Épreuve de section européenne

Euclid's Algorithm

In number theory, the Euclidean algorithm (also called Euclid's algorithm) is an algorithm to determine the greatest common divisor (gcd) of two integers. Its major significance is that it does not require factoring the two integers.

The Euclidean algorithm is one of the oldest algorithms known, since it appeared in Euclid's *Elements* around 300 BC (7th book, Proposition 2). Euclid originally formulated the problem geometrically, as the problem of finding the greatest common "measure" for two line lengths. However, the algorithm was probably not discovered by Euclid and it may have been known up to 200 years earlier. It was almost certainly known by Eudoxus of Cnidus (about 375 BC), and Aristotle (about 330 BC) hinted at it in his *Topics*, 158b, 29–35.

Given two natural numbers a and b, not both equal to zero : check if b is zero ; if yes, a is the gcd. If not, repeat the process replacing a by b and b by r, where r is the remainder when dividing a by b.

As an example, consider computing the gcd of 1071 and 1029, which is 21.

$$\gcd(1071, 1029) = \gcd(1029, 42) = \gcd(42, 21) = \gcd(21, 0) = 21.$$

Proof : Suppose a and b are the natural numbers whose gcd has to be determined. Now, suppose $b > 0$, and the remainder of the division of a by b is r. Therefore $a = qb + r$ where q is the quotient of the division.

Any common divisor of a and b is also a divisor of r. To see why this is true, consider that r can be written as $r = a - qb$. Now, if there is a common divisor d of a and b such that $a = sd$ and $b = td$, then $r = (s - qt)d$. Since all these numbers, including $s - qt$, are whole numbers, it can be seen that r is divisible by d.

The above analysis is true for any divisor d ; thus, the greatest common divisor of a and b is also the greatest common divisor of b and r. Therefore it is enough if we continue searching for the greatest common divisor with the numbers b and r. Since r is smaller in absolute value than b, we will reach $r = 0$ after finitely many steps.

From various sources.

Questions

1. When did Euclid's algorithm first appear ?
2. What do the letters g, c, d stand for ? What is the definition of the gcd of two integers ?
3. Explain the example that shows that $\gcd(1071, 1029)$ is equal to 21.
4. Do you know another method to find the gcd of two integers using prime numbers ? Use it on the previous example.
5. Explain the proof in your own words. How can we be sure that the algorithm will give the result in finitely many steps ?