COT 3100 2/14/23

(1) Prove Euclid's Alg is Correct

(2) Learn Extended Euclidean Alg.

(a) Solve eqn $ax+by = \gcd(a,b)$ for int sols x, y given pos int a, b

(b) Solve eqn $ax+by = c$ where $\gcd(a,b) \mid c \wedge c > \gcd(a,b)$

(c) Determine $b^{-1} \bmod a$. (Will define later)

Euclid's 126, 87	generic
(a) $126 = 1 \times 87 + 39$ $87 = 2 \times 39 + 9$ $39 = 4 \times 9 + \boxed{3}$ $9 = 3 \times 3$ $3 \mid 9$	$a = bq_0 + r_0$ $b = r_0 q_1 + r_1$ $r_0 = r_1 q_2 + r_2$ $r_1 = r_2 q_3 + r_3$ $\vdots$ $r_{k-2} = r_{k-1} q_k + \boxed{r_k}$ result of alg $\Rightarrow r_{k-1} = r_k q_{k+1}$, no remainder

(1) Prove $r_k | a \wedge r_k | b \rightarrow r_k$ is a common divisor.

(2) for any common divisor d, $d | r_k$. → means r_k is ~~terms~~ least of all common div.

(1) Proof

$r_k | r_{k-1}$ (last line)

$a|b \leftrightarrow \exists c \mid b = ac$

$3|12, 6|6, 27|108$

if $r_k | r_k \wedge r_k | r_{k-1} \Rightarrow r_k | r_{k-2}$ (second to last line)

if $r_k | r_{k-1} \wedge r_k | r_{k-2} \Rightarrow r_k | r_{k-3}$ (3rd to last line)

$r_k | r_1 \wedge r_k | r_0 \Rightarrow r_k | b$

$r_k | r_0 \wedge r_k | b \Rightarrow r_k | a$

$126 - 1 \times 87 = 39$

$87 - 2 \times 39 = 9$

$39 - 4 \times 9 = 3$

$d|a \wedge d|b$

$a - bq_0 = r_0 \rightarrow d(\text{INT}) = r_0 \rightarrow d | r_0$

$b - r_0 q_1 = r_1 \rightarrow d | r_1$

$r_0 - r_1 q_2 = r_2 \rightarrow d | r_2$

$\vdots$

$r_{k-2} - r_{k-1} q_k = r_k \rightarrow d | r_k$

Assume $a > b$.

$a = bq_0 + r_0$

$b = r_0 q_1 + r_1$ → $2r_0 < a$

$a \geq b + r_0$ because $q_0 \geq 1$, $r_0 < b$

$> r_0 + r_0$

$= 2r_0$

$\#\text{steps} \leq 2 \log_2 a$

Find all solutions (integers (x,y)) to

(a) $615x + 450y = 7$

(b) $615x + 450y = 15$

(c) $615x + 450y = 135$

$ax+by=c$
(a) if $\gcd(a,b) \nmid c$, no sols

(a) Find $30^{-1} \bmod 41$.

(a) $615 = 1\times450 + 165$
$450 = 2\times165 + 120$
$165 = 1\times120 + 45$
$120 = 2\times45 + 30$
$45 = 1\times30 + \boxed{15}$
$30 = 2\times15$

$\gcd(615,450) = 15$
To solve (a), note that $15 \nmid 7$, so this has no integer solutions.

Rewrite each eqn backward (sub term right → left)

$615 - 1\times450 = 165$
$450 - 2\times165 = 120$
$165 - 1\times120 = 45$
$120 - 2\times45 = 30$
$45 - 1\times30 = 15$

$45 - 1\times30 = 15$
$45 - 1(120 - 2\times45) = 15$
sub + simp ↓
$45 - 1\times120 + 2\times45 = 15$
$3\times45 - 1\times120 = 15$
$3(165 - 1\times120) - 1\times120 = 15$
$3\times165 - 4\times120 = 15$
$3\times165 - 4(450 - 2\times165) = 15$
$3\times165 - 4\times450 + 8\times165 = 15$
$11\times165 - 4\times450 = 15$

ok if can do accurately →

$11(615 - 1\times450) - 4\times450 = 15$
$\boxed{11\times615 - 15\times450 = 15}$
$615x + 450y = 15$
$\boxed{x = 11,\ y = -15}$

