

# **Bezout's Theorem - Extended Euclidean Algorithm**

**Arabic Animated  
intuition**



## Bezout's theorem

before learning about extended euclidean algorithm  
we need to know bezout's theorem

we only know a and b what bezout say is that there is always  
an integer x and an integer y that :

$$ax+by=\text{gcd}(a,b)$$

# Extended Euclidean algorithm

$$ax+by=\gcd(a,b)$$

①

we want find x and y and the gcd  
from the Euclidean algorithm we know that  
 $\gcd(a,b)=\gcd(b,a\%b)$

$$bx_1+(a\%b)y_1=\gcd(a,b)$$

②

$$a\%b=a-b*\text{floor}(a/b)$$

$$\text{Ex: } 10\%3=1$$

$$1=10-3*\text{floor}(10/3)$$

$$bx_1+(a-b*\text{floor}(a/b))y_1=\gcd(a,b)$$

③

$$ay_1+b(x_1-\text{floor}(a/b)*y_1)=\gcd(a,b)$$

the algorithm  
is that in every iteration  
 $x=y_1$   
 $y=x_1-\text{floor}(a/b)*y_1$   
and my base case when  $b=0$   
 $x=1,y=0$