Utrecht University

Faculty of Science

Integer Factorization using Elliptic Curves

Bachelor Thesis

Jun Jie Lin

Mathematics

Supervisor:

Dr. S. (Stefano) Marseglia Supervisor
Mathematical Institute, Utrecht University

June 16, 2021

Abstract

The aim of this thesis is to present the elliptic curve factorization algorithm invented in 1987 by H.W. Lenstra, Jr. and published, [1]. Some context regarding integer factorization algorithms and an introduction to the addition of points on elliptic curves will be provided. In particular, an overview of Pollard's $p-1$ algorithm is outlined, considering Lenstra's algorithm is obtained from this method by replacing the multiplicative group of the integers modulo a prime p by the group of points on a random elliptic curve. Let N be a composite integer and p its smallest prime divisor. It is conjectured that the expected time in which Lenstra's algorithm finds a non-trivial divisor of N is at most of order $(\log N)^2 e^{\sqrt{(2+o(1))\log p \log\log p}}$. In the worst case, this leads to a running time of $e^{(1+o(1))\sqrt{\log N \log\log N}}$ for $n \to \infty$, which is slower than the General Number Field Sieve. However, Lenstra's algorithm is the fastest algorithm that relies on the smallest prime divisor of a given composite integer and can be significantly faster if the number in question has a small prime factor.

Contents

1 Introduction

The main topic of this thesis is the algorithm invented in 1987 by H.W. Lenstra, Jr. which determines a non-trivial divisor of a given composite integer N, see [1]. In this thesis, the basic form of this algorithm is outlined, as it was presented by Lenstra. For modern adaptations, see [2]. Integer factorization is of great importance in some cryptosystems. One such cryptosystem is RSA which relies on the difficulty of finding the prime factors of $N = pq$, where p and q are large primes. It was published in 1978 by Rivest, Shamir and Adleman, refer to [3]. As of yet, there is no efficient algorithm for factoring the product of two considerably large prime numbers on a regular computer. Lenstra's algorithm is currently considered the third fastest algorithm in that regard. However, Lenstra's algorithm is substantially faster than the fastest two algorithms when the integer to be factored has a small prime divisor. The second fastest algorithm is the Quadratic Sieve, which was invented before Lenstra's algorithm, in 1981 by Pomerance, refer to [4]. In terms of expected running time, it is of the same order as the running time of Lenstra's algorithm in the worst case. On the other hand, the algorithm that is currently considered the fastest algorithm is the General Number Field Sieve, which was proposed in 1988 by Pollard, as a successor to the Quadratic sieve and later developed in 1993, refer to [5] for both statements.

In the first part of this thesis, we provide some general context regarding integer factorization algorithms. A distinction is made between two sorts of integer factorization algorithms and it is clarified why integer factorization is such a difficult problem by giving an introduction to order notation. Furthermore, some factorization algorithms are mentioned and their efficiency will be mentioned. In particular, we give an overview of Pollard's $p - 1$ algorithm, which was invented in 1974, see [6]. Lenstra's algorithm is an improvement on Pollard's $p - 1$ algorithm in the sense that it uses the same idea, but replaces the multiplicative group of integers by the group of points on an elliptic curve.

In the second part, a basic introduction to elliptic curves over fields is given. In particular, the Weierstrass equations are mentioned, which represent elliptic curves. We work mostly with coordinates on the affine plane for ease of use. It is explained how the rational points on an elliptic curve over a field naturally form a group by taking the line through two points and mirroring the unique third intersection point around the x-axis. Lastly, some useful properties of elliptic curves over finite fields are outlined. Notably, we discuss the possible values of the order of an elliptic curve over a finite field and groups that are isomorphic to the set of points on a given elliptic curve.

In the third part, we discuss Lenstra's algorithm. We use Lenstra's notes to determine the running time of the algorithm. We explain how the algorithm works and why it can find a non-trivial divisor of a given composite integer. Furthermore, we give some boundary conditions for the algorithm to find a non-trivial divisor successfully. Afterwards, we determine the number of different elliptic curves over a finite field up to isomorphism weighted by their automorphism group. In particular, we use the Kronecker class numbers and modular curves to determine the weighted number of elliptic curves with an order that is either divisible by a given prime l or not divisible by l. Using these results, the probability of success of the algorithm is determined which then leads to the efficiency. The thesis ends with a short comparison with the General Number Field Sieve.

2 Integer Factorization

The aim of this chapter is to give context to why integer factorization is considered a difficult problem, in particular the factorization of the numbers used in the RSA cryptosystem which are composite numbers of two very large primes. To ensure security RSA uses the difficulty of factoring an integer consisting of two large primes. While not every composite number is as difficult to factor, there are some composites that are both perceived as difficult to factor and comparatively easily generated. This is the underlying idea behind the RSA cryptosystem. Furthermore, we will discuss a common algorithm used to factor these composite integers.

2.1 Unique factorization

Firstly, recall the fundamental theorem of arithmetic. It ensures that if N is an integer such that $N = pq$ for prime numbers p and q, there is no other (non-trivial) divisor of N.

Proposition 2.1.1 (Fundamental theorem of arithmetic)**.** *Every integer greater than* 1 *can be represented as a product of prime integers. Moreover, this representation is unique up to ordering.*

Proof. The proof for existence uses the well-ordering principle. It states that if A is a nonempty set of positive integers, then A contains a smallest number, see [7, Section 1]. Suppose there are integers greater than 1 which cannot be expressed as a product of prime integers. Denote A as the set of such integers. Then A is a nonempty set of positive integers by assumption. By the well-ordering principle, there is a smallest integer $a \in A$. Since a does not have a representation of as a product of prime integers, a cannot be prime itself. Considering $a \geq 2$ and not prime, it must be a composite integer. Hence, write $a = bc$ for some integers $2 \leq b, c < a$. As a is the smallest integer in A, we know b and c must have prime representations $p_1 p_2 \dots p_k$ and respectively $q_1 q_2 \dots q_\ell$ for some prime integers $p_1, \dots, p_k$ and $q_1, \dots q_k$. Then, since $a = bc$, we get $a = p_1 p_2 \dots p_k q_1 q_2 \dots q_\ell$, which contradicts the assumption that a does not have a prime representation. Therefore, A must be empty and the existence must hold for every integer ≥ 2.

The proof for uniqueness uses Euclid's Lemma. It states that when a prime integer p divides the product of two integers a and b, then p divides a or p divides b, see [7, Section 1]. We will use the notation $p \mid a$ for p divides a. Let n be an integer with $n \geq 2$. Suppose n has representations

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$
$$n = q_1^{f_1} q_2^{f_2} \dots q_\ell^{f_\ell}$$

where $p_1, \dots, p_k, q_1 \dots, q_\ell$ are prime numbers with $p_i \neq p_j$ for $i \neq j$ and $q_i \neq q_j$ for $i \neq j$ and $e_1, \dots e_k, f_1, \dots f_\ell$ are integers. Assume without loss of generality that $k \geq \ell$. As $p_1 \mid n$, we must have $p_1 \mid q_1^{f_1} q_2^{f_2} \dots q_\ell^{f_\ell}$. As all q_i's are primes and distinct, we must have a unique i such that $p_1 = q_i$ with $1 \leq i \leq \ell$. Repeating this process for all p_j with $j = 1, 2, \dots, k$ gives us $k = \ell$ as otherwise it would lead to a contradiction with $p_i \neq p_j$ for $i \neq j$. Now rearrange the primes of one of the representations such that $p_i = q_i$ for all $i = 1, 2, \dots, k$. Suppose there is an $i \in \{1, 2, \dots, k\}$ such that $e_i \neq f_i$. Without loss of generality, assume that $e_i > f_i$. Considering $p_1^{e_1} \dots p_i^{e_i} \dots p_k^{e_k} = p_1^{f_1} \dots p_i^{f_i} \dots p_k^{f_k}$ we can divide by $p_i^{f_i}$, which gives $p_1^{e_1} \dots p_{i-1}^{e_{i-1}} p_i^{e_i - f_i} p_{i+1}^{e_{i+1}} \dots p_k^{e_k} = p_1^{f_1} \dots p_{i-1}^{f_{i-1}} p_{i+1}^{f_{i+1}} \dots p_k^{f_k}$. Using Euclid's lemma, we get that $p_i \mid p_1^{f_1} \dots p_{i-1}^{f_{i-1}} p_{i+1}^{f_{i+1}} \dots p_k^{f_k}$. However, this contradicts with the assumption that all primes are distinct. Thus, we must have $e_i = f_i$. Therefore, the conclusion is that the representation is unique up to ordering. □

A natural question that arises is how we can find the prime factorization of a given integer. Two types of methods are often distinguished when it comes to integer factoring: general purpose and special purpose methods, as described in [8].

Definition 2.1.2 (Factorization methods)**.** A factorization method is called a "general purpose method" if its running time is only dependent on the length of the input, i.e. the size of the composite number N. In contrast, if it relies on certain properties of N, such as one of its factors, it is considered a "special purpose method".

One general purpose method we will later mention is the General Number Field Sieve, which is considered the fastest algorithm for integer factorization for factoring composite numbers N of the form $N = pq$ with p and q being large primes. An example of a special purpose method, and perhaps one of the most naive, is trial division which relies on the smallest prime divisor of N. The main topic of this work, Lenstra's algorithm for factoring integers using elliptic curves is another special purpose method and also relies on the smallest prime factor of N. On average, special purpose methods can be very effective. There are many special purpose methods that depend on the smallest prime factor and there is a high probability that a random integer will have at least one small prime factor. However, in the particular case of RSA composites, special purpose methods are less efficient and therefore not as relevant as the general purpose methods. Later on in Section 2.3, we will discuss one special purpose method and how one can choose integers so that this specific algorithm is very inefficient in finding its factors.

2.2 Difficulty of integer factorization

To describe the difficulty of integer factorization, we will begin by giving an introduction to the *big-$\mathcal{O}$* in a similar way it is done in [9, Section 2.6]. It is commonly used to describe the running time of algorithms in terms of the size of the input.

Definition 2.2.1 (Order notation)**.** Let f and g be two real positive valued functions. We say that f is "big-$\mathcal{O}$ of g" and denote it by

$$f(x) = \mathcal{O}(g(x))$$

if there exists real positive constants c and C such that for all $x \geq c$ it holds that

$$f(x) \leq Cg(x).$$

One useful tool to prove $f(x) = \mathcal{O}(g(x))$ is by looking at the limit of $\frac{f(x)}{g(x)}$ as x approaches infinity. The proof of it mostly uses ideas that are not very relevant to this work, but is fairly straightforward. Hence, we will omit the details.

Proposition 2.2.2. *If the limit*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)}$$

exists and is finite, then $f(x) = \mathcal{O}(g(x))$

We will highlight three orders of functions ranging from what is considered a fast algorithm and what is considered a slow algorithm. Usually, we consider a (mathematical) problem "easy" if it can be solved in polynomial time, a generally faster algorithm. It is considered "hard" if it requires exponential time, a generally slower algorithm. The third order we will highlight is sub-exponential, which lies somewhere in between these two and a problem that requires sub-exponential time is considered "quite hard". The following definition makes these descriptions more precise.

Definition 2.2.3. If the size of the input of an algorithm is k digits, then we say that the running time of this algorithm is called the following.

- It is "polynomial", if there is a non-negative constant A such that the algorithm requires $\mathcal{O}(k^A)$ steps to solve the problem.
- It is "exponential", if there is a positive constant A such that the algorithm requires $\mathcal{O}(e^{kA})$ steps to solve the problem.
- It is "sub-exponential", if for every positive constant a the algorithm requires $\mathcal{O}(e^{ka})$ steps to solve the problem.

Remark 2.2.4. Note that while we gave difficulty expressions for problems, they are asymptotic descriptions and thus describe the case in which the size of the variables becomes very large, i.e. approaching infinity. Depending on the constants and the range of the inputs, it is possible that in practice a (sub-)exponential algorithm is faster than a polynomial one.

An example of a fast algorithm is the extended Euclidean algorithm which runs on polynomial time. It is often used to compute inverses modulo N and compute greatest common divisors, which we will be doing a lot later on. Therefore, we will describe the extended Euclidean algorithm briefly in case the reader does not know how it operates. Given two positive integers M, N it divides the greater number by the smaller number with remainder. If the remainder is nonzero, it divides the smaller integer by the remainder to produce another remainder. This process repeats itself until we get a remainder equal to zero. The last nonzero remainder is the greatest common divisor of the starting two integers. Then substituting every division with remainder onto the previous step gives an expression $aM + bN = \gcd(M, N)$ for some integers a, b. If $\gcd(M, N) = 1$, then a is the inverse of M modulo N and b is the inverse of N modulo M. For more details, we refer to [9, Section 1.2]

To understand the difficulty of integer factorization, let us discuss trial division in the general case as an example and see how it can be improved to be more efficient, as is outlined in [10, Section 6G].

Example 2.2.5. Given an integer N, we try to divide N by every integer $i = 2, 3, 4, \ldots$ until we either find a divisor or we get $i > \sqrt{N}$. This is due to the fact that if $N = ab$ for some integers a and b then at least one of them must be $\leq \sqrt{N}$. Therefore, this algorithm will always either give us the lowest prime divisor of N or no divisors at all, in which case N is prime itself. Thus, it is dependent on the size of the lowest prime factor p of N and is, as mentioned earlier, a special purpose algorithm. In particular, it requires at least $p - 1$ divisions, which is efficient if p is small relative to N, and at most $\sqrt{N}$. This implies that in the worst case, the required time grows exponentially with the digits in the number which is $\log(N)$, as it requires $\sqrt{N}$ divisions. Consequently, this algorithm is not well suited for dealing with considerably large primes, such as the RSA numbers. △

A possible improvement to the algorithm described in Example 2.2.5 to reduce a significant amount of divisions is to divide only by numbers up to a specific boundary. Even better would be to divide solely by prime numbers up to that boundary. This is due to how most numbers have some small prime divisor. For example, every even number is obviously divisible by 2 and every number that has a 5 or a 0 as the last digit is divisible by 5. Moreover, once we know N is not even, it is unnecessary to check whether it is divisible by another even number. Furthermore, after a certain boundary, it is likely more efficient to use different algorithms.

Definition 2.2.6 (Prime-counting function)**.** Let x be some real number. The number of prime integers smaller than or equal to x is denoted by $\pi(x)$.

For example, $\pi(6) = 3$, since the primes that are less than or equal than 6 are $2, 3, 5$. If we have a specific boundary B in mind, the improved trial division will at most require $\pi(B)$ divisions. However, this can still lead to an exponential running time due to the Prime Number Theorem proven by Hadamard and de la Vallée Poussin in 1896.

Proposition 2.2.7 (Prime Number Theorem)**.** *If $\pi(x)$ denotes the prime-counting function, then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

For the proof we refer to [7, Section 7]. Besides that, even though this improvement will lead to less divisions required, it does not take into consideration what is needed to determine all prime numbers that are less than or equal to B. We could perhaps store these prime numbers. However, that would require a lot of preparation and memory. Another possible solution would be to check whether each number (up to that boundary) is prime or not, so-called primality testing which we will mention in the next section. However, this will increase the running time.

2.3 Other factorization algorithms

There are many different factorization algorithms, both general purpose and special purpose. The fastest method for factoring numbers of the form $N = pq$ with p and q primes of approximately the same order of magnitude is is the General Number Field Sieve (GNFS). It uses monic integer polynomials $f(x) \in \mathbb{Z}[x]$ that are irreducible over $\mathbb{Q}$ and have a root m mod N, i.e. $f(m) \equiv 0 \bmod N$. The heuristic running time of GNFS is described as $L_N[1/3, c]$ with $c = (\frac{64}{9})^{\frac{1}{3}} \approx 1,923$, see [11]. Here, $L_N[t, c]$ is defined as

$$L_N[t, c] = e^{(c+o(1))(\log(N))^t(\log\log(N))^{1-t}}$$

with $o(1)$ being a function that goes to 0 as x approaches infinity. This "L-notation" is defined for $0 \leq t \leq 1$ and positive constants c. This notation is another way to express the complexity of algorithms for (quite) difficult problems mostly related to number theory. To relate back to Definition 2.2.3, the running time that $L_N[t, c]$ describes as follows.

1. It is polynomial if $t = 0$, since $e^{(c+o(1))\log\log N} = (\log N)^{c+o(1)}$.
2. It is exponential if $t = 1$, as $e^{(c+o(1))\log N} = N^{c+o(1)}$.
3. Furthermore, it is considered sub-exponential if $0 < t < 1$.

