Elliptic Curve Factorization

Eli Vigneron

October 2, 2020

1 Introduction

The main focus of this paper will be to look at Lenstra's Elliptic-Curve Factorisation method. The relevance of factoring can be tied to public-key cryptography (e.g., the RSA algorithm), and elliptic-curve factorisation is reasonably fast, and much easier algorithm to implement than most faster algorithms. We will start by providing the necessary background to understand and implement some of the outlined methods.

There are a number of equivalent definitons of elliptic curves; we state a few:

Definition 1. [Poo01, Definition 4.1] *Let K be a perfect field (every irreducible polynomial in K has distinct roots). Then an* ***elliptic curve*** *over K is*

1. *the projective closure of a nonsingular curve as described by what is often labeled a "Weierstrss equation" viz.*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
where the a_i's are in K. Whenever the characteristic of the field of interest is not 2 or 3, then it is sufficient to consider the projective closures of curves of the form:
$$y^2 = x^3 + Ax + B.$$
In fact, such a curve is nonsingular precisely when the roots of $x^3 + Ax + B$ are distinct in $\bar{K}$.

2. *A nonsingular projective curve of genus 1 lying over K, which comes with a K-rational point O.*

3. *A one-dimensional projective group variety over k.*

We will briefly recall some of the definitions of the terms in the above definition.

Definition 2. *A point (a, b) on the affine curve $f(x, y) = 0$ over K is* ***singular*** *if and only if $(0, 0)$ is singular on $f(X + a, Y + b) = 0$, where $(0, 0)$ is a singular point if $\partial f/\partial x$ and $\partial f/\partial y$ are zero at $(0, 0)$. An affine curve is* ***nonsingular*** *if it has no singular points and a projective curve $F(X, Y, Z) = 0$ is nonsingular if its "affine pieces" $F(x, y, 1) = 0$, $F(x, 1, z) = 0$, $F(1, y, z) = 0$ are nonsingular.*

An elliptic curve E over a field K is said to be a group variety when we can define a map $E \times E \to E$ in terms of rational functions, and this induces a group structure on $E(L)$ where L is any field extension of K. For an elliptic curve E, which is given in Weierstrass form, the **group law** on $E(K)$ is characterized by the following properties:

1. The identity of the group is the point $O = (0 : 1 : 0)$ at infinity

2. When a line ℓ intersects E at points $P, Q, R \in E(K)$, then $P + Q + R = O$ in the group law.

Remark 1. *From the above characterization, we obtain the following*

1. *Given a nonzero point $P \in E(K)$, then as the curve is symmetric about the x-axis, we can take $-P$ to be the point opposite to it, in other words: there is a vertical line through P which intersects E at P, O, and $-P$.*

2. *Given nonzero points $P, Q \in E(K)$, we can uniquely describe a third point, $P+Q$, in the following manner. First take the line through P and Q (let this be the tangent to E at the point P when $P=Q$) intersecting the curve E at the aforementioned points P and Q and at a third point $R \in E(K)$. If this third point R is O, then $P+Q=O$; otherwise, $P+Q=-R$, where $-R$ is constructed as in (1).*

We can represent the group law pictorially as follows. If we consider the following images,

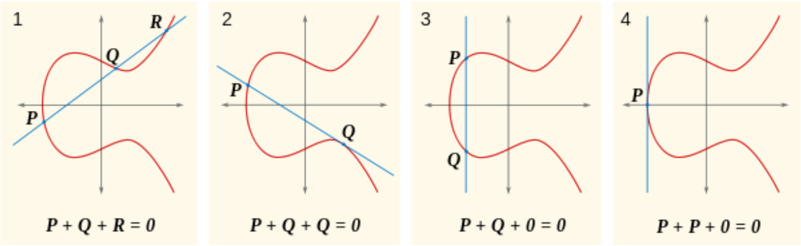

Figure 1: [Com18a]

Then as outlined above, we can indicate the locations of some of the derived data in the ensuing manner (where R' indicates $-R$ and so forth).

