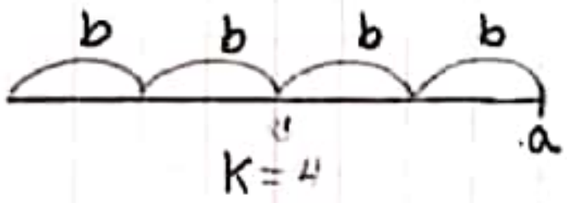
משפט החלוקה

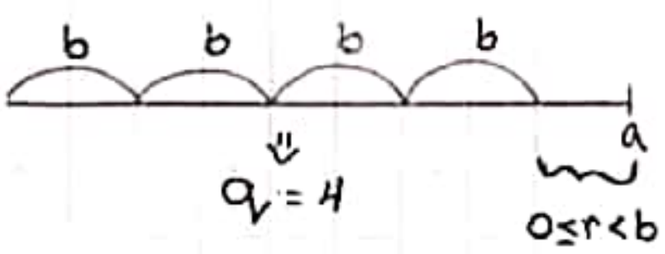
א) משפט החלוקה עבור שארית

יהי a,b זוג שלמים $(a,b\in\mathbb{Z})$, נאמר ש-b מחלק את a אם קיים $k\in\mathbb{Z}$ כך שמתקיים $a=k\cdot b$. במידה ו-b מחלק את a נסמן לפעמים: $b|a$.



ב) משפט החלוקה עם שארית

יהי a,b זוג שלמים כך ש-$b>0$, אזי קיימים זוג יחיד של מספרים שלמים q,r כך שמתקיים: $a=q\cdot b+r$ וכן $0\le r<b$,



ג) הוכחה

נתקן את ההוכחה ל-2. קודם נוכיח כי קיימים q,r, ולאחר מכן נוכיח יחידות.

(1) נגדיר קבוצה S כך $S=\{a-kb\ge 0 : k\in\mathbb{Z}, a-kb\}$. קבוצה S היא קבוצה לא ריקה ב-$\mathbb{Z}^+$ המקיימת את כל ההנחות של W.O.P, לפי עיקרון W.O.P לקבוצה זו יש איבר מינימלי, יהי איבר כזה r. מכיוון שמתקיים $a-kb=r$ עבור k כלשהו, נגדיר k כזה כתור q ונקבל $a=qb+r$. מהגדרת S נובע ש-$r\ge 0$ נותר להוכיח כי $r<b$. נניח בדרך השלילה כי $r\ge b$, אזי מתקיים $r-b\ge 0$, ולפי הגדרת r $a-qb-b=a-b(q+1)<r$. נשים לב כי $a-b(q+1)\ge 0$ מכך ש $r\ge b$ ולכן $r-b\ge 0$. מה שאומר ש-$a-b(q+1)$ גם כן שייך ל-S. ונו היא סתירה מכך שאמרנו ש-$a-b(q+1)<r$ ונו היא סתירה למינימליות של r ב-S. לכן לא יכול להתקיים $r\ge b$ אלא רק $r<b$.

(2) יהיו r_1,r_2,q_1,q_2 כך שמתקיים המשוואות: $a=q_1b+r_1$

$a=q_2b+r_2$ $r_1=r_2$ ונוכיח $q_1=q_2$.

אם נחסיר מינהם נקבל: $r_1-r_2=b(q_1-q_2)\Rightarrow b\mid r_1-r_2 \Leftarrow r_1-r_2=(q_2b+r_2)-q_1b=0$

נשכור כי $r_1,r_2\ge 0$ ומתקיים $r_1-r_2<b$, אפשר שאם r_2 קרוב ל-b ו-r_1 קרוב ל-0 נקבל r, ואם הפוך נקבל $-r$, כזה אפשר שאם $r_1-r_2\mid b$ אזי האפשר היחיד בתוקף שהוא 0 ומתקיים: $r_1=r_2\Leftarrow r_1-r_2=0\Leftarrow 0\cdot b=r_1-r_2$

ואם נחזור למשוואות ונזכיר נקבל גם $q_1=q_2$.

