Lenstra Elliptic Curve Factorization

Thomas Browning

June 2016

Contents

1 Introduction

The paper by H.W. Lenstra ”Factorizing Integers with Elliptic Curves” [3] outlines a method for finding nontrivial factors of integers. Asymptotically it is only the third fastest integer factorization algorithm known (beaten by the Quadratic Sieve and the General Number Field Sieve). Despite this, it is the fastest integer factorization algorithm known whose running time depends on the size of the smallest prime factor. In particular, although Lenstra's method is slightly slower than the fastest algorithms on products of two similarly sized primes, it will run much quicker when the number in question (however large) has a small prime factor. It is for this reason that Lenstra's algorithm is still widely used today. In this paper I will outline the most basic form of the algorithm. For modern implementations and performance techniques, refer to [1].

Lenstra's algorithm is a vast improvement on a previously known integer factorization algorithm known as Pollard's $p-1$ method. In this paper, I will first cover the basic set theory, number theory, and group theory required to understand Pollard's $p-1$ method. Then will discuss fields and elliptic curves and discuss the details of Lenstra's method.

2 Number Theory and Set Theory

Before we begin our discussion of elementary group theory, there are a couple results from elementary set theory and number theory that we shall need. Readers familiar with equivalence relations, congruence classes of integers modulo n, divisibility, and the greatest common divisor may skip ahead to section 3. Equivalence relations are central to the definition of projective space and finite fields modulo p which are needed for understanding Lenstra's algorithm.

Definition 1. A binary relation $\sim$ on a set S is a subset of $S \times S$. When $(a, b) \in S$ we write $a \sim b$.

Definition 2. An equivalence relation $\sim$ on a set S is a binary relation that satisfies the following properties:
1) For all $a \in S$, $a \sim a$ ($\sim$ is reflexive).
2) For all $a, b \in S$ such that $a \sim b$, $b \sim a$ ($\sim$ is symmetric).
3) For all $a, b, c \in S$ such that $a \sim b$ and $b \sim c$, $a \sim c$ ($\sim$ is transitive).

Definition 3. For an equivalence relation $\sim$ on a set S, an equivalence class of $\sim$ is a subset $T \subseteq S$ that satisfies the following properties:
1) For all $a, b \in T$, $a \sim b$.
2) For all $a \in T$ and $b \in S - T$, $a \not\sim b$.

The main utility of an equivalence relation is that it provides a formal way to partition a set and to equate different subsets of the set. This is defined and proved formally below.

Definition 4. A partition P of a set S is a collection of subsets of S that satisfies the following properties:
1) For all $a \in S$, there exists a $T \in P$ such that $a \in T$.
2) For all $T, T' \in P$, $T \cap T' = \varnothing$.

Proposition 1. *For an equivalence relation $\sim$ on a set S, the set of equivalence classes of $\sim$ partition S.*

Proof. For any $a \in S$, consider the set $T = \{b \in S \colon a \sim b\}$. For any $b, c \in T$, since we have that $a \sim b$ and $a \sim c$, by symmetry and transitivity we have that $b \sim c$ which shows condition 1 of T being an equivalence class. For any $b \in T$ and $c \notin T$, suppose that $b \sim c$. Then since we also have that $a \sim b$, by transitivity we have that $a \sim c$ which contradicts the fact that $c \notin T$. Then our assumption that $b \sim c$ was incorrect and $b \not\sim c$ which shows condition 2 of T being an equivalence class. Thus T is an equivalence class which shows condition 1 of the set of equivalence classes of $\sim$ being a partition. Now let T, T' be distinct equivalence classes. If $T \cap T' \neq \varnothing$ then there exists some $a \in T, T'$. If $b \in T$ then by condition 1 of the definition of equivalence classes applied to T, $a \sim b$. Then by condition 2 of the definition of equivalence classes applied to $T\prime$, $b \in T'$. Since this argument holds for all $b \in T$, we have that $T \subseteq T'$ and similar reasoning shows that $T' \subseteq T$. Thus, $T = T'$ which contradicts our assumption that T, T' be distinct. Thus, our assumption that $T \cap T' \neq \varnothing$ was false and we have shown condition 2 of the set of equivalence classes of $\sim$ being a partition. □

The central relation in elementary number theory is one the equates integers which differ by an integer multiple of some number n. This relation is an equivalence relation.