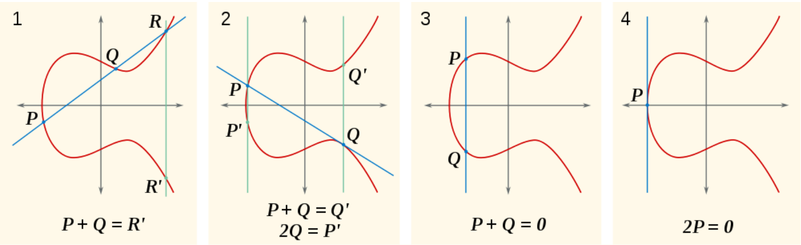

Figure 2: [Com18b]

Remark 2. *Note that $E(K)$ as above, is an abelian group.*

The next tool we will need is an explicit algorithm for computing $P+Q$ which will be necessary for the elliptic curve factoring method.

Let R denote the sum of points P and Q in $E(K)$ on a curve $y^2 = x^3 + Ax + B$ over K:

1. If $P = O, R = Q$ return.

2. If $Q = O, R = P$ return.

3. Else, Let $P = (x_0 : x_1 : 1)$ and $Q = (y_0 : y_1 : 1)$. If $x_0 \neq y_0$, set

$$\begin{aligned} \lambda &= \frac{x_1 - y_1}{x_0 - y_0}, \\ z_0 &= \lambda^2 - x_0 - y_0, \\ z_1 &= \lambda(x_0 - z_0) - x_1, \\ R &= (z_0 : z_1 : 1) \end{aligned}$$

   return.

4. if $x_0 = y_0$ and $x_1 = -y_1$, set $R = O$ return.

5. if $x_0 = y_0$ and $x_1 \neq -y_1$, set

$$\begin{aligned} \lambda &= \frac{3x_0^2 + A}{x_1 + y_1}, \\ z_0 &= \lambda^2 - x_0 - y_0, \\ z_1 &= \lambda(x_0 - z_0) - x_1, \\ R &= (z_0 : z_1 : 1) \end{aligned}$$

   return.

This algorithm takes $O(1)$ field operations in K, and further, passing to projective coordinates makes division unnecessary.

As a visual example we look at $(1, 0) + (0, 2) = (3, 4)$ on the curve $y^2 = x^3 - 5x + 4$

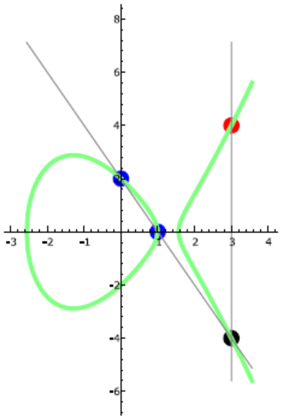

Figure 3: [Ste09, P.127]

2 Factoring methods

Factorization methods seek to solve the following type of problem, if p and q are unknown large primes and we are given their product $N = pq$ how do we determine p and q. One method of factoring N is to compute an integer m (using a some not yet specified method) such that $m \equiv_p 0$ but is non zero modulo q. Computing $gcd(m, N)$ will then yield p.

The method that we are going to turn our attention to is known as Lenstra's elliptic curve method, abbreviated ECM.

We will begin by outlining the method, then provide some examples and conclude with a discussion of why the algorithm works.

Lenstra's Elliptic Curve Method

Let N be a given integer: [1]

1. Pick random integers, a, x, y between 1 and N
2. Set $b = y^2 - x^3 - ax \mod N$
3. Compute $D = \gcd(4a^3 + 27b^2, N)$

[1] We will assume that $\gcd(N, 6) = 1$ and N is not a perfect power

    (a) If $1 < D < N$, return.
    (b) If $D = 1$, proceed to step 4.
    (c) If $D = N$, go back to step 1 and choose another a value.

