Distribution Agreement

In presenting this thesis as a partial fulfillment of the requirements for a degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter now, including display on the World Wide Web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Andrew Wilson April 17, 2017

Primality Testing and Integer Factorization Using Elliptic Curves by

Andrew Wilson

Ken Ono
Adviser

Department of Mathematics and Computer Science

Ken Ono
Adviser

James Nagy
Committee Member

Jed Brody
Committee Member

2017

Primality Testing and Integer Factorization Using Elliptic Curves by

Andrew Wilson

Ken Ono
Adviser

An abstract of a thesis submitted to the Faculty of Emory College of Arts and Sciences of Emory University in partial fulfillment of the requirements of the degree of Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2017

Abstract

Primality Testing and Integer Factorization Using Elliptic Curves

By Andrew Wilson

Testing integers for primality and factoring large integers is an extremely important subject for our daily lives. Every time we use a credit card to make online purchases we are relying on the difficulty of factoring large integers for the security of our personal information. Similar encryption methods are used by governments around the world to protect their classified information, stressing the importance of the subject of primality testing and factoring algorithms to both personal and national security. Elementary number theory has been a key tool in the foundation of primality testing and factoring algorithms, specifically the work of Euler and Fermat, whose developments on modular arithmetic give us key tools that we still use today in the more complex primality tests and factoring methods. More recently people have used deeper ideas from geometry, namely elliptic curves, to develop faster tests and algorithms. In this thesis we continue this trend, and develop new primality tests that utilize previous theory of elliptic curves over finite fields. The primary point is that the points on these curves form a special group, which breaks down when working over $\mathbb{Z}/N\mathbb{Z}$, when N is not prime. Our theorems make use of the work of Kubert, Hasse, Mazur, and many more to yield a primality test that gives no false positives.

Primality Testing and Integer Factorization Using Elliptic Curves by

Andrew Wilson

Ken Ono
Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences of
Emory University in partial fulfillment of the requirements of the degree of
Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2017

Contents

1 Introduction and Statement of Results

Number theory is a branch of Mathematics with a wide scope of topics, including, but not limited to, the study of primes, divisibility, and factoring. One of the most famous developments in abstract modern number theory was the proof of Fermat's Last Theorem by Andrew Wiles. Fermat's Last Theorem says that if a, b, and c are integers, then there are no solutions to the equation $a^n + b^n = c^n$ for $n > 2$. Wiles's proof made use of elliptic curves, but with a completely different goal in mind. We will focus more on applied number theory, specifically on the theory of elliptic curves and their applications to primality testing and factoring.

The seemingly simple task of determining if a number is prime or not, and factoring large numbers turns out to be extremely difficult to complete in a reasonable amount of time. Much of modern internet security and cryptography utilizes the difficulty of the factoring problem. The most commonly used encryption systems is called RSA, named after its creators Ron Rivest, Adi Shamir, and Len Adleman [5]. The fundamental security of the encryption system is based on the fact that even if someone knows a large number is the product of two distinct large primes, it is still difficult to find those primes in a reasonable amount of time, as we see in Section 2.1. This is where the theory of elliptic curves comes in. Some of the fastest methods currently used to factor large composite numbers, or test for primaility are based on the abstract theory of points on elliptic curves. This is rather beautiful if we think about it, that the extremely abstract number theoretical topic of the group of rational points on an elliptic curve can be utilized for one of the most important problems in modern security. In this paper we develop new techniques for proving the compositeness and factoring large numbers, by utilizing previous work in the study of elliptic curves.

In Section 3 we introduce previous work on elliptic curves, and describe a currently used elliptic curve primality test and factoring algortihm. In Section 4 we develop our own contributions to this field, first by extending the classification of all elliptic curves by Daniel Kubert into a more usable form for our applied number theoretic goals. We then introduce and prove theorems that check an integer N for compositeness; and finally, we prove that our test will never fail; namely, our test never falsely concludes that a composite number N is prime. In fact, to go even further, we demonstrate that we can detect all composite integers without ever having to divide by more than 7.

