פתרון תרגיל בית 2 מבוא לתורת החבורות
88-211 סמסטר א' תשע"ז

הוראות בהגשת הפתרון יש לרשום שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא בתרגול בשבוע המתחיל בתאריך כ"ו חשוון ה'תשע"ז, 27.11.2016.

שאלות חימום

שאלות החימום הן שאלות שאינן להגשה, והן בדרך כלל קלות יותר. אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

שאלה 1. יהיו n, m מספרים שלמים, ונניח $n|m$. האם בהכרח $-m|n$? האם בהכרח $-n|2m$? האם בהכרח $m \nmid n$ (כלומר m לא מחלק את n)?

פתרון. כן, כן, לא. למה לא? הוכיחו ש-$n|m$ וגם $m|n$, אם ורק אם $n = \pm m$.

שאלה 2. יהי p מספר ראשוני. מצאו את כל המספרים $x \in \mathbb{Z}$ כך ש-$x|p$.

פתרון. המספרים $1, p, -1, -p$.

שאלה 3. יהי n מספר טבעי. הגדרנו יחס על $\mathbb{Z}$ לפיו נאמר כי $a, b \in \mathbb{Z}$ שקולים מודולו n אם $n|a-b$, וסימנו יחס זה כ-$a \equiv b \pmod{n}$. הוכיחו כי שקילות מודולו n היא אכן יחס שקילות (כלומר יחס רפלקסיבי, סימטרי וטרנזיטיבי).

פתרון. היחס רפלקסיבי כי לכל $a \in \mathbb{Z}$ מתקיים כי $n|0$. לכן $n|a-a$, כלומר $a \equiv a \pmod{n}$. היחס סימטרי כי אם $n|x$, אז גם $n|-x$. בפרט

$$a \equiv b \pmod{n} \Leftrightarrow n|(a-b) \Leftrightarrow n|(b-a) \Leftrightarrow b \equiv a \pmod{n}$$

היחס טרנזיטיבי כי אם $n|x$ וגם $n|y$, אז $n|x+y$. בפרט אם $a \equiv b \pmod{n}$ וגם $b \equiv c \pmod{n}$, אז

$$n|(a-b) \wedge n|(b-c) \Rightarrow n|(a-b+b-c) \Rightarrow n|(a-c)$$

כלומר $a \equiv c \pmod{n}$.

שאלות להגשה

שאלה 4. יהי n מספר טבעי. נסמן את הכפולות שלו ב-$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. נזכיר כי סימנו $\gcd(a,b) = (a,b)$.

א. הוכיחו כי b מחלק את a אם ורק אם $a\mathbb{Z} \subseteq b\mathbb{Z}$.

ב. נגדיר סכום על קבוצות כאלו לפי $a\mathbb{Z}+b\mathbb{Z}=\{\alpha+\beta:\alpha\in a\mathbb{Z},\beta\in b\mathbb{Z}\}$. הוכיחו כי מתקיים $a\mathbb{Z}+b\mathbb{Z}=(a,b)\mathbb{Z}$.

ג. הוכיחו כי $((a,b)\cdot(a,c))\mathbb{Z}\subseteq a\mathbb{Z}+bc\mathbb{Z}$. רמז: העזרו בסעיפים הקודמים.

פתרון. א. מצד אחד, אם $a\mathbb{Z}\subseteq b\mathbb{Z}$, אזי בפרט $a\in b\mathbb{Z}$. לכן קיים $n\in\mathbb{Z}$ כך שמתקיים $a=bn$, כלומר $b|a$. מצד שני, אם $b|a$, אז קיים $n\in\mathbb{Z}$ כך שמתקיים $a=bn$. לכן אם $x\in a\mathbb{Z}$, קיים $m\in\mathbb{Z}$ כך ש-$x=am$ ולכן $x=bnm$, כלומר $x\in b\mathbb{Z}$.

ב. נוכיח בהכלה דו־כיוונית. נתחיל עם $\subseteq$: ידוע כי ניתן להציג את (a,b) כצירוף לינארי של a,b. כלומר קיימים $u,v\in\mathbb{Z}$ כך שמתקיים $(a,b)=au+bv$. יהי $x\in a\mathbb{Z}+b\mathbb{Z}$, ולכן קיימים $n_a,n_b\in\mathbb{Z}$ כך ש-$x=an_a+bn_b$. אנו צריכים למצוא $m\in\mathbb{Z}$ כך שיתקיים $(a,b)m=an_a+bn_b$. אפשר לבחור את $m=\frac{a}{(a,b)}n_a+\frac{b}{(a,b)}n_b$.
הכיוון השני $\supseteq$ הוא יותר קל כי ידוע לנו שניתן להציג את (a,b) כצירוף לינארי של a,b, ולכן גם כל כפולה שלו.