Definition 5. For $a, b \in \mathbb{Z}$, we say that $a|b$ when there exists some $k \in \mathbb{Z}$ such that $ak = b$.

Definition 6. For $a, b, n \in \mathbb{Z}$, we say that $a \equiv b \pmod{n}$ when $n|b - a$.

Proposition 2. *The $\equiv \pmod{n}$ relation is an equivalence relation.*

Proof. Let $a, b, c \in \mathbb{Z}$. Note that since $n0 = a - a$, we have that $a \equiv a \pmod{n}$ which shows that the relation is reflexive. Note that if $a \equiv b \pmod{n}$ then $nk = a - b$. Then we also have that $n(-k) = b - a$ and $b \equiv a \pmod{n}$ which show that the relation is symmetric. Note that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $nk_1 = a - b$ and $nk_2 = c - b$. Then adding these equation gives that $n(k_1 + k_2) = c - a$ and $a \equiv b \pmod{n}$ which shows that the relation is transitive. □

The equivalence classes produced by the $\equiv \pmod{n}$ relation partition the integers into equivalence classes. What makes this partitioning of the integers special is that for all $a, b, n \in \mathbb{Z}$ the equivalence classes of $a + b$ and ab modulo n are both completely determined by the equivalence classes of a and b modulo n. In particular, this means that we can define addition and multiplication on the congruence classes themselves.

Definition 7. The set of equivalence classes of $\equiv \pmod{n}$ on $\mathbb{Z}$ are referred to as the congruence classes modulo n and are denoted by $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3. *For $a, b \in \mathbb{Z}$, the congruence classes of $a+b$ and ab modulo n are completely determined by the congruence classes of a and b modulo n.*

Proof. Write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ where $0 \leq r_1, r_2 \leq n - 1$. Note that r_1, r_2 are completely determined by the congruence classes of a and b modulo n. Then $a + b = (q_1 + q_2)n + (r_1 + r_2)$ and the congruence class of $a + b$ is completely determined by $r_1 + r_2$. Additionally, $ab = (q_1 q_2 n + q_1 r_2 + q_2 r_1)n + r_1 r_2$ and the congruence class of ab is completely determined by $r_1 r_2$. □

Definition 8. For $a, b \in \mathbb{Z}$, the greatest common divisor of a and b is the largest $k \in \mathbb{Z}$ such that $k|a$ and $k|b$ and is denoted by $k = (a, b)$.

Definition 9. For $a, b \in \mathbb{Z}$, we say that a and b are relatively prime when $(a, b) = 1$.

We will need the following facts later on (whose proof is left to the reader).

Proposition 4. *For $a, b, n \in \mathbb{Z}$ such that $n|a$ and $n|b$, we also have that $n|(a, b)$.*

Proposition 5. *For $a, n \in \mathbb{Z}$ such that $(a, n) = 1$, there exists an $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$ (this can be proved by Bezout's identity).*

3 Group theory and Pollard's $p-1$ method

Now that we have reviewed some elementary number theory and set theory, we can begin to define the algebraic structures that Lenstra's method relies on. The most basic algebraic structure that we need is a group which is a set with one binary operation (such as the integers with addition).

Definition 10. A group is a set G equipped with a binary operation $G \times G \to G$ which satisfies the following properties:

1) For all $a, b, c \in G$, $(ab)c = a(bc) = abc$ (associativity).

2) There exists an $e \in G$ such that for all $a \in G$, $ea = ae = e$ (existence of an identity element).

3) For all $a \in G$, there exists an $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$ (existence of inverses).

Note that the definition of a group does not require that elements commute. When all elements of a group do commute, the group is called abelian (named after Niels Abel).

Definition 11. A group G is an abelian group when $ab = ba$ for all $a, b \in G$.

The group properties can be strengthened significantly without much additional work. In particular, it can be easily shown that both the identity element and inverse elements are unique.

Proposition 6. *The identity element of a group is unique.*

Proof. Note that if e, e' are both identity elements then by property 2 the the definition of a group we have that $e = ee' = e'$. □

Proposition 7. *The inverse element for every element of a group is unique.*

Proof. Note that if if $b, c \in G$ are both inverses for $a \in G$ then by property 3 of the definition of a group we have that $b = be = bac = ec = c$. □

Repeated application of the group law is referred to as exponentiation and can be extended to negative exponents using inverse elements.

