GCD

CS 491 Competitive Algorithmic Programming

Objectives

The Greatest Common Divisor (GCD) often comes up on competitive programming. The algorithm to compute it is relatively simple, but often competitive programming problems require you to have a quick intuition about the properties of GCD. This activity should help with that.

- Derive Euclid's algorithm for computing GCD
- Derive the properties of GCD of more than two numbers.
- Use GCD to compute the Least Common Multiple (LCM).

Part 1 --- Deriving Euclid's Algorithm

Example: 44 and 20

- Let's start with something simple. Let $a = 44$ and $b = 20$. Give the prime factorizations of a and b.

- What is $gcd(a, b)$?

- Now let $c = a - b$. What is the prime factorization of c?

- What is $gcd(b, c)$? What is $gcd(a, c)$?

- Sketch a proof that $gcd(a, b) = gcd(b, a - b)$ for general a, b where $a > b$.

Speeding Things Up

- Given our original $a = 44$ and $b = 20$, we said $gcd(a, b) = gcd(b, a - b)$. We can do better. Show that it is also true that $gcd(a, b) = gcd(b, a - nb)$ where $n = 2$.

- Could we have used a different value of n here? How large could n be?

- What is the formula for $r = a - nb$ such that $0 < a - nb < b$?

- Therefore: $gcd(a, b) =$ ... ?

- You are ready! Write a program `gcd(a,b)` using the insight above.

Part 2 --- Properties of GCD

- Suppose m is a positive common divisor of a and b. Show that $gcd(a/m, b/m) = gcd(a, b)/m$.

- Show that GCD is a *multiplicative function.* Show that if a_1 and a_2 are coprime (i.e., $gcd(a_1, a_2) = 1$, then $gcd(a1 * a2, b) = gcd(a1, b) * gcd(a2, b)$.

- Show that GCD is a commutative and associative: $gcd(a, b) = gcd(b, a)$ and $gcd(a, gcd(b, c)) = gcd(gcd(a, b), c)$. This means that we can compute the GCD of multiple arguments.

- The Least Common Multiple is related to GCD. Show that $gcd(a, b) * lcm(a, b) = |ab|$.

- Suppose we have a unique prime factorizations of $a = p_1^{e_1} * p_2^{e_2} \cdots p_m^{e_m}$ and $b = p_1^{f_1} * p_2^{f_2} \cdots p_m^{f_m}$. Let $e_i \geq 0$ and $f_i \geq 0$. What is $gcd(a, b)$?