

## Theorem (Bézout's Identity)

*For any  $m, n$  not both zero, there exists  $(x, y)$ , an integer solution of the equation*

$$mx + ny = \gcd(m, n).$$

The basic idea is to backpropagate the Euclidean algorithm.