

22. Factoring Numbers II. The Elliptic Curve Method

1. Introduction

We now consider the third factoring method, which is roughly as good as the previous one, at least in theory.

It is based on the fact that if we take a polynomial equation in two variables of the form

$$y^2 = x^3 + ax^2 + bx + c,$$

with coefficients in any field, solutions to it (along with a “point at infinity”) form a group, and a group whose size is somewhat random.

A curve of this kind is called an **elliptic curve**, and the method of factoring that makes use of it is called the **elliptic curve factoring algorithm**.

Elliptic curves can also be used for encryption by using the discrete logarithm method of encoding with multiplication in the elliptic curve group. We will not discuss it further here.

We will begin by outlining how the argument works, and then describe the elliptical curve group and how we can find and multiply solutions in such groups.

2. The idea of the algorithm

When we do computations with our algorithm we will always do so mod N . However, what goes on can, by the Chinese remainder theorem, be imagined separately mod p and mod q .

The procedure here will be to find a number congruent to 0 mod p or mod q but not the other way round, and to apply Euclid’s algorithm to it and to N .

If we perform squares or multiplications in the elliptic curve group for some equation, we will wander from one solution, or a pair of them to a third one. However when we encounter the identity in the group mod p or q but not both, we will actually factor N .

This is true because the act of multiplying two solutions involves a division mod N , which requires use of Euclid’s algorithm with N and when this multiplication produces the identity mod p it actually produces the “point at infinity” mod p which involves dividing by 0 mod p which is dividing by a multiple of p .

More concisely, this all means that the process you use to reach the identity in the group mod p involves applying Euclid’s algorithm on N and a multiple of p .

When you do so you find p as the gcd, so you have factored N .

Now remember Lagrange's theorem, which states that the order of any element of a group which is the order of the subgroup consisting of its powers, is a divisor of the order of the group. This implies that if you raise any element of the group to a power given by the order of the group you will get the identity element of the group.

Here this means that if you take any element of the group, and raise it to the power given by the order of the group, you will obtain the identity, and therefore factor N .

And of course if you raise it to any power that is an integer multiple of the order of the group, you will obtain the identity as well and factor N .

Now here comes the interesting point, The order of this group depends on what function you have chosen, and, $\text{mod } p$, is some number within $2p^{1/2}$ of p .

Now suppose by dumb luck, the equation you have chosen has a group whose order $\text{mod } p$ has all its prime factors less than M .

Then with a little bit of luck, if you pick x in the group and raise it to a power like $M! \text{ mod } N$, $M!$ (or maybe $2M!$) will be a multiple of the order of your group, and you will attain the identity $\text{mod } p$, and find p .

So the procedure is: pick an equation and a solution x and raise it to ever increasing factorial powers $\text{mod } N$. This is just raising it to higher and higher powers, which is something we have discussed already.

Thus, you first square x in the group then cube that then take the fourth power of that then the fifth power of that, and so on.

We can figure out exactly how many multiplications in the group must be made to raise an element to the $M!$ It comes out to be something on the order of $3M(\log_2 M)/2$.

If the order of your group is a product of primes less than M and if the power of each prime dividing N is less than the power that occurs in $M!$ (or $2M!$), then the order of your group will be a divisor of $M!$ and you will factor N .

We have seen that a proportion like $\log M / \log N$ of numbers will have this nice property, so most of the time that you try this, you will not succeed. However, if many work on this in a distributed way, each with one equation, you can hope that someone gets a group for which this works, and will factor N .

We now try to fill in what all this means, by defining the group of an equation, and showing how multiplication and squaring is done in such a group.

You might ask: why factorial powers? The answer is that M factorial has all small primes in it and has lots of copies of the smaller ones, so that a number with only relatively small prime factors is likely to be a divisor of $M!$ for reasonable small M . And computation of an $M!$ -th power here is an operation that is quite straightforward to accomplish.

3. The Group of an Elliptical Curve

Suppose we pick an equation

$$y^2 = x^3 + ax^2 + bx + c,$$

and specify a and b , and allow c to vary. Then for any specific value of x , the right hand side will be the sum of the first three terms and c , which we can call $A+c$, and our equation can be written as

$$y^2 = A + c.$$

Now every y has some square mod p , so as we vary c each of the p possibilities for y will be a solution for one value of c . On the other hand, when the right hand side is not 0, each equation which has a solution, has two solutions, y and $-y$.

There are thus two kinds of non-zero right hand sides here, those with two solutions, and those with none, and there are an equal number of each. Those right hand sides with two solutions to this equation are called **quadratic residues** mod p .

Now suppose we fix c , and let x vary. This will cause A to vary in a somewhat irregular way. Sometimes the right hand side will be a quadratic residue, and sometimes it will not be one. Roughly half of the time it will be one, and half not, but the exact number of values of x for which there are solutions will vary with the equation, though it can be shown that it never differs by more than $p^{1/2}$ from $p/2$.

The number of solutions to the equation is therefore somewhere within $2p^{1/2}$ of p .

We can always find an equation with a solution mod N by choosing x , evaluating A and choosing c to make any given y a solution.

So we can find an equation, and a solution (x,y) to it, mod N .

