמים ראשוניים הינו יחיד עד כדי סדר.

הוכחה: נניח ש $n = p_1^{\alpha_1}...p_m^{\alpha_m} = q_1^{\beta_1}...q_r^{\beta_r}$. מכיוון שכל ראשוני זר לכל ראשוני אחר, כל גורם שמופיע בצד ימין חייב להופיע גם בצד שמאל, על פי הטענה 2.11. אם כן, ניתן להתאים את כל ה־p_i באופן חח"ע עם כל ה־q_i. אנו נקבע כי סדרם אחיד, כלומר $p_i = q_i$ לכל i. כעת נראה את ההתאמה $\alpha_i = \beta_i$. נניח בשלילה כי $\alpha_i \neq \beta_i$, ובה"כ $\alpha_i < \beta_i$. אזי נחלק את שני הצדדים ב־$p_i^{\alpha_i}$. קיבלנו $p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_m^{\alpha_m} = p_1^{\beta_1} \cdots p_i^{\beta_i - \alpha_i} \cdots p_n^{\beta_n}$. אם כן, p_i מופיע באגף ימין בחזקה חיובית ממש, בעוד שבאגף שמאל הוא מופיע בחזקת אפס. אבל מכיוון שהוא ראשוני, הוא חייב לחלק את אחד הגורמים של אגף שמאל. מכיוון שכל הגורמים האחרים הם ראשוניים ושונים מ־p_i, אין ראשוני שכזה. סתירה. אם כן, לכל i, $\alpha_i = \beta_i$, והפירוק יחיד. ■

שתי הטענות האחרונות יחדיו מכונות בשם המשפט היסודי של האריתמטיקה.

4 שקילות מודולו n.

הגדרה 4.1 אנו אומרים a ו b שקולים מודולו n, אם $n \mid (a - b)$, ומסמנים $a \equiv b \pmod n$.

טענה 4.2 שקילות מודולו n היא יחס שקילות. כמו כן, כפל וחיבור מודולו n מוגדרים היטב על מחלקות שקילות, דהיינו:

אם $a \equiv a', b \equiv b' \pmod n$, אזי $a + b \equiv a' + b', ab \equiv a'b' \pmod n$.

4.1 משפט השאריות הסיני

משפט 4.3 אם n ו־m זרים, אזי לכל a ו־b קיים x יחיד עד כדי שקילות מודולו mn כך ש $x \equiv a \pmod n$, ו $x \equiv b \pmod m$.

הוכחה: קיום. מכיוון ש $(m, n) = 1$, קיימים α ו β כך ש $\alpha m + \beta n = 1$. נתבונן ב $a\alpha m + b\beta n$. מתקיים

$$a\alpha m + b\beta n \equiv a\alpha m \equiv a \cdot 1 \equiv a \pmod n$$

באופן דומה

$$a\alpha m + b\beta n \equiv b\beta n \equiv b \cdot 1 \equiv b \pmod{m}$$

לפיכך אנו נסמן $x = a\alpha m + b\beta n$, והמבוקש יתקיים. קל לראות כי הפתרון שמצאנו x מכבד את השקילות (מודולו mn). ניתן לבדוק לצורך זה את המקרה $x' = x + kmn$ ולגלות שגם זה פתרון טוב.

יחידות. נוכיח באופן קומבינטורי. לכל זוג (a,b) יש x (לפחות אחד) המתאים לו (מודולו mn). ישנם בסה"כ mn זוגות שונים (a,b) ו־mn אפשרויות שונות ל־x (מודולו mn). ההתאמה הזו היא פונקציה חח"ע בין קבוצות סופיות שוות עוצמה, ולכן היא גם על. ■