2 Background Number Theory and Factoring Algorithms

In this chapter we introduce some of the techniques of classical number theory that have modern applications to internet and national security. We first begin with a brief discussion of RSA, a protocol which inspires the questions considered in this thesis. In Section 2, we introduce Fermat's Little Theorem, which yields the most basic primality test other than trial division. In Section 3, we cover the Rabin-Miller Test, which is a much more advanced test for primality, still used in conjunction with modern primality testing algorithms. Finally in Section 4, we explain Pollard's $p-1$ factoring algorithm, which is the stepping stone to elliptic curve methods.

2.1 RSA

We now introduce RSA, the most commonly used public key crytographic system [5]. As we will see, the fundamental security of RSA is based on the fact that it is difficult to factor the product of two large primes. But first, before we introduce how the system works, we must prove the following proposition from Kraft and Washington [5].

Proposition 2.1. *Let $n = pq$ be the product of two distinct primes, and let d, and e satisfy $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then for all integers m,*

$$m^{ed} \equiv m \pmod{n}$$

Before our proof we will give an example.

Example 2.2. Let $p = 5$ and $q = 7 \implies N = 35$ and $(p-1)(q-1) = 24$. We want to find e and d such that $ed \equiv 1 \pmod{24}$. Notice $e = d = 5$ works, so now let's calculate

$$m^{5 \cdot 5} \pmod{35}$$

for a few m. Let $m = 13$. Then $13^{25} \equiv 13^{24}13 \equiv 13 \pmod{35}$ by Euler's Theorem. Now let $m = 25$. We have $25^{25} \equiv (25^4)^6 \cdot 25 \equiv 25^7 \equiv 25 \pmod{35}$.

Now we will prove the proposition.

Proof. First consider when $\gcd(m, n) = 1$. Then by Euler's Theorem, $m^{\phi(n)} \equiv 1 \pmod{n}$, and because $ed \equiv 1 \pmod{n}$ we can write $m^{ed} = m^{1+k\phi(n)}$ for some integer k. Therefore,

$$m^{ed} = m^{1+k\phi(n)} \equiv m(m^{\phi(n)})^k \equiv m1^k \equiv m \pmod{n}.$$

However, we are not done, as we must treat when $\gcd(m, n) \neq 1$, as Euler's Theorem would not apply. If $\gcd(m, n) = pq$, then $m \equiv 0 \pmod{n}$, and clearly $0^{ed} \equiv 0 \pmod{n}$. So now, without loss of generality, assume $\gcd(m, n) = p$. Clearly, $m \equiv 0 \pmod{p}$, so then $m^{ed} \equiv 0 \pmod{p}$. We know by Fermat's Little Theorem, that $m^{q-1} \equiv 1 \pmod{q}$, and that

$$m^{ed} = m^{1+k(p-1)(q-1)} \equiv mm^{\hat{k}(q-1)} \equiv m1^{\hat{k}} \equiv m \pmod{q}.$$

Therefore, combining the above, we have that

$$p|m^{ed} - m, \text{ and } q|m^{ed} - m.$$

Therefore, $pq|m^{ed} - m \implies m^{ed} \equiv m \pmod{pq = n}$. [5] □

Now that we have proved the proposition, we will give an outline of how the RSA encryption system works through example.

Example 2.3. (RSA)
In this example we want to send the message "TEST" using RSA, so only the correct person can read the message. This works as follows. Person 1 picks two large primes[1] and calculates $N = pq$ and $\phi(N) = (p-1)(q-1)$. They then choose an encryption key e, with $\gcd(e, \phi(N)) = 1$, and find a d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$. They then publish N and e, but keep d, p, and q secret. For our case, we choose $p = 8641$ and $q = 9749$, so $N = 84241109$. We choose $e = 65537$, and find that $e \cdot 49633793 \equiv 1 \pmod{(8641-1)(9749-1)}$, so $d = 49633793$.

The next step is for person 2 to encrypt the message they want to send to person 1, in our case, the message is "TEST", which they represent by taking the number corresponding to the position in the alphabet, giving "TEST" as $m = 2051920$. Person 2 then computes $c \equiv m^e \pmod{N}$, which for our example is $2051920^{65537} \equiv 81020401 \pmod{N}$. Person 2 then sends $m^e = c$ to person 1.