ג. בעזרת הסעיפים הקודמים אנו למעשה נדרשים להוכיח $(a,b)\,(a,c)\mid(a,bc)$. קיימים s,t,u,v כך שמתקיים

$$(a,b)=sa+tb$$
$$(a,c)=ua+vc$$

נכפול את שתי המשוואות האלו ונקבל

$$(a,b)\,(a,c)=(sa+tb)\,(ua+vc)=n_1a+n_2bc$$

עבור $n_1,n_2\in\mathbb{Z}$. לפי הגדרה $(a,bc)\,|a,bc$ ולכן (a,bc) מחלק כל צירוף לינארי של a ושל bc, בפרט את n_1a+n_2bc.

שאלה 5. הוכיחו כי לכל $a,n,m\in\mathbb{Z}$ מתקיים $(an,am)=|a|\,(n,m)$.

פתרון. נסמן $d=(n,m)$. בשורה אחת, שאינה הוכחה מלאה,

$$(an,am)=|a|\,d\Leftrightarrow\left(\frac{an}{d},\frac{am}{d}\right)=|a|\Leftrightarrow|a|\left(\frac{n}{d},\frac{m}{d}\right)=|a|\Leftrightarrow\left(\frac{n}{d},\frac{m}{d}\right)=1\Leftrightarrow(n,m)=d$$

דרך אחרת, היא דו־כיוונית (ומפורטת יותר). מצד אחד, ישנם מספרים u,v כך שמתקיים $(an,am)=uan+vam$. ידוע כי d מחלק כל צירוף לינארי של n ו-m, ובפרט את $un+vm$. לכן $|a|\,d$ מחלק את $uan+vam$, ולכן $(|a|\,d)|\,(an,am)$.
מצד שני, ישנם מספרים s,t כך שמתקיים $d=sn+tm$. נכפיל ב-$|a|$ ונקבל $|a|\,d=s'an+t'am$ עבור s',t' מתאימים. ידוע כי (an,am) מחלק כל צירוף לינארי של an ו-am, ובפרט את $s'an+t'am$. לכן $(an,am)\,|\,|a|\,d$. לסיכום קיבלנו $(an,am)=|a|\,d$, כדרוש.
ניתן להוכיח את הטענה גם בעזרת שימוש בהצגה של ממ"מ כמכפלת חזקות ראשוניים. במקרה זה מוכיחים כי $\min(n+a,m+a)=\min(n,m)+a$, שהיא אנלוגית להוכחת $(an,am)=|a|\,(n,m)$.

שאלה 6. מצאו בעזרת אלגוריתם אוקלידס את הממ"מ הבאים:

א. $(88,211)$

ב. $(-26400,63300)$, רמז: העזרו בשאלה הקודמת.

פתרון. א. נשתמש באלגוריתם אוקלידס:

$$\begin{aligned}(88,211)=(211,88)&=[211=2\cdot 88+35]\\ (88,35)&=[88=2\cdot 35+18]\\ (35,18)&=[35=1\cdot 18+17]\\ (18,17)&=[18=1\cdot 17+1]\\ (17,1)&=1\end{aligned}$$

ולכן $(88,211)=1$.

ב. נשים לב כי $-300\cdot 88=-26400$ וכן $300\cdot 211=63300$. לכן לפי השאלה הקודמת

$$(-26400,63300)=(26400,63300)=|300|\cdot(88,211)=300$$

שאלה 7. יהיו n,m מספרים שלמים. הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

$$\operatorname{lcm}(n,m)=[n,m]=\min\{d\in\mathbb{N}:n|d\wedge m|d\}$$

למשל $30=[6,10]$ ו-$10=[2,5]$. הוכיחו:

א. אם $m|a$ וגם $n|a$, אז $[n,m]\,|a$.

ב. $|nm|=(n,m)\,[n,m]$. למשל $6\cdot 4=24=12\cdot 2=(6,4)\,[6,4]$.

הוכחה. א. יהיו q,r כך ש-$a=q\,[n,m]+r$ כאשר $0\leq r<[n,m]$. מהנתון כי $n,m|a$ ולפי הגדרה $n,m|\,[n,m]$, נובע כי $n,m|r$. אם $r\neq 0$ זו סתירה למינימליות של $[n,m]$. לכן $a=q\,[n,m]$, כלומר $[n,m]\,|a$.

