פתרון תרגיל בונוס

18 בנובמבר 2012

1.2.2 נניח כי עבור $n,d>0$ מתקיימת הטענה של משפט 1.2.1 (האוקלידיות של $\mathbb{Z}$). הסיקו ממקרה זה את המשפט השלם.

פתרון ראשית נצטט את המשפט: לכל $n\in\mathbb{Z}$ ו־$d\neq 0$ קיימים q,r כך ש־$n=qd+r$ ו־$0\leq r<|d|$. נתון שטענה זו מתקיימת עבור $n,d>0$. נראה שהטענה מתקיימת גם בשאר המקרים. המקרה $n=0$ הוא טריוויאלי, כי ניתן לקחת $q=r=0$. נתחיל בהנחה ש־$n<0$ אבל עדיין $d>0$. נביט ב־$n'=-n$. ובכן $n'>0$, ולכן מתקיימים תנאי המשפט: קיימים q',r' בהתאם המקיימים $n'=q'd+r'$. אז

$$n=-q'd-r'=(-q'-1)\,d+(d-r')$$

כעת מצאנו כי $q=-q'-1$ ו־$r=d-r'$ הם פתרון טוב: הם שניהם שלמים, ומתקיים $0\leq r<|d|$.
נותר לראות מה קורה כאשר $d<0$. יהי n שלם נתון. אזי לפי מה שהוכחנו זה עתה, קיימים q',r' עבורם $n=q'\,(-d)+r'$. מכאן נובע $n=(-q')\,d+r'$, כך שמצאנו שהפתרון הוא $q=-q'$ ו־$d=d'$. ברור שמתקיימים התנאים. □

1.3.10 נניח שלמספרים $n_1,\ldots,n_t$ אין מחלק משותף גדול מ־1. הראו שקיימים $\alpha_1,\ldots,\alpha_t$ כך ש־$\alpha_1n_1+\cdots+n_t\alpha_t=1$.

פתרון נוכיח באינדוקציה על t. עבור $t=2$ זה משפט ידוע. נניח נכונות עבור t, ונראה נכונות ב־$t+1$. יהיו $n_1,\ldots,n_{t+1}$ מספרים ללא מחלק משותף גדול מ־1. נביט ב־t המספרים הראשונים. נסמן את המחלק המשותף הגדול ביותר שלהם על ידי d. כעת נביט ב־$\frac{n_1}{d},\ldots,\frac{n_t}{d}$. אלו מספרים שלמים שהמחלק הגדול ביותר שלהם הוא 1. לפי הנחת האינדוקציה, קיימים $\alpha_1,\ldots,\alpha_t$ כך ש־$\alpha_1\frac{n_1}{d}+\cdots+n_t\frac{\alpha_t}{d}=1$. נכפיל את המשוואה ב־$d$, ונקבל־$\alpha_1n_1+\cdots+n_t\alpha_t=d$. כעת נביט ב־$d,n_{t+1}$. אלו מספרים זרים, ולפי המשפט, קיימים α,β כך ש־$\alpha d+\beta n_{t+1}=1$. בסך הכל מקבלים $\alpha\,(\alpha_1n_1+\cdots+n_t\alpha_t)+\beta n_{t+1}=\alpha d+\beta n_{t+1}=1$. □

1.3.19 מצאו $\alpha,\beta\in\mathbb{Z}$ כך ש־$1525\alpha+927\beta=1$.

פתרון נעבוד עם אלגוריתם אוקלידס, ונחשב להפך. כמובן, על הדרך נוודא שהם באמת זרים.

$$\begin{aligned}
1525 &= 927 \cdot 1 + 598 \\
927 &= 598 \cdot 1 + 329 \\
598 &= 329 \cdot 1 + 269 \\
329 &= 269 \cdot 1 + 60 \\
269 &= 60 \cdot 4 + 29 \\
60 &= 29 \cdot 2 + 2 \\
29 &= 2 \cdot 14 + 1
\end{aligned}$$

כעת נחשב את הכיוון ההפוך, ונמצא את המקדמים:

$$\begin{aligned}
1 &= 1 \cdot 29 - 14 \cdot 2 = 1 \cdot 29 - 14 \cdot (60 - 2 \cdot 29) = 29 \cdot 29 - 14 \cdot 60 \\
&= 29 \cdot (269 - 4 \cdot 60) - 14 \cdot 60 = 29 \cdot 269 - 130 \cdot 60
\end{aligned}$$