Recall that the running time is relative to the size of the input, which is $\log N$ in this case. See [12] for more details.

At the start of this section we stated that RSA uses numbers that are relatively easy to generate relative to the difficulty of factoring them. To do that, they need to find two very large primes. They can generate some large numbers and use primality testing to check whether they are prime or composite. These primality tests rely often on Fermat's Little Theorem.

Proposition 2.3.1 (Fermat's Little Theorem)**.** *Let p be a prime number. Then for any integer a it holds that*

$$a^p \equiv a \bmod p.$$

Proof. There are a lot of ways to prove this theorem. We want to highlight the first proof given in [9, Section 1.5] which uses group theory. A proof without group theory can also be found there. Recall that for a prime p, the units of $\mathbb{F}_p$, the field of integers modulo p, form a group under multiplication denoted by $\mathbb{F}_p^*$. Note that since p is prime, this means every element in $\mathbb{F}_p$ aside from 0 is a unit. This group is of order $p - 1$, as $\mathbb{F}_p$ has p elements. In the case of $a = 0$, we can clearly see that $0^p \equiv 0 \bmod p$. By Lagrange's theorem, the order of an element of a finite group divides the order of the group. We refer to [10, Section 11C] for the proof of Lagrange's theorem and its corollary. This means that every element $u \in \mathbb{F}_p^*$ has an order that divides $p - 1$ and thus $u^{p-1} \equiv 1 \bmod p$. Multiplying both sides by u gives the required equivalence. □

This means that if we want to test whether an integer N is a prime or not, we can check for $a \in \{2, 3, \dots, N-1\}$ first if a is coprime to N and after that whether $a^p \equiv a \bmod N$ holds. If it does not hold for a certain a, then we can conclude that N is not prime and therefore composite. However, unless we find a number that is not coprime to N, we will not get any information on the factors of N. Note that it is a lot more likely to find a number for which Fermat's Little Theorem does not hold than it is to find a number that is not coprime. Therefore, this idea leads to an algorithm that is often faster than the factoring algorithms. One thing to keep in mind is that some algorithms do not guarantee that the integer N is a prime number, but rely on the probability that "a witness" is found, i.e. a number for which the congruence does not hold, .

Example 2.3.2. We want to check whether 377 is prime or composite using Fermat's Little Theorem. We can quickly see that 3 does not divide 377 and is therefore coprime. We calculate $3^{377} \equiv 48 \bmod 377$. Thus, 377 cannot be a prime number, since $16 \not\equiv 3 \bmod 377$. △

Remark 2.3.3. While Fermat's Little Theorem gives a generally good way to check whether an integer is not prime, there are some composite numbers such as 561 which satisfy the condition for every integer. This example is due to the fact that $561 = 3 \cdot 11 \cdot 17$ and 560 is a multiple of 2, 10 and 16. The integers with this property are called the "Carmichael numbers". For more information on Carmichael numbers, we refer to [10, Section 10B and Section 20].

The last algorithm that we would like to discuss in this section is Pollard's $p-1$ algorithm. Lenstra's Elliptic Curve Factorization algorithm draws heavily inspiration from it. Pollard's algorithm is another special purpose method. This is due to the fact that it is effective when a prime factor p of N has the property that $p-1$ can be factored entirely into small prime factors.
Let N be an integer we want to factor and p an unknown prime factor of N. If we take an arbitrary integer $a \geq 2$, we know that either p divides a or a is coprime to p. In the first case, we have that p divides $\gcd(a, N)$. In the other case, which Pollard's algorithm focuses on, we know by Proposition 2.3.1 that $a^{p-1} \equiv 1 \bmod p$. Hence, for any integer k we have

$$a^{k(p-1)} = (a^{p-1})^k \equiv 1 \bmod p,$$

which means p divides $a^{k(p-1)} - 1$ and thus p divides $\gcd(a^{k(p-1)} - 1, N)$. The greatest common divisor can be found using a fast method such as the Euclidean algorithm which we mentioned earlier. One question that arises is how a multiple of $p-1$ can be obtained when p is unknown.
In Pollard's algorithm, a positive integer m that is divisible by many small primes up to a specified boundary B is used in the hope that it is a multiple of $p-1$. Depending on B, some possible choices for m include $B!$, $\operatorname{lcm}(1, 2, \ldots, B)$ or the product of each prime up to the boundary with appropriate power, such as what is used in [10, Section 10C]

$$\prod_{\substack{q \leq B \\ q \text{ prime}}} q^{\lfloor \log_q B \rfloor}.$$

When choosing the boundary B, it is more likely to succeed if B is large, as we would like every prime divisor of $p-1$ to be smaller than B. However, the running time increases as B increases. Once this m and base integer a are chosen, we calculate $a^m \bmod N$ and check the greatest common divisor d of $a^m - 1 \bmod N$ and N. It is also an option to check the gcd of N and $a^i - 1 \bmod N$ in each intermediate step of calculating $a^m \bmod N$.

Remark 2.3.4. Note that $\gcd(a^m - 1, N)$ is equal to the greatest common divisor of N and $a^m - 1 \bmod N$. It is more convenient to compute the greatest common divisor using $a^m - 1 \bmod N$ as it has less digits and therefore uses less memory. Raising a number to a high power modulo N can be done efficiently using the Fast Powering Algorithm. This algorithm writes the exponent in binary form, computes $a^{2k} = (a^k)^2$ recursively modulo N and multiplies the powers used in the binary form. For more details, see [9, section 1.3.2]. A thing to note is that this calculation is done in polynomial time.

There are three possible cases for $\gcd(a^m - 1, N) = d$.

1. If the gcd d is an integer such that $1 < d < N$, we have found the non-trivial divisor d of N. We can repeat the algorithm on the quotient (and possibly d if it is not prime) until we end up with the prime factorization of N.

2. If $d = 1$, it is clear that $a^m \not\equiv 1 \bmod p$ for every prime divisor p of N. Therefore, m is definitely not a multiple of $p-1$ for any of the p. It is likely that a prime factor of $p-1$ is greater than the boundary B. Thus, we increase B and perform the algorithm again.

3. In the rare case that $d = N$, we have $a^m \equiv 1 \bmod p$ for every prime divisor p of N. It is quite unlikely that $p-1$ and $q-1$ have the same small prime factors. Thus, we could try lowering B so that m becomes a multiple of $p-1$ but not of $q-1$. Another possibility is that m is a multiple of the order of a modulo q, but not actually a multiple of $q-1$. For example, the order of 5 modulo 31 is 3, so $5^{48} \equiv 1 \bmod 31$, but $30 \nmid 48$. Choosing a different value for a modulo N could solve this.

Example 2.3.5. We would like to factorize $N = 4087$. We choose $a = 2$ and $m = 12!$. Note that m includes every prime up to 11. We compute

$$2^{12!} \equiv 1 \bmod 4087.$$

Observe that this already implies that we get 4087 as the greatest common divisor. Therefore, we should try a lower bound or a different base a. We choose for a a lower bound. If we actually try $m = 7!$, so that it does not include the prime number 11, we get

$$2^{7!} \equiv 550 \bmod 4087.$$

Now we find, with Euclid's algorithm, that $\gcd(549, 4087) = 61$. This leads to the factorization $4087 = 61 \cdot 67$. Observe that

$$\begin{aligned} 61 - 1 = 60 = 2^2 \cdot 3 \cdot 5 \\ 67 - 1 = 66 = 2 \cdot 3 \cdot 11. \end{aligned}$$

We leave it to the reader to check that 2 has indeed order 60 over $\mathbb{Z}/61\mathbb{Z}$ and order 66 over $\mathbb{Z}/67\mathbb{Z}$. △

Remark 2.3.6. Pollard's $p-1$ algorithm will not always succeed. In the cases where for every prime divisor p of N it holds that $p-1$ has a very large prime divisor, one might have to increase the boundary to a very large number. This makes it so that the algorithm runs on an unreasonable amount of time. Recall that RSA numbers are large composite integers of the form $N = pq$ with p, q two very large prime numbers. To ensure security, p and q should be chosen in such a way that $p-1$ and $q-1$ do not factor entirely into small primes. An extreme measurement would be to have $p - 1 = 2p'$ and $q - 1 = 2q'$ for different primes p', q' so that B would have to get almost as large as the prime divisors. These kind of primes are called "safe primes". In the cases when working with safe primes, even trial division would take less time, which is noted in [10, section 10C].

3 Elliptic Curves

This section will serve as an introduction to elliptic curves and the group law on it. We will try to make it intuitive by using both algebra and the projective space and work out examples in the real numbers. The graphs were made using GeoGebra [13]. Furthermore, we will apply it to the case where we have a finite field, in particular $\mathbb{F}_p$ for some prime number p and discuss some properties elliptic curves over finite fields have.

3.1 Weierstrass equations

We mention the abstract definition of an elliptic curve.

Definition 3.1.1 (Elliptic curve)**.** An elliptic curve over a field K is a non-singular projective curve over K of genus 1 equipped with a marked K-rational point.

Another way to define elliptic curves is as the set of solutions of a so-called Weierstrass equation together with a point at infinity, which we will denote by $\mathcal{O}$. Given a field K, the generalized Weierstrass equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

with $a_i \in K$ and $\Delta \neq 0$, where the Δ is the discriminant since it must be non-singular. In this case, the discriminant is given by the following, see [14].

$$\begin{aligned}
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6\\
d_2 &= a_1^2 + 4a_2\\
d_4 &= 2a_4 + a_1a_3\\
d_6 &= a_3^2 + 4a_6\\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

However, it is often more practical to work with the (simplified) Weierstrass equation

$$y^2 = x^3 + Ax + B. \tag{3.2}$$

This equation can be determined using a change of variables as long as the characteristic of K is not equal to 2 or 3. Since we will not work on these fields, we will omit the details on them. To make this change of variables, we use the same idea as in [15, Section 2.1]. If the characteristic of K is not equal to 2, then we can divide by 2 and complete the square

$$y^2 + a_1xy + a_3y = \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 - \frac{a_1^2}{4}x^2 - \frac{a_1a_3}{2}x - \frac{a_3^2}{4}.$$

If we substitute this in (3.1) and add $\frac{a_1^2}{4}x^2 + \frac{a_1a_3}{2}x + \frac{a_3^2}{4}$ to both sides, we get

$$\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right).$$

This equation can be rewritten as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{3.3}$$

with $y_1 = y + \frac{a_1}{2}x + \frac{a_3}{2}$ and some constants $a_2', a_4', a_6' \in K$. If the characteristic is also not 3, then we can divide by 3. Hence, let $x = x_1 - \frac{a_2'}{3}$. Substituting this in in (3.3) gives

$$y_1^2 = x_1^3 + Ax_1 + B,$$

for some constants $A, B \in K$. The discriminant of the equation in (3.2) is $\Delta = -16(4A^3 + 27B^2)$, see [14]. Therefore, we require $4A^3 + 27B^2 \neq 0$ for non-singularity.

Remark 3.1.2. When we say "to divide" by a certain number in a field, we mean to multiply with its multiplicative inverse, i.e. $\frac{p}{q} = p \cdot \frac{1}{q}$ where $\frac{1}{q} = r$ such that $r \cdot q = 1$. As we work in a field, every element aside from 0 has a multiplicative inverse, which is why we cannot divide by 2 in a field with characteristic 2 and similarly 3. There are many ways to find the multiplicative inverse of an element, e.g. the extended Euclidean algorithm when working with integers. As mention in previous sections, this particular algorithm can also determine that an integer A has no inverse modulo N. This is due to the algorithm calculating $\gcd(A, N)$ and the inverse of A modulo N not existing if $\gcd(A, N) \neq 1$.

We will mostly use Equation (3.2). The solutions of this equation are the affine points. Together with the point at infinity $\mathcal{O}$, they form the K-rational points $E(K)$ of an elliptic curve E, i.e.

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}. \tag{3.4}$$

A different way and perhaps a more precise way to describe $E(K)$ would be to use the projective plane over K, denoted by $\mathbb{P}^2(K)$. We will give a brief introduction to the projective plane where the focus lies on elliptic curves in particular.

Recall that $\mathbb{P}^2(K)$ consists of equivalence classes of triples $(x, y, z) \in K^3$ with at least one of them nonzero. We say that two triples (x, y, z) and (x', y', z') are equivalent if and only if there exists a nonzero $\lambda \in K$ such that $(x, y, z) = (\lambda x', \lambda y', \lambda z')$, as described in [15, section 2.3]. This means the equivalence classes are defined by the ratios between x, y and z, which is why it is common to denote them by $(x : y : z)$.

In order for a curve to be well-defined on a projective plane, the polynomial that defines the curve has to be homogeneous, i.e. every term of the polynomial or equation has to have the same degree. We will illustrate this with an example.

Example 3.1.3. Let $K = \mathbb{R}$ and consider $F(x, y, z) = x + y - z^2$. Observe that $(1, 0, 1)$ is a root of F. In other words, it is a point on the curve $F(x, y, z) = 0$. Furthermore, it is easy to see that $(2 : 0 : 2) = (1 : 0 : 1)$. However, $F(2, 0, 2) = -2$ and thus the point $(2, 0, 2)$ does not lie on $F(x, y, z) = 0$. △

The reason it is well-defined for homogeneous polynomials of degree n is because in that case we can factor out λ^n if $(x, y, z) = (\lambda x', \lambda y', \lambda z')$ with nonzero λ, which would lead to $F(x, y, z) = \lambda^n F(x', y', z')$. Then we get $F(x, y, z) = 0$ if and only if $F(x', y', z') = 0$. Observe that the equation used to define $E(K)$ in 3.4, which we can rewrite as $x^3 - y^2 + Ax + B = 0$, is not homogeneous. We need to introduce a third variable z and multiply each term with some power of z to get a homogeneous equation.

Definition 3.1.4 (Homogenization)**.** Given a field K and a curve $f(x, y) = 0$ over K^2, a "homogenization" of f of degree n is a curve $F(x, y, z)$ over $\mathbb{P}^2(K)$ such that the following holds, as described in [16, section 5]:

- $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$;
- $F(x, y, 1) = f(x, y)$.

The first statement implies what we mentioned earlier, that curves are well-defined. The second implies that by taking $z = 1$, we would end up with the original polynomial.

It is fairly easy to see that curves that are defined by polynomials can be homogenized. Thus, in order to homogenize the Weierstrass equation, we have to multiply each term with some power of z and we would like to get the Weierstrass equation back if $z = 1$. The Weierstrass equation is of degree 3, which is gives

$$y^2 z = x^3 + Axz^2 + Bz^3. \tag{3.5}$$

If we consider the solutions $(x : y : z)$ for this equation with $z \neq 0$, we can divide by z to get ratios $(x' : y' : 1)$. These correspond exactly to the solutions $(x', y') \in K^2$ of (3.2), i.e. the affine points. Furthermore, if we let $z = 0$, then we get $x = 0$ by (3.5), which leads to the unique solution $(0 : y : 0) = (0 : 1 : 0)$, as y cannot be 0 since we would otherwise have a $(0 : 0 : 0)$ which is not well-defined. The solution $(0 : 1 : 0)$ corresponds to the point at infinity, $\mathcal{O}$.

Remark 3.1.5. Note that $(0 : 1 : 0) = (0 : -1 : 0)$, which means that $\mathcal{O}$ lies both at the "top" of the y-axis and at the "bottom" of the y-axis. The importance of this will be clear in the next segment.