Finally, person 1 computes $m \equiv c^d \pmod{N}$ using the decryption key d. For our numbers, we get $81020401^{49633793} \equiv 2051920$ as we want.

A few remarks about the process are in order. First, when choosing e, it can be any integer with the condition that $\gcd(e, (p-1)(q-1)) = 1$, it just happens that 65537 is a popular choice because it is one more than a power of two, so it is easy to compute x^{65537} by sucessive squaring [5]. Second, the security of the system is based on the fact that it is not easy to factor N. If someone could factor N, then they could easily find d by the Extended Euclidean Algorithm, and then easily decrypt the message. We know that factoring N, when it is the product of two large distinct primes, is a hard problem, so we rely on the computational infeasibility of factoring N for our security. This stresses the importance of factoring algorithms to data security, as the encryption must stay one step ahead of the factoring algorithms. Right now, the best factoring methods for numbers around 130 digits are either the Elliptic Curve Method or the Number Field Sieve which work with running times of $L(N)^{1+o(1)}$,[2] and $O(e^{(\ln N)^{1/3}(\ln\ln N)^{2/3}(C+o(1))})$ for a small constant C, respectively, so we know that picking primes p and q with ≈ 100 digits gives N sufficient size that the best current factoring methods cannot break the code in any reasonable amount of time [1].

2.2 Fermat's Little Theorem

Before we consider modern methods for primality testing and factorization, we must study more basic methods. The majority of the most basic primality testing methods are based on Fermat's Little Theorem [5].

[1] In practice these are usually over 100 digits

[2] $L(x) = e^{\sqrt{\ln x \ln\ln x}}$

2.2.1 Fermat's Little Theorem

We begin with the statement of Fermat's Little Theorem.

Theorem 2.4 (Fermat's Little Theorem)**.** *Let p be a prime. then for every integer a, $a^p \equiv a \pmod{p}$. Moreover, if $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.*

Before we prove the theorem, let's look at an example.

Example 2.5. Consider $p = 7$. Notice

$a \pmod{7}$	$a^7 \pmod{7}$
0	$0^7 \equiv 0 \pmod{7}$
1	$1^7 \equiv 1 \pmod{7}$
2	$2^7 \equiv 2 \pmod{7}$
3	$3^7 \equiv 3 \pmod{7}$
4	$4^7 \equiv 4 \pmod{7}$
5	$5^7 \equiv 5 \pmod{7}$
6	$6^7 \equiv 6 \pmod{7}$

As we can see from the table, all of the congruence classes modulo 7 are themselves when raised to a power of 7. One important note is that this is *not* true for integers in general, and rather a property of primes.

Now we will prove the theorem.

Proof of Fermat's Little Theorem. First notice that if $a \equiv 0 \pmod{p} \implies 0^p \equiv 0 \pmod{p}$. Also notice that $a^{p-1} \equiv 1 \pmod{p} \overset{\times a}{\implies} a^p \equiv a \pmod{p}$, so it is sufficient to show that $a^{p-1} \equiv 1 \pmod{p}$. We begin with a Lemma.

Lemma 2.6. *If $a \not\equiv 0 \pmod{p}$, then the set $a, 2a, 3a, \ldots, (p-1)a \pmod{p}$ contains each nonzero congruence class exactly once.*

Proof. Let $a \not\equiv 0 \pmod{p}$. We will prove the Lemma by contradiction. Suppose the set $a, 2a, 3a, \ldots, (p-1)a$ has repeated elements.

$$\iff a \cdot i \equiv a \cdot j \pmod{p} \quad \text{where } 1 \leq i \neq j \leq p-1 \tag{1}$$
$$\iff p|(a \cdot i - a \cdot j) = a(i-j) \tag{2}$$
$$\iff p|(i-j) \tag{3}$$

But $i - j \in \{1, 2, 3, \ldots, p-2\}$ so it cannot be that $p|(i-j)$. So our assumption is false, and the set $a, 2a, 3a, \ldots, (p-1)a$ contains each nonzero congruence class $\pmod{p}$ exactly once. □

Now consider the product of all of the elements of $a, 2a, 3a, \ldots, (p-1)a$. Our Lemma says that

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} ai \pmod{p},$$

because the two sets contain the same elements.

