Back to the equation $ax + by = c$.

- (a,b) divides both a and b

$\Rightarrow$ (a,b) divides $ax + by$

No solution unless $(a,b) \mid c$.

What about $c = (a,b)$?

<u>Theorem:</u> There are integers x, y such that

$ax + by = (a,b)$

<u>Proof:</u> We'll give an algorithm that finds (a,b) and integers x, y such that $ax + by = (a,b)$ (Euclid's algorithm)

By Division algorithm, we can write

- $a = k_0 \cdot b + r_0$, $0 \leqslant r_0 < |b|$

<u>Lemma:</u> $(a,b) = (b, r_0)$.

Then, continue using Division algorithm to find (b, r_0)

(will prove later)

- $b = k_1 \cdot r_0 + r_1$, $0 \leqslant r_1 < r_0$ $\rightarrow$ $(b, r_0) = (r_0, r_1)$

- $r_0 = k_2 \cdot r_1 + r_2$, $0 \leqslant r_2 < r_1 < r_0$ $\rightarrow$ $(r_0, r_1) = (r_1, r_2)$

$\vdots$

- $r_{n-2} = k_n \cdot r_{n-1} + \underset{\substack{\| \\ 0}}{r_n}$ because $r_0, r_1, r_2, \cdots$ decreasing.

$$\Rightarrow (a,b) = (b, r_0) = (r_0, r_1) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, \underset{0}{\overset{\parallel}{r_n}}) = r_{n-1}.$$

Tracing back our steps, we can find x and y such that $ax + by = r_{n-1}$

- Begin with the equation (2^{nd} from last)

$$r_{n-3} = k_{n-1} \cdot r_{n-2} + r_{n-1} \Rightarrow r_{n-1} = r_{n-3} - k_{n-1} \cdot r_{n-2}$$

- Replace r_{n-2} on RHS using the equation

$$r_{n-4} = k_{n-2} \cdot r_{n-3} + r_{n-2} \Rightarrow r_{n-2} = r_{n-4} - k_{n-2} \cdot r_{n-3}$$

Now, $r_{n-1} = r_{n-3} - k_{n-1} \cdot (r_{n-4} - k_{n-2} \cdot r_{n-3})$

- Replace r_{n-3} similarly ...

$\vdots$

Moving upward, we eventually get $ax + by = r_{n-1}$.

Lemma: $a = kb + r$, then $(a,b) = (b,r)$

Proof: $c \mid a$ and $c \mid b \Rightarrow c \mid a - kb = r$

$\Rightarrow c \mid b$ and $c \mid r$

$d \mid b$ and $d \mid r \Rightarrow d \mid kb + r$

$\Rightarrow d \mid a$ and $d \mid b$

Same common divisors mean same gcd.

<u>Example:</u> $a = 600$ and $b = 136$

$$600 = 4 \cdot 136 + 56$$
$$136 = 2 \cdot 56 + 24$$
$$56 = 2 \cdot 24 + 8$$
$$24 = 3 \cdot 8 + 0$$

$$\Rightarrow (600, 136) = 8$$

$$8 = 56 - 2 \cdot 24 = 56 - 2 \cdot (136 - 2 \cdot 56)$$
$$= 5 \cdot 56 - 2 \cdot 136$$
$$= 5 \cdot (600 - 4 \cdot 136) - 2 \cdot 136$$
$$= 5 \cdot 600 - 22 \cdot 136 .$$

<u>Corollary:</u> $ax + by = c$ has solution if and only if $(a, b) \mid c$.

$$ax + by = (a, b) \Rightarrow a \cdot kx + b \cdot ky = k \cdot (a, b)$$

An alternative definition for gcd: (a, b) is the smallest positive integer that can be written $ax + by$.

(Very useful to prove some properties)

- a, b not all zero.

$a = 24 \quad b = 30$

$(a, b) = 6$

$c \mid a$ and $c \mid b \iff c \mid (a, b)$

common divisors

$\pm 1, \pm 2, \pm 3, \pm 6$

Common divisors are divisors of greatest common divisor

Proof: $(\Leftarrow)$: obvious.

$c \mid (a,b) \mid a$ and $c \mid (a,b) \mid b$

$(\Rightarrow)$: $c \mid a$ and $c \mid b \Rightarrow c \mid \underset{\substack{\parallel \\ (a,b)}}{ax + by}$

- a, b not both zero

$(a, b, c) = ((a, b), c)$

$\underbrace{x \mid a, x \mid b}, x \mid c \Rightarrow x \mid (a, b)$ and $x \mid c$

$y \mid (a, b)$ and $y \mid c \Rightarrow \underbrace{y \mid a \text{ and } y \mid b}, y \mid c$

Same common divisors, same gcd.

- $(ma, mb) = m \cdot (a, b)$ $\quad m > 0$

$(ma, mb) =$ smallest pos. int. $max + mby$

$=$ smallest pos. int. $m(ax + by)$

$= m \cdot$ smallest pos. int. $ax + by$

$= m \cdot (a, b)$