14/11 בס"ד

ג) ניסוח נוסף למשפט החלוקה

יהי a,b זוג שלמים כך ש- $b>0$, אזי תמיד מתקיים: $a=\lfloor \frac{a}{b}\rfloor\cdot b+(a \bmod b)$

$\lfloor\ \rfloor$ - היא סימן לפונקציה שמעגלת כלפי מטה כל מספר עשרוני שמכניסים אליה $\lfloor\ \rfloor:R\to Z$.

mod - היא פונקציה שמקבלת שני מספרים זורקת את השלם ומשאירה את השארית.

* נשים לב כי כעת ניתן לראות בבירור כי q ו- r יחודיים.

ה) משפטים חשובים

(1) משפט: יהיו a,b,c מספרים שלמים וגדולים מ-0 $(a,b,c\in Z^+)$ אם $a|b$ ו- $b|c$ אזי $a|c$.

הוכחה: לפי משפט החלוקה קיימים $k,j\in Z$ כך ש- $a\cdot k=b$ ו- $j\cdot b=c$, לכן מתקיים: $a\cdot(k\cdot j)=c$

נמצא ש- $a|c$.

(2) משפט: יהיו $a,b,c\in Z^+$, אם $a|b$ וגם $a|c$ אזי קיימים $e,d\in Z$ כך שמתקיים: $a|eb\pm dc$

הוכחה: לפי משפט החלוקה קיים $k,j\in Z$ כך ש- $a\cdot k=b$ ו- $a\cdot j=c$, $b\pm dc=eaj\pm dak=a(ej\pm dk)$:

נמצא ש- $a|eb\pm dc$.

14/11

בס״ד

GCD

א) הגדרה

יהי שני מספרים a,b שלמים וגדולים מ-0 ($a,b\in\mathbb{Z}^+$). אזי המחלק המשותף הגדול ביותר של a ו-b נקרא ה-GCD (Greatest Common Diviser) של a ו-b. ונסמנו (a,b) או: (b,a) או $\gcd(a,b)$.

דוגמאות: $(12,6)=6$, $(3,2)=1$, $(16,6)=2$, $(108203,108202)=1$

ב) משפט בזו

עבור $a,b\in\mathbb{Z}^+$ נגדיר את הקבוצה $L(a,b):=\{ma+nb : m,n\in\mathbb{Z}\}$. משפט בזו אומר שהאיבר השלם וחיובי הכי קטן בקבוצה $L(a,b)$ הוא ה-gcd של a,b. $(a,b)\in L(a,b)\wedge\mathbb{Z}^+$

ג) הוכחת משפט בזו

תהי הקבוצה $L(a,b)\wedge\mathbb{Z}^+$ שאינה קבוצה ריקה, ויהי d איבר מינימלי בה שקיומו מובטח לנו מעקרון ה W.O.P. כדי להוכיח שמתקיים $d=(a,b)$ יש להוכיח שלוש טענות:

(1) d מחלק את a - $d|a$.

(2) d מחלק את b - $d|b$.

קיום שני תנאים אלו יתן לנו פתרון אפשרי.

(3) יהי $D(a)$ קבוצת המחלקים של a ו-$D(b)$ קבוצת המחלקים של b. אזי d הוא המחלק המשותף הגבוה ביותר. $d=\max[D(a)\wedge D(b)]$. ביחד עם טענה 3 נקבל פתרון אופטימלי.

הוכחה:

(1) לפי משפט החלוקה מתקיים עבור a,d - $a=q\cdot d+r$ כאשר $0\le r<d$. אם נוכיח $r=0$ אזי אכן $d|a$. נניח בשלילה כי $0<r$. אם נבודד את r ונציב את ערכו של d נקבל ביטוי הגדול מ-0 ומהצורה $ma+nb$: $r=a-q\cdot d=a-q(ma+nb)=a(1-qm)+b(-qn)$

נמצא אם כן כי גם $r\in L(a,b)\wedge\mathbb{Z}^+$ כמו איבר d. אולם נשים לב כי לפי הגדרת משפט החלוקה $d>r$, וזו סתירה למינימליות של d בקבוצה $L(a,b)\wedge\mathbb{Z}^+$. לכן לא יכול להיות ש-$0<r$ וחייב להתקיים $r=0$, מכאן ההוכחה לכך ש-$d|a$.