The curve defined by our equation has an interesting geometric property. If we draw any line in the $x y$ plane that meets it at 2 points, it will meet it at a third point.

This fact is easy to verify. Suppose we consider the line $y=mx+q$ and examine the points that lie on the intersection of this line with our curve.

These are the points which obey both equations. We can therefore use the linear equation to substitute for y in our equation, to obtain

$$(mx)^2 + 2qmx + q^2 = x^3 + ax^2 + bx + c.$$

This is a cubic equation in x , and it will have either three real roots (which can be degenerate so that two are the same) or one real root.

This means that if we have two solutions, say (x_1, y_1) and (x_2, y_2) , there will be a third one.

And if we write our equation as

$$x^3 + (a-m^2)x^2 + (b-2qm)x + c-q^2 = 0,$$

we can recognize what the third solution is without much work.

Recall that x_1 and x_2 will both be solutions of this equation, and $m^2 - a$ here must be the sum of the three x -solutions, so that we have

$$x_3 = m^2 - a - x_1 - x_2$$

We can also deduce

$$y_3 = y_1 + m(x_3 - x_1).$$

Thus we can easily find the third solution given m .

And m is given by $(y_2 - y_1)/(x_2 - x_1)$.

So far we have described how to find the third solution here when we have two distinct solutions, which will determine how we multiply solutions in our group.

We must also consider how to find the third solution when the two solutions are the same, because that is how we will square a solution.

Suppose then we start with one solution (x_1, y_1) and want to find the third solution when this is a double solution.

What we then mean is that **the slope of the line** is not given by the formula above but instead **is the same as the slope of the curve at (x_1, y_1)** , which gives

$$m = (3x_1^2 + 2ax_1 + b_1)/2y_1.$$

What is strange and wonderful about these elementary algebraic manipulations is that we can define a group as follows:

The elements of the group are solutions (x_i, y_i) of the original equation, and a point at infinity, which serves as the identity element for the group.

The law of composition between two solutions (x_1, y_1) and (x_2, y_2) is:

Find the third solution on the same line, and reverse its y component: it is $(x_3, -y_3)$ with y_3 as given above.

$$(x_1, y_1) \circ (x_2, y_2) = (x_3, -y_3).$$

To square (x_1, y_1) you similarly find the third solution with the given slope and reverse the y component.

With this rule you can see that **the identity is the point at infinity on every line $x=\text{constant}$** . To multiply g by this point you find the other point on the $x=\text{constant}$ line, which is the point obtained from g by reversing g 's y component, and then you reverse it again, and get g which is what multiplying by the identity is supposed to do to g .

The inverse of a group element (solution) g is therefore its reflection obtained by reversing g 's y component.

You can see that we can perform operations in this group by simple algebraic manipulations (which do not involve c at all).

Of course the law of composition in this group is not quite so simple. To perform it you must multiply and divide, and these multiplications and divisions must be performed mod p or in our case mod N .

Multiplication is something we have discussed often. **But how do we divide mod N ?**

There is a standard way to do division. We find the inverse of the denominator d mod N by using Euclid's algorithm. That is, we find r such that $rd+sN=1$, and multiply by r mod N to divide by d .

But look what happens when the two solutions we are composing happen to be reflections of one another in the x axis mod p . In that case we will have $x_1 = x_2 \pmod{p}$ which means $x_1 - x_2$ is a multiple of p , and when we try to find the inverse of $x_2 - x_1 \pmod{N}$ so as to compute m , we will find that $x_2 - x_1$ has no inverse mod N . **$x_1 - x_2$ will be a multiple of p and Euclid's Algorithm will spit out p to us instead of giving us the inverse we were looking for. And this will happen whenever we try to form the identity element of this group.**

And that is how this algorithm goes. You choose a and b , pick a c to get some solution, and hope that your equation is a lucky one that has a group of an order having only small prime factors mod p or q .

If so, raising an initial solution to an $M!$ power mod N will produce the identity mod p or q and suddenly spit out a $+factor$ of N as it chugs along increasing M .

There have been recent announcements, I am told, that the distributed elliptic curve algorithm, (where different machines work together) now has the public factoring record.

4. A Comment

There was a prominent English number theorist of almost a century ago named Hardy, who developed an intense loathing for applied mathematics.

This was somewhat understandable at the time, because there was no such thing as a workable calculating machine (beyond an abacus) then, and all practical computations were extraordinarily tedious.

So I suppose people would come to him and ask him to help them with applied tasks, and when he tried to do so, and after intense effort came up with a solution to the problem that he interpreted that they had told him, he would discover that that was not what they wanted at all.

After a few such experiences he wrote off applied mathematics entirely, and he prided himself on the utter uselessness of number theory which was his favored field of endeavor.

You have to wonder what he would make of the modern world, where number theoretic questions have developed great practical importance, and applied mathematicians in some areas are obligated to search all the nooks and crannies of the field in the hopes of finding new one way hard problems to use for encryption, or to find ways to break encryption schemes.

He might be turning over in his grave, but I expect the opposite. Were he alive today he would most likely delight in the power that machines now give us to avoid tedious computations and and come to the conclusion that applications, which now invade number theory, are as exciting as the (identical) subjects that turned him on.

Exercise: Explain this algorithm in your own words.