האלגוריתם של אוקלידס

ראינו בשיעור קודם $(18,12)=6$

מה $(1298, 524) = ?$

האלגוריתם של אוקלידס יאפשר לנו לחשב ממ"מ ע"י בקלות וב"דיוק".

למת הכנה לאלגוריתם: לכל $a,b,c\in\mathbb{Z}$ מתקיים $(a\pm cb, b) = (a,b)$

הוכחת הלמה:

מספיק להראות: $\{n\in\mathbb{N} \mid n|a+cb \text{ וגם } n|b\} = \{n\in\mathbb{N} \mid n|a \text{ וגם } n|b\}$

כל המספרים שהם מחלקים משותפים של $a+cb$ ו-b = כל המספרים שהם מחלקים משותפים של a ו-b

ולכן ינבע שהמירבי בצד ימין הוא המירבי בצד שמאל.

נראה הכלה דו-כיוונית:

($\subseteq$) יהי e מחלק משותף של a ו-b $\Leftarrow$ $e|a$ וגם $e|b$ $\Leftarrow$ $e|a+cb$ $\Leftarrow$ $e|b$ וגם $e|a+cb$ $\Leftarrow$ e מחלק משותף של $a+cb$ ו-b.

המעבר הזה נקרא "פינג רונג"

מי שרוצה בכ"ז, הנה הסבר...

$\exists k,\ ke=a \Leftarrow e|a$

$\exists l,\ le=b \Leftarrow e|b$

$a+cb = ke+cle$

$= e(k+cl)$

($\supseteq$) יהי f מחלק משותף של $a+cb$ ושל b $\Leftarrow$ $f|a+cb$ וגם $f|b$ $\Leftarrow$ $f|\underbrace{a+cb-c\cdot b}_{=a}$ $\Leftarrow$ $f|a$ וגם $f|b$ $\Leftarrow$ f מחלק משותף של a ו-b.

מסקנה מלמת ההכנה: (תכף נראה שימוש!)

לכל $a>b$ טבעיים מתקיים $(a,b) = (b, a \bmod b)$

לדוגמא: $(\overset{a}{18},\overset{b}{12}) = (\overset{b}{12}, \overset{a \bmod b}{6})$

הוכחת המסקנה: לפי משפט החלוקה $a = \underbrace{q}_{=\lfloor \frac{a}{b} \rfloor} b + \underbrace{r}_{=(a \bmod b)}$ $[0\le r<b\ ,\ q,r \text{ שלמים}]$

$\begin{array}{r|l} 17 & 5 \\ \hline & 3\ (2) \end{array}$

לכן: $17 = \underbrace{3}_{=\lfloor \frac{17}{5} \rfloor}\cdot 5 + \underbrace{2}_{=17 \bmod 5}$

נציב בלמת ההכנה $c = -\lfloor \frac{a}{b} \rfloor$ ונקבל $(\underbrace{a - \lfloor \frac{a}{b} \rfloor b}_{=r\,=\,a \pmod b}, b) = (a,b)$

האלגוריתם של אוקלידס

EUCLID(a, b)

קלט: $a \ge b$ טבעיים. פלט: (a,b) //

1. אם $b=0$ החזר את a
2. אחרת, החזר את EUCLID(b, a mod b)

אינטואיטיבית: אין מחזיר את (a,b) כי $(a,b)=(b, a \bmod b)$. אבל צריך להוכיח למה זה. הסבר בקצרה: כי הקודם נהיה קטן לבסוף.

דוגמה.

$$\underset{}{(\overset{a}{72}, \overset{b}{30})} = (\underset{\text{שני}}{\overset{\overset{a}{b}}{30}}, \underset{\text{ראשון מוד שני}}{\overset{\overset{b}{a \bmod b}}{12}}) = (\underset{\text{שני}}{\overset{b}{12}}, \underset{\text{ראשון מוד שני}}{\overset{a \bmod b}{6}}) = (6,0) = 6$$

עוד דוגמה:

$$(4,15) = (15,4) = (4,3) = (3,1) = (1,0) = 1$$

(הפוך סדר כי כדי להפעיל את האלגוריתם צריך שהראשון יהיה גדול)

אלגוריתם אוקלידס המורחב: מאפשר לא רק למצוא את $d=(a,b)$ אלא גם למצוא מקדמים x,y כך ש- $d=ax+by$.