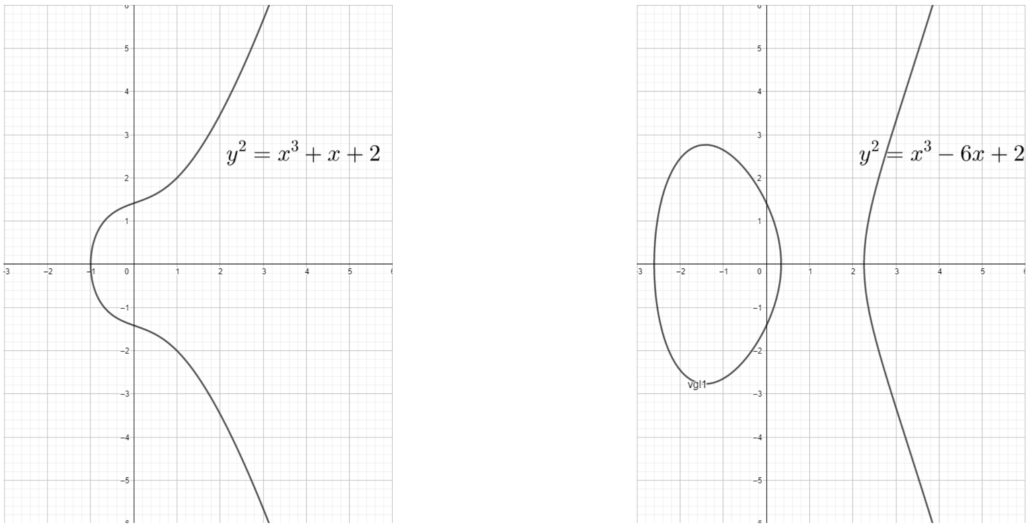
Thus, the set of points of an elliptic curve $E(K)$ can be defined as

$$E(K) = \{(x, y, z) \in \mathbb{P}^2(K) \mid y^2z = x^3 + Axz^2 + Bz^3\}.$$

In some cases, using the projective coordinates can be advantageous especially in the context of the next part. For instance, it is useful in the interpretation of $\mathcal{O}$. We have found earlier that $\mathcal{O}$ corresponds to the unique point $(0 : 1 : 0)$ at infinity. Observe that every vertical line $x = c$ in K^2 intersect each other at $\mathcal{O}$, as their homogenization is $x = cz$. Furthermore, it plays a big role in the proof of the associativity of the "group law". Besides that, using projective coordinates to compute the "addition" of two points on an elliptic curve uses heavily adjusted formulas that do not require taking multiplicative inverse. This is especially useful when the elliptic curves are taken over a ring, such as the integers modulo N with $\mathbb{Z}/N\mathbb{Z}$ not a field, see [15, section 2.11]. This can be helpful when calculating in certain (finite) fields and occasionally relevant in time considering taking inverses is considered significantly slower than multiplication and squaring, which those formulas mostly consist of. For more details, we refer to [15, section 2.6].

3.2 Group law

A very interesting aspect of elliptic curves is how a group law, often called the addition law, can be defined on the points on an elliptic curve. We will first describe it informally in order to make the formulas feel more intuitive. We will use the simplified Weierstrass equation as this gives the most natural interpretation. During this part, we will work out examples on the elliptic curve $y^2 = x^3 + x + 2$ with coordinates in $\mathbb{R}$. The graph of which can be seen in Figure 1a. Observe that its discriminant is nonzero.



(a) The elliptic curve $y^2 = x^3 + x + 2$ in $\mathbb{R}$

(b) The elliptic curve $y^2 = x^3 - 6x + 2$ in $\mathbb{R}$

Figure 1: Two types of elliptic curves in $\mathbb{R}$

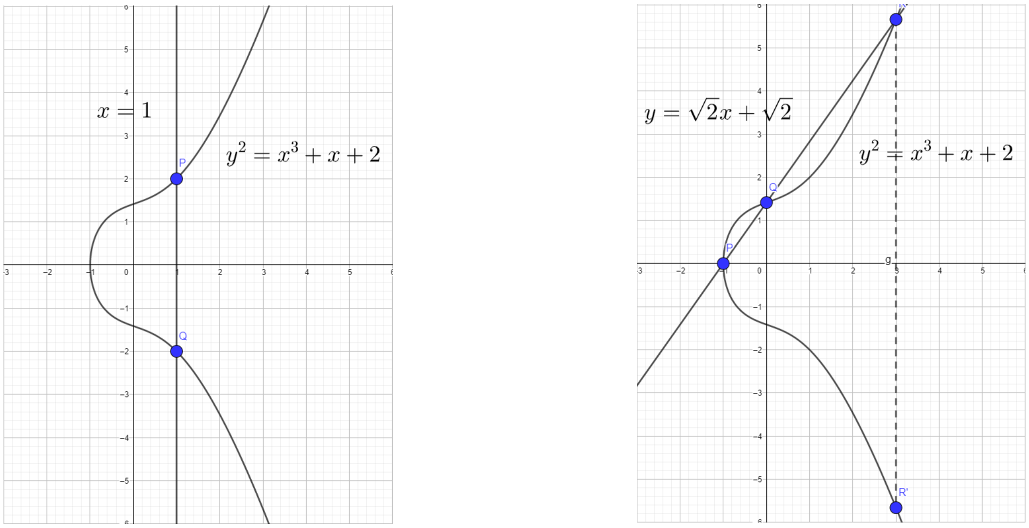
Firstly, observe that if the pair (x, y) is a solution to the equation $y^2 = x^3 + Ax + B$, then so is $(x, -y)$, i.e. an elliptic curve is symmetric about the x-axis. If $P = (x_P, y_P) \in K^2$ denotes a point on an elliptic curve $E(K)$, then we will use the notation $-P$ for the point $(x_P, -y_P) \in K^2$ that lies on the same elliptic curve. Using the observation made in Remark 3.1.5, we will consider $-\mathcal{O} = \mathcal{O}$.

Remark 3.2.1. Note that while the simplified version of the Weierstrass equation gives a curve that is symmetric about the x-axis, the generalized Weierstrass equation in (3.1), which we introduced at the start is not. The "inverse" element of $P = (x_P, y_P)$ on the generalized Weierstrass equation is therefore generally not $(x_P, -y_P)$ as it often does not lie on the same curve.

Suppose we are given an elliptic curve $E(K)$ of the form $y^2 = x^2 + Ax + B$ with two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on it. We will try to make it clear that when we take the line through P and Q, it intersects in a unique different point $R = (x_R, y_R)$ on $E(K)$. This will be done in a similar way as in [15, section 1]. Intuitively, note that the Weierstrass equation is of degree 3 and a line is of degree 1. Using Bézout's theorem from algebraic geometry, they have exactly $3 \cdot 1 = 3$ intersection points, taking into account their multiplicity and points at infinity or with coordinates in the algebraic closure. For more details on that, we refer to [17, appendix A]. Considering we have two points with coordinates in K and a polynomial in K, the third point will also generally have coordinates in K. In essence, the addition law is defined as "$P + Q = -R$".

For the first case, consider $Q = -P = (x_P, -y_P)$ with $y_P \neq 0$ and neither of them infinite. It is easy to see that the line through P and Q is the vertical line $x = x_P$. We know from the previous part about projective coordinates that the point on the elliptic curve at infinity, $\mathcal{O}$, lies on every vertical line. In particular, we discussed also why $\mathcal{O} = -\mathcal{O}$. Therefore, we end up with $P + Q = \mathcal{O}$.

Example 3.2.2. Consider the elliptic curve $E(\mathbb{R})$ defined by $y^2 = x^3 + x + 2$. Observe that $P = (1, 2)$ lies on this curve. Due to symmetry, $Q = -P = (1, -2)$ also lies on this curve. The line through P and Q is the vertical line $x = 1$ as seen in Figure 2a △



(a) $P = (1, 2)$ and $Q = (1, -2)$ gives $P + Q = \mathcal{O}$

(b) $P = (-1, 0)$ and $Q = (0, \sqrt{2})$ gives $R' = (3, -4\sqrt{2})$

Figure 2: The first two addition cases for $y^2 = x^3 + x + 2$

In the second case, suppose $P \neq \pm Q$ and neither of them infinite. We can construct the line ℓ through P and Q. Firstly, note that the slope of ℓ is $\frac{y_Q - y_P}{x_Q - x_P}$. We will denote $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$ Thus the line ℓ can be described using the equation

$$y = \lambda x + b \tag{3.6}$$

for some constant $b \in K$. As the point P lies on this line, we can fill its coordinates in (3.6) to find b, which gives us the following equation for ℓ

$$y = \lambda(x - x_P) + y_P. \tag{3.7}$$

Now we can substitute (3.7) in the Weierstrass equation and rearrange it, which gives us an equation of the form

$$x^3 - \lambda^2 x^2 + (A - 2\lambda\,(y_P - x_P\lambda))\,x + B - (\lambda^2 x_P^2 - 2y_P x_P \lambda + y_P^2) = 0. \tag{3.8}$$

Note that an equation of the form $x^3 + ax^2 + bx + c$ can be factored as $(x - x_1)(x - x_2)(x - x_3)$ where x_1, x_2 and x_3 are the roots of the polynomial. Furthermore, observe that

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \tag{3.9}$$

Note that in general, the factorization in (3.9) holds for $x_i \in \overline{K}$, the algebraic closure of K. However, in this case we already know two roots that are in K itself, namely x_P and x_Q, since P and Q lie on the intersection of the line with $E(K)$. This means that the third root must also lie on K as we have a K-polynomial. Therefore, R also has coordinates in K. Observe that by the coefficient of x^2 in both (3.8) and (3.9) we get

$$x_R = \lambda^2 - x_P - x_Q, \tag{3.10}$$

where x_R is the third root and therefore the x-coordinate of the third intersection. We can find the y-coordinate of the third intersection by filling this x_R in (3.7). In other words,

$$y_R = \lambda(x_R - x_P) + y_P. \tag{3.11}$$

Thus the resulting point we get from adding Q to P is $(x_R, -y_R)$ with x_R defined in (3.10) and y_R defined in (3.11).

Example 3.2.3. This example uses the same elliptic curve $E(\mathbb{R})$ defined by $y^2 = x^3+x+2$. Consider now the points $P = (-1, 0)$ and $Q = (0, \sqrt{2})$. The slope of the line through P and Q is equal to $\frac{\sqrt{2}}{1} = \sqrt{2}$. Furthermore, we know P is on the line, so the line is represented with the equation $y = \sqrt{2}(x + 1)$ in a similar way we found it in (3.7). Substituting this in the Weierstrass equation and rearranging gives $-x^3 + 2x^2 + 3x = 0$. Fortunately, we already know to roots of this polynomial, namely the x-coordinates of both P and Q, so -1 and 0 respectively. Using the trick described earlier, we get $x_R = 2 - (-1) - 0 = 3$. Filling this in the equation gives $y_R = 4\sqrt{2}$. Thus, reflecting around the x-axis gives us the point $P + Q = R' = (3, -4\sqrt{2})$. This process is demonstrated in figure 2b. △

For the third case, consider $P = Q$ with $y_P \neq 0$ and neither of them infinite. There are many lines that go through P, but contemplate what line we get if we have one point P and one point approaches P. This will lead to the tangent line to the curve at P. Note that the slope in this case can be found by differentiating $y^2 = x^3 + Ax + B$ with respect to x using the chain rule $2y\frac{dy}{dx} = 3x^2 + A$. Thus, the slope is

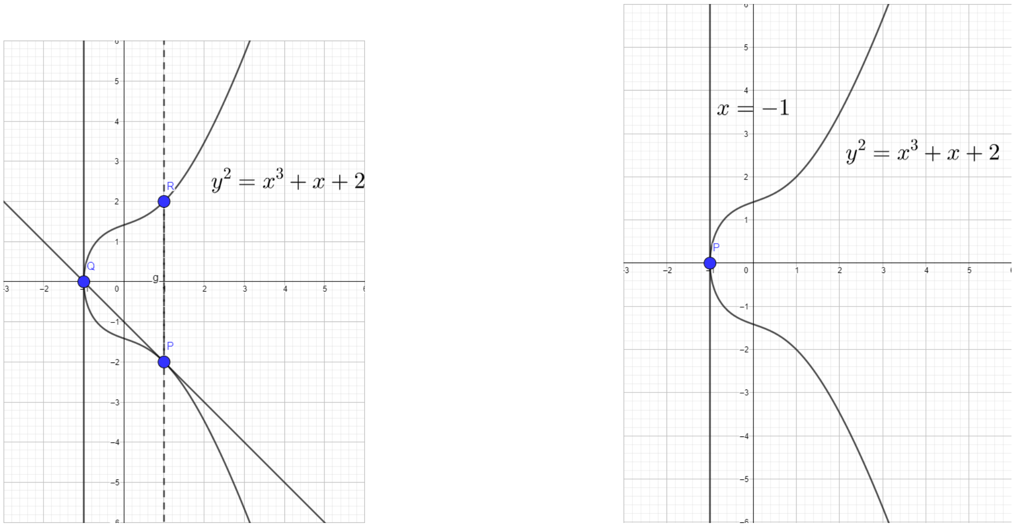
$$\frac{dy}{dx} = \frac{3x^2 + A}{2y}. \tag{3.12}$$

Analogous to the previous case, if we let $\lambda = \frac{3x^2+A}{2y}$, we will get the tangent line in (3.7). Using the same substitution gives us again the expression as in (3.8). However, the difference is that this time we have a double root in (3.9), as $x_P = x_Q$. Without loss of generality, assume $x_1 = x_2 = x_P$. Then we get $x_R = \lambda^2 - 2x_P$ and filling this in gives $y_R = \lambda(x_R - x_P) + y_P$ similar to (3.10) and (3.11). Thus, we get $(x_R, -y_R)$ from doubling P in this case.

Example 3.2.4. Again using the same example of the elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{R}$, we would like to find $2P = P+P$, where $P = (1, -2)$. The slope of the curve is $\frac{3x_P^2+1}{2y_P}$ by (3.12), thus on the point P it is equal to -1. Furthermore, substituting the coordinates of P gives us a formula for the tangent line of P, namely $y = -1(x - 1) - 2 = -x - 1$. Analogous to the previous example, if we substitute this in the Weierstrass equation and rearrange it, we get the equation $x^3 - x^2 - x + 1 = 0$, which has the root $x = 1$ with multiplicity 2 due to the line being tangent to the curve on P. We can factor $(x - 1)^2$ out to get $(x - 1)^2(x + 1)$. Hence, the other intersection is at $x = -1$, which leads to the point $R = (-1, 0)$. As the y-coordinate is zero, we have $R = -R$, so it leaves us with R, which can be seen in Figure 3a △

In the fourth case, we have $P = Q$ and $y_P = 0$. Here, the tangent line is a vertical line, which can be somewhat determined from the formula in (3.12). As we find the slope by dividing by y, which is in this case 0, it leads to an slope that goes to infinity, i.e. a vertical line. Therefore, it will lead to $\mathcal{O}$ similar to the first case, as $-\mathcal{O} = \mathcal{O}$.

Example 3.2.5. Continuing the previous examples with the elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{R}$, if we take $P = Q = (-1, 0)$, we need the tangent line. The tangent line at P, however, is vertical here as seen in 3b. Thus, we can conclude that $2P = P + P = \mathcal{O}$. △



(a) $P = Q = (1, 2)$ gives $2P = P + P = R = (-1, 0)$

(b) $P = Q = (-1, 0)$ and gives $2P = P + P = \mathcal{O}$

Figure 3: The third and fourth addition case for $y^2 = x^3 + x + 2$

In the last case, let at least one of them be $\mathcal{O}$. If $P = Q = \mathcal{O}$, then we consider the outcome to be $\mathcal{O}$ itself again. Without loss of generality, if $P \neq \mathcal{O}$ and $Q = \mathcal{O}$, then we get the vertical line through P, which intersects $E(K)$ in $-P$. Thus, we end up with P again.

As we have covered every possible case, we will now formulate the theorem that states the group law formally.

Theorem 3.2.6 (Group law)**.** *Let K be a field and E an elliptic curve defined over K by the equation $y^2 = x^3 + Ax + B$. Then the points on $E(K)$ form an abelian group with identity element $\mathcal{O}$ with the following group operation. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on $E(K)\backslash\{\mathcal{O}\}$. The inverse element of P is $-P = (x_P, -y_P)$. Now, if P and Q are both finite points and $Q \neq -P$, define*

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \textit{if } P \neq Q \\ \frac{3x_P^2 + A}{2y_P} & \textit{if } P = Q \end{cases}$$

and let

$$x_R = \lambda^2 - x_P - x_Q \quad \textit{and} \quad y_R = \lambda(x_P - x_R) - y_P.$$

Then the addition of $P, Q \neq \mathcal{O}$ and $Q \neq -P$ is defined as $P + Q = R = (x_R, y_R)$.