בשל מורכבות החישוב, אנו נפריד אותו כאן, ונחשב מכאן ואילך.

$$\begin{aligned}
60 &= 329 - 269 = 329 - (598 - 329) = -598 + 2 \cdot 329 \\
&= -598 + 2 \cdot (927 - 598) = (-3) \cdot 598 + 2 \cdot 927 \\
&= (-3) \cdot (1525 - 927) + 2 \cdot 927 = (-3) \cdot 1525 + 5 \cdot 927
\end{aligned}$$

$$\begin{aligned}
269 &= 598 - 329 = 598 - (927 - 598) \\
&= (1525 - 927) - (927 - (1525 - 927)) = 2 \cdot 1525 - 3 \cdot 927
\end{aligned}$$

$$\begin{aligned}
1 &= 29 \cdot 269 - 130 \cdot 60 = 29 \cdot (2 \cdot 1525 - 3 \cdot 927) - 130 \cdot ((-3) \cdot 1525 + 5 \cdot 927) \\
&= (29 \cdot 2 + 130 \cdot 3) \cdot 1525 - (29 \cdot 3 + 130 \cdot 5) \cdot 927 = 448 \cdot 1525 - 737 \cdot 927
\end{aligned}$$

אם כן, מצאנו כי $\alpha = 448, \beta = -737$ הוא פתרון אפשרי. $\square$

1.3.26 יהיו k, n, m. אזי $(kn, km) = k\,(n, m)$.

פתרון יהי d מחלק משותף של n, m. אזי ברור ש־kd מחלק משותף של kn, km. בפרט עבור $d = \gcd(n, m)$, kd הוא מחלק משותף.
נותר להראות כי הוא מקסימלי. נעשה זאת על ידי מציאת צירוף לינארי. נסמן $d = \gcd(n, m)$. אזי קיימים α, β כך ש־$\alpha n + \beta m = d$. נכפיל את שני הצדדים ב־k, ונקבל $\alpha kn + \beta km = kd$, ולפיכך kd מתחלק ב־$\gcd(kn, km)$.
לסיכום, kd הוא מחלק משותף וגם צירוף לינארי של kn, km, ולכן הוא המחלק המשותף המקסימלי שלהם. $\square$

1.3.27 אם $(m, k) = 1$, אז $(n, mk) = (n, m) \cdot (n, k)$.

פתרון נסמן $a=(n,m),b=(n,k)$. אנו רוצים להראות ש־ab הוא המחלק המשותף המקסימלי של n,mk. ברור ש־ab מחלק את mk. נראה כי הוא מחלק גם את n. נחשב את (a,b). מצד אחד, הוא מחלק את a ולכן גם את m. מצד שני הוא מחלק את b ולכן גם את k. מכיוון ש־m,k זרים, מחלק משותף שלהם הוא 1, ונקבל $(a,b)=1$. אנו יודעים ש־a ו־b מחלקים את n, ולכן $[a,b]$ מחלק את n. אבל $[a,b]=\frac{ab}{(a,b)}=ab$, וכך מצאנו ש־$ab$ מחלק את n. לסיכום עד כאן, מצאנו כי ab הוא מחלק משותף של n,mk.

כעת נותר להראות מקסימליות. כרגיל, נראה זאת על ידי קיום צירוף לינארי. אנו יודעים שקיימים $\alpha_1,\beta_1,\alpha_2,\beta_2$ כך ש

$$\begin{aligned}\alpha_1 n+\beta_1 m &= a\\ \alpha_2 n+\beta_2 k &= b\end{aligned}$$

על ידי הכפלת שתי המשוואות האלו ניתן לראות כי

$$\left(\alpha_1\alpha_2 n+\alpha_1\beta_2 k+\alpha_2\beta_1 m\right)n+\beta_1\beta_2 mk=ab$$

אם כן, ab הוא צירוף לינארי של n,mk. לפיכך ab הוא מחלק משותף וגם צירוף לינארי, וכך הוא המחלק המשותף המקסימלי של n,mk. □

1.3.29 אם $(n,m)=1$, אז $(n,mk)=(n,k)$.