Definition 12. For a group G, an $a \in G$, and an $n \in \mathbb{Z}$, we define

$$a^n = \begin{cases} a \cdots a & n \geq 1 \\ e & n = 0 \\ a^{-1} \cdots n^{-1} & n \leq -1 \end{cases} .$$

This definition of exponentiation retains many of its familiar properties (the proofs of which are left to the reader).

Proposition 8. *For a group G, an $a \in G$, and $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.*

Finally, the inverse of a product of two elements can be computed from the inverses of the two individual elements.

Proposition 9. *For a group G and $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Note that $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. □

One of the main theorems in elementary group theory is Lagrange's theorem. Before we can state and prove it, we must define subgroups and the order of a group.

Definition 13. H is a subgroup of G when H, G are both groups and $H \subseteq G$.

Definition 14. The cardinality of a group G is referred to as the order of G and is denoted by $|G|$.

We are now ready to state and prove Lagrange's theorem which states if H is a subgroup of G then $|H|$ divides $|G|$. The proof consists of partitioning G into equivalence classes of size $|H|$.

Theorem 1 (Lagrange's Theorem)**.** *If H is a subgroup of G then $|H|$ divides $|G|$.*

Proof. Define the relation $a \sim b$ when $b = ah$ for some $h \in H$. I claim that this is an equivalence relation. Since $e \in H$ and $a = ae$, we have that $a \sim a$ which shows that the relation is reflexive. If $a \sim b$ then $b = ah$ for some $h \in H$. Since $h^{-1} \in H$ and $a = bh^{-1}$, we have that $b \sim a$ which shows that the relation is symmetric. If $a \sim b$ and $b \sim c$, then $b = ah$ and $c = bh'$ for some $h, h' \in H$. Since $hh' \in H$ and $c = ahh'$, we have that the relation is transitive. Thus, our relation is, in fact, an equivalence relation which partitions G into equivalence classes (also known as left cosets). Now suppose that a is a member of some equivalence class, S, and define the function from S to H, $\varphi(b) = b^{-1}a$. Also define the function $\varphi^{-1}(h) = ah^{-1}$. Note that

$$\varphi(\varphi^{-1}(h)) = \varphi(ah^{-1}) = (ah^{-1})^{-1}a = (ha^{-1})a = h(a^{-1}a) = he = h$$

and

$$\varphi^{-1}(\varphi(b)) = \varphi^{-1}(b^{-1}a) = a(b^{-1}a)^{-1} = a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Then since φ is a bijection between S and H which shows that $|S| = |H|$. Then G is partitioned into equivalence classes of size $|H|$ which shows that $|H|$ must divide $|G|$. □

Now that we have proved Lagrange's theorem, we can start applying it to specific groups.

Definition 15. For a group G and an element $a \in G$,

$$\langle a \rangle = \{\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots\}$$

is referred to as the subgroup generated by a.

The proof the $\langle a \rangle$ is a group is left the the reader.

Definition 16. The order of an element $a \in G$ is defined as either the smallest k such that $a^k = e$ or as $|\langle a \rangle|$.

The proof that these definitions agree is also left the the reader. Then applying Lagrange's theorem to $\langle a \rangle$ and G gives the following result,

Corollary 1. *If $a \in G$ has finite order, then $a^{|G|} = e$.*

Proof. Let $k = |\langle a \rangle|$ be the order of a. By Lagrange's theorem, k divides $|G|$ and $|G| = nk$ for some integer n. Then $a^{|G|} = a^{nk} = \left(a^k\right)^n = e^n = e$. □

Proposition 3 demonstrates that multiplication of congruence classes modulo n is well defined. Proposition 5 demonstrates that congruence classes modulo n that are relatively prime to n have inverses. Then we can define the group $(\mathbb{Z}/n\mathbb{Z})^\times$ consisting of the set of the congruence classes modulo n that are relatively prime to n.

Definition 17. The multiplicative of integers modulo n is defined as the subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of congruence classes that are relatively prime to n under multiplication modulo n. This group is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$.

Showing that $(\mathbb{Z}/n\mathbb{Z})^\times$ satisfies the group properties is left to the reader. Then applying Corollary 1 to $(\mathbb{Z}/p\mathbb{Z})^\times$ for any prime p gives us Fermat's little theorem.