Proof. In the parts above, we have intensively discussed the underlying geometric process and how we get these formulas by finding the slope. In particular, the set of points on $E(K)$ is closed under addition. By the last case, $\mathcal{O}$ is the identity element. Moreover, by the first and fourth case, every point P has the inverse $-P$, which is on the curve due to symmetry about the x-axis. Commutativity is evident from the formulas and the fact that the line through P and Q is the same as the line through Q and P. It remains to prove associativity, i.e. the equality $(P + Q) + R = P + (Q + R)$ for arbitrary points $P, Q, R \in E(K)$. One possible proof could be by separating many cases, even more than what we did to find $P + Q$. In order not to drag out this part for too long, it will be left to the reader that it indeed holds using the formulas and definitions. Geometrically, one could also try to prove that the point of intersection of the line through $P + Q$ and R with $E(K)$ is the same point where the line through P and $Q + R$ intersects $E(K)$. In other words, these two lines intersect on a point on $E(K)$. This is for example done in [17, section 1.2]. Another possible approach that also uses a similar idea would be using the projective coordinates, as mentioned earlier. We refer to [15, section 2.4]. □

One particular corollary from the associativity is an algorithm to find a given multiple of an element P on an elliptic curve $E(K)$, called the “double-and-add algorithm” as in [9, section 6.3.1]. It is very similar to the Fast Powering Algorithm when calculating powers modulo N. This is a lot more efficient than adding every point one by one and likely the most efficient way to calculate a multiple of P. For an integer k, we will denote a multiple of P by

$$kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}.$$

For a given $P \in E(K)$ and integer n, the underlying idea is that we only need to compute kP for $k = 2^m$ for $m \in \{0, 1, \ldots, \lfloor \log_2(n) \rfloor\}$ by doubling every step and add the right points to find nP. Note that we can write n in binary form

$$n = n_0 2^0 + n_1 2^1 + \cdots + n_m 2^m,$$

where $m = \lfloor \log_2(n) \rfloor$ and $n_i \in \{0, 1\}$, with the assumption that $n_m = 1$. We will illustrate this with an example.

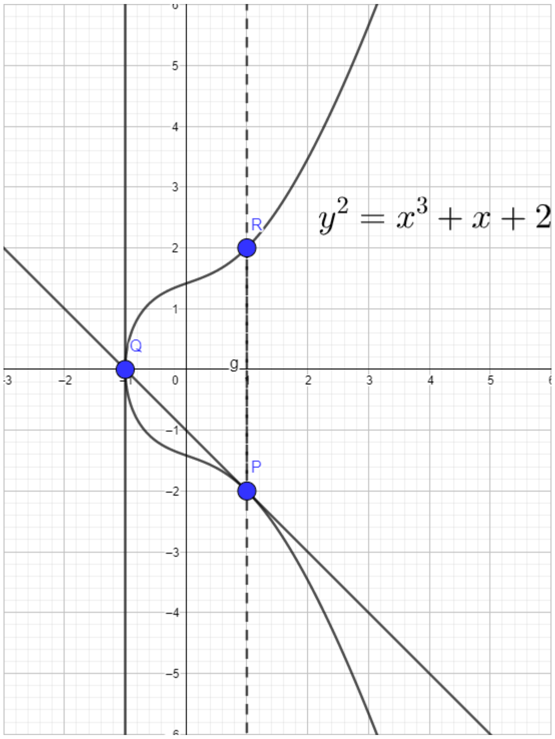


Figure 4: Computing $5P = P$ for $P = (1, -2)$

Example 3.2.7. We recall our previous examples, where we worked with the elliptic curve $E(\mathbb{R})$ defined by $y^2 = x^3 + x + 2$. We want to find $5P$ with $P = (1, -2)$. Observe that $\lfloor \log_2(5) \rfloor = 2$ and $5 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2$. Recall from Example 3.2.4 we found $2P = (-1, 0)$. Furthermore, Example 3.2.5 showed us that the double of $(-1, 0)$ is equal to $\mathcal{O}$, thus $4P = 2 \cdot 2P = \mathcal{O}$. Now we can compute $5P = P + 4P = P + \mathcal{O} = P$. We can confirm this by directly computing $5P = (((P + P) + P) + P) + P$. Recall that $2P = P + P = (-1, 0)$. Furthermore, observe that the line through P and $2P$ is the same as the tangent line to P as both intersect $E(\mathbb{R})$ in P and $2P$. The third intersection point is in this case again P, as it has multiplicity 2 so that $3P = 2P + P = -P$. We know that $P + (-P) = \mathcal{O}$ as in Example 3.2.2, so $4P = \mathcal{O}$. Thus, we end up again with $5P = \mathcal{O} + P = P$. The process of this is illustrated in Figure 4 with $Q = 2P$ and $R = 3P$. △

3.3 Over finite fields

We will now focus our attention to the case where the field K is a finite field, in particular when $K = \mathbb{F}_p$ for a prime number $p > 3$. Recall from field theory that there exists finite field of order q if and only if $q = p^k$

for some prime p. Furthermore, any two finite fields of the same order are isomorphic to each other. Thus if $N = pq$ for two primes $p \neq q$, then $\mathbb{Z}/N\mathbb{Z}$ is not a field, only a ring. As mentioned earlier, it is possible to take elliptic curves modulo N with $\mathbb{Z}/N\mathbb{Z}$ not a field by using projective coordinates. However, in this case, we require that $4A^3 + 27B^2$ is a unit modulo N, instead of it being nonzero, as the discriminant has to be invertible, which in a field is equivalent to being nonzero. There is another way to describe elliptic curves modulo N without using knowledge from elliptic curves over rings. This will be outlined with the following proposition and its corollary.

Proposition 3.3.1 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \dots, n_m$ be pairwise coprime positive integers and $a_1, a_2, \dots, a_m$ be any integers. Then there is a unique solution x modulo $N = n_1 n_2 \cdot \dots \cdot n_m$ such that*

$$\begin{aligned} x &= a_1 \bmod n_1 \\ x &= a_2 \bmod n_2 \\ &\vdots \\ x &= a_m \bmod n_m \end{aligned}$$

For the proof, see [10, section 12.A]. The important part here is that it is equivalent to say that the map

$$x \bmod N \mapsto (x \bmod n_1, x \bmod n_2, \dots, x \bmod n_m)$$

defines an isomorphism

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_m\mathbb{Z}.$$

In essence, what this tells us is given an elliptic curve over $N = pq$ with prime numbers $p \neq q$, we can view points on $E(\mathbb{Z}/N\mathbb{Z})$ as a combination of a point on $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$. Furthermore, we can work out the result of adding two points on $E(\mathbb{Z}/N\mathbb{Z})$ by computing them modulo p and modulo q separately. In other words, we add the points in $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ and find the point on $E(\mathbb{Z}/N\mathbb{Z})$ that corresponds to it. This can be done with the aforementioned formulas. It also explains why the discriminant has to be coprime with N, as that ensures it is nonzero modulo p and modulo q.

Corollary 3.3.2. *Let p, q be coprime odd integers. Let E be an elliptic curve defined over $\mathbb{Z}/N\mathbb{Z}$. with $N = pq$. Then there is a group isomorphism*

$$E(\mathbb{Z}/N\mathbb{Z}) \simeq E(\mathbb{Z}/p\mathbb{Z}) \oplus E(\mathbb{Z}/q\mathbb{Z}).$$

As the precise proof requires projective coordinates and the formulas using those, we will refer to [15, section 2.11].

Since we now know that elliptic curves modulo N can be projected onto the same curve modulo p and modulo q, we will discuss more on the group structure on $E(\mathbb{F}_p)$. Consider the elliptic curve $E(\mathbb{F}_p)$ defined by $y^2 = x^3 + Ax + B$, i.e.

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Observe that the affine points are a subset of $\mathbb{F}_p^2$, which is finite. Thus, in this case the number of points in $\mathbb{E}(\mathbb{F}_p)$, in other words the order of $\mathbb{E}(\mathbb{F}_p)$ is also finite. We will denote the order of $\mathbb{E}(\mathbb{F}_p)$ with $\#\mathbb{E}(\mathbb{F}_p)$.
We would like to find an approximation or upper bound of $\#\mathbb{E}(\mathbb{F}_p)$. When we take an $x \in \mathbb{F}_p$, there are either three possibilities. Firstly, it is possible that $x^3 + Ax + B$ is a quadratic residue modulo p, i.e. a nonzero square y^2 in $\mathbb{F}_p$. In this case, it has two solutions in $\mathbb{F}_p$, namely the two square roots of y^2 modulo p. This corresponds with the points $(x, \sqrt{y})$ and $(x, -\sqrt{y})$. In the second case, it is not a square modulo p, i.e. there is no $y \in \mathbb{F}_p$ such that $y^2 = x^3 + Ax + B$. This means there is no point on $E(\mathbb{F}_p)$ with that particular x-coordinate. In the last case, $x^3 + Ax + B = 0$, in which case there is one point $(x, 0)$. However, this last case is uncommon.

n mod 5	0	1	2	3	4
n^2 mod 5	0	1	4	4	1

Table 1: The squares of the integers modulo 5

n mod 5	0	1	2	3	4
$n^3 + n + 2$ mod 5	2	4	2	2	0

Table 2: The outcome of the polynomial modulo 5

Example 3.3.3. Consider the elliptic curve E represented by $y^2 = x^3 + x + 2$ defined over $\mathbb{F}_5$, the integers modulo 5. Note that the discriminant is nonzero, as $4 \cdot 1^3 + 27 \cdot 2^2 = 112 \equiv 2 \bmod 5$. We calculate $n^2 \bmod 5$ for $0 \leq n \leq 4$. The results can be found in Table 1. Furthermore, the result of $n^3 + n + 2 \bmod 5$ for each i is given in Table 2. We conclude that $E(\mathbb{F}_5) = \{\mathcal{O}, (1,2), (1,3), (4,0)\}$. Observe that $-2 \equiv 3 \bmod 5$ and one can compute $2(1,2) = 2(1,3) = (4,0)$ using the formulas given in the previous section. Therefore, this group is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. △

Since exactly half of the units of $\mathbb{F}_p$ are squares, we can approximate the amount of affine points with $\frac{p}{2} \cdot 2 = p$. As we always have the point $\mathcal{O}$ on every elliptic curve, this leads to the approximation

$$\#E(\mathbb{F}_p) \sim p + 1.$$

The following theorem reinforces this approximation and gives a boundary for $\#E(\mathbb{F}_p)$. For the proof, which goes beyond the scope of this work, we refer to [18, section V.1].

Theorem 3.3.4 (Hasse)**.** *Let E be an elliptic curve over $\mathbb{F}_p$. There exists an integer t with $|t| \leq 2\sqrt{p}$, known as the trace of Frobenius, such that the order of $E(\mathbb{F}_p)$ is*

$$\#E(\mathbb{F}_p) = p + 1 - t.$$

In other words, $\#E(\mathbb{F}_p)$ is bounded by

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

This interval is usually known as the Hasse interval. To find the exact value of $\#E(\mathbb{F}_p)$ efficiently, one can use Schoof's algorithm or improvements thereof. One thing to note is that these algorithms run on polynomial time. As it requires some knowledge of algebraic geometry to be fully understood, we refer to [18, section XI.3].

Remark 3.3.5. The reason the t in Hasse's theorem is known as the trace of Frobenius is due to it being the trace of a particular matrix. The Frobenius map defined by $\phi_p(x,y) = (x^p, y^p)$ is an endomorphism of the elliptic curve E defined over $\mathbb{F}_p$. By taking the trace of the matrix induced by the action of the Frobenius endomorphism on the Tate module of E, denoted by T_ℓ, one obtains t. The boundary follows from taking the characteristic polynomial $px^2 - tx + 1$ which must be non-negative for all real x. Therefore, the discriminant $t^2 - 4p \leq 0$, which gives the boundary in Hasse's theorem. See [15, section 4.2] and [18, section V].

Note that since $E(\mathbb{F}_p)$ is a finite group, we know that every point P on the elliptic curve is a "torsion point", i.e. there is an integer n such that $nP = \mathcal{O}$. This is due to Lagrange's theorem, which we mentioned earlier in the proof of Proposition 2.3.1.

Definition 3.3.6. Let K be a field and E an elliptic curve defined over K. For a given integer n, we will denote the set of torsion points of order dividing n as

$$E(K)[n] = \{P \in E(\overline{K}) \mid np = \mathcal{O}\}, \tag{3.13}$$

where $\overline{K}$ denotes the algebraic closure of K.

Note that this set is a group. We will look at an interesting property of $E(K)[n]$, in particular when K is a finite field. We start by giving an example

Example 3.3.7. Consider the case where $n = 2$. We know that $2P = \mathcal{O}$ if and only if $P = \mathcal{O}$ or the tangent line on P is vertical. This second case happens only when $y_P = 0$. Observe that we can write

$$x^3 + Ax + B = (x - x_1)(x - x_2)(x - x_3)$$

for $x_1, x_2, x_3 \in \overline{K}$. This leads to

$$E(K)[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}.$$

Observe that every point aside from $\mathcal{O}$ has order 2 and if we take the line through two of those points, it is a horizontal line and thus should give us the third point as the y-coordinate is zero. Therefore, we know that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. △

A generalisation of this is the following proposition, the proof of which we refer to [15, section 3.2].

Proposition 3.3.8. *Let K be a field with characteristic p and E an elliptic curve over K. Let n be a positive integer. Then the following holds.*

- *If $p \nmid n$ (which includes the possibility $p = 0$), then*

$$E(K)[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

- *If $p \mid n$, write $n = p^r m$ with $p \nmid m$, then*

$$E(K)[n] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \quad \text{or} \quad E(K)[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

With this proposition, we can describe the group structure on $E(\mathbb{F}_p)$ as in [15, section 4.1] using the following theorem.

Theorem 3.3.9. *Let E be an elliptic curve over $\mathbb{F}_p$ then either*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z},$$

for some positive integer n or

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z},$$

for some positive integers n_1, n_2 with $n_1 \mid n_2$.

Proof. By a result of group theory, we know that every finite abelian group is isomorphic to a direct sum of the cyclic groups

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z} \tag{3.14}$$

where n_i are positive integers and $n_i \mid n_{i+1}$. Observe that the group $\mathbb{Z}/n_i\mathbb{Z}$ has exactly n_1 elements of order dividing n_1, namely the elements of the subgroup $\{\frac{n_i}{n_1}j \mid 0 \leq j \leq n_1 - 1\}$. Thus, if $E(\mathbb{F}_p)$ is isomorphic to (3.14), then it has n_1^k elements with an order that divides n_1. Moreover, by Proposition 3.3.8, we know that $r \leq 2$. The case $r = 2$ corresponds with the second case in the theorem, while the case where $r = 0$ corresponds with the first case with $n = 1$ and $r = 1$ also corresponds with the first case. □

4 Lenstra's Algorithm

In this part of the thesis we will discuss an algorithm for factorization that uses elliptic curves which Lenstra proposed and discussed in his paper, see [1]. As mentioned earlier in Section 2.3, it is an improvement on Pollard's $p-1$ algorithm. Instead of computing powers modulo N, however, Lenstra's algorithm computes multiples of points on elliptic curves defined over $\mathbb{Z}/N\mathbb{Z}$, i.e. elliptic curves modulo N. While Pollard's algorithm relies on the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, which has order $p-1$, Lenstra's algorithm uses the group of rational points on an elliptic curve E of order $p+1-t$ for some $|t| \leq 2\sqrt{p}$ by Theorem 3.3.4. Similar as the conditions of $p-1$ in Pollard's algorithm, Lenstra's algorithm is more likely to find a non-trivial divisor if $p+1-t$ is divisible by small primes. However, the key difference here is that in Pollard's algorithm, if $p-1$ does not factor entirely into small primes, we cannot do much, while in Lenstra's algorithm, we can try different elliptic curves of different orders.

4.1 Explanation of the algorithm

Let $N = pq$ for two primes p and q. Firstly, we have to choose an elliptic curve E on $\mathbb{Z}/N\mathbb{Z}$ defined by $y^2 = x^3 + Ax + B$ modulo N and a point $P = (x_P, y_P)$ on it. Recall from Corollary 3.3.2 that even though $\mathbb{Z}/N\mathbb{Z}$ is not a field, we can view it as a direct sum of two elliptic curves over the finite fields $\mathbb{F}_p$ and $\mathbb{F}_q$. Therefore, we can consider the same equation modulo p and modulo q.