(2) באותה הדרך בדיוק שהוכחנו את טענה (1) $d|a$, ניתן להוכיח את טענה (2) $d|b$.

(3) נגדיר איבר c כך ש-$c\in D(a)\wedge D(b)$, כלומר ש-c מחלק גם את a וגם את b. צ״ל ש-$c|d$, מפני שאם לכל c המחלק גם את a וגם את b c מחלק את d אז בוודאי כי מהמשוואה בשמאל יוצא ש-$\frac{d}{c}$ הוא מספר שלם, לכן אכן $c|d$.

$$\frac{d}{c}=\frac{ma+nb}{c}=m\underset{\in\mathbb{Z}}{\left(\frac{a}{c}\right)}+n\underset{\in\mathbb{Z}}{\left(\frac{b}{c}\right)}$$

מספרים שלמים.

14/11 בס"ד

ז) הגדרות gcd

יש שני דרכים להגדיר את המחלק המשותף המקסימלי (gcd). למרות שכבר השתמשנו בהם בדרך ההוכחה של משפט בזו נגדיר אותם באופן מסודר כעת:

יהי a,b שני מספרים שלמים וגדולים מ-0, $0<a,b\in Z^+$. נגדיר את ה-gcd שלהם, אותו נסמן (a,b), בשני דרכים:

(1) יהי $D(a)$ קבוצת כל המחלקים של a ו-$D(b)$ קבוצת כל המחלקים של b, $D(a)=\{m\in Z: m|a\}$, $D(b)=\{n\in Z: n|b\}$. אזי מתקיים: $(a,b)=\max(D(a)\wedge D(b))$.

(2) מתקיימים שתי טענות: ① $(a,b)|a$ וגם $(a,b)|c$.

② לכל c שלם כך ש $c|a$ וגם $c|b$ אזי מתקיים גם $c|(a,b)$.

ה) מספרים זרים

שני מספרים שלמים a ו-b ייקראו "זרים" אם מתקיים: $(a,b)=1$. כלומר, שאין להם שום מחלק משותף פרט ל-1 שמחלק כל שני מספרים אפשריים. לכן הם נקראים "זרים".

<u>משפט</u>: שני מספרים שלמים עוקבים תמיד יהיו זרים - $(a+1,a)=1$.

<u>הוכחה</u>: לפי משפט בזו $(a+1,a)$ הוא האיבר הכי קטן בקבוצה $L(a,b)\wedge Z^+$ כאשר $L(a,b)=\{ma+nb: m,n\in Z\}$

נשים לב כי $(a+1)\cdot 1+a\cdot(-1)=1$ גם היא איבר בקבוצה $L(a,b)\wedge Z^+$. ומכיוון שערכו ש"ק ל-1 אז בוודאי שהוא המינימלי בקבוצה זו. לכן $(a+1,a)=1$.

ו) משפטים חשובים ב-gcd

(1) **משפט:** יהי a,b,c מספרים שלמים. אם $a|c$ וגם $b|c$ וגם $(a,b)=1$ אזי גם $ab|c$.

הוכחה: לפי משפט בזו קיימים $m,n\in Z$ כך ש- $ma+nb=1$. נבנה את המשוואה הבאה $c=c(ma+nb)=cma+cnb$. היות ו-$a|c$ אזי קיים $k\in Z$ כך ש-$c=k\cdot a$, וכן היות ש-$b|c$ אזי קיים $j\in Z$ כך ש-$c=j\cdot b$, נציב ערכים אלו במשוואה באופן הבא.

$c=jbma+kanb=ab(jm+kn)$. ומכאן ש-$ab|c$.

(2) **משפט:** יהיו a,b,c מספרים שלמים אם $a|bc$ ו-$(a,b)=1$ אזי $a|c$.

הוכחה: לפי משפט בזו קיימים $m,n\in Z$ כך ש-$ma+nb=1$. נבנה את המשוואה הבאה: $c=c\cdot(ma+nb)=cma+cnb$. היות ו-$a|bc$ קיים $k\in Z$ כך ש-$bc=a\cdot k$. נציב במשוואה $c=cma+kna=a(cm+kn)$. ומכאן ש-$a|c$.

