Example: Find $\gcd(100, 39)$

						a_k	
100	39	22	17	5	2	1	0
a_0	a_1	a_2				↑ $\gcd(100,39)$	↑ stop

In general: $\gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{k-1}, a_k)$

but $a_k \mid a_{k-1}$

So $a_k = \gcd(a_{k-1}, a_k)$

Euclidean Algorithm

Why is this good? It's fast.

Why is it fast ?

$$a_0 \quad a_1 \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_k \quad \underbrace{a_{k+1}}_{0}$$

$$a_{i-2} = a_{i-1} \cdot q_{i-1} + a_i$$

$$a_{i-2} \geqslant a_{i-1} + a_i \qquad (q_{i-1} \geqslant 1)$$

$$a_0 \quad a_1 \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_{k-1} \quad a_k$$

$$\geqslant 2 \qquad \geqslant 1$$

$$F_{k+2} \quad \dots \qquad F_{k+2-i} \quad \dots \quad F_3 \quad F_2$$

$$= 2 \qquad = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

Conclusion:

$$a_i \geq F_{k+2-i}$$

so

$$a_0 \geq F_{k+2}$$

$$a_0 \geq F_{k+2} \underbrace{\geq}_{\text{homework}} \phi^k$$

$$\phi^k \leq a_0 \Rightarrow \log_\phi \phi^k \leq \log_\phi a_0 \Rightarrow \boxed{k \leq \log_\phi a_0}$$

So, the number of steps is logarithmic in a_0.

The extended Euclidean Alg

$a_0 \quad a_1 \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_k \quad \overbrace{0}^{a_{k+1}}$

Claim: $\forall i,\ a_i = a_0 x_i + a_1 y_i \quad x_i, y_i \in \mathbb{Z}$ (not uniquely)

"Every number in the sequence is a linear combination of the first two"

Example: 300 18 12 6 0

(a_0 = 300, a_1 = 18)

$300 = a_0 \boxed{1} + a_1 \boxed{0}$

$18 = a_0 \boxed{0} + a_1 \boxed{1}$

$12 = a_0 \boxed{1} + a_1 \boxed{-16}$

$6 = a_0 \boxed{-1} + a_1 \boxed{17}$

$0 = a_0 \boxed{3} + a_1 \boxed{-50}$

Proof by induction: $a_i = a_0 X_i + a_1 y_i$

Base case: $a_0 = a_0 \times 1 + a_1 \times 0$

$a_1 = a_0 \times 0 + a_1 \times 1$

Inductive step: $P(0), P(1), \ldots, P(i)$ are true

Prove $P(i+1)$ is true

a_{i+1} = remainder of division $\frac{a_{i-1}}{a_i}$ (remainder)

$= a_{i-1} - q_i a_i$ $\quad (a_{i-1} = a_i q_i + a_{i+1})$

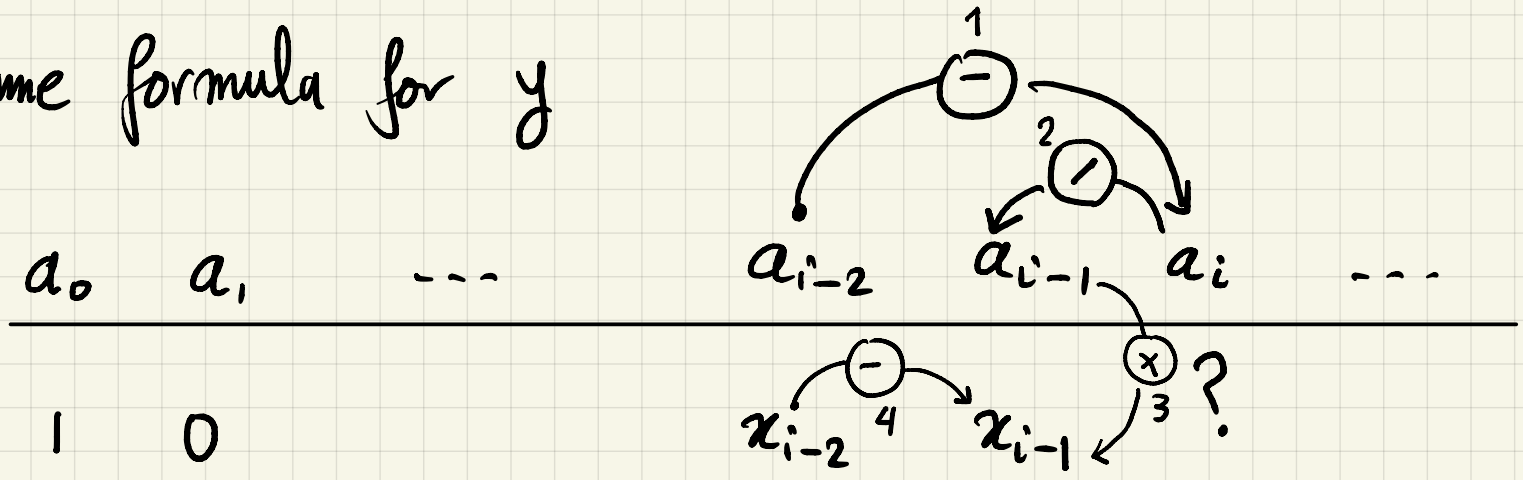
$= (a_0 x_{i-1} + a_1 y_{i-1}) - q_i (a_0 x_i + a_1 y_i)$

$= a_0 \underbrace{[x_{i-1} - q_i x_i]}_{x_{i+1}} + a_1 \underbrace{[y_{i-1} - q_i y_i]}_{y_{i+1}}$.

$$x_i = x_{i-2} - q_{i-1} x_{i-1}$$

$$= x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1}$$

Same formula for y



x	1	0
y	0	1

Example:

	300	18	12	6	0
x	1	0	1	−1	3
y	0	1	−16	17	−50

$$\gcd(300, 18) = 6 = 300(-1) + 18(17)$$

Remember: Not unique!

Idea: $ar + bs = a(r+b) + b(s-a)$

That's why we can always find

$$\gcd(a,b) = ar - bs \quad \text{where} \quad r, s \geq 0$$

Example: $300(-1) + 18(17) = 300(-1+18) + 18(17-300)$

$$= 300(17) - 18(283)$$