Bezout's Lemma

* Bezout's lemma tells you when a linear Diophantine equation has an integer solution and when it doesn't
* Read Example 3.1.23 for good idea of how useful Bezout's lemma is

$a, b, c \in \mathbb{Z} \qquad d = \gcd(a, b)$

$$\left(\begin{array}{c} ax + by = c \\ \text{has integer solution} \end{array} \right) \iff (d \mid c)$$

$ax + by = c$ } Linear Diophantine equation

Proof: (Mackey briefly went over it in lecture. You won't be asked to "prove Bezout's lemma" on a test, but it's nice to understand)

($\Rightarrow$) Assume $ax + by = c$ has integer solution

$a = a'd \qquad b = b'd$	since $d = \gcd(a,b)$, use #10
$c = a'd\,x + b'd\,y$	substitute a & b into $c = ax + by$
$c = (a'x + b'y)\,d$	factor out d
$d \mid c$	definition

($\Leftarrow$) Assume $d \mid c$

$c = kd$	definition
$d = au + bv$	Thm. 3.1.12 (gcd can be written as a linear comb.)
$c = kau + kbv$	subsitute into $c = kd$ and expand
$c = a(ku) + b(kv)$	rewrite
$c = ax + by$	☺