While it may seem natural to choose random integers A, B, x_P and compute y_P, we do not know whether $x_P^3 + Ax_P + B$ is a square modulo N or not. Furthermore, it can also take time to compute a root modulo N. A way to guarantee efficiently that a point is on an elliptic curve is to choose A, x_P, y_P and calculate

$$B \equiv y_P^2 - x_P^3 - Ax_P \bmod N.$$

Then we consider the curve $y^2 = x^3 + Ax + B$ modulo N which has point $P = (x_P, y_P)$ on it. To check that this indeed gives an elliptic curve, we can try to compute $d = \gcd(4A^3 + 27B^2, N)$ so that the discriminant is invertible modulo N. This leads to three possible cases:

1. If $1 < d < N$, then we have found a nontrivial divisor of N.
2. If $d = N$, we have to choose a different elliptic curve, since we will not get an elliptic curve modulo p nor modulo q. Therefore, change at least one of the variables A, x_P, y_P modulo N.
3. If $d = 1$, then we have successfully found an elliptic curve modulo N, which can also be viewed as an elliptic curve modulo p and modulo q. In this case, we continue the algorithm.

We try to compute mP for some integer m that is the product of many small primes, similar to Pollard's $p-1$ algorithm. In the computations, we use the formulas in Theorem 3.2.6 to "add" points. Note that while $\mathbb{Z}/N\mathbb{Z}$ is not a field, we may still use the formulas, despite the fact we only defined them on fields. As stated in Corollary 3.3.2, we can consider addition on the same elliptic curve modulo p and modulo q. However, during the computations it may occur that we have to take a multiplicative inverse of an integer modulo N that is not coprime to N. This can happen every step when we have to compute the slope of a line to produce a new point. During the calculations the (extended) Euclidean algorithm is usually used to compute if an integer has a multiplicative inverse modulo N and, if so, what its inverse is. Recall that this runs in polynomial time. Therefore, if we find an integer that has no inverse in $\mathbb{Z}/N\mathbb{Z}$, we also determine that its greatest common divisor with N is greater than 1. We distinguish two cases:

1. If the greatest common divisor is not N, then we have found a non-trivial divisor of N. This is the case when the addition modulo p and modulo q becomes different. The likely case is when a point is the neutral element $\mathcal{O}$ on $E(\mathbb{Z}/p\mathbb{Z})$, while it is not the neutral element on $E(\mathbb{Z}/q\mathbb{Z})$ or vice versa. The former is likely to happen if $\#E(\mathbb{Z}/p\mathbb{Z})$ is divisible by small primes. In essence, m is a multiple of the order of P on the curve $E(\mathbb{F}_p)$, while not being a multiple of the order of P on the curve $E(\mathbb{F}_q)$. Another possible cause is that the addition on the curve modulo p is a doubling of a point, while it is the addition of two different points on the curve modulo q.

2. In the second case, the greatest common divisor is N. Recall that $\#E(\mathbb{Z}/p\mathbb{Z})$ is close to $p+1$ and $\#E(\mathbb{Z}/q\mathbb{Z})$ is a number close to $q+1$ by Theorem 3.3.4. For a large enough prime p, the distribution of $\#E(\mathbb{F}_p)$ for random elliptic curves $E(\mathbb{F}_p)$ is sufficiently uniform. Thus, it is unlikely that they both have the same prime factors. In the rare case that we get N as a greatest common divisor, it corresponds to getting $\mathcal{O}$ on both $E(\mathbb{Z}/p\mathbb{Z})$ and $E(\mathbb{Z}/q\mathbb{Z})$ and thus $\mathcal{O}$ on $E(\mathbb{Z}/N\mathbb{Z})$. This means that m is also a multiple of the order of P on the curve modulo q. If this happens, we try a different curve.

Furthermore, if mP is calculated successfully without any problems regarding finding the inverses, then we can either try a different curve or increase m until we find a non-trivial divisor of N.

n	$n!$ with double-and-add	Calculating $n! \cdot P$ mod 403
1	$1! = 1$	$(1!)P = (2,6)$
2	$2! = 2 \cdot 1!$	$(2!)P = 2 \cdot (2,6) = (214,330)$
3	$3! = 3 \cdot (2!) = 2 \cdot 2! + 2!$	$2 \cdot (214,330) = (13,233)$ $(3!)P = (13,233) + (214,330) = (333,188)$
4	$4! = 4 \cdot (3!) = 2 \cdot 2 \cdot (3!)$	$2 \cdot (333,188) = (13,170)$ $(4!)P = 2 \cdot (13,170) = (360,0)$

Table 3: Multiples of $P = (2,6)$ on $y^2 = x^3 + 7x + 14$ mod 403

Example 4.1.1. Suppose we want to factor the composite integer 403. Observe that it is not divisible by 2 or 3. We choose $P = (2,6)$ and $A = 7$. Then we compute

$$6^2 - 2^3 - 7 \cdot 2 \equiv 14 \bmod 403.$$

Thus, our elliptic curve E is described by the equation $y^2 = x^3+7x+14$ modulo 403. Note that $4 \cdot 7^3 + 27 \cdot 14^2 \equiv 216 \bmod 403$, which is coprime to 403. Therefore, the discriminant is a unit, which means that we have indeed an elliptic curve. We take $m = 6!$, i.e. we want to try to compute $(6!)P$. Note that we can compute $n! \cdot P = n((n-1)!P)$ recursively and use the double-and-add algorithm we described in the last part of Section 3.2 to compute $n((n-1)!P)$ given $(n-1)!P$. This process up to 4! is described in Table 3. We leave it to the reader to check that these are indeed the points calculated from the formulas in Theorem 3.2.6 and lie on the curve. Note that since the y-coordinate of $(4!)P$ is 0, this leads to $2((4!)P) = \mathcal{O}$ and subsequently $(5!)P = (4!)P$ and $(6!)P = \mathcal{O}$. Therefore, we will try a different elliptic curve. In Remark 4.1.3, we will explain what happened here and why the following Example does indeed work. △

n	$n!$ with double-and-add	Calculating $n! \cdot P$ mod 403
1	$1! = 1$	$(1!)P = (5,7)$
2	$2! = 2 \cdot 1!$	$(2!)P = 2 \cdot (5,7) = (184,160)$
3	$3! = 3 \cdot (2!) = 2 \cdot 2! + 2!$	$2 \cdot (184,160) = (208,70)$ $(3!)P = (208,70) + (184,160) = (151,220)$
4	$4! = 4 \cdot (3!) = 2 \cdot 2 \cdot (3!)$	$2 \cdot (151,220) = (78,255)$ $(4!)P = 2 \cdot (78,255) = (168,78)$

Table 4: Multiples of $P = (5,7)$ on $y^2 = x^3 + 11x + 272$ mod 403

Example 4.1.2. Continuing our previous example, we choose $P = (5,7)$ and $A = 11$ to find

$$7^2 - 5^3 - 5 \cdot 11 \equiv 272 \bmod 403,$$

which gives us the elliptic curve $y^2 = x^3 + 11x + 272$ modulo 403. Note that $4 \cdot 11^3 + 27 \cdot 272$ is corpime to 403, so the discriminant is again a unit. We will work once again with $m = 6!$ and try to compute $(6!)P$ in a similar way as before. The computations up to 4! are demonstrated in Table 4. As with the previous example, it is left to the reader to check that these are the points gained from using the formulas. Now, if we try to compute $(5!)P = 4(4!)P + (4!)P$, we need to find $2(4!)P$ to compute $4(4!)P$. If we fill in the formula for the slope λ of the tangent line, we get

$$\lambda = \frac{3 \cdot x_{(4!)P}^2 + A}{2 \cdot y_{(4!)P}} = \frac{3 \cdot 168^2 + 11}{2 \cdot 78} = \frac{84683}{156}.$$

We try using the extended Euclidean algorithm to try to find the reciprocal of 156 modulo 403. However, during this computation we find that $\gcd(156, 403) = 13$ which means we cannot divide by 156 in $\mathbb{Z}/403\mathbb{Z}$. Therefore, we have found a non-trivial divisor 13 of 403. Dividing 403 by 13 results in the prime factorization of $403 = 13 \cdot 31$. △

Remark 4.1.3. In Example 4.1.1, if we take $y^2 = x^3 + 7x + 14$ modulo 13 and modulo 31, we get an elliptic curve of order 16 and 32 respectively. It is up to the reader to check that these are indeed the orders. Both of their respective order are powers of 2, which is why we eventually reached the neutral element both modulo 13 and modulo 31. On the other hand, the elliptic curve $y^2 = x^3 + 11x + 272$ modulo 31 has order $33 = 3 \cdot 11$. The elliptic curve with the same equation modulo 13 has order 16 again. Note that $2 \cdot (4!)$ is a multiple of 16 and by Lagrange's theorem, the order of P on $y^2 = x^3 + 11x + 272$ modulo 13 must divide 16. This lead to us getting the neutral element modulo 13 in the Example 4.1.2. On the other hand, we leave it to the reader to check that the order of P on $y^2 = x^3 + 11x + 272$ modulo 31 is 33, which does not divide $2 \cdot (4!)$.

We will prove the following theorem, see [1, Section 2.6]. It states that the algorithm is always successful under some assumptions which involve the smallest prime divisor p of $N = pq$ and the prime divisors of $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$. Theorem 4.1.4 also gives some upper bounds to estimate the running time of the algorithm. As usual, it is assumed that $p > 3$ as we work in fields with characteristic not equal to 2 or 3. Note that given an integer N, we can check quickly if N is divisible by 2 and/or 3. Furthermore, numbers that are a power of a prime can also usually be detected quickly.

Theorem 4.1.4. *Let N, v, w be positive integers greater than 1 and $A, x_P, y_P \in \mathbb{Z}/N\mathbb{Z}$. Set*

$$B = y_P^2 - x_P^3 - Ax_P \bmod N$$

and let $P = (x_P, y_P)$ be a point on the set of solutions of $y^2 = x^3 + Ax + B$, which we will denote by E. Furthermore, set

$$m = \prod_{r=2}^{w} r^{e(r)},$$

where $e(r)$ is the largest integer k such that $r^k \leq v + 1 + 2\sqrt{v}$. Suppose $N = pq$ with p, q distinct prime integers such that the following conditions are satisfied.

- *$p \leq v$.*
- *$4A^3 + 27B^2 \not\equiv 0 \bmod p$.*
- *Each prime r that divides $\#E(\mathbb{F}_p)$ has the property that $r \leq w$.*
- *$4A^3 + 27B^2 \not\equiv 0 \bmod q$.*
- *$\#E(\mathbb{F}_q)$ is not divisible by the largest prime number dividing the order of P on $E(\mathbb{F}_p)$.*

When Lenstra's algorithm attempts to compute the point mP recursively with $(k_1k_2)P = k_1(k_2P)$ starting with the lower factors, and using the double-and-add method to find kP, it will find a non-trivial divisor of N.

Remark 4.1.5. Observe that the second and fourth condition imply that E is an elliptic curve modulo p and modulo q respectively so that we can consider the group structures on $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$. Therefore, it is also an elliptic curve modulo N. Furthermore, since the coordinates of P is a solution to the polynomial, we know that it is not the neutral element $\mathcal{O}$. In particular, it is not the neutral element on the curve modulo p nor modulo q. Therefore, the largest prime described in the fifth condition exists. Note that the fifth condition also implies $q \neq p$.

Proof. The boundary in Hasse's theorem, which we mentioned in Theorem 3.3.4, and the first condition lead to $\#E(\mathbb{F}_p) \leq v + 1 + 2\sqrt{v}$. Therefore, if r is a prime dividing $\#E(\mathbb{F}_p)$, then its exponent in the factorization of $\#E(\mathbb{F}_p)$ is at most $e(r)$. Note that this is also true for primes that do not divide $\#E(\mathbb{F}_p)$, as those have exponent 0. Since the order ω_p of P in $E(\mathbb{F}_p)$ is a divisor of $\#E(\mathbb{F}_p)$ by Lagrange's theorem, the statement is also true for ω_p. In other words, the exponent of r in ω_p is also at most $e(r)$. Let s be the largest prime dividing ω_p and t as its exponent in the prime factorization of ω_p, so that $1 \leq t \leq e(s)$. Write

$$m_0 = \left(\prod_{r=2}^{s-1} r^{e(r)}\right) \cdot s^{t-1}.$$

Note that m_0 is not a multiple of ω_p, since ω_p is a multiple of s^t, while m_0 is not due to the assumption that s is prime. However, $s \cdot m_0$ is a multiple of ω_p. Hence, m_0P is not $\mathcal{O}$ in the elliptic curve modulo p, while $s \cdot m_0P$ is.

By the third condition, we know that $s \leq w$, so m_0 and $s \cdot m_0$ both are divisors of m. In particular, Lenstra's algorithm will calculate m_0P and $s \cdot m_0P$ at some point while trying to calculate mP. Hence, to prove Theorem 4.1.4, it suffices to show that m_0P and $s \cdot m_0P$ cannot both be points on the curve modulo N. In other words, it must hold that m_0P or $s \cdot m_0P$ has the property that it is the neutral element in either $E(\mathbb{F}_p)$ or $E(\mathbb{F}_q)$ while not being the neutral element in the other. Then, when the algorithm arrives at m_0P, $s \cdot m_0P$, or earlier, it should find a greatest common divisor that is not 1 nor N.

We assumed that $s \cdot m_0$ is a multiple of the order ω_p of P on $E(\mathbb{F}_p)$, thus $s \cdot m_0P$ is $\mathcal{O}$ on $E(\mathbb{F}_p)$. Therefore, if it exists on the curve modulo N, it must be also $\mathcal{O}$ on $E(\mathbb{F}_q)$. That means $s \cdot m_0$ is a multiple of the order ω_q of P on $E(\mathbb{F}_q)$, which must be a divisor of $\#E(\mathbb{F}_q)$ by Lagrange's theorem. By the fifth condition, s does not divide $\#E(\mathbb{F}_q)$ and thus it does not divide ω_q. Hence, m_0 is also a multiple of ω_q, which means m_0P is $\mathcal{O}$ on $E(\mathbb{F}_q)$. Consequently, if m_0P also exists on the curve modulo N, we must have it also being $\mathcal{O}$ on the curve modulo N. Note that this implies that m_0P is also $\mathcal{O}$ modulo p. However, this contradicts with the earlier assumption that m_0 is not a multiple of ω_p. □

In the following two sections we will give an overview of the arguments made in Lenstra's paper to give an estimate on the running time of this algorithm, for more details and proofs see [1]. We will use the same notation and a similar structure as in the paper. The first part is about counting the number of elliptic curves over $\mathbb{F}_p$ up to isomorphism (weighted by the size of their automorphism class). Then a connection is made between the weighted number of elliptic curves over $\mathbb{F}_p$ with a specific number of points up to isomorphism and the Kronecker class numbers. After that, he discusses the weighted number of elliptic curves that have an order (not) divisible by a given prime using modular curves, which we will mention briefly.

The second section uses these results to give an approximation of the running time of the algorithm. The first part is about the probability that the algorithm succeeds in finding a non-trivial divisor with a random triple (a, x, y) and the boundaries mentioned in Theorem 4.1.4. This then leads to an estimate of the running time of the elliptic curve factoring algorithm. We will also give a comparison with the fastest factoring algorithm thus far, the General Number Field Sieve, which we mentioned earlier in Section 2.3.

4.2 Counting elliptic curves

The first point we want to highlight when we work on finite fields is the number of different elliptic curves over $\mathbb{F}_p$ up to isomorphism, where p is a prime greater than 3. Note that there are finite combinations for A and B in $\mathbb{F}_p$. This means there are finitely many different elliptic curves as they are represented by the equation $y^2 = x^3 + Ax + B$. Considering $\mathbb{F}_p$ has exactly p elements, we see that there are p^2 combinations for the pair (A, B). However, recall that we required that the discriminant is nonzero, i.e. $4A^3 + 27B^2 \neq 0$. Observe that $4A^3 + 27B^2 = 0$ if and only if $A = -3C^2$ and $B = 2C^3$ for some $C \in \mathbb{F}_p$. Note that $C = \frac{-3B}{2A}$ as long as $A \neq 0$, which means C is uniquely determined by A and B (if $A = 0$ then we must also have $B = C = 0$). Thus, there are $p^2 - p$ different equations to describe an elliptic curve over $\mathbb{F}_p$.

We will make clear what we mean when we say that two elliptic curves are isomorphic.

Definition 4.2.1 (Isomorphism)**.** Let K be a field and E_1, E_2 be two elliptic curves defined over K represented by the equations $y^2 = x^3 + A_1x + B_1$ and $y^2 = x^3 + A_2x + B_2$ respectively. An isomorphism $E_1 \to E_2$

(over K) is a nonzero element $u \in K$ such that

$$A_2 = u^4 A_1 \quad \text{and} \quad B_2 = u^6 B_1. \tag{4.1}$$

If such an isomorphism exists, then we call E_1 and E_2 isomorphic.