4. Let E be an elliptic curve $y^2 = x^3 + ax + b$ so that let $P \coloneqq (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$
5. Pick a number k which is a product of 'small' primes each raised to a small power — for instance set $k = \mathrm{lcm}(2, 3, \dots, B)$ for an integer B for $B \leq 100$
6. Compute $kP \mod n$
7. If kP is on E, go to step 1 and choose different a, x and y values, otherwise kP is a factor of N

We note that steps 1 and 2 will produce coefficients for an elliptic curve E that we know P will lie on.

Example 1. *We look at the case where $N = 493$. Suppose that E is $y^2 = x^3 + x + 1$, $P = (0, 1)$. Now we are looking to compute $k!P$ for $k = 2, 3, \dots,$ as far as we can, or up to some bound B. In the computation of these $k!P$, we will make use of the Fast Powering Algorithm as well as the algorithm we outlined for computing $P + Q$.*

We have:

$$\begin{aligned} 2!(0,1) &= (370, 307) \\ 3!(0,1) &= 3(2!(0,1)) \\ &= 3(370, 307) \\ &= (316, 29) \\ 4!(0,1) &= 4(3!(0,1)) \\ &= 4(316, 29) \end{aligned}$$

Now we are looking to find the point $4(316, 29)$, using the Fast Powering Algorithm, we begin by finding $2(316, 29)$, this requires us to calculate the slope:

$$\lambda = \frac{3(316)^2 + 1}{2(29)} = \frac{318}{58}$$

Next, we need to compute the multiplicative inverse of 58 modulo 493. We can attempt to do this using the extended euclidean algorithm; however, when we proceed we find that the algorithm fails. Thus, 58 and 493 must have a common divisor. We find this to be $(58, 493) = 29$ and then a division yields 17 as the other factor.

Let us look at a slightly more sophisticated example.

Example 2. *Consider $N = 455839$ and let E be given by $y^2 = x^3 + 5x - 5$, take our point to be $P = (1, 1)$ and let $k = 10!$.*

We have:

$$\begin{aligned} 2!P &= 2P \mod N \\ x(2P) &= \frac{56}{4} = 14 \\ y(2P) &= \frac{3+5}{2} \cdot (1 - 14) - 1 = -53 \\ \Rightarrow 2P &= (14, -53) \end{aligned}$$

Since the pair $(14, -53)$ consists of integers, we do not need to look for any inverses. We proceed by computing $3!P = 2P + 4P \mod N$.

$$\begin{aligned} x(4P) &\equiv \frac{37041}{11236} \mod N \\ &\equiv 37041 \cdot 271694 \mod N \\ &\equiv 259851 \mod N \\ y(4P) &\equiv \frac{593}{-106} \cdot (-259837) + 53 \mod N \\ &\equiv 116255 \mod N \\ \Rightarrow 4P &= (259851, 116255) \mod N \end{aligned}$$

Now we need to compute

$$\begin{aligned} \lambda &\equiv \frac{116255 + 53}{259851 - 14} \mod N \\ &\equiv 206097 \mod N \end{aligned}$$

Plugging this in to $x(6P) \equiv \lambda^2 - 14 - 259851 \mod N$ and $y(6P) \equiv \lambda x(6P) + y(2P) - \lambda x(2P) \mod N$, we find that

$$\begin{aligned} x(6P) &\equiv 179685 \mod N \\ y(6P) &\equiv 28708 \mod N \\ \Rightarrow 6P &= (179685, 28708) \mod N \end{aligned}$$

We can continue in this manner, finding that $4!P, 5!P, \ldots, 7!P$ are on E. When we reach $8!P$, we need to invert $599 \mod N$; however, this is not possible. So we have found a factor, namely 599 of N, from which we can deduce that $N = 599 \cdot 761$.