$$\implies (p-1)!a \equiv (p-1)! \pmod{p}$$

But notice, $p \nmid (p-1)!$, because it does not divide any of $1, 2, \ldots, p-1$. Therefore, $(p-1)!$ has a multiplicative inverse $\pmod{p}$, and we can divide by $(p-1)!$ to obtain

$$a^{p-1} \equiv 1 \pmod{p},$$

and this concludes the proof of Fermat's Little Theorem. □

2.2.2 Fermat Primality Test

Clearly, we can use Fermat's Little Theorem as the most basic of primality tests, because if we have a number N, that we wish to test for primality, and $a^{N-1} \not\equiv 1$ for any $a \not\equiv 0 \pmod{N}$, then N is clearly composite.

Example 2.7. We will show that 12 is not prime using this test. Notice $2^{11} \equiv 2^{10} \cdot 2 \equiv 32^2 \cdot 2 \equiv 8^2 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \not\equiv 1 \pmod{12}$, so 12 is composite.

However, some numbers will pass this simple test for compositeness, leading us to two definitions.

Definition. A composite integer $n > 1$ is called *b-pseudoprime* if $b^{n-1} \equiv 1 \pmod{n}$.

To illustrate the issue with Fermat's composite test, we give a few examples of b-psdeudoprimes.

Example 2.8. Consider $b = 2$ and $N = 341$. We know $341 = 11 \times 31$, but notice that $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{341}$, so if we only tried this, we might wrongly conclude N is prime. However, notice that $3^{340} \equiv 56 \pmod{341}$, so we can tell 341 is composite.

Example 2.9. Now consider $N = 1729 = 7 \times 13 \times 19$. We try to show that n is composite using 2.

$$2^{1728} = (2^{108})^{16} \equiv 1^{16} \equiv 1 \pmod{1729}$$

So 2 does not work. Now let's try another number like we did with the example above.

$$5^{1728} = (5^{108})^{16} \equiv 1^{16} \equiv 1 \pmod{1729}$$

So 5 also does not work.

Now one might ask, are there some numbers that are b-pseudoprimes for a large percentage of $b \pmod{N}$? The answer is yes, which leads to the following definition.

Definition. A composite integer $N > 1$ is called a **Carmichael Number** if $b^{N-1} \equiv 1 \pmod{N}$ for all integers b with $\gcd(b, N) = 1$

While it may not seem like there would be many Carmichael Numbers, there are enough that the Fermat primality test is not nearly sufficient to be confident a number is prime.

Example 2.10. Consider $N = 561$. Clearly N is divisible by 3, because the sum of its digits are divisible by 3. But, suppose we did not know that, and want to test for compositeness using the Fermat test. Let's try with $b = 16, 124,$ and 395.

$$16^{560} = (16^{70})^8 \equiv 1^8 \equiv 1 \pmod{561}$$

So 16 does not help us prove that 561 is composite. Now let's try 124.

$$124^{560} = (124^{2}80)^2 \equiv 1^2 \equiv 1 \pmod{561}$$

Again, this does not help us. Finally let's try 395.

$$395^{560} = (395^{140})^4 \equiv 1^4 \equiv 1 \pmod{561}$$

At this point we might ask whether 561 is a Carmichael Number, and the answer is yes, but we will leave it at 3 examples.

Remark 2.11. Note that 1729 from our example above is also a Carmichael Number, so while rare, they do appear often enough to cause problems with these simple primality tests. In fact, it was proved by Alford, Granville and Pomerance that there are infinitely many Carmichael numbers.[4]

There are improvements to the Fermat primality test, such as the Strong Fermat Test, but we will not discuss these in this paper, rather let's look at a more advanced test.

2.3 Rabin-Miller Test

In this section we introduce the Rabin-Miller Test, which will either prove a number is composite, or determine that it is "probably" prime. This is an important distinction to make; many of the tests used will only determine that a certain number is probably prime, not actually *prove* primality. The Rabin-Miller test is very important for us, because later on, when using elliptic curve algorithms, we want to be fairly sure that the number is prime for the sake of time and computer memory. Now we introduce the algorithm [1].