Observe that this is an equivalence relation, as K is a field and u is an element of K with a multiplicative inverse. Furthermore, $u : E_1 \to E_2$ induces a group isomorphism $E_1(K) \to E_2(K)$ which sends (x, y) to (u^2x, u^3y) and of course the point at infinity to itself. We will denote this group isomorphism with u as well.

Example 4.2.2. Let E be the elliptic curve over $\mathbb{F}_5$ defined by $y^2 = x^3 + x + 2$. Recall from Example 3.3.3 that $E(\mathbb{F}_5) = \{\mathcal{O}, (1, 2), (1, 3), (4, 0)\}$. Consider the elliptic curve E' over $\mathbb{F}_5$ represented by $y^2 = x^3 + x + 3$. We leave it to the reader to check that $E'(\mathbb{F}_5) = \{\mathcal{O}, (1, 0), (4, 1), (4, 4)\}$. Note that $1 \equiv 2^4 \cdot 1 \bmod 5$ and $3 \equiv 2^6 \cdot 2 \bmod 5$. We can see that E and E' are isomorphic. Furthermore, $2 \in \mathbb{F}_5^*$ maps $(1, 2), (1, 3)$ and $(4, 1)$ to $(4, 4), (4, 1)$ and $(1, 0)$ respectively. △

Remark 4.2.3. We mentioned in Section 3.1 the generalized Weierstrass equation, which is $y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$. In this case, two curves are isomorphic if and only if the coefficients of one of them can be written as u^ia_i, where a_i are the coefficients of the other one. This explains the numbering of the coefficients.

Let E be an elliptic curve over K. We want to determine how many $u \in K^*$ map E to itself.

Definition 4.2.4 (Automorphism)**.** Let E be an elliptic curve defined over the field K. An automorphism of E is an isomorphism $E \to E$. We will denote the set of automorphisms with $\mathrm{Aut}_K E$.

Remark 4.2.5. We know that -1 is always an automorphism, as every elliptic curve is symmetrical about the x-axis (when using the short Weierstrass equation). This automorphism sends (x, y) to $(x, -y)$.

Note that $\mathrm{Aut}_K E$ is a subgroup of K^*. Furthermore, if u is an automorphism, we have $A_2 = A_1$ and $B_2 = B_1$ in (4.1). Let E be an elliptic curve defined as $y^2 = x^3 + Ax + B$. From the fact that $\mathrm{Aut}_K E$ is a group and the equations in (4.1), we can deduce that the following holds:

- If $A = 0$ and K^* has an element of order 6, then $\#\mathrm{Aut}_K E = 6$.
- If $B = 0$ and K^* has an element of order 4, then $\#\mathrm{Aut}_K E = 4$.
- If none of the above holds, then $\mathrm{Aut}_K E = \{1, -1\}$, thus $\#\mathrm{Aut}_K E = 2$.

Example 4.2.6. Continuing Example 4.2.2, we see that $2 \notin \mathrm{Aut}_{\mathbb{F}_5} E$, as $E \neq E'$. Note that this also immediately implies that $3 \equiv -2 \bmod 5$ is not an automorphism of E either. We see that the automorphism class of E is $\{1, -1\}$, which is what we expected, since $A \neq 0$ and $B \neq 0$. △

The number of elliptic curves isomorphic to E (including E itself) is equal to

$$\frac{\#\mathbb{F}_p^*}{\#\mathrm{Aut}_K E} = \frac{p-1}{\#\mathrm{Aut}_K E}.$$

Recall that there are $p^2 - p = p(p - 1)$ elliptic curves in total. Thus, if we sum over a set of representatives of each isomorphism class, we get

$$\sum_E \frac{p-1}{\#\mathrm{Aut}_K E} = p(p-1).$$

We can divide both sides by $p - 1$. This gives us

$$\sum_E \frac{1}{\#\mathrm{Aut}_K E} = p,$$

where the sum ranges over all isomorphism classes. We will express the left side of the equation as

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p\}/ \cong_{\mathbb{F}_p},$$

which denotes "the weighted cardinality", i.e. the number of isomorphism classes with the isomorphism class of E being counted with $(\#\mathrm{Aut}_K E)^{-1}$. We will use this expression $\#'$ later on as well.

Example 4.2.7. We apply this to $\mathbb{F}_5$. Let $E_{A,B}$ be an elliptic curve over $\mathbb{F}_5$ defined by $y^2 = x^3 + Ax + B$. Note that this equation defines an elliptic curve for $A = 0$ if and only if $B \neq 0$ and vice versa. Hence, there are 4 elliptic curves $E_{0,B}$. As $\mathbb{F}_5^*$ clearly has no element of order 6, these elliptic curves all have automorphism classes $\{1, -1\}$. Thus, we get $\frac{4}{2} = 2$ isomorphism classes with $A = 0$.
Furthermore, since $\mathbb{F}_5^*$ has elements of order 4, $\#\mathrm{Aut}_{\mathbb{F}_5} E_{A,0} = 4$. Thus, their isomorphism classes only consist of one element. With the same argument as before, there are 4 different elliptic curves $E_{A,0}$. Therefore, we get 4 isomorphism classes with $B = 0$.
Lastly, if $A \neq 0$ and $B \neq 0$, there are exactly $4 \cdot 3 = 12$ unique elliptic curves $E_{A,B}$. As their automorphism class all consist of 2 elements, we get isomorphism classes of cardinality 2, thus $\frac{12}{2} = 6$ isomorphism classes. If we sum over all these classes with their respective weight, we get

$$2 \cdot \frac{1}{2} + 4 \cdot \frac{1}{4} + 6 \cdot \frac{1}{2} = 5,$$

which is exactly what we are supposed to find. △

Remark 4.2.8. Since most of the time $\#\mathrm{Aut}_K E = 2$, we can deduce that there are in total approximately $2p$ isomorphism classes. Hence, there are around $2p$ different elliptic curves on $\mathbb{F}_p$ up to isomorphism. A more precise number for different cases can be found using the different possible cardinalities of automorphism groups, see [1, Section 1.4].

A useful property to determine whether two elliptic curves are possibly isomorphic or not is the "j-invariant".

Definition 4.2.9 (j-invariant)**.** Let E be an elliptic curve defined over a field K by the equation $y^2 = x^3 + Ax + B$. The j-invariant of E is

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Note that the denominator is nonzero, since the discriminant of E is nonzero. One can prove that two elliptic curves E and E' are isomorphic over $\overline{K}$, the algebraic closure of K, if and only if $j(E) = j(E')$ in K, see [15, Section 2.7] and [18, Section III.1].
Let p be a prime. We say that an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) \equiv 1 \bmod p$, see [15, Section 4.6]. If it is not supersingular, we call them ordinary. Two ordinary elliptic curves E and E' over $\mathbb{F}_p$ are isomorphic over $\mathbb{F}_p$ if and only if $j(E) = j(E')$ and $|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)|$, see [19, Section 14C].

Example 4.2.10. Recall from Example 4.2.2 that E defined by $y^2 = x^3 + x + 2$ and E' defined by $y^2 = x^3 + x + 3$ are isomorphic over $\mathbb{F}_5$. Observe that $3 \equiv -2 \bmod 5$, thus $3^2 \equiv 2^2 \bmod 5$, which leads to $j(E) = j(E')$ in $\mathbb{F}_5$. A quick calculation shows $j(E) \equiv 1 \bmod 5$. Remember that in Example 4.2.7, we found that there are 12 isomorphism classes over $\mathbb{F}_5$. However, there are only 5 possible values for the j-invariant in $\mathbb{F}_5$. For example, the curve E'' defined by $y^2 = x^3 + 4x + 1$ also has j-invariant $j(E'') = 1$ meaning E and E'' are isomorphic over $\overline{\mathbb{F}}_5$. However, $E(\mathbb{F}_5)$ contains 4 points, whereas $E''(\mathbb{F}_5)$ has 8 points. △

Let p be a prime. Recall Theorem 3.3.4, which states that for a given elliptic curve E, there exists an integer t with $|t| \leq 2\sqrt{p}$ such that $\#E(\mathbb{F}_p)$. Now, let t be an integer satisfying $|t| \leq 2\sqrt{p}$. We will look at the weighted number of elliptic curves E over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - t$ up to isomorphism, i.e.

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p, \#E(\mathbb{F}_p) = p + 1 - t\} / \cong_{\mathbb{F}_p}.$$

The following formula is given by Deuring in his paper [20], also see [21, Section 4].

Theorem 4.2.11 (Deuring)**.** *Let $\#'$ denote the number of isomorphism classes with the class of an elliptic curve E being counted with $(\#Aut_K E)^{-1}$. Then the following equality holds:*

$$\#'\{E \mid E \textit{ elliptic curve over } \mathbb{F}_p, \#E(\mathbb{F}_p) = p + 1 - t\} \cong_{\mathbb{F}_p} = H(t^2 - 4p),$$

where $H(t^2 - 4p)$ is the Kronecker class number of $t^2 - 4p$.

We will define what these Kronecker class numbers, also called Hurwitz class numbers, are and give some context behind them. Note that in some literature, a weight of $\frac{2}{\#\mathrm{Aut}E}$ is used so that the number becomes twice as large as we define it here.

Firstly, we study some properties of "integral quadratic forms" in two variables, which are polynomials of the following form

$$f(x,y) = ax^2 + bxy + cy^2 \quad a,b,c \in \mathbb{Z}.$$

For details and proofs, see [22, Section 2], [19, Section 14D], [23] and [24, Section 14C and D]. Such a form is called "primitive" if $\gcd(a,b,c) = 1$. The "discriminant" of $ax^2 + bxy + cy^2$ is defined as $\Delta = b^2 - 4ac$. A form is called "positive definite" if $\Delta < 0$ and $a > 0$. We say that two forms $f(x,y) = a_1x^2 + b_1xy + c_1y^2$ and $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ are "(properly) equivalent" if there exists an isomorphism from f to g. In this case, an isomorphism means there is a matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$a_1x^2 + b_1xy + c_1y^2 = a_2\tilde{x}^2 + b_2\tilde{x}\tilde{y} + c_2\tilde{y}^2,$$

where $\tilde{x} = \alpha x + \beta y$ and $\tilde{y} = \gamma x + \delta y$, i.e. $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ with $\alpha\delta - \beta\gamma = 1$.

Example 4.2.12. Consider the discriminant $\Delta = -4$. One quadratic form with this disciminant is $f(x,y) = 13x^2 + 16xy + 5y^2$. Another form that is much simpler is $g(x,y) = x^2 + y^2$. Notice $f(x,y) = g(2x+y, 3x+2y)$. Furthermore, the determinant of the corresponding matrix is $2 \cdot 2 - 3 \cdot 1 = 1$. Therefore, these two forms are considered equivalent. △

An "automorphism" of a form f is an "isomorphism" form f to f. The set of automorphisms of a form f is a subgroup of $\mathrm{SL}(2,\mathbb{Z})$, which we will denote by $\mathrm{Aut}f$. We can make the following distinctions.

- If f is equivalent to $ax^2 + axy + ay^2$ for some positive integer a, then $\mathrm{Aut}f$ is cyclic of order 6. In this case $\Delta = -3a^2$.
- If f is equivalent to $ax^2 + ay^2$ for some positive integer a, then $\mathrm{Aut}f$ is cyclic of order 4. In this case $\Delta = -4a^2$.
- In all other cases, the group $\mathrm{Aut}f$ has two elements, namely the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

For a fixed negative integer Δ such that $\Delta \equiv 0 \bmod 4$ or $\Delta \equiv 1 \bmod 4$, there is a finite number of equivalence classes of forms of discriminant Δ, see [24, Section 2A]. From now on, we will work with these criteria on Δ.

Definition 4.2.13 (Kronecker class numbers)**.** The Kronecker class number $H(\Delta)$ of Δ denotes the weighted cardinality of the set of equivalence classes of forms of discriminant Δ. Here, weighted means similar as in $\#'$ earlier, i.e. the equivalence class of f is counted with weight $(\#\mathrm{Aut}f)^{-1}$. We express this as

$$H(\Delta) = \#'\{f : f \text{ integral quadratic form of discriminant } \Delta\}/\sim$$

with $\sim$ denoting the equivalence.

Remark 4.2.14. Note that for the cases where $\Delta \equiv 0 \bmod 4$ or $\Delta \equiv 1 \bmod 4$, there exists an integer b such that $b^2 \equiv \Delta \bmod 4$. This leads to the existence of the form $x^2 + bxy - \frac{\Delta - b^2}{4}y^2$, which has exactly discriminant Δ. Therefore, we always have $H(\Delta) > 0$ for $\Delta \equiv 0 \bmod 4$ and $\Delta \equiv 1 \bmod 4$.

The expression $h(\Delta)$ is used for the weighted number of primitive forms up to isomorphism of discriminant Δ. Here, each isomorphism class is again weighted by the automorphism group. Note that

$$H(\Delta) = \sum_{d \in D} h\left(\frac{\Delta}{d^2}\right), \tag{4.2}$$

where $D = \{d \in \mathbb{Z} \mid \frac{\Delta}{d^2} \in \mathbb{Z}_{<0}, \frac{\Delta}{d^2} \equiv 0 \bmod 4 \text{ or } \frac{\Delta}{d^2} \equiv 1 \bmod 4\}$. As D is nonempty, since $1 \in D$, and bounded, as $d^2 \leq \Delta$, we know there is a largest element d_0 in D. This d_0 is called the "conductor" of Δ

and $\frac{\Delta}{d_0^2}$ is called the "fundamental discriminant" associated with Δ. Observe that D consists of exactly the positive divisors of d_0.

To find some boundaries for H, we will use the analytic class number formula for $h(\Delta)$. Firstly, recall the "quadratic character" $\chi : \mathbb{Z}_{>0} \to \{0, 1, -1\}$ associated with Δ. For odd primes l, $\chi(l)$ is defined as the Legendre symbol $\left(\frac{\Delta}{l}\right)$. Furthermore, $\chi(2) = 0$ is defined for $\Delta = 0 \bmod 4$. For $\Delta \equiv 1 \bmod 4$, we distinguish the cases $\chi(2) = 1$ for $\Delta \equiv 1 \bmod 8$, and if $\Delta \equiv 5 \bmod 8$, then define $\chi(2) = -1$. Lastly, define $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}_{>0}$. In other words, for a given Δ, χ is defined as

- $\chi(l) = \Delta^{\frac{l-1}{2}} \bmod l$ for odd primes l.
- $\chi(2) = 0, 1, -1$ for $\Delta \equiv 0 \bmod 4$, $\Delta \equiv 1 \bmod 8$, $\Delta \equiv 5 \bmod 8$ respectively.
- $\chi(mn) = \chi(m)\chi(n)$ recursively for all $m, n \in \mathbb{Z}_{>0}$.

The analytic class number formula formula for $h(\Delta)$ is

$$h(\Delta) = \frac{\sqrt{-\Delta}}{2\pi} L(1, \chi), \tag{4.3}$$

where

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{for } s \in \mathbb{C},\ \operatorname{Re}(s) > 0.$$

Let χ_0 be the quadratic character associated to a negative discriminant Δ_0 with $\Delta_0 \equiv 0 \bmod 4$ or $\Delta_0 \equiv 1 \bmod 4$ that has conductor d_0. Then one can determine that

$$L(1, \chi) = L(1, \chi_0) \cdot \prod_{l \mid d_0} \left(1 - \frac{\chi_0(l)}{l}\right),$$

with l ranging over the prime divisors of d_0. We can combine the formulas (4.2) and (4.3) with the expression above. This leaves us with

$$H(\Delta) = \frac{\sqrt{-\Delta}}{2\pi} \cdot L(1, \chi_0) \cdot \psi(d_0), \tag{4.4}$$

where ψ is a function $\psi : \mathbb{Z}_{>0} \to \mathbb{R}$ defined by

- $\psi(l^k) = \frac{l - l^{-k}}{l-1}, 1, \frac{l+1-2l^{-k}}{l-1}$ for prime numbers l, $k \geq 0$ and $\chi_0(l) = 0, 1, -1$ respectively.
- $\psi(mn) = \psi(m)\psi(n)$ recursively for all coprime $m, n \in \mathbb{Z}_{>0}$.

