A practical guide to the extended Euclid algorithm

Harald Hanche-Olsen

http://www.math.ntnu.no/~hanche/

In this note we are given two positive integers $a > b$. Recall that Euclid's algorithm finds $\gcd(a, b)$ by repeated division, with the greatest common divisor being the last nonzero remainder.

The Euclidean algorithm is quite easy to follow. The extended Euclidean algorithm uses data found during the Euclidean algorithm to find solutions x and y to the equation

$$ax + by = \gcd(a, b).$$

It is somewhat harder, when doing it by hand, to organize the steps in the extended algorithm appropriately.

Since this is a *practical* guide, we consider an example. For our numbers, we choose $a = 2011$ and $b = 1534$.

The colour has significance: We use red for the remainders (noting that the original numbers naturally belong among these), and blue for the quotients.

So here is the usual Euclidean algorithm in action:

$$\begin{aligned}
2011 &= 1534 \cdot 1 + 477 \\
1534 &= 477 \cdot 3 + 103 \\
477 &= 103 \cdot 4 + 65 \\
103 &= 65 \cdot 1 + 38 \\
65 &= 38 \cdot 1 + 27 \\
38 &= 27 \cdot 1 + 11 \\
27 &= 11 \cdot 2 + 5 \\
11 &= 5 \cdot 2 + 1 \\
5 &= 1 \cdot 5 \quad \text{(no remainder) and therefore} \\
\gcd(2011, 1534) &= 1.
\end{aligned}$$

Notice how the remainders migrate to the left from one line to the next.

Now we turn to solving the equation

$$ax + by = 1.$$

First, the basic idea: We are trying to write the greatest common divisor (which is the last remainder, 1 in this case) as a (linear) *combination* of a and b. Clearly, the first line in the algorithm expresses the *first* remainder as such a combination:

$$477 = a - b.$$

And the next line expresses the next remainder 103 as a combination of the previous two remainers 1534 and 477, and thus as a combination of a and b,

$$103 = b - 477 \cdot 3 = b - (a - b) \cdot 3 = -a + 4b$$

and so we can proceed downwards until we reach the bottom.

However, we can effectively *halve the work* by reducing everything modulo one of the original numbers! Let $\equiv$ stand for congruence modulo $a = 2011$. On the left below is the original Euclid's algorithm, on the right is the new calculation. Notice that the new name of the game is to write each remainder *as a multiple of b modulo a*. Each line on the right is first a rewrite on the line on its left, then simplifying using data from the two lines above (except for the opening moves):

$$\begin{array}{rlrl}
2011 &= 1534 \cdot 1 + 477 & \qquad 477 &\equiv -1534 = -b \\
1534 &= 477 \cdot 3 + 103 & 103 &= 1534 - 477 \cdot 3 \equiv b - (-b) \cdot 3 = 4b \\
477 &= 103 \cdot 4 + 65 & 65 &= 477 - 103 \cdot 4 \equiv -b - 4b \cdot 4 = -17b \\
103 &= 65 \cdot 1 + 38 & 38 &= 103 - 65 \cdot 1 \equiv 4b - (-17b) = 21b \\
65 &= 38 \cdot 1 + 27 & 27 &= 65 - 38 \cdot 1 \equiv -17b - 21b = -38b \\
38 &= 27 \cdot 1 + 11 & 11 &= 38 - 27 \cdot 1 \equiv 21b - (-38b) = 59b \\
27 &= 11 \cdot 2 + 5 & 5 &= 27 - 11 \cdot 2 \equiv -38b - 59b \cdot 2 = -156b \\
11 &= 5 \cdot 2 + 1 & 1 &= 11 - 5 \cdot 2 \equiv 59b - (-156b) \cdot 2 = 371b.
\end{array}$$

If we have made no mistake, we have in fact shown that

$$371b \equiv 1 \pmod{a},$$

in other words, that 371 is the inverse of 1534 modulo 2011. This sort of result is of course one of the reasons to perform the extended Euclidean algorithm in the first place, so if that were our goal, we could stop here.

But we wanted to find x and y. From what we have shown, we are pretty certain that $371b - 1$ is a multiple of a. So we perform the division:

$$(371b - 1)/a = (371 \cdot 1534 - 1)/2011 = 283$$

with no remainder, which of course confirms our calculation and can also be rearranged as

$$283a - 371b = 1,$$

so a solution to the problem is

$$x = 283, \quad y = -371.$$