Algorithm 2.12 (Rabin-Miller)**.** Given and odd integer $N \geq 3$, this algorithm determines if N is composite or probably prime.

Step 1: Write $N - 1 = 2^t \cdot q$, and set $c = 20$.

Step 2: Use a random number generator to pick $1 < a < N$. Set $e = 0$, $b \equiv a^q \pmod{N}$. If $b \equiv 1 \pmod{N}$ go to Step 4.

Step 3: While $b \not\equiv \pm 1 \pmod{N}$ and $e \leq t-2$, set $b \equiv b^2 \pmod{N}$ and $e = e+1$. If the loop ends before $b = N-1$, then N is composite, and end the algorithm.

Step 4: Set $c = c-1$. If $c > 0$ go to Step 2. If $c = 0$, then N is probably prime.

We now will try to illustrate the algorithm with an example.

Example 2.13. Let's try to show that 1729 is composite using the Rabin-Miller Test. First we write $1728 = 2^6 \cdot 27$, so $t = 6$, and $q = 27$. Next we choose a random number $1 < a < 1729$, say $a = 1011$. We now compute $b = 1011^{27} \equiv 818 \pmod{1729}$. So we enter the while loop. We see that $b^2 \equiv 818^2 \equiv 1$, so we end our loop, and $b \neq 1728$, so 1729 is composite! Notice how quickly the Rabin-Miller Test succeeded, when we could not determine 1729 was composite from the Fermat test.

However, there are numbers that are composite that also pass the Rabin-Miller Test. We illustrate that with an example below.

Example 2.14. Consider $N = 2047$. The first step is to write $2047 - 1 = 2046$ as $2^1 \cdot 1023$. Now we use a random number generator to pick a number between 1 and 2047. Let $a = 967$. we set $b = 967^{2046} \equiv 1013 \pmod{2047}$. Now we do successive squaring while $e = 0 \leq t-2$. For our case, we can't do another step, so we go back and choose a new random a. Continuing in this way, we eventually determine that 2047 is probably prime. However, it is not! $2047 = 23 \cdot 89$, so we see that the Rabin-Miller test fails for some composite numbers.

Now that we have a fairly advanced test for compositeness, we turn to the issue of how to factor that number in the following section.

2.4 Pollard's $p-1$ Method

This subsection introduces a factoring method proposed in 1974 by John Pollard [5], that was, at the time, one of the best method for factoring large numbers. The idea is as follows; if the number N that we wish to factor has a prime factor p, then by Fermat's Little Theorem, if $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod{p},$$

so clearly p divides $\gcd(a^{p-1}, N)$. The problem is we do not know p, so we cannot compute a^{p-1}. To get around this we choose a number k that is a product of small primes to small powers. Then we compute $\gcd(a^k - 1, N)$. We hope that $p-1|k$, so that $p|a^k - 1$, and then $\gcd(a^k - 1, N) \geq p \geq 1$, and we have found a factor of N. If $\gcd(a^k - 1, N) = N$, then we choose a new a, and if $\gcd(a^k - 1, N) = 1$, we choose a larger k. We continue this process until we have found a nontrivial factor of N [5].

Now let's make this idea a bit clearer with a step by step algorithm from Kraft and Washington.

Algorithm 2.15 (Pollard's $p-1$ Algorithm)**.** Let $N \geq 2$ be a composite integer we want to factor.

Step 1: Choose an an integer a between 1 and N.

Step 2: Calculate $\gcd(a, N)$. If it is between 1 and N it is a nontrivial factor of N. If it is 1, continue.

Step 3: Choose a k that is a product of small primes to small powers.

Step 4: Calculate $\gcd(a^k - 1, N)$. If it is between 1 and N it is a nontrivial factor of N. If it is 1, choose a new a or k. If it is N, choose a new k.

One final thing to notice about Pollard's Method is that given infinite time, the method *will* find a nontrivial factor of N, because eventually k will reach $\frac{p-1}{2}$, for some prime $p|N$. However, if $p-1$ is *not* the product of smaller primes to small powers, the algorithm will take a long time to run, so it is quite limited [5]. To illustrate the process, consider the following two examples.

Example 2.16. We will attempt to factor 1729, one of the Carmichael Numbers from section 2.2.