נראה זאת בדוגמה: נמצא את $d=(252,198)$ ונמצא x,y שלמים כך ש- $d = 252\cdot x + 198\cdot y$.

	שלב ②	שלב ① - מפעילים EUCLID:
$(252,198)$	$252 = \boxed{1}\cdot 198 + 54$	$18 = (-1)198 + 4\cdot 54 = (-1)198 + 4(252-198) = 4\cdot 252 + (-5)198$ חייבים להפטר מה-54 ולמקומו להשתמש ב-252
$(198,54)$	$198 = \boxed{3}\cdot 54 + 36$	$18 = 1\cdot 54 + (-1)\cdot[198 - 3\cdot 54] = (-1)198 + 4\cdot 54$ רוצים להיפטר מה-36 ולמקומו להשתמש ב-198
$(54,36)$	$54 = \boxed{1}\cdot 36 + 18$	$18 = 1\cdot 54 + (-1)\cdot 36$ (מכיוון שמה להיות מזמן)
$(36,18)$	$36 = \boxed{2}\cdot 18 + 0$	$18 = 0\cdot 36 + 1\cdot 18$ (בסיס)
$(18,0)$	$d=18$	

שלב ③ - מלמטה למעלה - מציבים את 18 בכל שורה כצירוף לינארי של ה-a וה-b של אותה שורה!

מומלץ מאוד להמציא לכם דוגמאות ולהתאמן עליהן.

הוכחת האלגוריתם

→ שהוא עוצר

→ שהוא מחזיר את (a,b)

טענה: לכל $a \ge b > 0$, $EUCLID(a,b)$ עוצר.

הוכחה: נתבונן בסדרת הקריאות הרקורסיביות של האלגוריתם

(סימון כדי לא לבלבל עם gcd) →

$EU(a, \overset{a_1}{b})$

$EU(b, \overset{a_2}{a \bmod b})$

$EU(a \bmod b, \underbrace{\overset{a_3}{b \bmod (a \bmod b)}})$

$EU(b \bmod (a \bmod b), \overset{a_4}{(a \bmod b) \bmod} \;\_\_\_\_)$

נסמן

$\vdots$

$a_1 = b$

$a_2 = a \bmod b$, $a_3 = a_1 \bmod a_2$

$a_{i+1} = a_{i-1} \bmod a_i$

נראה באינדוקציה על i כי $a_i \le b-(i-1)$, לכל $i \ge 2$

בדיקה עבור $i=2$: $a_2 \overset{?}{\le} \underbrace{b-(2-1)}$

$$\underset{a \bmod b}{a_2} \le \underset{b-1}{b-(2-1)}$$

$a \bmod b \le b-1$

נניח נכונות עבור i כלשהו: $a_i \le b-(i-1)$

צ"ל עבור $i+1$ כי $a_{i+1} \le b-i$

הוכחה

$$\underset{\text{מהגדרת } a_{i+1}}{a_{i+1} \le a_i - 1} \underset{\text{לפי הנחה}}{\le} b-(i-1)-1 = b-i$$

סוף הוכחה

קיבלנו: $\forall i \ge 2, \quad a_i \le b-(i-1)$

נרצה להראות שאם ממשיכים הרבה בסדרה, מגיעים למספרים שליליים.

$a_{b+1} \le b-(b) = 0$

ונובע כי $a_{b+1}=0$, מכיוון שבשום איטרציה של האלגוריתם לא מגיעים לערכים קטנים מ-0, (כמו $a \bmod b$ שהוא מוגדר כמספר ≥ 0) ולכן האלגוריתם עוצר כאשר הארגומנט השני הוא 0.

טענה:
לכל $a \geq b > 0$, $EUC(a,b)$ מחזיר את $gcd(a,b)$.

