The Euclidean Algorithm and Multiplicative Inverses

Lecture notes for Access 2011

The Euclidean Algorithm is a set of instructions for finding the greatest common divisor of any two positive integers. Its original importance was probably as a tool in construction and measurement; the algebraic problem of finding $gcd(a, b)$ is equivalent to the following geometric measuring problem: Given two different rulers, say of lengths a and b, find a third ruler which is as long as possible, but so that you can still use it as a scale on both of the longer rulers. There's a neat "movie" demonstration of how the algorithm works geometrically, on the *Wikipedia* page for "Euclidean Algorithm". Euclid probably wasn't thinking about finding multiplicative inverses in modular arithmetic, but it turns out that if you look at his algorithm in reverse, that's exactly what it does!

The Euclidean Algorithm makes repeated used of integer division ideas: We "know" that if a and b are positive integers, then we may write

$$\frac{a}{b} = q + \frac{r}{b}$$

where q is the quotient, and the remainder r satisfies $0 \leq r < b$. If we clear fractions, this is the equation

$$a = bq + r.$$

We really do know that this last equation is possible: starting with $(b)(0)$, then $(b)(1)$ etc. we may subtract increasing multiples of b from a until what remains is a non-negative number less than b. And that's actually the mathematical reason that the integer division fact we started with is true. (This procedure is called the division algorithm.)

Here is the algebraic formulation of Euclid's Algorithm; it uses the division algorithm successively until $gcd(a, b)$ pops out:

Theorem 1 (The Euclidean Algorithm)**.** Given two integers $0 < b < a$, we make a repeated application of the division algorithm to obtain a series of division equations, which eventually terminate with a zero remainder:

$$a = bq_1 + r_1, 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2,$$

$$\dots$$

$$r_{j-2} = r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}$$

$$r_{j-1} = r_jq_{j+1}.$$

The greatest common divisor $gcd(a, b)$ of a and b is r_j, the last nonzero remainder in the division process.

Let's look at an example of the Euclidean algorithm in action - it's really quick at finding gcd's when your two integers are large. We should be able to verify these steps with our scientific calculators:

Example 1. Find the gcd of 42823 and 6409.

Solution.

$$\begin{aligned} \mathbf{42823} &= \mathbf{6409}(6) + \mathbf{4369} \\ \mathbf{6409} &= \mathbf{4369}(1) + \mathbf{2040} \\ \mathbf{4369} &= \mathbf{2040}(2) + \mathbf{289} \\ \mathbf{2040} &= \mathbf{289}(7) + \mathbf{17} \\ \mathbf{289} &= \mathbf{17}(17) \end{aligned}$$

Therefore $gcd(42823, 6409) = 17$. □

Why does the Euclidean Algorithm actually give the gcd? It seems kind of strange that we can get the gcd of two numbers a and b by looking at the gcd's of the subsequent remainder values. Let's look at successive equations in this process: From the first equation $a = bq_1 + r_1$, we deduce that since the gcd divides a and b it must divide r_1. Similarly in the next equation $b = r_1q_2 + r_2$, the gcd divides b and r_1, so it must also divide r_2. Thus the $gcd(a, b)$ divides all the remainders, including the final non-zero one, r_j. On the other hand, by working up from the last equation $r_{j-1} = r_jq_{j+1}$ we deduce that r_j divides r_{j-1}. From the second to last equation r_j also divides r_{j-2}, and working all the way back to the top we see that r_j divides both a and b, so is a divisor. Putting our reasoning together, r_j must be the greatest common divisor! But enough of these explanations, let's try some exercises!

Exercise 1. Find the gcd's of the following pairs of numbers. Save your work because you'll need it later.

