

# The Extended Euclidean Algorithm

Example 1:  $m = 65, n = 40$

Step 1: The (usual) Euclidean algorithm:

$$(1) \quad 65 = 1 \cdot 40 + \boxed{25}$$

$$(2) \quad 40 = 1 \cdot \boxed{25} + 15$$

$$(3) \quad \boxed{25} = 1 \cdot 15 + 10$$

$$(4) \quad 15 = 1 \cdot 10 + 5$$

$$10 = 2 \cdot 5$$

Therefore:  $\gcd(65, 40) = 5$ .

Step 2: Using the method of back-substitution:

$$5 \stackrel{(4)}{=} 15 - 10$$

$$\stackrel{(3)}{=} 15 - (25 - 15) = 2 \cdot 15 - 25$$

$$\stackrel{(2)}{=} 2(40 - 25) - 25 = 2 \cdot 40 - 3 \cdot 25$$

$$\stackrel{(1)}{=} 2 \cdot 40 - 3(65 - 40) = 5 \cdot 40 - 3 \cdot 65$$

Conclusion:  $65(-3) + 40(5) = 5$ .

# The Extended Euclidean Algorithm

Example 2:  $m = 1239, n = 735$

Step 1: The (usual) Euclidean algorithm:

$$(1) \quad 1239 = 1 \cdot 735 + \boxed{504}$$

$$(2) \quad 735 = 1 \cdot \boxed{504} + 231$$

$$(3) \quad \boxed{504} = 2 \cdot 231 + 42$$

$$(4) \quad 231 = 5 \cdot 42 + 21$$

$$42 = 2 \cdot 21$$

Therefore:  $\gcd(1239, 735) = 21$ .

Step 2: Using the method of back-substitution:

$$21 \stackrel{(4)}{=} 231 - 5 \cdot 42$$

$$\stackrel{(3)}{=} 231 - 5(504 - 2 \cdot 231) = 11 \cdot 231 - 5 \cdot 504$$

$$\stackrel{(2)}{=} 11(735 - 504) - 5 \cdot 504 = 11 \cdot 735 - 16 \cdot 504$$

$$\stackrel{(1)}{=} 11 \cdot 735 - 16(1239 - 735) = 27 \cdot 735 - 16 \cdot 1239$$

Conclusion:  $1239(-16) + 735(27) = 21$ .