Warm-Up: Use the Euclidean algorithm to compute $\gcd(616, 252)$.

"Reverse Euclidean Algorithm"

Thm: Let $a, b \in \mathbb{Z}$, not both zero. Set $d = \gcd(a,b)$. Then there exist integers $x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

Ex: $a = 616$, $b = 252$. $\gcd(616, 252) = 28$. Then to solve

$$616x + 252y = 28,$$

- Run the Euclidean algorithm

$$616 = 252 \cdot 2 + 112$$
$$252 = 112 \cdot 2 + \boxed{28}$$
$$112 = 28 \cdot 4 + 0$$

Last non-zero remainder is $\gcd(616, 252)$.

- Solve for each non-zero remainder

① $112 = 616 - 252(2)$

② $28 = 252 - 112(2)$

- Start from the bottom, and substitute up

② $28 = 252 - 112(2)$

①

$= 252 - (616 - 252(2)) \cdot (2)$

$= 616(-2) + 252(5)$

So $\boxed{x = -2,\ y = 5}$ is a solution.

Proof: It is enough to prove the theorem for $a, b \in \mathbb{N}$

OMIT

- If $a < 0$, then $d = \gcd(a,b) = \gcd(-a,b)$, and if $x, y \in \mathbb{Z}$ solves

$$(-a)x + by = d$$

then $a(-x) + by = d$.

Sim. if $b < 0$.

- If $a=0$ and $b>0$, then $\gcd(0,b)=b$ and $0x+by=b$ is solved by $y=1$ (and any $x\in\mathbb{Z}$).

Sim. if $b=0$.

So we assume $a,b\in\mathbb{N}$ and write $d=\gcd(a,b)$. Let $P(n)$ be the sentence

"If $a\le n$ and $b\le n$, then there exist $x,y\in\mathbb{Z}$ such that $ax+by=d$."

We will be done if we can prove $P(n)$ is true for every $n\in\mathbb{N}$, which we will do by induction.

<u>Base Case</u>: If $a\le 1$ and $b\le 1$, then $a=b=1$ (since $a,b\in\mathbb{N}$). So $d=\gcd(1,1)=1$ and

$$1x+1y=1$$

is solved by taking $x=1$ and $y=0$. Thus, $P(1)$ is true.

__Inductive Step__: Let $n \in \mathbb{N}$ and suppose that $P(n)$ is true.

Assume $a \leq n+1$ and $b \leq n+1$.

__Case 1__: If both $a \leq n$ and $b \leq n$, then

$$ax + by = d$$

has a solution $x, y \in \mathbb{Z}$ because $P(n)$ is true.

__Case 2__: If $a = n+1 = b$, then $d = n+1$ and

$$(n+1)x + (n+1)y = (n+1)$$

is solved by $x = 1$ and $y = 0$.

__Case 3__: One of a, b is $n+1$, and the other is at most n. Without loss of generality, $a = n+1$ and $b \leq n$.

By the division algorithm, we have

$$a = qb + r$$

where $0 \le r \le b-1$. Then $r \le n$.
Also, $\gcd(b,r) = \gcd(a,b) = d$ by AW 17.

Thus, because $P(n)$ is true, there exist integers $z, w \in \mathbb{Z}$ such that

$$bz + rw = d.$$

Making the substitution $r = a - qb$, we get

$$bz + (a-qb)w = d$$

or

$$aw + b(z-qw) = d.$$

That is, $x = w$ and $y = z - qw$ are integers satisfying

$$ax + by = d.$$

Since we have considered all cases, we conclude that $P(n+1)$ is true. This completes the inductive step. $\blacksquare$

Congruence

<u>Def</u>: Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. We say <u>a is congruent to b modulo m</u> if $m \mid (b-a)$.

We write this as $a \equiv b \mod m$.

<u>Ex</u>: • $10 \equiv 4 \mod 3$ because $3 \mid (4-10)$

<u>Note</u>: 10 and 4 both leave a remainder of 1 when divided by 3.

• $11 \equiv 23 \mod 3$ because $3 \mid (23-11)$

• $3 \equiv 0 \mod 3$ " $3 \mid (0-3)$

<u>Thm</u>: Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then $a \equiv b \mod m$ if and only if a and b leave the same remainder when divided by m.

Proof: Use the division algorithm to write

$$a = mq_1 + r_1$$
$$b = mq_2 + r_2$$

where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \le r_1 \le m-1$, $0 \le r_2 \le m-1$.

We must show $a \equiv b \bmod m \iff r_1 = r_2$.

($\Rightarrow$) Suppose $a \equiv b \bmod m$. Then m divides

$$b - a = (mq_2 + r_2) - (mq_1 + r_1)$$
$$= m(q_2 - q_1) + (r_2 - r_1)$$

Since m divides $b-a$ and $m(q_2-q_1)$, m must divide

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

But $-(m-1) \le r_2 - r_1 \le m-1$, so the only possibility is that $r_2 - r_1 = 0$, i.e. $r_1 = r_2$.

($\Leftarrow$) Conversely, suppose $r_1 = r_2$. Then $r_2 - r_1 = 0$, so

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

is divisible by m. That is,

$$a \equiv b \mod m.$$

$\blacksquare$