Page 19

Thm: Let a and b be integers. Then a and b are relatively prime (i.e., $(a,b)=1$) if and only if there exist integers x and y such that

$$ax + by = 1.$$

Proof: ($\Leftarrow$) Thm 1.39, proved by Will.

($\Rightarrow$) Thm 1.38.

We'll first assume that $a, b \geq 0$.

The proof is by strong induction.

Base cases:

- $a = b = 0$: This is not allowed, because $(0,0)$ is undefined.
- $a = 1, b = 0$: $1x + 0y = 1$ is solved by $x = 1$, $y = \text{anything}$
- $a = 0, b = 1$: similar.
- $a = 1, b = 1$: $1x + 1y = 1$ is solved by $x = 1, y = 0$

Inductive step: Let $n \geq 1$ be a natural number.

Assume the theorem holds for every pair of integers a, b with $(a,b)=1$ and $0 \leq a, b \leq n$.

Now, suppose a and b satisfy $(a,b)=1$ and that

$$0 \leq a, b \leq n+1.$$

Goal: Find integers x and y satisfying $ax+by=1$.

- If both $a \leq n$ and $b \leq n$, then we can apply the inductive hypothesis to find x and y. ✓
- If $b=0$, then $(a,b) = (a,0) = a \Rightarrow a=1$

  1''

  and we already did this case. ✓
- If $a=0$, then similarly $b=1$ and we already did this. ✓
- $a=n+1$ and $b=n+1$, then $(a,b)=(n+1,n+1)=n+1 \neq 1$, so the hypothesis is not satisfied. ✗

So, without loss of generality, we can assume

$$a = n+1$$

and

$$1 \le b \le n.$$

Now, run the division algorithm:

$$a = n+1 = q \cdot b + r, \qquad 0 \le r \le b-1 < n$$

By Thm 1.33, $(a, b) = (b, r)$

1 "

Since $(b, r) = 1$ and $0 \le b, r \le n$, by the inductive hypothesis, we can find integers z, w such that

$$bz + rw = 1$$

$$a = qb + r \rightarrow r = a - qb$$

Now,

$$bz + rw = 1$$

$$bz + (a - qb)w = 1$$

$$aw + (z - qw)b = 1$$

So $x = w$ and $y = z - qw$ solves

$$ax + by = 1.$$

This completes the inductive step. ✓

So the theorem is true if $a, b \geq 0$.

What if one or both is negative?

Solve $|a|x + |b|y = 1$ instead

+ use this to find a solution to $ax + by = 1$.

<u>Ex</u>: (last time) $18x + 7y = 1$ is solved by $x = 2$, $y = -5$.

$-18x + 7y = 1$ is solved by $x = -2$, $y = -5$

$-18x - 7y = 1$ " " " $x = -2$, $y = 5$

etc.