1. 7469 and 2464

2. 2689 and 4001

3. 2947 and 3997

4. 1109 and 4999

The fact that we can use the Euclidean algorithm work in order to find multiplicative inverses follows from the following algorithm:

Theorem 2 (Multiplicative Inverse Algorithm)**.** Given two integers $0 < b < a$, consider the Euclidean Algorithm equations which yield $gcd(a, b) = r_j$. Rewrite all of these equations except the last one, by solving for the remainders:

$$r_1 = a - bq_1,$$

$$r_2 = b - r_1q_2,$$

$$r_3 = r_1 - r_2q_3,$$

$$\dots$$

$$r_{j-1} = r_{j-3} - r_{j-2}q_{j-1}$$

$$r_j = r_{j-2} - r_{j-1}q_j.$$

Then, in the last of these equations, $r_j = r_{j-2} - r_{j-1}q_j$, replace r_{j-1} with its expression in terms of r_{j-3} and r_{j-2} from the equation immediately above it. Continue this process successively, replacing $r_{j-2}, r_{j-3}, \dots$, until you obtain the final equation

$$r_j = ax + by,$$

with x and y integers. In the special case that $gcd(a, b) = 1$, the integer equation reads

$$1 = ax + by.$$

Therefore we deduce

$$1 \equiv by \mod a$$

so that (the residue of) y is the multiplicative inverse of b, $\mod a$.

Examples!

Example 2. Find integers x and y to satisfy

$$42823x + 6409y = 17.$$

Solution. We begin by solving our previous equations for the remainders. We have:
$4369 = 42823 - 6409(6)$
$2040 = 6409 - 4369$
$289 = 4369 - 2040(2)$
$17 = 2040 - 289(7)$
Now we do the substitutions starting with that last equation and working backwards and combining like terms along the way:
$17 = 2040 - 289(7) = 2040 - (4369 - 2040(2))(7) = 2040(15) - 4369(7)$
$17 = (6409 - 4369)(15) - 4369(7) = 6409(15) - 4369(22)$
$17 = 6409(15) - (42823 - 6409(6))(22) = 6409(147) - 42823(22)$
Therefore $x = -22, y = 147$. □

Example 3. Find the multiplicative inverse of $8 \mod 11$, using the Euclidean Algorithm.

Solution. We'll organize our work carefully. We'll do the Euclidean Algorithm in the left column. It will verify that $gcd(8, 11) = 1$. Then we'll solve for the remainders in the right column, before backsolving:

$$\begin{array}{rcrcr|rcrcr} \mathbf{11} & = & \mathbf{8}(1) & + & \mathbf{3} & 3 & = & 11 & - & 8(1) \\ \mathbf{8} & = & \mathbf{3}(2) & + & \mathbf{2} & 2 & = & 8 & - & 3(2) \\ \mathbf{3} & = & \mathbf{2}(1) & + & \mathbf{1} & 1 & = & 3 & - & 2(1) \\ \mathbf{2} & = & \mathbf{1}(2) & & & & & & & \end{array}$$

Now reverse the process using the equations on the right.

$1 = 3 - 2(1)$
$1 = 3 - (8 - 3(2))(1) = 3 - (8 - (3(2)) = 3(3) - 8$
$1 = (11 - 8(1))(3) - 8 = 11(3) - 8(4) = 11(3) + 8(-4)$

Therefore $1 \equiv 8(-4) \mod 11$, or if we prefer a residue value for the multiplicative inverse,

$$1 \equiv 8(7) \mod 11.$$

□

Be careful about the order of the numbers. We do not want to accidentally switch the bolded numbers with the non-bolded numbers!

Exercise 2. Find the greatest common divisor g of the numbers 1819 and 3587, and then find integers x and y to satisfy

$$1819x + 3587y = g$$

Exercise 3. Find the multiplicative inverses of the following:

1. $50 \mod 71$

2. 43 mod 64

Exercise 4. Using the information from the previous exercise, solve the following equation for x and check your answer.

$$50x \equiv 63 \mod 71.$$

Exercise 5. Solve $12345x \equiv 6 \mod 54321$. Hint: First find the gcd.