Using the expression for $H(\Delta)$, we can formulate some lower and upper bounds for $H(\Delta)$. By [25, Theorem 328], some boundaries for $\psi(d_0)$ are

$$1 \leq \psi(d_0) \leq \left(\frac{d_0}{\phi(d_0)}\right) = \mathcal{O}((\log\log d_0)^2),$$

where $\phi(d_0)$ denotes the Euler ϕ-function. Furthermore, by [26, Section VI], we have

$$L(1, \chi_0) = \mathcal{O}(\log |\Delta_0|)$$

and there is an positive effectively computable constant c_1 such that for all $z \in \mathbb{Z}_{>1}$ there exists an integer $\Delta_z < -4$ with the property that if $|\Delta_0| \leq z$ and $\Delta_0 \neq \Delta_z$, then

$$L(1, \chi_0) \geq \frac{c_1}{\log z}. \tag{4.5}$$

We combine these boundaries with the formula in (4.4). This results in the existence of two effectively computable constants c_2 and c_3 such that for each $z \in \mathbb{Z}_{>1}$, there exists a $\Delta_z < -4$ such that

$$\frac{c_2\sqrt{-\Delta}}{\log z} \leq H(\Delta) \leq c_3 \cdot \sqrt{-\Delta} \cdot \log|\Delta| \cdot (\log\log|\Delta|)^2 \tag{4.6}$$

for all such that $\Delta \in \mathbb{Z}$ with $-z \leq \Delta < 0$, $\Delta \equiv 0 \bmod 4$ or $\Delta \equiv 1 \bmod 4$, and $\Delta \neq \Delta_z$. This leads to the following proposition by using the formula in Theorem 4.2.11 and filling in $\Delta = t^2 - 4p$ in (4.6).

Proposition 4.2.15. *There exist effectively computable positive constants c_4, c_5 such that for each prime number $p > 3$ the following assertions are valid.*

- *If S is a set of integers s with $|s - (p+1)| \leq 2\sqrt{p}$, then*

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p,\ \#E(\mathbb{F}_p) \in S\}/\cong_{\mathbb{F}_p} \leq c_4 \cdot \#S \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

- *If S is a set of integers s with $|s - (p+1)| \leq \sqrt{p}$, then*

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p,\ \#E(\mathbb{F}_p) \in S\}/\cong_{\mathbb{F}_p} \geq c_5 \cdot (\#S - 2) \cdot \frac{\sqrt{p}}{\log p}.$$

Here, $\#'$ denotes the weighted cardinality of the set of isomorphism classes weighted by their automorphism group.

Proof. The left-hand side in both assertions is equal to

$$\sum_{t,p+1-t \in S} H(t^2 - 4p)$$

by Theorem 4.2.11. The first inequality follows immediately from the inequalities in (4.6). For the second assertion, we fill in $z = 4p$ in (4.6). Observe that $|t^2 - 4p| \leq 3p$ if $p + 1 - t \in S$, since that implies $|t| \leq \sqrt{p}$. Furthermore, t with $|t| \leq \sqrt{p}$ such that the fundamental discriminant associated with $t^2 - 4p$ is Δ_z is unique up to sign, with Δ_z as in the condition in (4.5). This can be deduced by considering the polynomial $x^2 - tx + p$ in $\mathbb{Q}(\sqrt{\Delta_z})$ and noticing that $t = \alpha + \overline{\alpha}$, where α and $\overline{\alpha}$ are the roots of the polynomial. These roots are unique up to sign and conjugation. For more details, see [1, Section 1.9]. □

Corollary 4.2.16. *There exists a positive effictively computable constant c_6 such that for every prime integer $p > 3$ the following statement holds. Let S be a set of integers s with $|s - (p+1)| \leq \sqrt{p}$. Denote by m the number of triples $(A, x_P, y_P) \in \mathbb{F}_p^3$ for which $4A^3 + 27B^2 \neq 0$ and $\#E(\mathbb{F}_p) \in S$, where $B = y_P^2 - x_P^3 - Ax_P$ and $E(\mathbb{F}_p)$ is the elliptic curve $y^2 = x^3 + Ax + B$. Then the following inequality holds*

$$m \geq c_6 \cdot (\#S - 2) \cdot p^{\frac{5}{2}} \cdot (\log p)^{-1}.$$

Proof. The described number m is precisely the number of quadruples $(A, B, x_P, y_P) \in \mathbb{F}_p$ such that $y^2 = x^3 + Ax + B$ defines an elliptic curve E over $\mathbb{F}_p$ of order $\#E(\mathbb{F}_p) \in S$ and with point $P = (x_P, y_P)$ on it. Recall that the number of elliptic curves isomorphic to a given elliptic curve E is exactly $(p-1)(\#\mathrm{Aut}_{\mathbb{F}_p}E)^{-1}$. Furthermore, every elliptic curve E has $\#E(\mathbb{F}_p) - 1$ affine points, i.e. $\#E(\mathbb{F}_p) - 1$ different combinations of (x_P, y_P) with $x_P, y_P \in \mathbb{F}_p$. Hence, m must equal

$$\sum_E \frac{(p-1) \cdot (\#E(\mathbb{F}_p) - 1)}{\#\mathrm{Aut}_{\mathbb{F}_p}E},$$

where the summation ranges over the elliptic curves E over $\mathbb{F}_p$ up to isomorphism, for which $\#E(\mathbb{F}_p) \in S$. By Theorem 3.3.4, we know $\#E(\mathbb{F}_p) - 1 \geq p - 2\sqrt{p}$. Thus, using Proposition 4.2.15, we get

$$m \geq (p-1) \cdot (p - 2\sqrt{p}) \cdot c_5 \cdot (\#S - 2) \cdot \frac{\sqrt{p}}{\log p}.$$

This satisfies the statement for a suitable choice c_6. □

Lastly, we are also interested in the weighted number of elliptic curves that have a number of points divisible by a given prime l.

Consider two pairs (E_1, P_1) and (E_2, P_2), where E_1 and E_2 are both elliptic curves over $\mathbb{F}_p$ that contain the point P_1 and P_2 respectively with both points having prime order $l \neq p$. We consider these two pairs equivalent if there exists an isomorphism $u : E_1 \to E_2$ over $\mathbb{F}_p$, as in Definition 4.2.1, such that $u(P_1) = P_2$. If E_1 and E_2 are both ordinary, this means that (E_1, P_1) and (E_2, P_2) are equivalent if and only if E_1 and E_2 have the same j-invariant, the same number of points and P_1 and P_2 have the same order. The set of the resulting equivalence classes are denoted by $Z_1(l)(\mathbb{F}_p)$. If we allow E_1 and E_2 to be isomorphic over $\overline{\mathbb{F}}_p$, i.e. E_1 and E_2 not necessarily having the same number of points with coordinates in $\mathbb{F}_p$, while still mapping P_1 to P_2, we obtain a different equivalence relation. We will denote the set of these equivalence classes by $Y_1(l)(\mathbb{F}_p)$.

Additionally, let $p \equiv 1 \bmod l$ and a $\zeta \in \mathbb{F}_p$ be a l-th root of unity. We consider triples of the form (E, P, Q) with E and P as before and Q another point on $E(\mathbb{F}_p)$ of order l such that $e_l(P, Q) = \zeta$, where e_l denotes the Weil pairing, see [18, Section III.8] and [15, Section 3.3 and 11.2]. As before, it is possible to define an equivalence between triples (E_1, P_1, Q_1) and (E_2, P_2, Q_2) with the additional requirement that Q_1 is mapped to Q_2 by the isomorphism. As above, we will denote the sets of equivalence classes over $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$ by $Z(l)(\mathbb{F}_p)$ and $Y(l)(\mathbb{F}_p)$, respectively.

Note that there are obvious surjections $Z_1(l)(\mathbb{F}_p) \to Y_1(l)(\mathbb{F}_p)$ and $Z(l)(\mathbb{F}_p) \to Y(l)(\mathbb{F}_p)$, since an isomorphism over $\mathbb{F}_p$ implies an isomorphism over $\overline{\mathbb{F}}_p$ in this case. To determine the weighted number of elliptic curves up to isomorphism, which follows from finding the cardinalities of $Y_1(l)(\mathbb{F}_p)$ and $Y(l)(\mathbb{F}_p)$, we need some knowledge on the modular curves $X(l)$ and $X_1(l)$. For details and proofs, see [18, Appendix C11-13], [1, Sections 1.10-1.15] and [19, Section 14D]. The modular curves $X(l)$ and $X_1(l)$ have some useful properties. The ones that we will use are the following.

- $X_1(l)$ and $X(l)$ are complete non-singular irreducible curves defined over $\mathbb{F}_p$.
- The genus of $X_1(l)$ and $X(l)$ both equal 0 for $l = 2, 3$ and $l = 2$ respectively. For $l \geq 5$, the genus of $X_1(l)$ is equal to $1 + \frac{1}{24}(l-1)(l-11)$ and for $l \geq 3$, the genus of $X(l)$ is equal to $1 + \frac{1}{24}(l^2-1)(l-6)$.
- The sets $Y_1(l)(\mathbb{F}_p)$ and $Y(l)(\mathbb{F}_p)$ can be viewed as subsets of $X_1(l)(\mathbb{F}_p)$ and $X(l)(\mathbb{F}_p)$ respectively.
- The cardinalities of the complement of $Y_1(l)(\mathbb{F}_p)$ in $X_1(l)(\mathbb{F}_p)$ and the complement of $Y(l)(\mathbb{F}_p)$ in $X(l)(\mathbb{F}_p)$ are both bounded from above by the number of cusps of $X_1(l)$ and $X(l)$ respectively. For $l = 2$, the numbers of cusps of $X_1(l)$ and $X(l)$ are equal to 2 and 3 respectively. For $l > 2$, these numbers are $l - 1$ and $\frac{l^2-1}{2}$ respectively.

The Hasse-Weil bound states an upper bound for the cardinality of a complete non-singular irreducible curve C of genus g defined over $\mathbb{F}_p$. The cardinality of $C(\mathbb{F}_p)$ satisfies

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

For proof, see [27, Section 3.1]. We can apply this to $X_1(l)$ and $X(l)$ so that we get

$$\#Y_1(l)(\mathbb{F}_p) = p + \mathcal{O}(l^2\sqrt{p}),$$
$$\#Y(l)(\mathbb{F}_p) = p + \mathcal{O}(l^3\sqrt{p}).$$

After finding these bounds, Lenstra proves a lemma in his paper, for more details see [1, Section 1.13]. It tells us the following. The number of elements of $Z_1(l)(\mathbb{F}_p)$ that gets mapped by the aforementioned surjection to the class of $Y_1(l)(\mathbb{F}_p)$ is equal to the number of automorphisms of E that send P to P. He proves this by determining the conditions that two pairs (E_1, P_1) and (E_2, P_2) are are the same element in $Y_1(l)(\mathbb{F}_p)$ and $Z_1(l)(\mathbb{F}_p)$. That is, if $(A_1, B_1, x_1, y_1) = (u^4A_2, u^6B_2, u^3x_2, u^2y_2)$ for some $u \in \overline{\mathbb{F}}_p$, possibly $u \in \mathbb{F}_p$. Using this, he notes that the sought-after number is the index of two specific sets regarding those isomorphisms and continues to find the cardinalities of those sets. A very similar statement and proof can be made regarding $Y(l)(\mathbb{F}_p)$ and $Z(l)(\mathbb{F}_p)$ and the automorphisms that send P to P and Q to Q. Using this lemma and some previous results, the following proposition can be determined. For the proof, we refer to [1, Section 1.14]

Proposition 4.2.17. *Let p and l be primes such that $p > 3$ and $l \neq p$. Then the weighted number of elliptic curves of order divisible by l up to isomorphism has the following upper bounds.*

$$\#'\{E \mid E \textit{ elliptic curve over } \mathbb{F}_p,\, \#E(\mathbb{F}_p) \equiv 0 \bmod l\}/\cong_{\mathbb{F}_p} = \begin{cases} \frac{1}{l-1}p + \mathcal{O}(l\sqrt{p}) & \textit{if } p \not\equiv 1 \bmod l \\ \frac{l}{l^2-1}p + \mathcal{O}(l\sqrt{p}) & \textit{if } p \equiv 1 \bmod l. \end{cases}$$

Remark 4.2.18. Recall that at the start of this subsection, we found that

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p\}/\cong_{\mathbb{F}_p} = p.$$

Let E be a random elliptic curve over $\mathbb{F}_p$ and fix a prime l different from p. Notice that by Proposition 4.2.17 if p tends to infinity, the probability that the order of E is divisible by l tends to $\frac{1}{l-1}$ and $\frac{l}{l^2-1}$ for $p \equiv 1 \bmod l$ and $p \not\equiv 1 \bmod l$ respectively.

Applying previous results, we can determine a boundary for the weighted number of elliptic curves that have an order that is not divisible by l.

Proposition 4.2.19. *There exists a positive effectively computable constant c_7 such that for all pairs of primes (p, l) with $p > 3$ we have*

$$\#'\{E \mid E \textit{ elliptic curve over } \mathbb{F}_p,\, \#E(\mathbb{F}_p) \not\equiv 0 \bmod l\}/\cong_{\mathbb{F}_p} \geq c_7 p.$$

Proof. We know that

$$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p\}/\cong_{\mathbb{F}_p} = p.$$

Thus, by Proposition 4.2.17, the left-hand side is equal to

$$\begin{aligned} &\frac{l-2}{l-1}p + \mathcal{O}(l\sqrt{p}) && \text{for } p \not\equiv 1 \bmod l, \\ &\frac{l^2-l-1}{l^2-1}p + \mathcal{O}(l\sqrt{p}) && \text{for } p \equiv 1 \bmod l. \end{aligned}$$

In both cases, the coefficient of p is non-negative for all $l \geq 2$. Therefore, if l is bounded from above by $c_8\sqrt{p}$ for a appropriate constant c_8, we find the desired lower bound. This is due to $\mathcal{O}(l\sqrt{p})$ implying the possibility that the coefficient of $l\sqrt{p}$ could be negative.
We can apply Proposition 4.2.15, where S is the set containing the integers in the interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ that are divisible by l. This set S has cardinality $\mathcal{O}(1 + \sqrt{p} \cdot l^{-1})$. We consider a two cases.

1. By Proposition 4.2.15, we know that

   $$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p,\, \#E(\mathbb{F}_p) \equiv 0 \bmod l\}/\cong_{\mathbb{F}_p} \leq c_4(1 + \sqrt{p} \cdot l^{-1}) \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

   Hence,

   $$\#'\{E \mid E \text{ elliptic curve over } \mathbb{F}_p,\, \#E(\mathbb{F}_p) \not\equiv 0 \bmod l\}/\cong_{\mathbb{F}_p} \geq p - c_4(1 + \sqrt{p} \cdot l^{-1}) \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

   Therefore, if $p \geq c_9$ and $l \geq c_{10}(\log p)(\log\log p)^2$ for appropriate positive constants c_9 and c_{10}, the proposition holds.

2. In the other cases, where $p < c_9$ or $c_{10}(\log p)(\log\log p)^2 \geq c_8\sqrt{p}$, we can see that p is bounded. Recall Theorem 4.2.11 and Remark 4.2.14. For both $t = 0$ and $t = -1$, we have $H(t^2 - 4p) > 0$. Thus, by Deuring's theorem, there exist elliptic curves over $\mathbb{F}_p$ of order $p+1$ and elliptic curves of order p. We know that l cannot be a divisor of both p and $p+1$, thus we can choose c_6 in Proposition 4.2.19 small enough, e.g. $\frac{1}{p}$, so that the proposition holds.

□

This leads to a similar point made in Corollary 4.2.16 with similar proof.

Corollary 4.2.20. *There exists an effectively computable constant c_{11} such that for every prime number $p > 3$ the following holds. Let l be any prime number. Then the number of triples $(A, x_P, y_P) \in \mathbb{F}_p^3$ for which $y^2 = x^3 + Ax + B$ defines an elliptic curve of order not divisible by l, where $B = y_P^2 - x_P^3 - Ax_P$, is at least $c_{11}p^3$.*

Proof. The proof of Corollary 4.2.16 also applies to this corollary. A similar argument made at the start of the proof of Corollary 4.2.16 gives that the left-hand side equals the same summation

$$\sum_E \frac{(p-1) \cdot (\#E(\mathbb{F}_p) - 1)}{\#\mathrm{Aut}_{\mathbb{F}_p} E}.$$

In this case S is the set of integers divisible by l, which has cardinality $\mathcal{O}(1 + \sqrt{p} \cdot l^{-1})$ as mentioned earlier. Furthermore, instead of Proposition 4.2.15, it uses Proposition 4.2.19. This means this summation is at least

$$(p-1)(p - \sqrt{p}) \cdot c_7 p,$$

which proves required lower bound for a suitable constant c_{11}. □

With these results, we can determine the probability that Lenstra's algorithm succeeds given a random triple (A, x_P, y_P). This then leads into the running time of the algorithm in the worst case scenario.