ב. נראה דרך קלה לחישוב הממ"מ והכמ"מ בעזרת הפירוק של מספר למכפלת גורמים ראשוניים. נניח כי הפירוק הוא

$$|n|=\prod_{i=1}^{\infty}p_i^{\beta_i}=p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}\dots\qquad |m|=\prod_{i=1}^{\infty}p_i^{\alpha_i}=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\dots$$

כאשר $\alpha_i,\beta_i\geq 0$ (והם כמעט תמיד אפס כי המכפלה סופית). כעת צריך להשתכנע כי

$$(n,m)=\prod_{i=1}^{\infty}p_i^{\min(\alpha_i,\beta_i)}\qquad [n,m]=\prod_{i=1}^{\infty}p_i^{\max(\alpha_i,\beta_i)}$$

ומפני שלכל שני מספרים α,β מתקיים $\alpha+\beta=\min(\alpha,\beta)+\max(\alpha,\beta)$, אז $|nm|=(n,m)\,[n,m]$.

$\square$

שאלה 8. הוכיחו:

א. לכל n שלם מתקיים $(4n+3,7n+5)=1$.

ב. מצאו $s,t\in\mathbb{Z}$ (התלויים ב-n) כך ש-$(4n+3)s+(7n+5)t=1$.

פתרון. א. נשתמש כמה פעמים שאם $n=qm+r$, אז $(n,m)=(m,r)$.

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

אפשר לעשות את החישוב בכמה דרכים, למשל כאשר נמנעים ממקדמים שליליים ל-n:

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

ב. משתמשים בשלבים של אלגוריתם אוקלידס המורחב, לפי הסעיף הקודם:

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

ולכן נקבל $s=7,t=-4$, שאינם תלויים ב-n!

שאלה 9. מצאו את כל המספרים השלמים n כך ש-$(n+1)|(n^2+11)$.

פתרון. נשים לב כי $n+1$ מחלק את עצמו, ואם הוא מחלק את n^2+11, הוא גם יחלק את הממ"מ שלהם (ולכן גם יחלק כל צירוף לינארי של $n+1$ ושל n^2+11). בעזרת החישוב

$$n^2+11=(n-1)\cdot(n+1)+12$$

ושימוש בטענה שאם $n=qm+r$, אז $(n,m)=(m,r)$, נקבל

$$\left(n^2+11,n+1\right)=(n+1,12)$$

כלומר מספיק למצוא את המספרים n כך ש-$(n+1)|12$. המחלקים של 12 הם ידועים, ולכן המספרים המבוקשים הם $-13,-7,-5,-4,-3,-2,0,1,2,3,5,11$.

החישוב שעשינו היה למעשה

$$\frac{n^2+11}{n+1}=\frac{n^2-1+12}{n+1}=\frac{(n+1)(n-1)}{n+1}+\frac{12}{n+1}=(n-1)+\frac{12}{n+1}$$

ומפני ש-$n-1$ הוא שלם, נותר לבדוק מתי $\frac{12}{n+1}$ שלם.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה צרפו את הפתרון שלהן.

שאלה 10. בחרו שפת תכנות (לא איזוטרית) כרצונכם וכתבו פונקציה בשם xgcd המממשת את אלגוריתם אוקלידס המורחב. כלומר כתבו פונקציה המקבלת כקלט שני מספרים שלמים a, b ומחזירה שלשה של מספרים (d, s, t) כך שמתקיים $d = (a, b) = sa + tb$.

הוסיפו את התוצאות של הרצת

$$\text{xgcd}(5777, 2016) \qquad \text{xgcd}(437437, 142142) \qquad \text{xgcd}(288211, -141421)$$

הערה: בעוד ש-d הוא יחודי, המקדמים s, t הם לא בהכרח יחודיים. לדוגמה $\text{xgcd}(24, 44)$ תוכל להחזיר את השלשה $(4, 2, -1)$ כי $4 = 2 \cdot 24 - 1 \cdot 44$ אבל גם $(4, 13, -7)$ זו תוצאה מותרת, ולכן יתכנו מימושים נכונים שונים. דוגמאות נוספות

$$\text{xgcd}(100, 11) \longrightarrow (1, 1, -9) \qquad \text{xgcd}(-5, 0) \longrightarrow (5, -1, 0)$$

פתרון. נזכר כי באלגוריתם אוקלידס הרגיל מתחילים עם זוג מספרים (a, b) כשמניחים כי $0 \le b < a$. אם $b = 0$, אזי $(a, b) = a$. אחרת נכתוב $a = qb + r$ כאשר $0 \le r < |b|$ ונמשיך בשלב הבא עם חישוב $(a, b) = (b, r)$. בכל שלב באלגוריתם קיבלנו כי ניתן להציג את השארית r כצירוף לינארי $r = a - qb$.