Theorem 2 (Fermat's Little Theorem)**.** *For any prime p and integer a not divisible by p, $a^{p-1} \equiv 1 \ (mod\ p)$.*

Proof. Applying Corollary 1 to $(\mathbb{Z}/p\mathbb{Z})^\times$ gives that $a^{p-1} \equiv 1 \pmod{p}$. □

We are now in a position to describe Pollard's $p-1$ method [4] for integer factorization. Suppose that we wish to factor some integer N. We pick some a relatively prime to N and an integer k that is divisible by many small prime powers. For example, we could choose k to be least common multiple of $\{1, 2, \cdots, b\}$ for a suitable bound b. Then we compute $a^k \pmod{N}$ and hope that $(a^k - 1, N)$ will be a nontrivial factor of N. Note that since we are taking the gcd of $a^k - 1$ and N at the end, our computing $a^k \pmod{N}$ (as opposed to simply computing a^k) is unnecessary but is much faster. The reason for choosing k to be divisible by many small prime powers is that if $k = p_1 p_2 \cdots p_m$ then we can compute $a^k \pmod{N}$ by iteratively exponentiating a to the power p_j for each j (which is quick if p_j is small). Additionally, we can take the remainder modulo N after each exponentiation which keeps the numbers that we are working with small.

The algorithm is works best when N has a prime factor p such that $p-1$ is a product of small primes. In this case, $p-1|k$ and a does not divide p. If we write $k = (p-1)q$, then by Fermat's little theorem,

$$a^k \equiv a^{(p-1)q} \equiv \left(a^{p-1}\right)^q \equiv 1^q \equiv 1 \pmod{p}.$$

Then $p|a^k - 1$ and $p|N$. By Proposition 4, $p|(a^k - 1, N)$. Then $(a^k - 1, N)$ will be a factor of N. In order for $(a^k - 1, N)$ to be a nontrivial factor of N, it cannot be 1 or N itself. It is impossible for $(a^k - 1, N)$ to be 1 since it is divisible by p. In the case that $(a^k - 1, N) = N$, we have that $a^k - 1|N$ which is very unlikely and can be resolved by picking a different a.

4 Group factorization algorithms

Pollard's $p-1$ algorithm falls under into a larger class of group factorization algorithms with the group used in Pollard's $p-1$ algorithm is $(\mathbb{Z}/p\mathbb{Z})^\times$. In such an algorithm, roughly speaking, you wish to factor an integer N which has a prime factor p. You then take a group G_p dependant on p whose group operation can be computed efficiently without knowledge of p. For example, in the case of Pollard's $p-1$ algorithm, we could multiply elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ without knowing p. Then you take some element $a \in G_p$ (without knowing p), and an integer k divisible by many small prime powers. If $|G_p|$ is a product of small primes, then $|G|$ will divide k. If we write $k = |G_p|q$, by Corollary 1,

$$a^k = a^{|G_p|q} = \left(a^{|G_p|}\right)^q = e^q = e.$$

Then G_p should have the property that $a^k = e$ allows you to find an integer m such that $p|m$ (still without knowing p). Since we also have that $p|N$, by the property of the gcd, $p|(m, N)$. Then you hope that (m, N) is a nontrivial factor of N.

There are two main issues with this style of algorithm. Firstly, the group G_p that you choose needs to be very special in that you can apply the group operation efficiently without knowing p. Additionally, G_p must have that property that knowing that $a^k = e$ allows you to compute an integer m such that $p|m$. Finally, the algorithm will fail if $|G_p|$ (which is dependant on p) has a large prime factor. If $|G_p|$ has a large prime factor for all prime factors p of N then the entire algorithm will fail. For example, if $p-1$ has a large prime factor for all prime factors p of N then Pollard's $p-1$ algorithm will fail. In this case you would have to try a completely different factorization algorithm. For instance, you could then try Williams' $p+1$ algorithm [5] which will fail when $p+1$ has a large prime factor for all prime factors p of N. Once N gets large, however, it is quite probably that $p-1$ and $p+1$ always have large prime factors for all prime factors p of N. Thus, this type of specialized algorithm will not perform well as N gets large.

This is where elliptic curve groups come in. Elliptic curve groups have all of the special properties required for G_p. For Lenstra's elliptic curve method [3], you repeatedly run the group factorization algorithm on different random elliptic curve (modulo p) and each time you choose a new elliptic curve, you will get an elliptic curve group (modulo p) whose order is quite random. Then it is likely that after some point you will happen to choose an elliptic curve (modulo p) whose order has no large prime factors and in this case the algebraic group factorization algorithm will be successful. Essentially, the strength of the elliptic curve algorithm is that it provides a family of groups with a variety of orders rather than Pollard's $p-1$ method and William's $p+1$ method which each provide only one group with a fixed order (either $p-1$ or $p+1$).