4.3 Running time estimate

In this part, we will give an overview of the arguments Lenstra uses in the second part [1, Sections 2.6-2.10] to determine the running time of this algorithm using the previous results, in particular Corollary 4.2.16 and Corollary 4.2.20. Furthermore, with the boundaries in Theorem 4.1.4, one can determine the following.

Theorem 4.3.1. *There exists a positive, effectively computable constant c_{12} with the following property. Let N, v, w be integers greater than 1 such that N has at least two distinct prime divisors greater than 3 and such that the smallest prime divisor $p > 3$ of N satisfies $p \leq v$. Let S be the set of integers s in the interval $(p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$ such that the largest prime divisor of s is at most w. In other words,*

$$S = \{s \in \mathbb{Z} \mid |s - (p+1)| \leq \sqrt{p}, \text{ and each prime divisor of } s \text{ is equal to or smaller than } w\}.$$

Then the number n of triples $(A, x_P, y_P) \in (\mathbb{Z}/N\mathbb{Z})^3$ for which Lenstra's algorithm finds a non-trivial divisor of N satisfies

$$\frac{n}{N^3} > \frac{c_{12}}{\log p} \cdot \frac{\#S - 2}{2\lfloor\sqrt{p}\rfloor + 1}.$$

Remark 4.3.2. The probability that a random integer s in the interval $(p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$ has all its prime divisors $\leq w$ is equal to $\frac{\#S}{2\lfloor\sqrt{p}\rfloor+1}$, while the probability the algorithm finds a non-trivial divisor of N with a random triple (A, x_P, y_P) is on the left-hand side, $\frac{n}{N^3}$. Hence, the theorem implies that the latter is at least close to the same order of magnitude as the former.

Proof. Let p and q be distinct prime divisors of N such that $p, q > 3$. We use the notation $E_{A,B}$ for the elliptic curve defined by the equation $y^2 = x^3 + Ax + B$. For each $s \in S$, define

$$T_s = \{(\alpha_p, \xi_p, \eta_p) \in \mathbb{F}_p^3 \mid \#E_{\alpha_p,\beta_p}(\mathbb{F}_p) = s, \text{ where } \beta_p = \eta_p^2 - \xi_p^3 - \alpha_p\xi_p\}.$$

For each triple $(\alpha_p, \xi_p, \eta_p) \in T_s$, let $l_{\alpha_p,\xi_p,\eta_p}$ denote the order of the point (ξ_p, η_p) in $E_{\alpha_p,\beta_p}(\mathbb{F}_p)$. Furthermore, for each triple $(\alpha_p, \xi_p, \eta_p) \in T_s$, let $U_{\alpha_p,\xi_p,\eta_p}$ denote the set

$$U_{\alpha_p,\xi_p,\eta_p} = \{(\alpha_q, \xi_q, \eta_q) \in \mathbb{F}_q^3 \mid \#E_{\alpha_q,\beta_q}(\mathbb{F}_q) \not\equiv 0 \bmod l_{\alpha_p,\xi_p,\eta_p}, \text{ where } \beta_q = \eta_q^2 - \xi_q^3 - \alpha_q\xi_q\}.$$

We use the expression $V_{\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q}$ for the set of triples $(A, x, y) \in (\mathbb{Z}/N\mathbb{Z})^3$ such that the following congruences hold.

$$(A \bmod p, x \bmod p, y \bmod p) = (\alpha_p, \xi_p, \eta_p),$$
$$(A \bmod q, x \bmod q, y \bmod q) = (\alpha_q, \xi_q, \eta_q).$$

Recall Theorem 4.1.4 and note that each triple in $V_{\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q}$ satisfies the conditions in the theorem for the earlier specified $\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q$. Thus, if Lenstra's algorithm uses one of these triples, it will succeed in finding a non-trivial divisor of N. Hence,

$$n \geq \sum_{s\in S} \sum_{(\alpha_p,\xi_p,\eta_p)\in T_s} \sum_{(\alpha_q,\xi_q,\eta_q)\in U_{\alpha_p,\xi_p,\eta_p}} \#V_{\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q}.$$

Clearly, for each combination of $\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q$, the set $V_{\alpha_p,\xi_p,\eta_p,\alpha_q,\xi_q,\eta_q}$ consists of $N^3(pq)^{-3}$ elements. Furthermore, by Corollary 4.2.20 we know that for a given triple (α_p,ξ_p,η_p), it holds that $\#U_{\alpha_p,\xi_p,\eta_p} \geq c_{11}q^3$. This leads to

$$\frac{n}{N^3} \geq c_{11} \sum_{s\in S} \frac{\#T_s}{p^3}.$$

Now, we can apply Corollary 4.2.16 for our specified set S. Notice that

$$\sum_{s\in S} \#T_s = m,$$

with m as in the corollary. Hence, we get

$$\frac{n}{N^3} \geq c_{10}c_6(\#S-2)p^{-\frac{1}{2}}(\log p)^{-1},$$

which proves the theorem for a suitable constant c_{12}. □

When describing Lenstra's algorithm, we mentioned that if the algorithm did not succeed in finding a non-trivial divisor of N with a given triple (A, x_P, y_P), we could try it with a triple that is different modulo N. Suppose we can generate random triples $(A, x_P, y_P) \in (\mathbb{Z}/N\mathbb{Z})$ with each individual triple having equal probability and that each iteration is independent of each other. Then, with the theorem above we can determine the following.

Corollary 4.3.3. *There exists an effectively computable constant $c_{13} > 1$ with the following property. Let N and v be integers greater than 1 such that N has at least two distinct prime factors greater than 3 and such that the smallest prime divisor of N that is greater than 3 is at most v. Furthermore, let w be an integer greater than 1 such that the set S defined by*

$$S = \{s \in \mathbb{Z} \mid |s-(p+1)| \leq \sqrt{p}, \text{ and each prime divisor of } s \text{ is smaller than or equal to } w\}$$

satisfies $\#S \geq 3$. Moreover, let $f(w) = \#S(2\lfloor\sqrt{p}\rfloor+1)^{-1}$ denote the probability that a random integer in the interval $(p+1-\sqrt{p}, p+1+\sqrt{p})$ does not have a prime divisor greater than w. Then for any integer $h > 1$, the probability that the algorithm with boundaries v and w succeeds in finding a non-trivial divisor of N after h iterations is at least $1 - c_{13}^{-hf(w)/\log v}$.

Proof. Observe that the probability does not find a non-trivial divisor after h applications of the algorithm is $(1-n/N^3)^h$, where n is the number of triples for which the algorithm succeeds, as Theorem 4.3.1. By this theorem, we know that

$$\frac{n}{N^3} > \frac{c_{12}}{\log p} \cdot \frac{\#S-2}{2\lfloor\sqrt{p}\rfloor+1} \geq \frac{c_{12}}{3\log v} \cdot f(w).$$

Hence, the probability of the algorithm not succeeding has upper bound

$$\left(1-\frac{n}{N^3}\right)^h \leq e^{\frac{-hc_{12}f(w)}{3\log v}}.$$

We conclude that for a suitable constant c_{13}, the statement holds. □

Given this result, we want to find a way to manipulate the values v, w and h so that the running time is minimal and the probability of success is fairly high. By Corollary 4.3.3, the value for h should be of the same order of magnitude as $\frac{\log v}{f(w)}$ to have a reasonable chance of success. To determine appropriate values for v and w, we firstly discuss the running time.
We assume the algorithm tries to determine m times a point, where m is the number described in Theorem 4.1.4. Notice that $\log m = \mathcal{O}(w \log v)$. We denote $M(N)$ as the complexity of a single addition on an elliptic curve modulo N using the extended Euclidean algorithm. Then an upper bound would be $M(N) = \mathcal{O}((\log N)^2)$. The expected running time of one iteration of Lenstra's algorithm without accounting for generating a random triple is of $\mathcal{O}(w \log v M(N))$. Thus, for $h = \frac{\log v}{f(w)}$ iterations, we get $\mathcal{O}(\frac{w}{f(w)}(\log v)^2 M(N))$. We would like to choose w so that $\frac{w}{f(w)}$ is minimal.
At this point, Lenstra refers in his paper to a result from Canfield, Erdös and Pomerance [28, Section 3], which implies the following. Let α be a positive integer. The probability that the biggest prime factor a random positive integer $s \leq x$ is at most $L(x)^\alpha = e^{\alpha\sqrt{\log x \log\log x}}$ approaches $L(x)^{(-1/(2\alpha)+o(1))}$ for $x \to \infty$. Here $o(1)$ is any function that goes to 0 as $x \to \infty$, as in the L-notation we mentioned at the start of Section 2.3. Lenstra conjectures that the same result holds for a random integer s in the interval $(x+1-\sqrt{x}, x+1+\sqrt{x})$. In other words, if we put $x = p$, then with our previous definition of $f(w)$ and a fixed positive integer α

$$f(L(p)^\alpha) = L(p)^{-\frac{1}{2\alpha}+o(1)} \quad \text{for } p \to \infty.$$

This results in

$$\frac{w}{f(w)} = L(p)^{\frac{1}{2\alpha}+\alpha+o(1)} \quad \text{for } p \to \infty,$$

suggesting the optimal choice for w as

$$w = L(p)^{\frac{1}{\sqrt{2}}+o(1)} \quad \text{for } p \to \infty.$$

However, as we do not know the smallest prime divisor p of N that is greater than 3 beforehand, we can try replacing p with v. Note that $\log v$ is of order $L(v)^{o(1)}$. Hence, $\frac{w}{f(w)}(\log v)^2$ is of the same order as $\frac{w}{f(w)}$, i.e. $L(v)^{\frac{1}{2\alpha}+\alpha+o(1)}$.

This leads into the following conjecture regarding the running time of the algorithm. Let N be a composite number and g be any positive integer. With probability of at least $1 - e^{-g}$, Lenstra's algorithm with appropriate values for v, w, h finds a non-trivial divisor of N within time

$$ge^{\sqrt{(2+o(1))\log p \log\log p}}M(N),$$

where p is the smallest prime divisor greater than 3 of N and $M(N) = \mathcal{O}(\log N)^2$. In the worst case scenario, N is made up of two primes of equal size, i.e. two primes of the same order of magnitude as $\sqrt{N}$. Asymptotically, this is then equal to

$$e^{(1+o(1)\sqrt{\log N \log\log N}}, \quad \text{for } N \to \infty.$$

With the L-notation, this is $L_N[\frac{1}{2}, 1]$, which corresponds to a sub-exponential running time.

We finish this thesis with a short comparison with the Number Field Sieve. Recall from Section 2.3 that the running time of the NFS is

$$e^{\left(\frac{64}{9}\right)^{\frac{1}{3}}(\log N)^{\frac{1}{3}}(\log\log(N))^{\frac{2}{3}}}.$$

This is slightly faster than Lenstra's algorithm in the worst case. However, Lenstra's algorithm has the advantage that is a lot faster if N does have a small prime factor, since then the algorithm will find a non-trivial divisor earlier in the computations. Furthermore, an advantage Lenstra mentions in his paper [1, Section 2.11] is that the elliptic curve factoring method only requires $\mathcal{O}(\log N)$ memory, while the memory required for the Number Field Sieve is $L_N[\frac{1}{3}, \frac{c}{2}]$, as described in [11].

References

[1] H. W. Lenstra. “Factoring Integers with Elliptic Curves”. In: *Annals of Mathematics* 126.3 (1987), pp. 649–673. ISSN: 0003486X. URL: http://www.jstor.org/stable/1971363.

[2] Daniel Bernstein et al. “ECM using Edwards curves”. In: *Mathematics of Computation* 82.282 (2013), pp. 1139–1179.

[3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[4] Carl Pomerance. “The Quadratic Sieve Factoring Algorithm”. In: *Advances in Cryptology*. Ed. by Thomas Beth, Norbert Cot, and Ingemar Ingemarsson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 169–182. ISBN: 978-3-540-39757-1. DOI: 10.1007/3-540-39757-4_17.

[5] Arjen K. Lenstra and Hendrik W. Jr. Lenstra. *The development of the number field sieve*. 1st ed. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1993. ISBN: 978-3-540-57013-4. DOI: 10.1007/BFb0091534.

[6] John M Pollard. “Theorems on factorization and primality testing”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 76. 3. Cambridge University Press. 1974, pp. 521–528.

[7] Tom M. Apostol. *Introduction to analytic number theory*. 1st ed. Undergraduate Texts in Mathematics. Springer, New York, 1976, p. 13. DOI: 10.1007/978-1-4757-5579-4.

[8] Arjen K. Lenstra. “Integer Factoring”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 611–618. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_455.

[9] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. 2nd ed. Undergraduate Texts in Mathematics. Springer, New York, NY, 2014. DOI: 10.1007/978-1-4939-1711-2.

[10] Lindsay N. Childs. *A Concrete Introduction to Higher Algebra*. 3rd ed. Undergraduate Texts in Mathematics. Springer, New York, NY, 1979. DOI: 10.1007/978-0-387-74725-5.

[11] Alexander Kruppa and Paul Leyland. “Number Field Sieve for Factoring”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 862–867. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_465.

[12] Arjen K. Lenstra. “L Notation”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 709–710. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_459.

[13] M. Hohenwarter et al. *GeoGebra*. version: 6.0.507.0-w. Oct. 2018. URL: http://www.geogebra.org/.

[14] Darrel Hankerson and Alfred Menezes. “Elliptic Curves”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 408–410. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_244.

[15] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2nd ed. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, 2008. ISBN: 9781420071467.

[16] Thomas Browning. *Lenstra Elliptic Curve Factorization*. Tech. rep. University of Washington: Department of Mathematics, June 2016. URL: https://sites.math.washington.edu/~morrow/336_16/2016papers/thomas.pdf.

[17] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. 2nd ed. Undergraduate Texts in Mathematics. Springer, Cham, 2014. DOI: 10.1007/978-3-319-18588-0.

[18] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics. Springer, New York, NY, 2009. DOI: 10.1007/978-0-387-09494-6.

[19] “Additional Topics”. In: *Primes of the Form x2 + ny2*. John Wiley & Sons, Ltd, 2013. Chap. 4, pp. 283–333. ISBN: 9781118400722. DOI: 10.1002/9781118400722.ch4.

[20] Max Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14.1 (Dec. 1941), pp. 197–272. ISSN: 1865-8784. DOI: 10.1007/BF02940746.

[21] William C. Waterhouse. “Abelian varieties over finite fields”. In: *Annales scientifiques de l’École normale supérieure*. Vol. 2. 4. 1969, pp. 521–560.

[22] “From Fermat to Gauss”. In: *Primes of the Form x2 + ny2*. John Wiley & Sons, Ltd, 2013. Chap. 1, pp. 7–85. ISBN: 9781118400722. DOI: 10.1002/9781118400722.ch1.

[23] Z.I. Borevich and I.R. Shafarevich. “Teoriya chisel: 3-e izd”. In: *M.: Nauka* (1985).

[24] David A. Cox. *Primes of the form* $x^2 + ny^2$. 2nd ed. Graduate Texts in Mathematics. Springer, New York, NY, 1987. DOI: 10.1007/978-1-4612-4752-4.

[25] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers*. 4th ed. Oxford University Press, 1960.

[26] K. Prachar. *Primzahlverteilung*. Grundlehren Math. Wiss 91. Springer-Verlag, Berlin, 1957.

[27] G.V. Shabat. “Curves with many points”. PhD thesis. University of Amsterdam, Korteweg-de Vries Institute, Feb. 2001. URL: https://pure.uva.nl/ws/files/3265182/16638_Thesis.pdf.

[28] E.R Canfield, Paul Erdös, and Carl Pomerance. “On a problem of Oppenheim concerning “factorisatio numerorum””. In: *Journal of Number Theory* 17.1 (1983), pp. 1–28. ISSN: 0022-314X. DOI: 10.1016/0022-314X(83)90002-1.