3 Why ECM works

At the start, when we defined elliptic curves, we defined them over a field K; however, in the ECM algorithm that we just outlined, we considered a curve that was defined over a ring $\mathbb{Z}/N\mathbb{Z}$ (with N being the integer we were looking to factor). Speaking loosely, we can say that for almost any element we pick in $\mathbb{Z}/N\mathbb{Z}$ this element will have a multiplicative inverse, so in a sense we could say that $\mathbb{Z}/N\mathbb{Z}$ is 'almost' a field. The elements which will fail to have a multiplicative inverse are precisely those y for which $\gcd(y, N) > 1$, in other words the zero divisors of $\mathbb{Z}/N\mathbb{Z}$. What Lenstra's ECM algorithm does is attempt to find these zero divisors by systematically adding rational points to the curve, until the addition of some point fails whereupon the zero divisor is produced.

When ECM is performed, in particular, in the process of computing $kP \mod N$, the denominators d involved are required to have a multiplicative inverse modulo N, which is the case exactly when $\gcd(d, N) = 1$ (otherwise $dN/\gcd(N, d) \equiv 0 \mod N$). So, as long as the gcd of d and N remains 1, we can continue to find $kP \mod N$. As soon as this gcd is larger than 1, we have found a divisor of N which is what we were looking for.

For a more in-depth analysis of when ECM will be most effective (as in the second example), we will need the following theorem due to Hasse.

Theorem 1. *(Hasse) Let E be an elliptic curve over a finite field $\mathbb{F}_p$ for some prime p, then*

$$p + 1 - 2\sqrt{p} < |E(\mathbb{F}_p)| < p + 1 + 2\sqrt{p}$$

Proof. In order to prove this theorem, we will require the following lemma (the proof of which we will admit).

Lemma 1. *Let ϕ and ψ be endomorphisms of an elliptic curve E. Then we have the below bound*

$$|\deg(\phi - \psi) - \deg(\phi) - \deg(\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}$$

Returning to the proof of the theorem in question, we will make use of the Frobenius endomorphism on E in $\mathbb{F}_p$ (p prime). That is the map

$$\phi : (x, y) \mapsto (x^p, y^p)$$

Fermat's little theorem gaurantees that $x^p \equiv x \mod p$, from which it follows that ϕ must fix E pointwise: $\phi(P) = P$. Thus, $\phi(P) - P = 0$ so $(\phi - 1)(P) = 0$, and we see that P must lie in the kernel $\ker(\phi - 1)$. This tells us that E is isomorphic to kernel of $\phi - 1$, and consequently we find that

$$|E(\mathbb{F}_p)| = |\ker(\phi - 1)| = \deg(\phi - 1)$$

Using the above cited lemma, we have

$$|\deg(\phi - 1) - \deg(\phi) - \deg(1)| \leq 2\sqrt{\deg(\phi)\deg(1)}$$

and we know that $\deg(\phi - 1) = |E(\mathbb{F}_p)|, \deg(\phi) = p$ and $\deg 1 = 1$.
All said, we see that $p + 1 - 2\sqrt{p} < |E(\mathbb{F}_p)| < p + 1 + 2\sqrt{p}$.

□

The intuition of the above proof is that E has many points in $\overline{\mathbb{F}_p}$ not all of which are in $\mathbb{F}_p$. But, if we have a point $\overline{\mathbb{F}_p}$, then this is in fact a point of $\mathbb{F}_p$ precisely when it is fixed by the p^{th} power map. Indeed this is the case since the p solutions to $x^P = x$ in $\overline{\mathbb{F}_p}$ are cannonically identified with $\mathbb{F}_p$. Thus counting the solutions of $\phi(P) = P$ is the same as finding the number of points of $E \mod p$

For Lenstra's ECM we want $|E(\mathbb{F}_p)|$ to be smooth (a product of small primes), where p is the smallest prime factor of N. Hasse's Theorem tells us that we have some flexibility — picking different curves E_1 and E_2 will produce different results for the size $|E(\mathbb{F}_p)|$, but they will be within the bounds specified.