5 Elliptic Curve Groups

In order to define elliptic curve groups, we must first outline the definition of an elliptic curve over a field.

Definition 18. A field is a set F equipped with two binary operations $F \times F \xrightarrow{+} F$ and $F \times F \xrightarrow{\times} F$ which satisfies the following properties:

1) F equipped with addition forms an abelian group F^+ whose identity is denoted by 0.
2) $F - \{0\}$ equipped with multiplication forms an abelian group.
3) For all $a, b, c \in F$, $(a + b)c = ac + bc$.

We will be defining our elliptic curves in the projective plane over K which essentially consists of K along with some points ”at infinity.”

Definition 19. The projective plane over a field K is denoted by $\mathbb{P}^2(K)$ and is defined as the set of equivalence classes of nonzero triples $(x, y, z) \in K^3$ where two triples (x, y, z) and (x', y', z') are equivalent when there exists a $c \in K - \{0\}$ such that $cx = x'$, $cy = y'$, $cz = z'$.

The proof that the stated relation is an equivalence relation is left to the reader. Note that all points of K can be expressed as $(x, y, 1)$ or as $(x, y, 0)$. The first set of points corresponds to the usual plane K^2 but the second set of points corresponds to points ”at infinity.” Informally, for $a, b \in K$, we would like to define $E_{a,b}(K)$ as the set of solutions to

$$H(x, y) = x^3 - y^2 + ax + b = 0$$

but we would like to include solutions in $\mathbb{P}^2(K)$ rather than just in K^2. Then we would like to extend $H(x, y)$ to a function $H(x, y, z)$ with the following properties:

Definition 20. For a field K and a curve $H(x, y) = 0$ over K^2, a homogenization of $H(x, y)$ of degree d is a curve $H(x, y, z)$ over $\mathbb{P}^2(K)$ with the following properties:

1) $H(cx, cy, cz) = c^d H(x, y, z)$ ($H(x, y, z) = 0$ is determined within each equivalence class)
2) $H(x, y, 1) = H(x, y)$ (the extension agrees with the original function on K^2).

Proposition 10. *For a field K and a curve $H(x, y) = \sum_i \sum_j a_{i,j} x^i y^j = 0$ over K^2 has a homogenization of degree d, $H(x, y, z) = \sum_i \sum_j a_{i,j} x^i y^j z^{d-i-j} = 0$.*

Proof. Note that

$$H(cx, cy, cz) = \sum_i \sum_j a_{i,j} (cx)^i (cy)^j (cz)^{d-i-j} = c^d \sum_i \sum_j a_{i,j} x^i y^j z^{d-i-j} = c^d H(x, y, z)$$

and

$$H(x, y, 1) = \sum_i \sum_j x^i y^j 1^{d-i-j} = \sum_i \sum_x^i y^j = H(x, y)$$

which demonstrate that $H(x, y, z)$ is a homogenization of $H(x, y)$ of degree d. □

We are now in a position to homogenize $H(x, y)$ and define $E_{a,b}(K)$.

Definition 21. For a field K and $a, b \in K$, let

$$H_{a,b}(x, y) = x^3 - y^2 + ax + b = 0$$

and let the set of points of the elliptic curve, $E_{a,b}$, be given by

$$E_{a,b}(K) = \{(x, y, z) \in \mathbb{P}^2 \colon H_{a,b}(x, y, z) = x^3 - y^2 z + axz^2 + bz^3 = 0\}.$$

Note that the only point in $E_{a,b}(K)$ with $z = 0$ is the point $(0, 1, 0)$ which is denoted by O. Then all other points of $E_{a,b}(K)$ are in the form $(x, y, 1)$ and $E_{a,b}(K)$ consists of the set of solutions to $H(x, y) = 0$ in K^2 along with one point "at infinity."

