Euclidean algorithm

Greatest common divisor

The **greatest common divisor** (GCD) of two integers a and b, written $\gcd(a, b)$, is the largest positive integer that divides both a and b.
Example: $\gcd(12, 18) = 6$ because 6 is the largest number that divides both 12 and 18.

The Euclidean algorithm

The Euclidean algorithm finds $\gcd(a, b)$ efficiently using repeated division.
Key idea: $\gcd(a, b) = \gcd(b, a \mod b)$
Steps:

1. Divide a by b to get quotient q and remainder r: $a = bq + r$
2. Replace a with b and b with r
3. Repeat until the remainder is 0
4. The last non-zero remainder is the GCD

Example: Find $\gcd(252, 105)$.

$$252 = 105 \cdot 2 + 42$$
$$105 = 42 \cdot 2 + 21$$
$$42 = 21 \cdot 2 + 0$$

The last non-zero remainder is 21, so $\gcd(252, 105) = 21$.
Example: Find $\gcd(1071, 462)$.

$$1071 = 462 \cdot 2 + 147$$
$$462 = 147 \cdot 3 + 21$$
$$147 = 21 \cdot 7 + 0$$

Therefore, $\gcd(1071, 462) = 21$.
Example: Find $\gcd(89, 55)$.

Student Learning Support, Teaching and Learning Centre
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning

OntarioTech UNIVERSITY

$$89 = 55 \cdot 1 + 34$$
$$55 = 34 \cdot 1 + 21$$
$$34 = 21 \cdot 1 + 13$$
$$21 = 13 \cdot 1 + 8$$
$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Therefore, $\gcd(89, 55) = 1$. (These numbers are **coprime**.)

Extended Euclidean algorithm

The **extended Euclidean algorithm** finds integers x and y such that:

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

This is called **Bézout's identity**.
Method: Work backwards through the Euclidean algorithm, expressing each remainder in terms of a and b.
Example: Find x and y such that $\gcd(252, 105) = 252x + 105y$.
From the Euclidean algorithm:

$$252 = 105 \cdot 2 + 42 \quad \Rightarrow \quad 42 = 252 - 105 \cdot 2$$
$$105 = 42 \cdot 2 + 21 \quad \Rightarrow \quad 21 = 105 - 42 \cdot 2$$

Now substitute backwards:

$$\begin{aligned} 21 &= 105 - 42 \cdot 2 \\ &= 105 - (252 - 105 \cdot 2) \cdot 2 \\ &= 105 - 252 \cdot 2 + 105 \cdot 4 \\ &= 105 \cdot 5 - 252 \cdot 2 \\ &= 252 \cdot (-2) + 105 \cdot 5 \end{aligned}$$

Therefore, $x = -2$ and $y = 5$.
Check: $252(-2) + 105(5) = -504 + 525 = 21$ ✓

Applications

Application	How GCD is used
Simplifying fractions	$\frac{a}{b}$ in lowest terms: divide by $\gcd(a, b)$
Modular inverses	$a^{-1} \mod n$ exists iff $\gcd(a, n) = 1$
Solving $ax + by = c$	Has integer solutions iff $\gcd(a, b) \mid c$
Cryptography	Finding modular inverses for RSA, etc.

Finding modular inverses

To find $a^{-1} \mod n$ (when $\gcd(a, n) = 1$):

1. Use extended Euclidean algorithm to find x such that $ax + ny = 1$
2. Then $a^{-1} \equiv x \pmod{n}$

Example: Find $7^{-1} \mod 26$.
Find x such that $7x + 26y = 1$:

$$\begin{aligned} 26 &= 7 \cdot 3 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Back-substitute:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (7 - 5) \cdot 2 = 5 \cdot 3 - 7 \cdot 2 \\ &= (26 - 7 \cdot 3) \cdot 3 - 7 \cdot 2 = 26 \cdot 3 - 7 \cdot 11 \\ &= 7 \cdot (-11) + 26 \cdot 3 \end{aligned}$$

So $x = -11 \equiv 15 \pmod{26}$.
Therefore, $7^{-1} \equiv 15 \pmod{26}$.
Check: $7 \cdot 15 = 105 = 4 \cdot 26 + 1 \equiv 1 \pmod{26}$ ✓

Quick reference

Task	Method
Find $\gcd(a, b)$	Euclidean algorithm: repeat $a = bq + r$
Express gcd as $ax + by$	Back-substitute through the algorithm
Find $a^{-1} \mod n$	Solve $ax + ny = 1$, then $a^{-1} \equiv x$
Check if coprime	$\gcd(a, b) = 1$

Student Learning Support, Teaching and Learning Centre
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning

OntarioTech UNIVERSITY