## ***אלגוריתם gcd***

כזכור, בהינתן זוג מספרים שלמים $a,b$ הגדרנו $\gcd(a,b)$ כשלם החיובי המקסימלי $d$ כך ש $d \mid x$ וכן $d \mid y$. ראינו שאלגוריתם אוקלידס מחשב את $\gcd(a,b)$.

**<u>טענה</u>**: אלגוריתם אוקלידס הוא יעיל. אם הקלט הוא זוג שלמים $a,b$ (נניח $a \geq b$), ונגדיר $m = \lceil \log_2 a \rceil$ אז זמן הריצה הוא $O(m^3)$.

**<u>הוכחה</u>**:

*<u>טענת עזר1</u>*: אם אנחנו מחזיקים כרגע את הזוג $a,b$ (מניחים $a \geq b$), ובצעד הבא הזוג הוא $x,y$ אז מתקיים $y \leq a/2$.

*<u>הוכחה</u>*: נזכור שלפי האלגוריתם $x = b$ וכן $y = a \bmod b$. נפריד לשני מקרים. נניח $a \geq 2b$. אז ברור שמתקיים $y \leq x \leq a/2$. (כי $x = b$ ולפי ההנחה $b \leq a/2$), וסיימנו מקרה זה. נניח $a \leq 2b$. אז, אם נעביר אגפים, נקבל $2(a-b) \leq a$. והיות ש $y = a \bmod b \leq a - b$ אז מתקיים $y \leq a/2$ וסיימנו להוכיח את טענת העזר.

*<u>טענת עזר 2</u>*: אם אנחנו מחזיקים כרגע את הזוג $a,b$ (מניחים $a \geq b$), ואחרי **שני צעדים** הזוג הוא $u,v$ אזי מתקיים $u \leq a/2$.

*<u>הוכחה</u>*: מסקנה ישירה מהטענה הקודמת, שכן $u = y$.

מסקנה: בכל שני צעדים של האלגוריתם האיבר הגדול בזוג קטן לפחות פי 2. לכן אחרי לכל היותר $2m$ צעדים נקבל זוג שהאיבר המכסימלי בו הוא 1. בכל צעד עשינו פעולת $\bmod$ שצורכת זמן $O(m^2)$ פעולות (אפילו פחות, כי המספרים הולכים וקטנים). לכן בסה"כ ביצענו $O(m^3)$ פעולות, והוכחה הטענה.

## ***מהי צורת ה*** $\gcd$ ***?***

עבור זוג שלמים $a,b$ נתבונן בקבוצה $S(a,b) = \{ua + vb \ : \ u,v \in \mathbb{Z}\}$, כאשר $\mathbb{Z}$ היא קבוצת המספרים השלמים. נגדיר $Q(a,b) = \{x : \gcd(a,b) \mid x\}$. כלומר S היא קבוצת המספרים שהם צירופים ליניאריים שלמים ב $a,b$, וכן Q היא קבוצת השלמים המתחלקים ב $\gcd(a,b)$.

**<u>טענה</u>**: $S \subset Q$.

**<u>הוכחה</u>**: זה קל, כי אם נגדיר $d = \gcd(a,b)$, אז קיימים $l,m \in \mathbb{Z}$ כך ש $a = ld, b = md$. לכן $ua + vb = uld + vmd = (ul + vm)d$ ואכן מתחלק ב d.

**<u>טענה:</u>** $S \supset Q$

**<u>הוכחה</u>**: קל לראות שמספיק להוכיח שקיימים $u,v \in \mathbb{Z}$ כך ש $d = \gcd(a,b) = ua + vb$. נוכיח זאת באינדוקציה על $a$. כזכור $\gcd(a,b) = \gcd(b, a \bmod b)$. בזוג החדש ניתן להפעיל את הנחת האינדוקציה, ולקבל (נזכור ש $a \bmod b = a - floor(a/b) * b$)

$$\gcd(a,b)=\gcd(b,a \bmod b)=u'b+v'(a \bmod b)=u'b+v'(\ a-\ floor[\frac{a}{b}]*b\ )=$$

$$v'a+(\ u'-v'*floor[\frac{a}{b}]\ )*\ b$$

כעת אם נציב $u=v', v=(\ u'-v'\ floor([\frac{a}{b}]\ )*b$, נקבל הפתרון הדרוש.

ראינו, אם כך, שיש הצגה $\gcd(a,b)=ua+vb$. נרצה להכליל את אלגוריתם ה gcd כך שיחזיר גם את המספרים u,v.

ext-gcd(a,b) *// extended gcd – returns three numbers (d,u,v) such that d=ua+vb*

```
if (a<b) return gcd(b, a);
if b = = 0  return(a,1,0);
(d, u', v') = gcd(b, a mod b);
return(d , v' , u'-v' * floor(a/b) );

end
```

### *פתרון משוואות מודולריות*

משוואה מודולרית היא $ax=b(\bmod n)$. כאשר $a,b,n$ נתונים ושואלים אם יש פתרון בנעלם x. במלים אחרות, שואלים אם יש שלמים $x,l$ כך ש $ax=b+nl$. כך למשל, למשוואה 2x=1(mod 5) יש פתרון x=3, אך למשוואה 2x=1(mod 6) אין פתרון, מכיוון שנדרשים שלמים $x,l$ כך ש $2x=1+6l$ ולזה אין פתרון כי צד שמאל זוגי וצד ימין לא.

**<u>טענה</u>**: קיים פתרון למשוואה $ax=b(\bmod n)$. אם ורק אם $\gcd(a,n)\mid b$

**<u>הוכחה:</u>** נגדיר $d=\gcd(a,b)$. ונניח $d=ua+vn$. נניח שיש פתרון, כלומר קיימים שלמים $x,h$ כך ש $ax=b+nh$. אז $b=ax-nh$, וברור מכאן (d מחלק את שני המספרים באגף ימין) ש $d\mid b$. זה מוכיח כיוון אחד של הטענה. בכיוון השני, נניח ש $d\mid b$. אז $b=kd=k(ua+vn)$ עבור איזה שלם k. המשוואה שואלת האם קיימים שלמים $x,h$ כך ש $ax=b+nh$. נציב הערך שקיבלנו עבור b ונקבל המשוואה $ax=k(ua+vn)+nh$. על ידי העברת אגפים מקבלים $ax=k(ua+vn)+nh$. למשוואה זו יש פתרון: $x=ku, h=-v$, וסיימנו הוכחת הטענה.

אנו רואים, אם כך, שבעזרת אלגוריתם אוקלידס אפשר לפתור משוואות מודולריות. יש לכך שימושים רבים, למשל באלגוריתם RSA. הנה דוגמה נוספת

**<u>טענה</u>**: אוסף המספרים מודולו n, הוא ***שדה*** אם ורק אם n ראשוני.
**<u>הוכחה</u>**:כזכור, דרישות השדה הן קיום פעולות חיבור וכפל קומוטטיביות, וכן קיום 0 – איבר נייטרלי לחיבור וכן 1 – איבר נייטרלי לכפל. דרישות אלה מתקיימות על ידי המספרים השלמים מודולו n לכל שלם n. הדרישה הנוספת היא שלכל מספר a יש מספר b כך ש $ab=1(\bmod n)$. אם n הוא ראשוני, אז אכן $\gcd(a,n)=1$, ולכן לפי הטענה הקודמת יש פתרון b כנדרש. אם n איננו ראשוני, אז למשל יש לו מחלק k. אז $\gcd(k,n)=k$, ולפי הטענה לעיל (וגם קל לבדוק ישירות) אין פתרון b למשוואה $kb=1(\bmod n)$.