The definition of group law on $E_{a,b}$ requires that any line in K^2 intersects $E_{a,b}$ at exactly 3 points. This can be intuitively seen from the fact that the elliptic curve is of degree 3 but a rigorous proof of this requires that we work in projective space and count intersections with multiplicity. This is an immediate consequence of Bezout's theorem from algebraically geometry which is beyond the scope of this paper but essentially states that curves of degree d_1 and d_2 will intersect $d_1 d_2$ times. We are now ready to define the group law geometrically. Note that due to convention, we will denote the group operation by $+$ and inverse elements by $-$. Given points $P, Q \in E_{a,b}(K)$, consider the unique line L_1 through P and Q. If $P = Q$ then we let L_1 be the unique tangent line which is only well defined when $4a^3 + 27b^2 \neq 0$ (it ensures that no equivalent of cusps or self-intersections exist). Thus, in what follows we shall assume that $4a^3 + 27b^2 \neq 0$. Then let R be the third intersection point of L_1 and let L_2 be the unique line through R and O. Finally, let $P + Q$ be the unique intersection point of L_2 and $E_{a,b}(K)$.

Proposition 11. *For a field K and $a, b \in K$, O is the identity of the group on $E_{a,b}(K)$.*

Proof. Consider the case where $Q = O$ (the case where $P = O$ is analogous). In this case L_1 passes through P, O, R and L_2 passes through $R, O, P + O$. Then since lines through two points are unique, $P + O = P$. □

Proposition 12. *For a field K and $a, b \in K$, The group on $E_{a,b}(K)$ has inverse elements.*

Proof. Let O' let the third intersection point of the tangent line to O. Then for a point $P \in E_{a,b}(K)$, let $-P$ be the third intersection point of the line through O' and P. Then if we consider $P - P$, L_1 passes through $P, -P, O'$ and L_2 passes through $O', O, P - P$. Then since lines through two points are unique, $P - P = O$. □

The proof of associativity is quite involved and shall not be presented here. Thus, we have that our group on $E_{a,b}(K)$ is actually a group. The group law can also be described algebraically as in [2] as follows. First, let O be the identity element (so that $O + P = P + O = O$ for all $P \in E_{a,b}(K)$). Given nonzero $P, Q \in E_{a,b}(K)$, we can write $P = (x_1, y_1, 1)$ and $Q = (x_2, y_2, 1)$ but in what follows we will drop the 1 (and work in K^2 rather than $\mathbb{P}^2(K)$) for the sake of brevity brevity. Then we let $P + Q = O$ if and only if $x_1 = x_2$ and $y_1 = -y_2$. Otherwise we let λ be the slope of L_1 which is the line through $P = (x_1, y_1)$ and

$Q = (x_2, y_2)$. It turns out that $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$ and $\lambda = (3x_1^2 + a)/(2y_1)$ if $P = Q$. Then L_1 be the line defined by $y = \lambda(x - x_1) + y_1$. It turns out that the only other solution to $E_{a,b}$ on L_1 is the point

$$R = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_3 - x_1) + y_1).$$

Then since L_2 passes through O and $R = (x_3, y_3)$, L_2 is the vertical line through $R = (x_3, y_3)$ and $P + Q$. Since the definition of $E_{a,b}(K)$ is symmetric in y (the only occurrence of y is a y^2 term), the other solution ot $E_{a,b}$ on L_2 is

$$P + Q = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, -\lambda(x_3 - x_1) - y_1) = (\lambda^2 - x_1 - x_2, \lambda(2x_1 + x_2 - \lambda^2) - y_1).$$

The full details of why these two definitions of the group law agree is left to the reader.

6 Elliptic Curve Groups over $\mathbb{F}_p$

Lenstra's Algorithm involves elliptic curves defined over the field $\mathbb{Z}/p\mathbb{Z}$.

Definition 22. For a prime p, the field of congruence classes modulo p $\mathbb{Z}/p\mathbb{Z}$ forms a field under addition and multiplication. This field is denoted by $\mathbb{F}_p$.

Now for a positive integer n, even if n is not prime and $\mathbb{Z}/n\mathbb{Z}$ is not a field, we can still discuss $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ provided that we remember that multiplication is not invertible. Then let $O = (0, 1, 0)$ and let V_n be the set of finite points of $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ along with O.

Definition 23. We define the subset $V_n \subset \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ by

$$V_n = \{(x, y, 1) \colon x, y \in (\mathbb{Z}/n\mathbb{Z})\} \cup \{O\}.$$

Definition 24. For a point $P \in V_n$ and a prime $p|n$, let $P_p \in \mathbb{P}^2(\mathbb{F}_p)$ be the point obtained by reducing the coordinates of P modulo p.