הוכחה:
נוכיח באינדוקציה על מספר האיטרציות שמבצע EUC על הקלט הנתון.
בסיס האינדוקציה: $i=1$ כלומר $b=0$. אז $EUC(a,b)=a$ וגם $gcd(a,b)=a$.
הנחת האינדוקציה עבור i: אם EUC רץ i איטרציות אז EUC מחזיר את ה-gcd של הקלט.
נוכיח עבור $i+1$ כי אם EUC רץ $i+1$ איטרציות אז הוא מחזיר את ה-gcd של הקלט.
הוכחה: נניח כי $EUC(a,b)$ רץ $i+1$ איטרציות.
נבצע איטרציה אחת ונקבל כי הוא מחזיר את $EUC(b, a \bmod b)$.
כעת $EUC(b, a \bmod b)$ רץ i איטרציות ולכן לפי הה״א מחזיר את $gcd(b, a \bmod b)$. אבל לפי ה״מסקנה מלמה הקודמת״ (עמ׳ 21) זה שווה בדיוק ל-$gcd(a,b)$ כנדרש.

[נראה שאם נבחר [illegible] הזמן [illegible] (נקבל איטרציות [illegible]). הזמן הוא שיהיה $b<F_{k+1}$ (איבר סדרת פיבונאצ'י) אז [illegible] מבצע [illegible]]

ריצה קוואדרטית כלומר סיבוכיות זמן ריצה [illegible] ב-a.

משוואות דיופנטיות לינאריות

משוואה דיופנטית: $3x+6y=18$

פתרונות עם x,y שלמים:

$3\cdot\boxed{1}+6\cdot\boxed{2}=18$

$3\cdot\boxed{-6}+6\cdot\boxed{6}=18$

$\vdots$

האם יש ∞ פתרונות? יש אפילו שאלה איך ברגע שמצאנו פתרון אחד אפשר למצוא את כל האחרים?

$2x+10y=17$

אין פתרון עם x,y שלמים. [illegible] (צד שמאל זוגי [illegible])

(כמובן שיש פתרון [illegible] כמו [illegible] קווים הנ״ל)

בס"ד

משוואה דיאופנטית (לינארית): משוואה מהצורה $ax+by=c$. $a,b,c\in\mathbb{Z}$ (כאשר x,y נעלמים)

<u>למה</u> "מתי אפשר למצוא פתרון בשלמים למשוואה דיאופנטית":
למשוואה $ax+by=c$ $(a,b,c\in\mathbb{Z})$ יש פתרון ב-$\mathbb{Z}$ אמ"מ $(a,b)|c$.
(אינטואיטיבית: הגיוני שאגף שמאל בטוח מתחלק ב-(a,b) ולכן אם c לא מתחלק אז אין פתרון בשלמים.)
(דוגמא ראשונה: $(3,6)=3\,|\,18$ דוגמא שניה: $(2,10)=2\nmid 17$)

<u>הוכחה</u>

$(\Leftarrow)$ נתון: יש פתרון בשלמים, (x_0,y_0).
צ"ל: $(a,b)\,|\,c$

<u>הוכחה:</u> נסמן $d=(a,b)$ $\Leftarrow$ יש $r,s\in\mathbb{Z}$ כך ש $\begin{cases} a=dr \\ b=d\cdot s \end{cases}$.

(x_0,y_0) פתרון בשלמים $\Leftarrow$

$$\underset{\text{כי } (x_0,y_0) \text{ פתרון}}{c=}ax_0+by_0\underset{\text{הצבה}}{=}(dr)x_0+(d\cdot s)y_0=d(rx_0+sy_0)$$

$\Leftarrow$ $d\,|\,c$

$(\Rightarrow)$ נתון: $\overset{(a,b)}{d}|c$
צ"ל: יש פתרון בשלמים למשוואה.

<u>הוכחה:</u> (מאיזה משפט נשתמש? בזו, כי הוא עוסק אלמנט מממממ למשהו שדומה למשוואה דיאופנטית.)

$d|c$ $\Leftarrow$ קיים $t\in\mathbb{Z}$ כך ש- $d\cdot t=c$

לפי משפט בזו יש $x_1,y_1\in\mathbb{Z}$ כך ש $d=ax_1+by_1$ $\Leftarrow$ דומה לנדרש

$$c=d\cdot t=(ax_1+by_1)t=a(tx_1)+b(ty_1)$$

לכן tx_1, ty_1 הם פתרון בשלמים למשוואה. <u>מש"ל</u>

מההוכחה:
<u>"מתכון למציאת פתרון אחד למשוואה דיאופנטית $ax+by=c$ כאשר $\overset{d}{(a,b)}|c$"</u>