(3) <u>משפט:</u> יהיו a,b,c שלמים וגדולים מ-0 ($a,b,c \in \mathbb{Z}^+$), אזי מתקיים: $(ca,cb)=c(a,b)$.

<u>הוכחה:</u> לפי משפט בעל $c\cdot(a,b)$ הוא מהצורה $c(ma+nb)$. נשים לב שמתקיים:

$c(ma+nb)=(ca)\cdot m+(cb)\cdot n$, שגם הוא תואם להגדרה $L(a,b)\wedge\mathbb{Z}^+$. לכן נקבל $(ca,cb)=c(a,b)$.

14/11

בס"ד

b) LCM (Least Common Multiple).

עבור שני מספרים שלמים $a,b\in\mathbb{Z}$ נגדיר את $c\in\mathbb{Z}^+$ להיות המכפלה המשותפת הקטנה ביותר של a ו-b, בסימון $\text{lcm}(a,b)=c$, אם מתקיימים התנאים הבאים:

(1) $a|c$ וגם $b|c$.

(2) לכל מספר $k\in\mathbb{N}$ כך ש-$a|k$ וגם $b|k$, אזי בהכרח $c\le k$.

דוגמא: הכפולות המשותפות של 12- ו-30 הם: $60, 120, 180,\dots$. נשים לב כי $\text{lcm}(a,b)=60$.

נוכיח כי ה-lcm קיים לכל שני מספרים: יהיו $a,b\in\mathbb{Z}$ ונגדיר קבוצה $S=\{c\in\mathbb{Z}^+: c|a\wedge c|b\}$ קבוצה זו היא קבוצת כל המכפלות המשותפות של a ו-b. נשים לב כי $ab\in S$ לכן קבוצה זו אינה ריקה. ולפי עיקרון W.O.P יש בה איבר מינימלי, איבר זה הוא $\text{lcm}(a,b)$.

משפט: יהיו $a,b\in\mathbb{Z}$ אזי מתקיים: $(a,b)\cdot\text{lcm}(a,b)=a\cdot b$. המסקנה היא: $\text{lcm}(a,b)=\frac{a\cdot b}{(a,b)}$.

הוכחה: נגדיר $d=(a,b)$ ו-$m=\frac{a\cdot b}{d}$. נוכיח כי m מקיים את שני התנאים בהגדרה.

(1) מכיוון ש-d מחלק משותף של a ו-b אז $d|a$ וגם $d|b$, ולפי משפט החלוקה קיימים $k,j\in\mathbb{Z}$ כך ש-$d\cdot k=a$ ו-$d\cdot j=b$. נציב ערכים אלו ונקבל: $m=\frac{a\cdot\cancel{d}j}{\cancel{d}}=aj$. $m=\frac{\cancel{d}k\cdot b}{\cancel{d}}=bk$. לכן אכן מתקיים $a|m$ וגם $b|m$.

(2) יהי c מכפלה משותפת של a ו-b, אזי קיימים $u,v\in\mathbb{Z}$ כך ש-$c=ua=vb$. נוכיח כי $m\le c$ ויותר מכך $m|c$. לפי משפט בזו קיימים $x,y\in\mathbb{Z}$ כך ש-$d=ax+by$. נבדוק את המשוואה הבאה:

$$\frac{c}{m}=\frac{c}{\frac{ab}{d}}=\frac{cd}{ab}=\frac{c(ax+by)}{ab}=\frac{c\cancel{a}x}{\cancel{a}b}+\frac{c\cancel{b}y}{a\cancel{b}}=\frac{cx}{b}+\frac{cy}{a}=\frac{v\cancel{b}x}{\cancel{b}}+\frac{u\cancel{a}y}{\cancel{a}}=vx+uy$$

מכאן שמתקיים $m(vx+uy)=c$, לכן אכן הוכחנו כי $m|c$.

דוגמא: עבור 30 ו-12- מתקיים: $30\cdot(-12)=-360$, $(30,-12)=6$, לכן: $\text{lcm}(30,-12)=\frac{-360}{6}=|-60|=60$.

