Algorithmic Problem Solving 17ECSE309

Stein's Algorithm

-Vaishnavi J H
-01FE15BEC216

Introduction

The **Stein's algorithm**, also known as **binary GCD algorithm**, is an algorithm that computes the greatest common divisor of two nonnegative integers. Stein's algorithm uses simpler arithmetic operations than the conventional Euclidean algorithm; it replaces division with arithmetic shifts, comparisons, and subtraction.

Algorithm

- GCD(0, v) = v, because everything divides zero, and v is the largest number that divides v. Similarly, GCD(u, 0) = u. GCD(0, 0) is not typically defined, but it is convenient to set GCD(0, 0) = 0.
- If u and v are both even, then GCD(u, v) = 2·GCD(u/2, v/2), because 2 is a common divisor.
- If u is even and v is odd, then GCD(u, v) = GCD(u/2, v), because 2 is not a common divisor. Similarly, if u is odd and v is even, then GCD(u, v) = GCD(u, v/2).
- If u and v are both odd, and $u \geq v$, then GCD(u, v) = GCD(($u - v$)/2, v). If both are odd and $u < v$, then GCD(u, v) = GCD(($v - u$)/2, u). These are combinations of one step of the simple Euclidean algorithm, which uses subtraction at each step, and an application of step 3 above. The division by 2 results in an integer because the difference of two odd numbers is even.
- Repeat steps 2–4 until u = v, or (one more step) until u = 0

Efficiency

- The algorithm requires $O(n^2)$ worst-case time, where n is the number of bits in the larger of the two numbers.
- Binary GCD can be about 60% more efficient on average than the Euclidean algorithm as it uses bitwise operations.
- It uses Bitwise-Shift for division and multiplication with 2 , Ands with 1 to check even or odd. Hence faster computation is done using this alogorithm.

References:

https://en.wikipedia.org/wiki/Binary_GCD_algorithm