פתרון קל לראות כי (n,k) מחלק את (n,mk). אנו נראה כי ניתן לכתוב את (n,k) כצירוף לינארי של n,mk. לפי הנתון קיימים a,b כך ש־$an+bm=1$. כמו־כן ידוע לנו שקיימים c,d כך ש־$cn+dk=(n,k)$. נציב משוואות אלו זו בזו, ונקבל

$$(n,k)=cn+dk=cn+d\left(an+bm\right)k=\left(c+dak\right)n+bmk$$

אם כן מצאנו כאן ש־(n,k) הוא צירוף לינארי של n,mk. ביחד נקבל את השויון המיוחל. □

1.3.35 לכל n,m,k מתקיים $[n,(m,k)]=([n,m],[n,k])$.

פתרון נסמן את המחלק המשותף המקסימלי של n,m,k על ידי $e=\gcd(n,m,k)=\gcd(n,\gcd(m,k))$, וכן נסמן $d=\gcd(m,k)$. לפי סימונים אלו קיימים n',d' שלמים כך שמתקיים $d=d'e,n=n'e$. נחשב כל אגף בנפרד. נתחיל באגף שמאל. $[n,(m,k)]=\frac{n(m,k)}{(n,m,k)}=\frac{nd}{e}=n'd'e$. השתמשנו כאן בזהות שהוכחנו בשיעור (תרגיל 1.3.33), $(n,m)[n,m]=nm$.

נביט כעת באגף ימין. נסמן סימונים חדשים: m',k' הם הפתרונות השלמים של $m=m'd,k=k'd$. אנו ניעזר בתרגיל 1.3.26. לפי הגדרת d',n', הם זרים, ולכן ניתן להשתמש גם בתרגיל 1.3.29. לסיום נזכיר כי גם m',k' זרים, לפי הגדרתם, ולכן גם כל מחלקיהם זרים.

$$\begin{aligned}([n,m],[n,k]) &= ([n'e,m'd'e],[n'e,k'd'e]) \overset{(33)}{=} \left(\frac{n'm'd'e^2}{(n'e,m'd'e)},\frac{n'k'd'e^2}{(n'e,k'd'e)}\right)\\ &\overset{(26)}{=} \left(\frac{n'm'd'e^2}{e\,(n',m'd')},\frac{n'k'd'e^2}{e\,(n',k'd')}\right)=\left(\frac{n'm'd'e}{(n',m'd')},\frac{n'k'd'e}{(n',k'd')}\right)\\ &\overset{(29)}{=} \left(\frac{n'm'd'e}{(n',m')},\frac{n'k'd'e}{(n',k')}\right)\overset{(26)}{=} n'd'e\left(\frac{m'}{(n',m')},\frac{k'}{(n',k')}\right)\\ &= n'd'e\cdot 1\end{aligned}$$

נעיר כאן כי בשימוש בתרגיל 26 יש צורך לוודא שמה שנשאר בתוך הסוגריים הוא מספר שלם. לסיכום, מצאנו כי שני האגפים שווים, כמבוקש. □

1.5.3 אם $a \equiv a' \pmod{n}$ ו־$b \equiv b' \pmod{n}$, אז $a+b \equiv a'+b' \pmod{n}$ וכן $ab \equiv a'b' \pmod{n}$.

פתרון יהיו $a \equiv a' \pmod{n}$ ו־$b \equiv b' \pmod{n}$, כנתון בשאלה. נסמן $c = a' - a$ וכן $d = b' - b$. מהשקילות נובע ש־c ו־d שניהם מתחלקים ב־n. נחשב את אגף ימין של החיבור ושל הכפל:

$$\begin{aligned} a'+b' &= (a+c)+(b+d) = a+b+(c+d) \equiv a+b \pmod{n} \\ a'b' &= (a+c)\cdot(b+d) = ab+(bc+dc+ad) \equiv ab \pmod{n} \end{aligned}$$

השתמשנו כאן בכך שסכומם של איברים המתחלקים ב־n מתחלק גם הוא, וכן בכך שמכפלת מספר המתחלק ב־n במספר אחר מתחלקת גם היא. □

1.5.11 הראו שלמערכת $\left\{\begin{array}{rcl} x & \equiv & 5 \pmod{12} \\ x & \equiv & 6 \pmod{8} \end{array}\right\}$ אין פתרונות.
הראו שלמערכת $\left\{\begin{array}{rcl} x & \equiv & 2 \pmod{12} \\ x & \equiv & 6 \pmod{8} \end{array}\right\}$ יש יותר מפתרון אחד (מודולו $8 \cdot 12$).
מדוע אין זו סתירה למשפט?