21/11 בס״ד

אלגוריתם אוקלידס - מציאת gcd

א) באמצעות המשפט היסודי של האריתמטיקה

הצעה ראשונה למציאת gcd של שני מספרים עוברת דרך המשפט היסוד של האריתמטיקה. נפרק כל מספר למכפלת המחלקים הראשוניים שלו: $n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$, וניקח את החלק שמופיע בפירוק של שני המספרים. מספר זה הוא ה-gcd שלהם

דוגמא: עבור שני המספרים 72 ו-54 ה-gcd הוא:

$72=2^3\cdot 3^2 \quad , \quad 54=2\cdot 3^3$

$(72,54)=2\cdot 3^2=18$

ב) אלגוריתם אוקלידס (Euclid)

יש שני דרכים לכתוב את אלגוריתם אוקלידס: בדרך איטרטיבית או רקורסיבית.

איטרטיבית

קלט: שני מספרים טבעיים $a,b\in\mathbb{Z}^+$.

פלט: (a,b).

```
while (a ≠ b·k) {        // עבור k∈Z כלשהו.
    a = b·q + r          // יישום משפט החלוקה
    a = b
    b = r
}
return b
```

רקורסיבית

קלט: שני מספרים טבעיים $a,b\in\mathbb{Z}^+$ המקיימים: $a\geq b>0$

פלט: (a,b).

```
if (b=0)
    return a
else
    return Euclid(b, a mod b)
```

ג) הוכחת האלגוריתם

נחלק את ההוכחה לשני שלבים: קודם נוכיח שהאלגוריתם עוצר, ולאחר מכן נוכיח שאכן מחזיר gcd

האלגוריתם עוצר:

נתבונן בערכי הסדרה שנוצרת מערכי הסדרה b לאורך הרצת האלגוריתם:

$, a \bmod b, b \bmod (a \bmod b), (a \bmod b) \bmod [b \bmod (a \bmod b)] =$

נגדיר סדרה זו בצורה נוחה יותר: $X_{i+1}=X_{i-1} \bmod X_i$.

טענה: לכל $i\geq 2$ מתקיים: $X_i\leq b-(i-1)$. אם נוכיח שטענה זו נכונה אזי נוכל לומר בוודאות שעבור $2\leq i\leq b+1$ האלגוריתם עוצר, מפני שעבור $i=b+1$ נקבל $X_i\leq 0$, ומכיוון שכל X_i הוא

21/11

בס"ד

השארית r ממשפט החלוקה מקיים $0 \le r$, נקבל $0 \le x_{b+1} \le 0$, כלומר $x_{b+1}=0$. ולכן האלגוריתם עוצר.

הוכחה באינדוקציה: בסיס - עבור $i=2$ ולפי הגדרת משפט החלוקה: $x_2 = a \bmod b = r \le b-1 = b-(2-1)$ ✓

צעד - נניח עבור i כי מתקיים: $x_i \le b-(i-1)$

נוכיח עבור $i+1$. לפי הגדרת הסדרה $x_{i+1} = x_{i-1} \bmod x_i$, ביטוי זה לפי הגדרת משפט החלוקה על x_{i-1} ו-x_i מקיים: $x_{i-1} \bmod x_i \le x_i - 1$. ולפי הנחת האינדוקציה $x_i - 1 = b-(i-1)-1 = b-[(i+1)-1]$. נמצא ש-$x_{i+1} \le b-[(i+1)-1]$. מ.ש.ל. לכן האלגוריתם עוצר.

האלגוריתם מחזיר gcd

מכך שהוכחנו שהאלגוריתם עוצר הוכחנו שיש ערך חזרה. כעת כל שעלינו להוכיח הוא שה-gcd בכל הקלטים לאורך ריצת האלגוריתם נשמר. נסתכל על סדרת הקלטים של האלגוריתם:

$$(a,b)\to(b,a \bmod b)\to(a \bmod b,\ b \bmod (a \bmod b))\to\ldots\to(d,0)\to \text{return } d.$$

ניתן לראות כי בכל קלט (a,b) של האלגוריתם הקלט הבא יהיה $(b, a \bmod b)$. לכן כל שעלינו להוכיח הוא שמתקיים: $(a,b)=(b, a \bmod b)$.