1. ע"י אלגוריתם אוקלידס המורחב מוצאים את $d=(a,b)$ ומוצאים x_1,y_1 כך ש $ax_1+by_1=d$
2. מוצאים t כך ש $d\cdot t=c$.
3. הפתרון המבוקש הוא $\underbrace{tx_1}_{x_0},\ \underbrace{ty_1}_{y_0}$

<u>הדוג' של $3x+6y=18$</u>

$d=(3,6)=3$

$\underset{3}{d}=3\boxed{1}+6\boxed{0}$ ($x_1=1$, $y_1=0$)

$\underset{3}{d}\cdot\boxed{6}=\underset{18}{c}$

$\underset{6\cdot 1}{tx_1}$, $\underset{6\cdot 0}{ty_1}$

$\boxed{3\cdot 6+6\cdot 0=18}$

עכשיו נלמד - את משפט איך להגיע מפתרון אחד לכל הפתרונות:

נאמר את המשפט בלי הוכחה לגבי:

③ אם רוצים למצוא ∞ פתרונות, הם כולם מהצורה

$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$ לכל $t\in\mathbb{Z}$

(מי שרוצה הוכחה יש בספר הקורס שבמודל).

מספרים ראשוניים

הגדרה: מספר $1<a\in\mathbb{N}$ נקרא ראשוני אם הוא מתחלק רק בעצמו וב-1.

מספר שאינו ראשוני נקרא פריק.

1-לא ראשוני, 2-ראשוני, 7-ראשוני, 9-לא ראשוני.

המשפט היסודי של האריתמטיקה: "לכל טבעי יש פירוק יחיד לראשוניים" לדוג': $24=2\cdot2\cdot2\cdot3=2^3\cdot3$ (הצורה הקנונית)

כל טבעי גדול מ-1 ניתן להצגה כמכפלת ראשוניים. ההצגה יחידה עד כדי סדר הגורמים.

צורה קנונית של פירוק לראשוניים: $n=p_1^{a_1}\cdot p_2^{a_2}\cdots p_k^{a_k}$, $a_i>0$ $\forall i\in[k]$ (הסבר טוב), $\underbrace{p_1<\dots<p_k}_{\text{נקראים "גורמים ראשוניים"}}$

(נמצא בספר את הוכחת המשפט היסודי. כדי להוכיח כמה הכנות)

למה: לכל $n>1$ טבעי, יש מחלק ראשוני. (זו גרסה הרבה יותר חלשה מאשר המשפט היסודי).

הוכחה: נניח בשלילה שלא ויהי n הטבעי הקטן ביותר שאין לו מחלק ראשוני. (שמש ב-WOP!). אם n ראשוני אז חלוקה סתירה. אם n פריק אז $n=a\cdot b$ עבור $2\le a,b<n$, ומהמינימליות n יש ל-a מחלק ראשוני p ⇐ חלק, סתירה.

מסקנה: אם $n>1$ פריק אז יש לו מחלק ראשוני $\le\sqrt{n}$. (כי אחרת, נקבל בהוכחה הקודמת $a,b>\sqrt{n}$ ⇐ $n<a\cdot b$.)

אמת/שקר: אם p ראשוני $p|ab$ אז $p|a$ או $p|b$! (אם p לא ראשוני זה לא נכון $12|6\cdot4$ אבל $12\nmid4, 12\nmid6$)

אמת!

תזכורת: הלמה של אוקלידס "אם מספר מחלק מכפלת שני מספרים וזר לאחד מהם, אז הוא מחלק את השני".

הוכחה: אם $p|a$ סיימנו. אחרת $(p,a)=1$ (כי p ראשוני ו-$(p,\square)$ הוא 1 או p). ואז לפי הלמה של אוקלידס $p|b$.

הכללה:

("אם ראשוני p מחלק מכפלה, אז הוא מחלק את אחד הגורמים")

אם p ראשוני ו- $p|a_1\cdots a_n$ $(\forall i\in[n], a_i>0)$

אז קיים $j\in[n]$ כך ש-$p|a_j$.

$\underbrace{6}_{3\cdot2} | \underbrace{9}_{3\cdot3}\cdot\underbrace{2}_{2}\cdot\underbrace{2}_{2}$ ← לא ראשוני, ולכן גורם אחד של 6 הגיע מ-9 והשני מ-2, אבל כשראשוני זה לא קורה