

Euclid's algorithm for GCD(a,b)

Parameters a and b are integers and $b > 0$

According to division algorithm, there exists integers q and r, where 0

- $r < b$, called quotient and remainder, for which

$$A = qB + r$$

It is obvious, that if a and b has a common divisor, then $R = A - qB$ has the same divisor, too

Algorithm:

Algorithm implements division repeatedly

$$A = q_1 B + R_1$$

$$B = q_2 R_1 + R_2$$

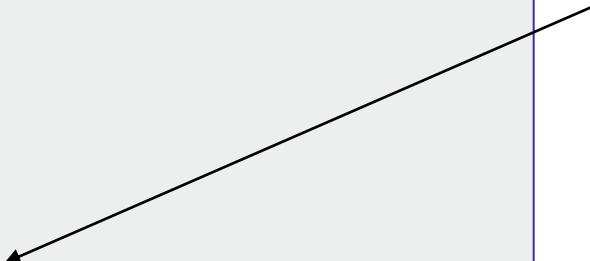
$$R_1 = q_3 R_2 + R_3$$

...

$$R_{n-2} = q_n R_{n-1} + R_n$$

$$R_{n-1} = q_{n+1} R_n + 0$$

GCD(A,B) is the
last non-zero
remainder



Example: GCD(42, 26)

$$42 = 1 * 26 + 16$$

$$26 = 1 * 16 + 10$$

$$16 = 1 * 10 + 6$$

$$10 = 1 * 6 + 4$$

$$6 = 1 * 4 + 2 \leq \text{gcd}$$

$$4 = 2 * 2 + 0$$