Step 1: Choose $a = 2$

Step 2: Compute $\gcd(2, 1729) = 1$.

Step 3: Let's pick $k = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

Step 4: Calculate $\gcd(2^{210} - 1, 1729) = 7$, so we have found a factor!

We now know that $1729 = 7 \cdot 247$, and can either stop here, or plug 247 into Pollard's method.

Example 2.17. Now let's try to factor $N = 10585$.

Step 1: Choose $a = 2$

Step 2: Compute $\gcd(2, 10585) = 1$.

Step 3: Let's pick $k = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

Step 4: Calculate $\gcd(2^{30}-1, 10585) = 1$, so we will try going back and choosing a new k.

Step 5: We choose $k = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 7 \cdot 11$.

Step 6: Calculate $\gcd(2^{9240} - 1, 10585) = 145$, so we have found a nontrivial factor!

We have found that $10585 = 145 \cdot 73$, and can continue until we have a prime factorization, or stop here.

We now understand how Pollard's $p-1$ algorithm works, and can move on to elliptic curve applications, since many of the elliptic curve factoring algorithms are based on similar ideas to that of Pollard's method.

3 Elliptic Curve Primality Testing and Factorization

In this chapter we turn our focus from classical number theory to the study of elliptic curves. We first will introduce the group law and Weierstrass Normal Form, and then will discuss the previous developments by Mazur, Nagell, Lutz, and Kubert. We will then introduce the current factoring algorithms and primality tests due to Lenstra and others.

3.1 Rational Points and the Group Law

If we let

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

be the equation for a general cubic, we say that the cubic is *rational* if all of its coefficients are rational numbers. In general, if we have two points on an elliptic curve E, we can draw a line connecting the two points, which will give rise to a third point at the third intersection of the line with the cubic, and if two of the points are rational, then so is the third. This is the basis for our group law on the group of rational points on an a certain elliptic curve E. Let P and Q be two rational points on our curve E, and let $P * Q$ be the third point of intersection of the line connecting P and Q on E. If we only have one point P, we can get around this by taking the line tangent to P, and setting the other intersection point as $P * P$. Now let's add a point at infinity to the curve E, and denote this point as $\mathcal{O}$. This will be the zero element of our group of rational points on E. We denote the group law by $+$, and to add P and Q, we take the third intersection point $P * Q$, draw the vertical line to connect it to $\mathcal{O}$, and then take the third intersection point to be $P + Q$. Notice that $P + \mathcal{O} = P$ because $P * \mathcal{O}$ joined to $\mathcal{O}$ is itself P [9].

We now will introduce the *Weierstrass Normal Form*, which is a special form that any cubic equation with rational coefficients can be expressed in. The general equation for a cubic in Weierstrass Normal Form is

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

The Weierstrass Normal Form [9] is the result of a birational transformation, that puts our elliptic curve E into a more workable form. From the Weierstrass Normal Form it is easy to derive formulas for adding or doubling points, which we will use in our applications later on. First let's show how to compute $P + Q$. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. The equation of the line connecting P and Q is $y = \lambda x + \nu$ where $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$ and $\nu = y_P - \lambda x_P = y_Q - \lambda x_Q$. Now to get the coordinates of $P * Q$, we know it must lie on $y = \lambda x + \nu$, so we plug this into our equation for E. This gives

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

But notice, we know two of the three roots of this equation, so this equation factors as $(x - x_P)(x - x_Q)(x - x_+)$ where x_+ is the x-coordinate of $P * Q$. By multiplying out and equating the coefficients, we see that $x_+ = \lambda^2 - a - x_P - x_Q$, and thus $y_+ = \lambda x_+ + \nu$. Now suppose we have a point $P = (x_1, y_1)$ and want to compute $2P = P + P$. To compute $2P$ we cannot just use the addition formula, because our formula for λ would not make sense. Therefore we need to use implicit differentiation to calculate the slope of the tangent line as follows,

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}.$$

If we substitute in our general Weierstrass equation for E, and plug λ into the equations from above, we get

$$x_{2P} = \lambda(x_1, y_1)^2 - a - 2x_1 = \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)^2 - a - 2x_1,$$

or if we expand and simplify we get

$$x_{2P} = \frac{x_1^4 - 2bx_1 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c}.[9]$$

To get y_{2P} we notice that

$$\lambda(x_1, y_1) = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

Now we can plug in to get

$$y_{2P} = \lambda(x_1, y_1) \cdot (x_2 - x_1) + y_1.$$

Remark 3.1. It is often easier for us to find y_{2P} by simply plugging in x_{2P} into E, but that will involve square roots, which looks a bit more complicated. In practice if the square root was not defined that would mean that the group law would break down. Later on we will attempt to break down the group law to prove compositeness, so we do not need to worry about this square root.

