

USING THE GCD PROBLEM TO COMPARE THE EFFICIENCY OF ALGORITHMS

Definition of GCD

By definition, the *Greatest Common Divisor* (GCD) of two positive integers is the largest integer that divides both integers exactly. **e.g.** $\text{gcd}(18, 12) = 6$, $\text{gcd}(3, 6) = 3$ $\text{gcd}(21, 49) = 7$

Algorithm 1: Exhaustive Search (Very Slow)

Describe how an exhaustive search algorithm can be used to compute the gcd of two integers.

Algorithm 2: Euclidean Algorithm (Very Fast)

Background

More than 2000 years ago, Euclid, the ancient Greek mathematician and teacher, published an algorithm for finding the GCD of two numbers. His version was strictly geometric since algebra had not been invented yet, but the algebraic version is described below. (**Note:** It is likely that the algorithm was known centuries before Euclid's time.)

Take any two positive integers a and b .

Euclid noted that there are integers r (the remainder) and q (the quotient) such that $a = qb + r$:

If b is divided into a , q is the quotient and r is the remainder.

(For example, if $a = 120$, $b = 25$, then $120 = 4(25) + 20$, which means that $q = 4$ and $r = 20$.)

Any common factor, N , of b and r divides a exactly:

If N divides b , it also divides qb . Since N divides r , it must also divide the sum, $qb + r$, which is a of course.

(Continuing the above example, $N = 5$ divides both $b = 25$ and $r = 20$. Therefore, $N = 5$ must also divide $qb + r = 4(25) + 20 = 120$ since $N = 5$ is a common factor of $4(25)$ and 20 .)

Any common factor, M , of a and b divides r exactly:

Since $r = a - qb$, $\frac{r}{M} = \frac{a}{M} - \frac{qb}{M}$. Since $\frac{a}{M}$ and $\frac{qb}{M}$ are both integers, then their difference, $\frac{r}{M}$, must also be an integer.

Therefore, M divides r .

($M=5$ divides both $a = 120$ and $b = 25$. Therefore it must also divide $a - qb = 120 - 4(25) = 20$)

It follows that the largest N must equal the largest M . In other words, $\text{gcd}(a,b) = \text{gcd}(b,r)$. Since b is less than a and r is less than b , we can repeat these steps substituting b for a and r for b until r becomes 0. The final step has $a = qb + 0$ and b is the desired GCD.

Summary

The Euclidean algorithm can be expressed concisely by the following recursive formula:

$$\text{gcd}(N, M) = \text{gcd}(M, N \bmod M)$$

Note: Please recall that $N \bmod M$ means the remainder obtained when N is divided by M .

Example

Here is an example of Euclid's algorithm in action.

Find the GCD of 2322 and 654.

$$\gcd(2322, 654) = \gcd(654, 2322 \bmod 654) = \gcd(654, 360)$$

$$\gcd(654, 360) = \gcd(360, 654 \bmod 360) = \gcd(360, 294)$$

$$\gcd(360, 294) = \gcd(294, 360 \bmod 294) = \gcd(294, 66)$$

$$\gcd(294, 66) = \gcd(66, 294 \bmod 66) = \gcd(66, 30)$$

$$\gcd(66, 30) = \gcd(30, 66 \bmod 30) = \gcd(30, 6)$$

$$\gcd(30, 6) = \gcd(6, 30 \bmod 6) = \gcd(6, 0)$$

$$\gcd(6, 0) = 6$$

Therefore, $\gcd(2322, 654) = 6$.

Exercise

Use Euclid's method to calculate $\gcd(4896, 432)$