Why does Euclid's GCD ALGORITHM work?

SEETHA RAMA RAJU SANAPALA

We start with the definition of the *GCD* of two numbers. (Throughout this article, 'number' means 'integer.')

Definition: The *GCD* or 'Greatest Common Divisor' of two numbers, also called the Highest Common Factor *(HCF)*, is:

- A divisor of both the numbers, i.e., it is a common divisor.
- Of all the common divisors, it is the greatest.

Note that the *GCD* is a multiple of every other common factor of the two numbers.

Example 1: Consider the numbers 8 and 20. Notice that some factors are common to both 8 and 20, namely: 1, 2 and 4. Of these common factors, 4 is the greatest and it is called the *GCD* of 8 and 20. We write: *GCD* (8, 20) = 4.

Example 2: Consider the numbers 24 and 36.

- The factors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24
- The factors of 36 are 1, 2, 3, 4, 6, 9, 12, 18 and 36.

The common factors of 24 and 36 are 1, 2, 3, 4, 6 and 12. The largest of these, 12, is the *GCD*. We write: *GCD* (24, 36) = 12. Notice that 12 is a multiple of the other common factors.

The above method of enumeration for finding the *GCD* is cumbersome and error-prone. The genius Euclid came up with an efficient and less vulnerable algorithm for this problem. Before we discuss this, we look at some facts about the *GCD* (we encourage you to justify these claims).

Keywords: Positive Integer, GCD, Algorithm, Reasoning, Proof

1. *GCD* (0, 0) is not defined.
2. When x, y are both non-zero, $GCD(x, y) = GCD(y, x)$.
3. When $x \neq 0$, $GCD(x, 0) = GCD(0, x) = |x|$.
4. $GCD(x, y) = GCD(x, -y) = GCD(-x, y) = GCD(-x, -y) = GCD(|x|, |y|)$.

In view of these facts, we may consider both x and y to be non-negative and $x \leq y$, with no loss of generality.

Euclid's algorithm is based on the following two properties:

(i). $GCD\ (x, y) = GCD\ (y - xk, x)$;

(ii). $GCD\ (x, xk) = |x|$,

where k is any integer and where neither x nor y is zero.

Using these properties, the algorithm converts the problem of finding the *GCD* of a given pair of numbers, x and y, to finding the *GCD* of a smaller pair of numbers, $y - xk$ and x. This is repeated till we reach situation (ii) above.

Consider these examples:

- $GCD\ (12, 32) = GCD\ (8, 12) = GCD\ (4, 8) = 4$;
- $GCD\ (25, 60) = GCD\ (10, 25) = GCD\ (5, 10) = 5$.

Proof of property (i): $GCD\ (x, y) = GCD\ (y - xk, x)$, for any integer k.

It is clearly enough if we prove the following:

(a) Every common divisor of x and y is a common divisor $y - xk$ and x;

(b) Every common divisor of $y - xk$ and x is a divisor of x and y.

Proof of (a): Suppose that d is a common divisor of x and y, i.e., $d \mid x$ and $d \mid y$. Let k be any integer; then $d \mid xk$. Hence $y - xk$ is a difference of two multiples of d and is therefore a multiple of d. Hence d is a common divisor of $y - xk$ and x.

Proof of (b): Let $d \mid y - xk$ and $d \mid x$; then $d \mid xk$. So $(y - xk) + xk = y$ is a sum of two multiples of d and is therefore a multiple of d. Hence d is a common divisor of y and x.

And that's why Euclid's algorithm works! QED

References

1. https://answers.yahoo.com/question/index?qid=20070625061113AAPWfC1

SEETHA RAMA RAJU SANAPALA completed his BE from Andhra University (1984) and his ME from Osmania University (1986). He worked in DRDO as a scientist for 16 years and at AT&T Bell Labs Innovations for 11 years. Currently, he teaches engineering students. He has publications in popular science magazines and technical journals. He may be contacted at manjuvenamma@yahoo.co.in.