In Example 2, $N = 455839$ was found to factor as $599 \cdot 761$ where E was chosen to be $y^2 = x^3 + 5x - 5$. An observation worth noting is that $|E(\mathbb{F}_{599})| = 640 = 2^7 \cdot 5$ happens to be 5-smooth, on the other hand $|E(\mathbb{F}_{761})| = 777 = 3 \cdot 7 \cdot 37$ is not 5-smooth.

In general, if we have prime factors p and q of N, then a point on a curve $y^2 = x^3 + ax + b \mod N$ will lie on both $E \mod p$ and $E \mod q$. As p and q are prime, $E(\mathbb{Z}/p\mathbb{Z})$ as well as $E(\mathbb{Z}/q\mathbb{Z})$ will form additive groups ($\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ being fields). Then, as mentioned, we know from Hasse's Theorem that our choice of curve E will result in different sizes of $|E(\mathbb{F}_p)|$ and $|E(\mathbb{F}_q)|$.

If we find a curve E such that $|E(\mathbb{F}_p)|$ is p'-smooth and $|E(\mathbb{F}_q)|$ is not p'-smooth, and only $|E(\mathbb{F}_p)|$ divides the chosen k value in step 5 of the algorithm, then Lenstra's ECM algorithm will yield a factor p of N. Upon finding such a curve, $kP \equiv O \mod p$, this is due to P being an integer point so a torsion point by say Mordell's Theorem, and since the order of $P \mod p$ divides $|E(\mathbb{F}_p)|$. Thus, $kP = s|E(\mathbb{F}_p)|P \equiv O \mod p$ for some integer s. On the other hand, $kP \not\equiv O \mod q$ because $|E(\mathbb{F}_q)|$ does not divide k. This all happens "behind the scenes" so to speak since we compute $kP \mod N$.

Returning again to our example, we see that $|E(\mathbb{Z}/599\mathbb{Z})| = 640$ divides $k = 8!$; whereas $|E(\mathbb{Z}/761\mathbb{Z})| = 777$ does not. Consequently $8!P \equiv O \mod 599$; however, $8!P \not\equiv O \mod 761$. This was captured when we tried to compute $8!P \not\equiv \mod N$ and could not find the multiplicative inverse.

It would be ideal if we could pick E so that only the order of $E(\mathbb{Z}/p\mathbb{Z})$ is smooth from the outset. Fortunately, even if we pick a curve at random, the order of the groups $E(\mathbb{Z}/p\mathbb{Z})$ and $E(\mathbb{Z}/q\mathbb{Z})$ will fall within the bounds specified by Hasse's Theorem. So as in our running example,

$$|E(\mathbb{F}_{599})| \in [551, 649], \ \ |E(\mathbb{F}_{761})| \in [707, 817]$$

Of course this is a sort of post hoc analysis, but it gives us insight into why Lenstra's ECM is more powerful than some of the analogous algorithms, say for example Pollard's algorithm.

References

[Com18a] Wikimedia Commons. File:ecclines.svg — wikimedia commons, the free media repository. `https://commons.wikimedia.org/w/index.php?title=File:ECClines.svg&oldid=285404337`, 2018. [Online; accessed 14-December-2019].

[Com18b] Wikimedia Commons. File:ecclines.svg — wikimedia commons, the free media repository. `https://upload.wikimedia.org/wikipedia/commons/thumb/a/ae/ECClines-2.svg/1000px-ECClines-2.svg.png`, 2018. [Online; accessed 14-December-2019].

[Poo01] Bjorn Poonen. Elliptic curves. 2001.

[Ste09] William Stein. *Elementary Number Theory: Primes, Congruences, and Secrets*. Springer-Verlag New York, 2009.

[Swi08] J. Swierczewski. Connections between the riemann hypothesis and the sato-tate conjecture. `https://wstein.org/projects/swierczewski.pdf`, 2008. Theorem 2.2.

[Zel15] Lukas Zeller. Improving lenstra's elliptic curve method. 2015.