Lenstra's algorithm requires being able to perform a type of "pseudo-addition" on any two points of $P, Q \in V_n$ so that $P_p + Q_p = (P + Q)_p$ in the elliptic curve group $E(\mathbb{F}_p)$ for all primes $p|n$. The precise statement of this is that given $P, Q \in V_n$, $a \in \mathbb{Z}/n\mathbb{Z}$ we wish to either find a nontrivial divisor of n or to find a $P + Q \in V_n$ such that for any $p|n$ and for any $b \in \mathbb{F}_p$ such that $E_{a,b}(\mathbb{F}_p)$ is an elliptic curve group that contains P_p and Q_p, then $(P + Q)_p = P_p + Q_p$. We will now outline the algorithm for computing $P + Q$ but notice the extreme similarity between this algorithm and the for computing valid addition in $E_{a,b}(K)$. First we compute $d_1 = (x_1 - x_2, n)$ or $d_2(y_1 + y_2, n)$ efficiently using the Euclidean algorithm. First note that if either d_1 or d_2 are not 1 or n then we have found a nontrivial divisor of n and can stop. In the case that $d_1 = d_2 = n$ then $x_1 = x_2$ and $y_1 = -y_2$ and we let $P + Q = O$. If $d_1 = 1$ then $x_2 - x_1 \in (\mathbb{Z}/n\mathbb{Z})^\times$ and is invertible. Then we can let $\lambda = (y_2 - y_1)/(x_2 - x_1)$. Otherwise $d_1 = n$ and $d_2 = 1$. Then $y_1 + y_2 \in (\mathbb{Z}/n\mathbb{Z})^\times$ and is invertible. Then we can let $\lambda = (3x_1^2 + a)/(y_1 + y_2)$. Then, similar to addition in $E_{a,b}(K)$, let

$$P + Q = (\lambda^2 - x_1 - x_2, \lambda(2x_1 + x_2 - \lambda^2) - y_1, 1).$$

It is straightforward and left to the reader to show that if this procedure is successful, then for all elliptic curve groups $E_{a,b}(\mathbb{F}_p)$ where $p|n$ and $b \in \mathbb{F}_p$, we have that $P_p + Q_p = (P + Q)_p$ in $E_{a,b}(\mathbb{F}_p)$.

Now that we have defined addition on V_n, for integers $k > 0$, we can define multiplication as $kP = P + \cdots + P$ so that $(kP)_p = kP_p$ in the elliptic curve group $E(\mathbb{F}_p)$ for all primes $p|n$. Remember that it's possible (and desirable) that our multiple procedure could break down and instead give us a non-trivial factor of n. Then we can proceed as in Pollard's $p-1$ algorithm by choosing some k that is divisible by many small prime powers. Then we compute kP by repeatedly multiplying P by each factor of k. It turns out that $kP \neq O$. Now suppose that the order of $E_{a,b}(\mathbb{F}_p)$ is divisible by k for some prime $p|n$. If the algorithm is successful then by Corollary 1, $kP = O$ which is a contradiction. Thus, in this case, the algorithm must break down and find a nontrivial factor of n.

When running this algorithm, many different elliptic curves are used and the initial value of P is chosen arbitrarily for each curve. If for any elliptic curve and any $p|n$, the order of $E_{a,b}(\mathbb{F}_p)$ is a product of small primes, then the order of $E_{a,b}(\mathbb{F}_p)$ is divisible by k and we will find a nontrivial factor of n. Hasse's theorem on elliptic curves states that for an elliptic curve $E_{a,b}(\mathbb{F}_p)$,

$$|E_{a,b}(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

Thus, the order of $E_{a,b}(\mathbb{F}_p)$ varies between $p+1-2\sqrt{p}$ and $p+1-2\sqrt{p}$ which is known as the Hasse interval. In fact, the order of $E_{a,b}(\mathbb{F}_p)$ for various curves is known to vary randomly. Thus, it is quite likely that eventually the chosen curve will happen to have an order which is the product of small primes.

References

[1] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. *ECM using Edwards curves.* 2008.

[2] R. P. Brent. *Some Integer Factorization Algorithms using Elliptic Curves.* Australian Computer Science Communications 8 (1986), 149-163.

[3] H. W. Lenstra, Jr. *Factoring integers with elliptic curves.* Ann. Math. 126 (1987), 649-673.

[4] J. M. Pollard. *Theorems in factorization and primality testing*, Proc. *Cambridge Philos. Soc.* 76 (1974), 521–528.

[5] H. C. Williams. *A p+1 method of factoring.* Math. Comp. 39 (1982), 225-234.