$615 \times 11 - 450 \times 15 = 15$

$615 \times (11 + 450) - 450 \times (15 + 615)$ → new sol $x = 461, y = -630$

$= 615 \times 11 + 615 \times 450 - 450 \times 15 - 450 \times 615$

$= 615 \times 11 - 450 \times 15 = 15$

Observations

I can take any soln (x, y) and $(x+450, y-615)$ is another solution

$\Rightarrow$ infinite # solns

BUT are there others? Let (x, y) be "base solution"

$615(x + M) + 450(y - N) = 615x + 450y$

$615x + 450y + 615M - 450N = 615x + 450y$

$\Rightarrow \quad \frac{615M}{15} = \frac{450N}{15}$ } can divide both sides by gcd

$41M = 30N$

smallest pos soln is $M = 30, N = 41$

we know that $30 \mid (41M)$

$\gcd(30, 41) = 1$

$\Rightarrow 30 \mid M$

no smaller soln for M than 30

$\gcd(41, 30) = 1$

~~$41x + 30y = 1$~~

$41x + 30y = 1$ has an int soln

$30 \times 41x + 30^2 y = 30$

$a=30,\ b=41,\ c=M$

$ax+by=1$

$30x+41y=1$

$c\ \boxed{30^2x}+\boxed{(30\cdot 41)y}=\boxed{30}\ c$

if $a \mid (bc)$ and $\gcd(a,b)=1$,
then $a \mid c$.

$ax+by=1$

$acx+\boxed{bc}y=c$, $bc=ad$, $d\in\mathbb{Z}$

$acx+ady=c$

$a(cx+dy)=c \Longrightarrow a \mid c$

old info $41M=30N$, $a=30,\ b=41,\ c=M$

$\Longrightarrow 30 \mid M$, since $M>0$, $M \geq 30$

All solns $615x+450y=15$ are

$\{(x,y) \mid x=11+30c,\ y=-15-41c,\ c\in\mathbb{Z}\}$

$\{(x,y) \mid x=11-30c,\ y=-15+41c,\ c\in\mathbb{Z}\}$

$\downarrow$ $\frac{450}{\gcd(450,615)}$ $\qquad$ $\downarrow$ $\frac{615}{\gcd(450,615)}$

(c) $615x + 450y = 135$ $\quad 135 = 9 \times 15$

$9\left(615 \times 11 + 450(-15)\right) = (15)\,9$

$615 \times (99) + 450(-135) = 135$

$\{(x,y) \mid x = 99 + 30c,\ y = -135 - 41c,\ c \in \mathbb{Z}\}$

Plug in $c = -3$, equivalent way of stating set

$\{(x,y) \mid x = 9 + 30c,\ y = -12 - 41c,\ c \in \mathbb{Z}\}$

What does $b^{-1} \bmod a$ mean?

$(?)30x \equiv 17(?) \pmod{41}$

$\equiv 1 \pmod{41}$

exists only if $\gcd(a,b) = 1$

$b^{-1} \bmod a$ is the # such that

$b \times (b^{-1}) \equiv 1 \bmod a$

Old work $\quad \frac{615}{15} \times 11 + \frac{450}{15} \times (-15) = \frac{15}{15}$

$41 \times 11 + 30(-15) = 1$

Consider eqn mod 41

$41 \times 11 + 30(-15) \equiv 1 \pmod{41}$

$0 \times 11 + 30(-15) \equiv 1 \pmod{41}$

$30 \times (-15) \equiv 1 \pmod{41}$

$-15 \equiv 26 \pmod{41}$

$30^{-1} \equiv 26 \pmod{41}$

$30x \equiv 17 \pmod{41}$

$26 \cdot 30x \equiv 26 \cdot 17 \pmod{41}$

$x \equiv 442 \equiv 32 \pmod{41}$

$30 \times 32 = 960 \rightarrow$

$$\begin{array}{r} 23 \text{ R } 17 \\ 41\overline{)960} \\ 82 \\ \hline 140 \\ -123 \\ \hline 17 \end{array}$$

$$\begin{array}{r} 26 \\ \times 17 \\ \hline 182 \\ 26 \\ \hline 442 \end{array}$$

$$\begin{array}{r} 10 \\ 41\overline{)442} \\ 41 \\ \hline 32 \end{array}$$

If $ax + by = 1$ $\gcd(a,b) = 1$ and $b < a$

then $b^{-1} \equiv y \pmod{a}$