משפט עזר: לכל שלושה מספרים טבעיים $a,b,c \in \mathbb{Z}^+$ מתקיים: $(a,b)=(b,a+cb)$.

הוכחה: נוכיח באמצעות הכלה דו כיוונית שקבוצת כל המחלקים של a,b שווה לקבוצת המחלקים של $a+cb,b$, כלומר שמתקיים: $D(a)\wedge D(b) = D(a+cb)\wedge D(b)$.

(1) $D(a)\wedge D(b) \subseteq D(a+cb)\wedge D(b)$ - יהי $e \in D(a)\wedge D(b)$. היות ו-$e|b$ נותר להוכיח $e|a+cb$. לפי משפט (2) במשפט החלוקה מכיוון ש-$e|a$ ו-$e|b$ אזי $e|a+cb$ עבור $c\in\mathbb{Z}$.

(2) $D(a+cb)\wedge D(b) \subseteq D(a)\wedge D(b)$ - יהי $e \in D(a+cb)\wedge D(b)$. היות ו-$e|b$ נותר להוכיח $e|a$. לפי משפט (2) במשפט החלוקה מכיוון ש-$e|a+cb$ ו-$e|b$ אזי עבור $k=-c$ מתקיים $e|a+cb+kb \Rightarrow e|a+cb-cb \Rightarrow e|a$. מ.ש.ל.

משפט עזר

לפי משפט החלוקה עבור כל שני מספרים טבעיים $a,b\in\mathbb{Z}^+$ מתקיים $a=qb+r$, לפיכך $r = a-qb = a \bmod b$. לפי המשפט עזר אם נבחר $c=-q$ נקבל: $,b)=(b,a-qb)=(b,a \bmod b)$ נמצא שה-gcd נשמר לכל אורך האלגוריתם, ולכן הפלט של האלגוריתם יהיה (a,b) כנדרש.

21/11 בס״ד

ד) אלגוריתם אוקלידס המורחב (Extended Euclid)

יהי שני מספרים $a,b\in\mathbb{Z}^+$, לפי משפט בזו ה-gcd שלהם יכול להיות מבוטא באופן "יחודי" באמצעות הקומבינציה הלינארית $(a,b)=ma+nb$ כאשר $n,m\in\mathbb{Z}$. אלגוריתם אוקלידס המורחב יעזור לנו למצוא את m ו-n אלו. אלגוריתם אוקלידס המורחב הוא בעצם אלגוריתם אוקלידס הרגיל אלא שעובד בצורה הפוכה, נסתכל על אלגוריתם אוקלידס עבור $(252,198)$ ⇙

$$252=1\cdot198+\boxed{54}$$
$$198=3\cdot54+\boxed{36}$$
$$54=1\cdot36+\boxed{18}$$
$$36=2\cdot18+0$$
$$(252,198)=18$$

כפי שאנו יודעים ש-$(252,198)=18$, ניקח את כל האיברים בצד הימני של כל משוואה שאינם 0 ונחשב אותם; נקבל:

$$\begin{cases}(1)\ 18=54-1\cdot36\\(2)\ 36=198-3\cdot54\\(3)\ 54=252-1\cdot198\end{cases}$$

נציב את המשוואה השנייה בראשונה, לא נחשב תוצאה אלא רק נחבר מקדמים של מספרים זהים.

ואז נציב את המשוואה השלישית במשוואה שהתקבלה, שוב לא נחשב אלא רק נחבר מקדמים של מספרים זהים.

$$18=54-1(198-3\cdot54)=4\cdot54-198$$
$$18=4(252-1\cdot198)-198=\boxed{4\cdot252-5\cdot198}$$

מצאנו כי $m=4$, $n=-5$.

ה) משוואה דיופנטית

הגדרה: משוואה דיופנטית היא משוואה מהצורה $ax+by=c$.

משפט: משוואה דיופנטית $ax+by=c$ כאשר $a,b,c\in\mathbb{Z}$ "פתירה" אם ורק אם $(a,b)|c$.

הכוונה בפתירה היא שיש שני מספרים שלמים $x_0,y_0\in\mathbb{Z}$ כך שאם נציב במקום x,y נקבל שהמשוואה נכונה.