We now must define an important quantity associated to the models of elliptic curves.

Definition 3.2. Let E be an elliptic curve defined as

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Then the *Discriminant* of E is defined to be

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Remark 3.3. The discriminant is also often represented by Δ_E.

Example 3.4. Let's look at the curve

$$E : y^2 = x^3 - 11x^2 - 120x + 900.$$

We plug into our formula for D given above, to get the discriminant of E is

$$D = 12960000 = 2^8 \cdot 3^4 \cdot 5^4.$$

Notice that all of the points of finite order on E are given by

$$\{(0, -30), (15, 0), (0, 30), (6, 0), (30, -120), (-10, 0), (30, 120), \mathcal{O}\},$$

where the set of points of order 4 is $\{(0, -30), (0, 30), (30, 120), (30, -120)\}$ and the other points have order 2. It is important to notice that all of the points of order 2 have a y coordinate of 0, and that the y coordinate of all of the points of order 4 divides D.

This example gives a glimpse of the Nagell-Lutz Theorem, an important theorem in the following section, but first we have the following theorem about rational points on E.

Theorem 3.5 (Mordell-Weil Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ as above. Then the rational points on E, along with the point $\mathcal{O}$ at infinity form a finitely generated abelian group.*

Remark 3.6. Points of finite order on such a curve is called the *torsion subgroup* of E, which we will denote by E_{tor}.

Remark 3.7. The proof of the Mordell-Weil Theorem is not simple, and involves the theory of heights. However, the idea is that generally if a group G is abelian, and $G/2G$ is finitely generated, one would expect G to also be finitely generated. However, this is not always true. An easier thoerem about rational points on elliptic curves corresponds to elliptic curves over the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, where p is prime. Notice that if $p \nmid D$, all formulas from above hold. Clearly $E/\mathbb{F}_p$ is finitely generated because it has only finitely many points, specifically p^2 many. The applications of this thesis make use of this fact, and more importantly, as we will see, that this property does not hold if p were composite.

3.2 Theorems of Mazur, Nagell-Lutz, and Kubert

We now will mention a few key theorems that are the basis for the methods we will use for primality testing and factorization in later sections. Some of the proofs are beyond the scope of this paper, but we will discuss the importance of these theorems. First we give a statement of the Nagell-Lutz Theorem.

Theorem 3.8 (Nagell-Lutz Theorem). *Let*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a nonsingular cubic curve with integer coefficients, and let D be the discriminant of the cubic polynomial $f(x)$,

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3.$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers; and either $y = 0$, in which case P has order 2, or else y^2 divides D.

It should be clear that this is an extremely powerful theorem. We now know that the coordinates of *any* point of finite order in the group of rational points on an elliptic curve E are integers. This gives us the ability to reduce this group modulo N, which is the source of our primality testing and factoring algorithms. The reduction is well defined when N is prime, but if N is composite, the group law can break down. We now prove a weaker version of the theorem, following the exposition in Silverman and Tate pages 49-55 [9].

Remark 3.9. The proof falls short of the claim in Theorem 3.8, we will prove only that $y|D$. In practice, to compute the torsion subgroup of E the weaker version is sufficient.

Proof of Theorem 3.8. As the remark stated above, here we prove Theorem 3.8 with $y|D$ instead of $y^2|D$. We begin the proof with a Lemma.

Lemma 3.10. *Let $P = (x, y)$ be a point on the elliptic curve*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c,$$

such that P and $2P$ have integer coordinates. Then either $y = 0$ or $y|D$.