פתרון נתון $x \equiv 5 \pmod{12}$. 12 הוא פריק, ולכל גורם k של 12, מתקיים $x \equiv 5 \pmod{k}$.
בפרט עבור 2 מתקיים $x \equiv 5 \pmod{2}$, קרי: x אי־זוגי. מנגד, $x \equiv 6 \pmod{8}$ גורר עבור גורם מתאים $x \equiv 6 \pmod{2}$, קרי זוגי. אבל כידוע $6 \not\equiv 5 \pmod{2}$ $x \equiv x \pmod{2}$, וזו סתירה. לכן אין פתרון למערכת.
במערכת השנייה, ניתן לראות פתרונות לדוגמא $x = 14, 86$.
הדוגמאות הנ"ל אינן סותרות את משפט השאריות הסיני, מכיוון ש־8 ו־12 אינם זרים, ובמשפט השאריות הסיני יש דרישה ש־n, m זרים. ניתן להכליל ולומר שכאשר n, m אינם זרים אין פתרון יחיד מודולו nm. במקרה שכזה מתקיים אחד מן השניים: אין כלל פתרון למערכת או יש (n, m)פתרונות שונים מודולו nm. □

1.5.12 נתון כי n, m שלמים. מצאו תנאי הכרחי ומספיק על a, b לכך שלמערכת

$$\left\{\begin{array}{rcl} x & \equiv & a \pmod{n} \\ x & \equiv & b \pmod{m} \end{array}\right\}$$

יהיה פתרון יחיד מודולו $[n, m]$.

פתרון התנאי הוא $a \equiv b \pmod{\gcd(n, m)}$.
הכרחי. $\gcd(n, m)$ הוא מחלק של n ושל m. לכן ניתן להחליף אותו בתור בסיס השקילות ולקבל עדיין תוצאה נכונה. אם כן,

$$\left\{\begin{array}{rcl} x & \equiv & a \pmod{n} \\ x & \equiv & b \pmod{m} \end{array}\right\} \implies \left\{\begin{array}{rcl} x & \equiv & a \pmod{\gcd(n,m)} \\ x & \equiv & b \pmod{\gcd(n,m)} \end{array}\right\} \implies a \equiv b \pmod{\gcd(n,m)}$$

מספיק. נתון $a \equiv b \pmod{\gcd(n, m)}$. עלינו להראות כי קיים פתרון יחיד למערכת מודולו $[n, m]$. אנו נשחזר את ההוכחה הרגילה של משפט השאריות הסיני, בהתאמה

למקרה הנוכחי. נסמן $d = \gcd(n, m)$, וכן נסמן $n' = \frac{n}{d}, m' = \frac{m}{d}$. נפתח בניתוח הנתון שלנו, $a \equiv b \pmod{d}$. בניסוח אחר ניתן לומר שקיים k שלם המקיים

$$a - b = dk \tag{1}$$

לפי האלגוריתם של אוקלידס קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש־$\alpha m + \beta n = d$. נחלק את שני האגפים ב־d, ונקבל

$$\alpha m' + \beta n' = 1 \tag{2}$$

כעת נביט בביטוי $x = a\alpha m' + b\beta n'$, אותו "שלפנו" כגירסה מתאימה של הפתרון ממשפט השאריות המקורי. כמו שם, נראה ש־x פותר את שתי המשוואות במערכת.

$$\begin{aligned} x &= a\alpha m' + b\beta n' \overset{(1)}{=} a\alpha m' + (a - dk)\beta n' = a(\alpha m' + \beta n') - dk\beta n' \\ &\overset{(2)}{=} a - dk\beta n' \equiv a \pmod{n} \end{aligned}$$

$$\begin{aligned} x &= a\alpha m' + b\beta n' \overset{(1)}{=} (b + dk)\alpha m' + b\beta n' = b(\alpha m' + \beta n') + dk\alpha m' \\ &\overset{(2)}{=} b + dk\alpha m' \equiv b \pmod{m} \end{aligned}$$

וכך מצאנו x הפותר את שתי המערכות, כמבוקש. נותר רק להראות שהפתרון יחיד מודולו $[n, m]$. נניח כי קיים עוד פתרון x' למערכת. אז מתקיים

$$\left.\begin{array}{rcl} x & \equiv & a \equiv x' \pmod{n} \\ x & \equiv & b \equiv x' \pmod{m} \end{array}\right\} \Longrightarrow x \equiv x' \pmod{[n, m]}$$

כמבוקש. □