

## Euclid's Algorithm

$$\gcd(a, b) = \gcd(\text{rem}(b, a), a)$$

$$\begin{aligned} \gcd(105, 224) &= \gcd(\text{rem}(224, 105), 105) \\ &= \gcd(14, 105) \end{aligned}$$

Why this works?

$$\begin{aligned} \rightarrow \gcd(105, 224) &= 105x + 224y \\ &= 14x + 105y \end{aligned}$$

i.e., the gcd of  $(105, 224)$  also divides a linear combination of 105 & 224

The  $x$  &  $y$  value can be anything

$$\text{eg: } 224 - 2(105) = 14$$

This is  $\checkmark$  rem itself

When  $a$  becomes, then last  
non-zero remainder is the answer which  
won't change.

And this gcd call is the  
recursive function