באלגוריתם אוקלידס המורחב אנו שומרים בשלב מספר i את המקדמים s_i, t_i והשארית r_i כך שמתקיים $r_i = s_i a + t_i b$, שבעזרתם נביע לבסוף את d כצירוף לינארי. נניח ובשלב קודם באלגוריתם קיבלנו כי

$$r_{\text{prev}} = s_{\text{prev}} a + t_{\text{prev}} b$$

ובשלב הנוכחי $r = sa + tb$. נרצה לדעת מי יהיו המקדמים $s_{\text{new}}, t_{\text{new}}$ לשלב הבא. נבצע חלוקה אוקלידית של השאריות מהשלב הקודם והשלב הנוכחי $r_{\text{prev}} = qr + r_{\text{new}}$. כעת נשתמש במשוואות לעיל ונקבל

$$r_{\text{new}} = r_{\text{prev}} - qr = (s_{\text{prev}} a + t_{\text{prev}} b) - q\,(sa + tb) = (s_{\text{prev}} - qs)\,a + (t_{\text{prev}} - qt)\,b$$

לכן

$$t_{\text{new}} = t_{\text{prev}} - qt \qquad s_{\text{new}} = s_{\text{prev}} - qs$$

האלגוריתם מתחיל בשלב שבו $r_0 = a, r_1 = b$, כלומר

$$r_1 = b = s_1 a + t_1 b \qquad r_0 = a = s_0 a + t_0 b$$

ולכן $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$.

נציג פתרון איטרטיבי בפייתו'ן, ולאחריו נוסיף הערות על המימוש.

```python
def xgcd(a, b):
    """
    Extended Euclidean algorithm

    Returns (d, s, t) where 'd' is the greatest common
    divisor of the integers 'a' and 'b' where the
    numbers 's' and 't' are such that 'd = sa+tb'.
    """
    prev_r, r = a, b
```

```
10      prev_s, s = 1, 0
11      prev_t, t = 0, 1
12      while r:
13          q = prev_r // r
14          prev_s, s = s, prev_s - q*s
15          prev_t, t = t, prev_t - q*t
16          prev_r, r = r, prev_r - q*r
17
18      if prev_r < 0:
19          return (-prev_r, -prev_s, -prev_t)
20      else:
21          return (prev_r, prev_s, prev_t)
```

שורות $2-8$ נועדו לתיעוד הפונקציה. בשורה 9, וגם בהמשך הקוד, מופיע שימוש בהשמה מקבילית (בפיית’ון המינוח הוא tuple packing and sequence unpacking) ובו בו־זמנית מציבים ערכים בשני משתנים. הערכים באגף ימין בהשמה מקבילית מחושבים לפני ההשמה באגף שמאל.

בשורה 13 מופיע שימוש ב”חלוקת רצפה”, המחזירה את המנה השלמה של שני מספרים. בשפות תכנות רבות זו החלוקה הרגילה.

הלולאה שמתחילה בשורה 12 מבטיחה רק כי $0 \le |r|$, ולא בהכרח $0 \le r$. האלגוריתם עדין יעצר שכן $|r_i|$ קָטֵן. במקרה וקיבלנו $a < b$, האיטרציה הראשונה בלולאה תהפוך את הסדר שלהם (עד כדי שינוי בסימן, שאינו משפיע על הממ”מ).

הבדיקה בשורה 18 מוודאת כי הממ”מ המתקבל הוא לא שלילי.

פתרון רקורסיבי לבעיה בפיית’ון:

```
 1  def rxgcd(a,b):
 2      "Recursive version of xgcd."
 3      if b == 0:
 4          if a < 0:
 5              return (-a, -1, 0)
 6          else:
 7              return (a, 1, 0)
 8      else:
 9          q, r = divmod(a, b)
10          d, s, t = rxgcd(b, r)
11          return (d, t, s - q*t)
```

הפונקציה divmod בשורה 9 היא פונקציה סטנדרטית המחזירה שני מספרים q, r שהם המנה והשארית בחלוקה a/b כך שמתקיימים $a = qb + r$. בשורה 10 נקבל $d = sb + tr$, ולכן בשורה 11 מחזירים לאחר הצבה

$$d = sb + tr = sb + t(a - qb) = ta + (s - qt)b$$

תוצאות אפשריות לחישובים שנתבקשו בשאלה הן

$$\texttt{xgcd}(5777, 2016) = (1, 305, -874)$$
$$\texttt{xgcd}(437437, 142142) = (1001, 13, -40)$$
$$\texttt{xgcd}(288211, -141421) = (7, -3793, -7730)$$

שאלה 11. יהיו $P(x), Q(x) \in \mathbb{R}[x]$ פולינומים עם מקדמים ממשיים. נאמר כי $P(x)$ מחלק את $Q(x)$ אם קיים פולינום $f(x) \in \mathbb{R}[x]$ כך ש-$Q(x) = f(x) \cdot P(x)$, ונסמן $P(x)|Q(x)$.

נסחו והוכיחו גרסאות של משפט החילוק ואלגוריתם אוקלידס עבור פולינומים עם מקדמים ממשיים. ממשו פונקציית `xgcd` לפיהם. מה יקרה אם נחליף את $\mathbb{R}[x]$ ב-$\mathbb{Z}[x]$?

בהצלחה!