CSE 15 7-28-20

Euclid's algorithm in Pseudo-code:

input : $a, b \in \mathbb{Z}$

output : gcd(a, b)

r = rem. of a upon div. by b (a % b)

while r > 0

    a = b

    b = r

    r = rem. of a on div. by b

end while.

return b

Ex. $\gcd(235, 136) = 1$

a	$=$	q	$\cdot b$	$+$	r
136	$=$	0	$\cdot 235$	$+$	136
235	$=$	1	$\cdot 136$	$+$	99
136	$=$	1	$\cdot 99$	$+$	37
99	$=$	2	$\cdot 37$	$+$	25
37	$=$	1	$\cdot 25$	$+$	12
25	$=$	2	$\cdot 12$	$+$	$\boxed{1}$
12	$=$	12	$\cdot \boxed{1}$	$+$	0

Defn

We say a and b are relatively Prime iff

$$\gcd(a, b) = 1 .$$

Equivalently, a and b have no Prime factor in common.

Goal Prove correctness of Euclidean algorithm.

Exercise (hw)

Show for any $a, b, d \in \mathbb{Z}$ that

$$d|a \wedge d|b \Rightarrow d|(a+b).$$

Lemma 3

Let $a, d, n \in \mathbb{Z}$. Then

$$d|a \Rightarrow d|na$$

Proof.

$$\begin{aligned} d|a &\Rightarrow a = kd \text{ (for some } k \in \mathbb{Z}.) \\ &\Rightarrow na = (nk)d \\ &\Rightarrow d|na \text{ (since } na \in \mathbb{Z}). \end{aligned}$$

■

Lemma 4

Let $a, b, n, m, d \in \mathbb{Z}$. Then

$$d \mid a \wedge d \mid b \implies d \mid (na + mb)$$

Proof.

$$\left.\begin{array}{l} d \mid a \implies d \mid na \\ d \mid b \implies d \mid mb \end{array}\right\} \implies d \mid (na + mb)$$

$\uparrow$ Lemma 3 — $\uparrow$ exercise. ∎

Lemma 5

Suppose $a = qb + r$ $(a, q, b, r \in \mathbb{Z}.)$

Then

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

Proof.

observe, if $d \in \mathbb{Z}$, then

$$d|a \wedge d|b \Rightarrow d|(a-qb)=r \Rightarrow d|b \wedge d|r.$$

Also

$$d|b \wedge d|r \Rightarrow d|(qb+r)=a \Rightarrow d|a \wedge d|b$$

Thus

$$d|a \wedge d|b \iff d|b \wedge d|r.$$

$\therefore \{\text{com. div. of } a, b\} = \{\text{com. div. of } b, r\}$

$\therefore$ $$\gcd(a,b) = \gcd(b,r).$$

∎

Correctness of Euclidean Algorithm:

Proof

1st division gives

$$a = qb + r \quad (0 \le r < b)$$

Let $r_0 = a$, $q_1 = q$, $r_1 = b$, $r_2 = r$. Then

$$r_0 = q_1 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

$$r_2 = q_3 r_3 + r_4 \qquad 0 \leq r_4 < r_3$$

$$\vdots \qquad\qquad \vdots$$

the sequence of remainders is strictly decreasing: $r_1 > r_2 > r_3 > \cdots \geq 0$,

and must therefore reach zero.

Let r_n be the last non-zero remainder.

$$\vdots \qquad\qquad \vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n + 0$$

By lemma 5, we have:

$$\begin{aligned}
\gcd(a,b) &= \gcd(r_0, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\vdots \\
&= \gcd(r_{n-1}, r_n) \\
&= \gcd(r_n, 0) \\
&= r_n
\end{aligned}$$

as required. ∎

Defn

Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a, b are congruent modulo m iff $m \mid (a-b)$.

notation: $a \equiv b \pmod{m}$

alternate notation: $a \equiv_m b$

Ex.

