מחלק משותף מקסימלי: $\max\{d\in\mathbb{N} \mid d|a,\ d|b\} = \gcd(a,b)$

$\gcd(n,m)=\gcd(\pm n,\pm m)$

משפט: חילוק עם שארית

לכל a שלם, ו-$b\neq 0$ שלם קיימים $q,r\in\mathbb{Z}$ כך ש $a=qb+r$ כאשר $0\le r<|b|$

הערה: אם $d|a$ וגם $d|b$ אז $d|as+bt$ לכל $s,t\in\mathbb{Z}$

מסקנה:

יהיו $a,b\in\mathbb{Z}$, $b\neq 0$ ואם $a=qb+r$ אז

$$\underbrace{\gcd(a,b)}_{d}=\underbrace{\gcd(b,r)}_{d'}$$

$d'|b$ לפי ההגדרה

$d'|a \Rightarrow d'\le d$

$d|b$, $d|r \Rightarrow d\le d'$

אלגוריתם אוקלידס למציאת gcd:

יהיו a,b שלמים בה"כ

a,b טבעיים או 0, לא שניהם 0 $a\geq b$

1) אם $b=0$ $\quad gcd(a,0)=a$

2) $b\neq 0$. לפי משפט החלוקה $a=qb+r$

$0\leq r<b$ ובצורה רקורסיבית נחשב

$gcd(a,b)=gcd(b,r)$

הגדרה:

a,b יקראו זרים אמ"מ $gcd(a,b)=1$

הערה: כל מס' ראשוני p זר לכל מספר שאינו מתחלק ב-p

תרגיל:

$gcd(224,63)=?$

פתרון:

$224=3\cdot 63+35 \Rightarrow 63=1\cdot 35+28$

$\Downarrow$

$35=28+7 \Rightarrow 28=4\cdot 7+0$

$gcd(224,63)=7$

משפט והגדרה שקולה ל- gcd

יהיו $a,b\in\mathbb{Z}$ שלמים, לא שניהם 0

$$\gcd(a,b)=\min\{as+bt\in\mathbb{N}\mid s,t\in\mathbb{Z}\}$$

הוכחה:

נסמן $d=\gcd(a,b)$, $d'=\min\{as+bt\in\mathbb{N}\mid s,t\in\mathbb{Z}\}$

$d\le d'$: d מחלק את a,b ולכן כל צירוף לינארי שלהם, $d\mid d'$ ולכן $d\le d'$

$d'\le d$: נראה $d'\mid a$, $d'\mid b$ ואז מהגדרת gcd
$d'\le d$

$d'\mid a$: אם $a=0$ ברור.

$a\neq 0$ קיימים q,r כך ש $a=qd'+r$
$(0\le r<d')$

$\Downarrow$

$r=a-qd'\in\{as+bt\mid s,t\in\mathbb{Z}\}$

אם $r\neq 0$ נקבל $r\in\mathbb{N}$ ולכן $r<d'$
בסתירה

לכן $r=0$, מש"ל.

לכן גם $d'\mid b$

מסקנה:

$\exists s,t\in\mathbb{Z}: \gcd(a,b)=as+bt$

מסקנה:

יהיו a,b שלמים ו-$\tilde{d}|a$, $\tilde{d}|b$ אז $\tilde{d}|gcd(a,b)$

(כי $\tilde{d}$ מחלק כל צ"ל של a ו-b)

הערה: אם $a=\prod_{n\in\mathbb{N}} p_n^{\alpha_n}$ $b=\prod_{n\in\mathbb{N}} p_n^{\beta_n}$

הצגה כמכפלה סופית של ראשוניים

($\alpha_n,\beta_n\in\mathbb{N}\cup\{0\}$) אז $gcd(a,b)=\prod_{n\in\mathbb{N}} p_n^{\min\{\alpha_n,\beta_n\}}$

טענה:

יהיו a,b,c שלמים כך ש: a,b זרים, $a|bc$

אז $a|c$

הוכחה:

$$gcd(a,b)=1=as+bt$$
$$\Downarrow$$
$$c=\underbrace{acs}_{a|a}+\underbrace{bct}_{a|bc}$$

מסקנה:

יהי p ראשוני. אם $p|ab$ אז $p|a$ או $p|b$

הוכחה:

אם $p|a$ סיימנו

אחרת $p\nmid a$ אז $gcd(p,a)=1$ ולכן מהטענה הקודמת

$p|ab$, $gcd(p,a)=1$ נקבל כי $p|b$

איך מוצאים את הצ"ל שווה ל-gcd?