הוכחה: לפי דרך ההוכחה של משפט "אם ורק אם" נוכיח את שני הכיוונים.

(1) נניח כי המשוואה פתירה עם הערכים x_0 ו-y_0 כך שמתקיים: $a\cdot x_0+b\cdot y_0=c$, צ"ל $(a,b)|c$.

לפי הגדרת gcd קיימים $k,j\in\mathbb{Z}$ כך ש-$(a,b)\cdot k=a$ ו-$(a,b)\cdot j=b$. נציב ערכים אלו במשוואה.

נקבל: $c=(a,b)k\cdot x_0+(a,b)\cdot j\cdot y_0=(a,b)\cdot(k\cdot x_0+j\cdot y_0)$, ומכאן שאכן $(a,b)|c$.

(2) נניח כי $(a,b)|c$, צ"ל שהמשוואה פתירה. לפי משפט החלוקה קיים $k\in\mathbb{Z}$ כך ש-$(a,b)\cdot k=c$.

ולפי משפט בזו קיימים $m,n\in\mathbb{Z}$ כך ש-$(a,b)=ma+nb$. נאחד את המשוואות ונקבל כי $c=(ma+nb)k=a(mk)+b(nk)$. נגדיר $x_0=mk$ ו-$y_0=nk$. מכיוון ש-$x_0,y_0\in\mathbb{Z}$ הם מהווים פתי

משפט: יהי x_0,y_0 פתרון למשוואה דיופנטית $ax+by=c$, אזי כל פתרון אחר למשוואה זו הוא מהצורה: $x=x_0+\left(\frac{b}{d}\right)\cdot t$, $y=y_0-\left(\frac{a}{d}\right)\cdot t$, כאשר $(a,b)=d$ ו-$t\in\mathbb{Z}$ שרירותי.

1) שימוש באלגוריתם אוקלידס המורחב

נשתמש באלגוריתם אוקלידס המורחב לפתיר משוואה דיאפנטית $ax+by=c$, כלומר למצוא $x_0,y_0\in\mathbb{Z}$ כך שהמשוואה: נכונה. סדר הפעולות שלנו לשם כך הוא:

(1) באמצעות אלגוריתם אוקלידס נמצא את (a,b). נבדוק אם $(a,b)|c$ עובדה שהמשוואה פתירה.

(2) באמצעות אלגוריתם אוקלידס המורחב נמצא $m,n\in\mathbb{Z}$ המקיימים: $(a,b)=bn+am$.

(3) נכפיל את מה שנקבל ב-c: $(a,b)c=bnc+amc$.

(4) נחלק ב-(a,b) $a\left(\frac{mc}{(a,b)}\right)+b\left(\frac{nc}{(a,b)}\right)=c$.

(5) נגדיר: $x_0=\left(\frac{mc}{(a,b)}\right)$, $y_0=\left(\frac{nc}{(a,b)}\right)$. אם x_0,y_0 מספרים שלמים סיימנו.

דוגמא: נחפש פתרונות למשוואה: $56x+72y=40$.

נמצא את $(72,56)$ באמצעות אלגוריתם אוקלידס:

$72=1\cdot56+16$

$56=3\cdot16+8$

$16=2\cdot8+0\Rightarrow(72,56)=8$

נפעיל את אלגוריתם אוקלידס המורחב למציאת $m,n\in\mathbb{Z}$

$8=56-3\cdot16$

$16=72-1\cdot56$

$8=56-3(72-1\cdot56)=4\cdot56-3\cdot72$

כך ש- $56m+72n=8$:

אצלנו $m=4$, $n=-3$.

$56\frac{4\cdot40}{8}+72\frac{-3\cdot40}{8}=\frac{8\cdot40}{8}$.

נכפיל משוואה זו ב-40 ונחלק ב-8.

$x_0=\frac{4\cdot40}{8}=\boxed{20}$, $y_0=\frac{-3\cdot40}{8}=\boxed{-15}$

נחלף את x_0 ו-y_0 אתוך המשוואה.

אכן קיבלנו $x_0,y_0\in\mathbb{Z}$. עובדה שהמשוואה הראשונה נכונה: $56\cdot20+72\cdot(-15)=1120-1080=40$ ✓