Factoring with Elliptic Curves

Justin Wyss-Gallifent

April 25, 2022

0.1 Introduction

The idea is to use elliptic curves to factor numbers.

0.2 Elliptic Curves mod a Composite

First note that an elliptic curve equation modulo a composite number does not allow us to construct a group. For example if we consider:

$$y^2 \equiv x^3 + 2x + 2 \mod 35$$

We note a few problems:

- All of $(4, 2)$, $(4, 12)$, $(4, 23)$ and $(4, 33)$ are on the curve, meaning we have lines that meet the curve too many times.
- Both $(4, 12)$ and $(9, 7)$ are on the curve but our addition formula in this case necessarily requires the multiplicative inverse of $9 - 4 = 5$ mod 35 and this does not exist.

0.3 Analogy for the $p-1$ Factoring Method

Suppose we have an EC $y^2 \equiv x^3 + Ax + B \mod n$ where $n = pq$. Note that this is still an EC, there's just no underlying group structure anymore.

Suppose we pick a basepoint P_b and a large M and we attempt to find $M!P_b$ through repeated addition as if there were an underlying group structure:

$$\begin{aligned} 1!P_b &= P_b \\ 2!P_b &= 2(1!P_b) \\ 3!P_b &= 3(2!P_b) \\ \vdots & \;\vdots \end{aligned}$$

It's highly likely that we'll encounter a situation in which we have an $x_2 - x_1$ with no multiplicative inverse mod n, meaning $\gcd(x_2 - x_1, n) \neq 1$. This gcd will potentially then be our factor, assuming it's not n itself, for example when $x_2 \equiv x_1 \mod n$.

0.4 What's Going On Under the EC Hood?

If a point (x, y) satisfies $y^2 \equiv x^3 + Ax + B \mod n = pq$ then it satisfies $y^2 \equiv x^3 + Ax + B \mod p$ and $y^2 \equiv x^3 + Ax + B \mod q$ and in fact every equation mod $n = pq$ will also be valid mod p and mod q, including those where we find those multiplicative inverses which do exist mod n.

Thus as we go through our repeated addition process mod $n = pq$ we can imagine we are going through it mod p and mod q at the same time, in the background. We don't need to actually do it, and we couldn't even if we wanted to, because we don't know p and q.

Note that mod p and mod q these are actually group calculation since the EC does create a group mod p and mod q.

Suppose $y^2 \equiv x^3 + Ax + B \mod p$ has N_p points and $y^2 \equiv x^3 + Ax + B \mod q$ has N_q points. It's highly likely that N_p and N_q have very different factorizations.

Suppose WLOG that N_p has small factors. In that case it's likely that $N_p \mid M!$ and then there is some positive integers k with $kN_p = M!$ and then:

$$M!P_b = kN_pM! = k(N_pM!) = k(\infty) = \infty \qquad \text{on } y^2 \equiv x^3 + Ax + B \mod p$$

In our calculation process we will probably notice this earlier than $M!$. Instead we'll notice it as soon as we try to do an addition for which yields ∞ on $y^2 \equiv x^3 + Ax + B \mod p$. In addition if those many small factors are in fact small and not too numerous then we are likly to encounter this issue fairly early in the calculation.

Chances are also high that since N_q has a different factorization that the same addition will not result in ∞ on $y^2 \equiv x^3 + Ax + B \mod q$ simply because we won't have hit a multiplicand (repeated sum) yielding ∞ on the mod q version just yet.

This means that at this instant in the calculation we will have some j with:

$$\begin{aligned} jP_b = \infty \text{ on EC mod } p &\Longrightarrow \gcd(x_2 - x_1, p) \neq 1 \\ jP_b = \infty \text{ on EC mod } q &\Longrightarrow \gcd(x_2 - x_1, q) = 1 \end{aligned}$$

It then follows that $1 < \gcd(x_2 - x_1, n) < n$ is a factor of n.

0.5 In Practice

In practice it's really simple:

1. Pick an EC mod n, pick a basepoint P_b, pick an upper bound $M!$.
2. Attempt to calculation $1!P_b$, $2!P_b$, ... ,$M!P_b$.
3. If we encounter a problem calculating a multiplicative inverse arising from a $\gcd(x_2 - x_1, n) \neq 1$ then this gcd is almost certainly a factor. The only way it won't be is if the calculation fails simultaneously both on the EC mod p and on the EC mod q which is highly unlikely.
4. If we reach $M!P_b$ and no problem is encountered we can either choose a larger $M!$, a different P_b, or a different EC all together.

The strength in this method over the standard $p - 1$ method is that we have a wider variety of choices to make.

0.6 Examples

Example:

Suppose we wish to factor $n = 529019$. We choose the elliptic curve $y^2 \equiv x^3 + 5x - 5 \mod 529019$, the base point $P_b = (1, 1)$ and $M = 10$. We calculate:

$$\begin{aligned} 1!(1,1) &= (1,1) \\ 2!(1,1) &= (14, 528966) \\ 3!(1,1) &= (75488, 399254) \\ 4!(1,1) &= (169486, 129530) \\ 5!(1,1) &= (196888, 94940) \\ 6!(1,1) &= \infty \end{aligned}$$

In the process of calculating $6!(1, 1)$ we encounter x_1 and x_2 with $\gcd(x_2 - x_1, 529019) = 613$ and we have a factor.

Example:

We don't have to have just two factors, this will work for any n.

I just randomly added a 1 to the end of the above number to get $n = 5290191$ and fed it to Python without changing the basepoint or M. The calculation of $7!(1, 1)$ fails, producing a gcd of 27.

Example:

Just for fun if we revisit the first example and use $y^2 \equiv x^3+2x-2 \mod 529019$ with the same basepoint and same M we encounter a problem much earlier:

$$\begin{aligned} 1!(1,1) &= (1,1) \\ 2!(1,1) &= (132259, 198373) \\ 3!(1,1) &= \infty \end{aligned}$$

In the process of calculating $3!(1, 1)$ we encounter x_1 and x_2 with $\gcd(x_2 - x_1, 529019) = 613$ and we have a factor.