$10 \equiv 7 \pmod 3$ since $3 \mid 10-7=3$

$25 \equiv 11 \pmod 7$ $\because$ $7 \mid 25-11 = 14$

$-13 \equiv 106 \pmod{17}$ $\because$ $17 \mid (-13-106) = -119 = (-7)\,17$

$18 \not\equiv 5 \pmod 4$ $\because$ $4 \nmid 18-5 = 13$

Lemma 6

$a \equiv b \pmod m$ $\Leftrightarrow$ iff $\Rightarrow$ $a = b + km$ for some $k \in \mathbb{Z}$.

Proof: (exercise)

Theorem

$a \equiv b \pmod{m}$ iff a and b have the same remainder upon division by m.

Proof.

($\Leftarrow$) Suppose a, b have the same remainder on division by m. Then

$$\begin{cases} a = q_1 m + r \\ b = q_2 m + r \end{cases} \quad \text{and} \quad 0 \le r < m$$

Then

$$\begin{aligned} a - b &= (q_1 m + r) - (q_2 m + r) \\ &= q_1 m - q_2 m \\ &= (q_1 - q_2) m \end{aligned}$$

$\therefore \quad m \mid (a - b)$

$\therefore \quad a \equiv b \pmod{m}$.

($\Rightarrow$) Suppose $a \equiv b \pmod{m}$. Then

$$m \mid (a-b)$$

$\therefore$ $a - b = km$, for some $k \in \mathbb{Z}$.

Divide both a and b by m:

$$a = q_1 m + r_1 \qquad (0 \le r_1 < m)$$

and

$$b = q_2 m + r_2 \qquad (0 \le r_2 < m) .$$

we must show that $r_1 = r_2$.

Assume (to get a $\lightning$) that $r_1 < r_2$.

Then $0 \le r_1 < r_2 < m$, and hence

$$0 < r_2 - r_1 < m$$

But

$$r_2 - r_1 = (b - q_2 m) - (a - q_1 m)$$

$$= b - a - q_2 m + q_1 m$$

$$= -(a-b) - q_2 m + q_1 m$$

$$= -km - q_2 m + q_1 m$$

$$= (q_1 - q_2 - k)m$$

$\therefore$ $0 < (q_1 - q_2 - k)m < m$

$\therefore$ $0 < q_1 - q_2 - k < 1$

which is impossible since $q_1 - q_2 - k \in \mathbb{Z}$.

This contradiction shows $r_1 \neq r_2$.

Exercise show $r_2 < r_1$ yields a similar contradiction.

We conclude that $r_1 = r_2$, as required. ∎

Theorem

Let $a, b, c, d, m \in \mathbb{Z}$ $(m > 0)$, and suppose

$$a \equiv c \pmod{m}$$

and

$$b \equiv d \pmod{m}$$

Then

(1) $a + b \equiv c + d \pmod{m}$

(2) $a \cdot b \equiv c \cdot d \pmod{m}$

i.e. congruences can be added (and subtracted) and multiplied.

Proof of (1)

$$\left.\begin{array}{l} a \equiv_m c \Rightarrow m \mid a-c \\ b \equiv_m d \Rightarrow m \mid b-d \end{array}\right\} \Rightarrow m \mid (a-c)+(b-d)$$

$\therefore \quad m \mid (a+b)-(c+d)$

$\therefore \quad a+b \equiv_m c+d$. ∎

Proof of (2): exercise, actually hw. ∎

Theorem

Let $a, b, c, m \in \mathbb{Z}$ $(m>0)$. Then

$$\left.\begin{array}{l} a \equiv b \pmod m \\ \text{and} \\ b \equiv c \pmod m \end{array}\right\} \Rightarrow a \equiv c \pmod m$$

Proof.

$$\left.\begin{array}{l} a \equiv_m b \Rightarrow m \mid (a-b) \\ b \equiv_m c \Rightarrow m \mid (b-c) \end{array}\right\} \Rightarrow m \mid (a-b)+(b-c)$$

$\therefore \quad m \mid (a-c)$

$\therefore \quad a \equiv_m c.$ ∎