אלגוריתם אוקלידס המוכלל:

כגון $\gcd(53,47)=1$

$$53=1\cdot 47+6$$
$$47=7\cdot 6+5$$
$$6=1\cdot 5+1$$
$$\Downarrow$$
$$1=6-5=6-(47-7\cdot 6)=8\cdot 6-47=$$
$$=8(53-47)-47=8\cdot 53-9\cdot 47$$

עובדה:

לכל n טבעי ניתן להגדיר יחס שקילות על $\mathbb{Z}$

$n|a-b \iff a\equiv_n b$ ו-a שקול מודולו n ל-b

מגדירים את הקבוצת המנה $\mathbb{Z}_n=\{[0],\dots,[n-1]\}$

ניתן להגדיר פעולות על $\mathbb{Z}_n$

$[a]+[b]=[a+b]$ $\qquad$ $[ab]=[a][b]$

ואלו פעולות מוגדרות

כי אם $a\equiv a'$, $b\equiv b'$ $\iff$ $([a]=[a']\ \ [b]=[b'])$

אזי $a+b=a'+b'$ $\quad$ $ab=a'b'$ $\quad$ $\left(\begin{array}{l}[a+b]=[a'+b'] \\ [ab]=[a'b']\end{array}\right)$

הוכחה:

נניח $a \equiv a'$ $\quad n | a-a'$

$b \equiv b'$ $\quad n | b-b'$

א. ① $n \mid (a-a')+(b-b') = (a+b)-(a'+b')$

ולכן $a+b \equiv a'+b'$

②

$$\begin{matrix} n \mid ab-a'b \\ n \mid a'b-a'b' \end{matrix} \Rightarrow n \mid ab-a'b'$$

תרגיל:

מצאו את הספרה האחרונה 333^{333}

פתרון:

$333^{333} \bmod 10 = ?$

ב- $\mathbb{Z}_{10}$ $\quad [333^{333}] = [x]$ $\quad x \in \{0, \dots, 9\}$

$$[333^{333}] = [333 \cdot \ldots \cdot 333] = [333] \cdot \ldots \cdot [333] = [333]^{333} =$$

$$= [3]^{333} = [3]^{166 \cdot 2+1} = ([3]^2)^{166} \cdot [3] =$$

$$= [9]^{166} [3] = [(-1)^{166}][3] = [3]$$

משפט השאריות הסיניות (מקרה פרטי):

יהיו n_1, n_2 טבעיים זרים

א. לכל a_1, a_2 (שלמים) ניתן לפתור את המערכת

$x \equiv a_1 \bmod n_1$ $\quad x \equiv a_2 \bmod n_2$

ב) x שפותר קיים יחיד עד כדי $\bmod n_1 n_2$

הוכחה:

כיוון ש- $gcd(n_1,n_2)=1$ $\Leftarrow$ $\exists s,t : 1 = n_1\cdot s + n_2\cdot t$

$e_1 := 1-n_1 s = n_2 t$

$e_1 \bmod n_1 = 1$

$e_1 \bmod n_2 = 0$

$e_2 := 1-n_2 t = n_1 s$

$e_2 \bmod n_1 = 0$

$e_2 \bmod n_2 = 1$

נגדיר $x = a_1 e_1 + a_2 e_2$

$x \bmod n_1 = a_1$

$x \bmod n_2 = a_2$

תרגיל:

מצאו x כך ש- $x \equiv 5 \bmod 3$ $\quad$ $x \equiv 2 \bmod 5$

פתרון:

$gcd(3,5)=1 = 3\cdot 2 + 5(-1)$

$e_1 = 1-6 = -5$

$e_2 = 1-5(-1) = 6$

$x = 5\cdot\underbrace{(-5)}_{e_1} + 2\cdot\underbrace{6}_{e_2}$

הערה: ניתן להכליל את המשפט:

יהיו $n_1,\dots,n_k$ זרים בזוגות

ויהיו $a_1,\dots,a_k$ שלמים

אז קיים x יחיד עד כדי $\bmod n_1\cdot\ldots\cdot n_k$

$$x \equiv a_1 \bmod n_1$$

$$\vdots$$

$$x \equiv a_k \bmod n_k$$