CS 512: Are Eucliding Me?

16:198:512

Instructor: Wes Cowan

Euclid's algorithm for computing the GCD has an immediate and natural importance as having the GCD (and therefore being able to compute the GCD) is a useful thing. But what of the Extended Euclidean Algorithm? If we have that $\gcd(a, b) = d$, of what use are integers x, y such that

$$ax + by = d?$$

There are a couple of immediately useful instance: for instance, doing division mod N requires the notion of multiplicative inverses. Given a, how can we find an x such that $ax \equiv 1(\bmod N)$? If $\gcd(a, N) = 1$, this is a natural application of the Extended Euclidean Algorithm to give us x, y such that

$$ax + Ny = 1,$$

or equivalently, $ax - 1 \equiv 0(\bmod N)$.

But another vast and useful area of application is that of *Diophantine Equations*, and variously related integer programming problems. The basic problem is, given an equation (or system of equations) in terms of some variables, can you solve for those variables *restricting the solutions to be integers?*

As a simple application - suppose you need 31 units of something. But one supplier sells them in packages of 5, the other in packages of 7. How many packages should you buy from each supplier to yield the desired total? i.e., find integers x and y such that

$$5x + 7y = 31.$$

Notice that the Extended Euclidean Algorithm is not immediately useful here, as $\gcd(5, 7) \neq 31$. However, the EEA yields a pair (x_0, y_0) such that

$$5x_0 + 7y_0 = 1.$$

Depending on your implementation, such a pair might be $x_0 = 3, y_0 = -2$. From this, we naturally get that

$$5(31x_0) + 7(31y_0) = 31.$$

At first blush, it seems we've yielded a solution $x = 93, y = -62$.

However, this is by no means an acceptable answer to the problem as stated - we can't buy -62 packages from the supplier. (There might be an interpretation of this involving buying too many packages from one supplier, and selling excess to the other, but this is a CS class not an economics class.) What is there to be done? Are there any solutions that might satisfy us?

One thing to remember is that the equation $5x + 7y = 31$ actually represents a line in two dimensional space - there are in fact infinitely many real valued solutions (x, y). We have identified one integral solution $(93, -62)$ - it is possible there are others. Observe that for any solution (x, y), we get that $(x - 7t, y + 5t)$ is also a solution:

$$5(x - 7t) + 7(y + 5t) = (5x + 7y) - 35t + 35t = 31.$$

Hence we can ask the question, is there any t such that $93 - 7t \geq 0, -62 + 5t \geq 0$? Rearranging, we get

$$12.4 \leq t \leq 13.29.$$

The only integer solution for t in this range is $t = 13$, yielding a final solution of

$$x = 93 - 7 * 13 = 2$$
$$y = -62 + 5 * 13 = 3.$$

We see from this that the core solution to $5x_0 + 7y_0 = 1$, given to us by the Extended Euclidean Algorithm, could then be leveraged to a solution to the actual equation we were interested in, subject to the indicated constraints.

Questions

Let a, b, c be positive integers, and $d = \gcd(a, b)$.

- Argue that if $ax + by = c$ has integer solutions for x, y, it must be that d divides c.
- Let (x_0, y_0) be the pair returned by the Extended Euclidean Algorithm. Argue that $x' = (c/d)x_0, y' = (c/d)y_0$ solves $ax + by = c$.
- What are the smallest positive integers α, β such that

$$a(x - \alpha t) + b(y + \beta t) = c?$$

- Argue that any integer solution (x, y) to $ax + by = c$ must be of the form, for (possibly negative) integer t

$$x = \frac{c}{d}x_0 - \frac{\text{lcm}(a,b)}{a}t,$$
$$y = \frac{c}{d}y_0 - \frac{\text{lcm}(a,b)}{b}t.$$

- Under what conditions on a, b, c will non-negative solutions to $ax + by = c$ exist?
- What can you conclude about the complexity of solving $ax + by = c$ with $x, y \geq 0$?

Extensions:

- Given constants $(A_1, \ldots, A_n, D)$, and an equation such as

$$A_1x_1 + A_2x_2 + \ldots + A_nx_n = D,$$

, how can you extend this analysis to solve for integer solutions $(x_1, x_2, \ldots, x_n)$? Hint: What can you say about the expression $A_1x_1 + A_2x_2$? What is the additional complexity of solving these types of equations for $n > 2$?

- Consider *non-linear* equations such as $ax^2 + by^2 = c$. What can you say about solutions for x, y? Can you use this previous analysis for the linear case to simplify the problem of solving in this non-linear case? What is the complexity of solving this non-linear case?