Proof. We will assume that $y \neq 0$. With $y \neq 0$, we know $2P \neq \mathcal{O}$, so let $2P = (u, v)$. By hypothesis, $x, y, u, v \in \mathbb{Z}$. By our formula for doubling points we have

$$2x + u = \lambda^2 - a$$

with $\lambda = \frac{f'(x)}{2y}$. Because our points and coefficients are integers, we know that λ is also an integer, which means $2y|f'(x)$, so $y|f'(x)$. However, we know $y^2 = f(x) \implies y|f(x)$. We now claim that

$$D = \{(18b - 6a^2)x - (4a^3 - 15ab + 27c)\}f(x) + \{(2a^2 - 6b)x^2 \\ +(2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)\}f'(x), \tag{4}$$

which we will not expand here, however it is quite easy to check by simply plugging in. But this means we can write

$$D = r(x)f(x) + s(x)f'(x),$$

where the coefficients of $r(x)$ and $s(x)$ are integers, and so they have integer values at integer inputs. Thus $y|D$.

□

We will see how this lemma is used later on in our proof. Now let E be defined as in the statement of the theorem. We define the order of a rational number to be

$$\text{ord}\left(\frac{m}{n}p^{\nu}\right) = \nu,$$

where m and n are relatively prime to p and the fraction is in lowest terms. We say the order is zero if and only if p does not divide the numerator or denominator. Let (x, y) be a point on E with $p|$(denominator of x), so we have

$$x = \frac{m}{np^{\mu}} \text{ and } y = \frac{u}{wp^{\sigma}},$$

where $\mu > 0$ and p does not divide m, n, u, or w. If we plug into E and find a common denominator we get

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}},$$

so we have

$$\text{ord}\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma \text{ and ord}\left(\frac{m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

The order of p on the left must equal the order on the right, so we have $2\sigma = 3\mu \implies 2|\mu$ and $3|\sigma$, so $\mu = 2\nu$ and $\sigma = 3\nu$ for some $\nu > 0$. If we assume instead that p divides the denominator of y we get the same result, so if p is in the denominator of x or y, it is in the denominator of both. We now define

$$C(p^{\nu}) := \{(x, y) \in C(\mathbb{Q}) : \text{ord}(x) \leq -2\nu \text{ and ord}(y) \leq -3\nu\}.$$

We now will make a smart subsitution; we set

$$t = \frac{x}{y} \text{ and } s = \frac{1}{y}.$$

Then E becomes

$$\tilde{E} : s = t^3 + at^2 s + bts^2 + cs^3.$$

Similarly, a line in the x, y plane corresponds to a line in the s, t plane. Say $y = \lambda x + \nu$, then we have

$$\frac{1}{\nu} = \frac{\lambda}{\nu}\frac{x}{y} + \frac{1}{y}$$

so $s = -\frac{\lambda}{\nu}t + \frac{1}{\nu}$. We now denote the ring R as the set of all rational numbers with no p in the denominator[3], a fact we will use later.[4] If we let (x, y) be some point on E in $C(p^\nu)$, then we can convert it to coordinates in s and t, Let $P_1 = (t_1, s_1)$, and $P_2 = (t_2, s_2)$ be distinct points coming from an x and y in $C(p^\nu)$. Then if $t_1 = t_2$, $P_1 = -P_2$, $P_1 + P_2$ is also in $C(p^\nu)$. We now assume $t_1 \neq t_2$, and let $s = \alpha t + \beta$ be the line intersecting P_1 and P_2. By plugging into E and subtracting, we can factor out some $(t_2 - t_1)$ and $(s_2 - s_1)$ terms to get an alternate formula for the slope $\alpha = \frac{s_2 - s_1}{t_2 - t_1}$. We get

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1^2(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)},$$

where the numerator and denominator lie in $p^{2\nu}R$, because t_1, s_1, t_2, and s_2 all are in $p^\nu R$. Therefore, α is a unit in R. If $P_1 = P_2$ then we have

$$\alpha = \frac{ds}{dt}\bigg|_{P_1} = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2},$$

which is the same as the slope from above if we subsitute in $t_2 = t_1$. Now let $P_3 = (t_3, s_3)$ be the third point on $\tilde{E}$ and the line above. We plug into $\tilde{E}$ to get

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3.$$

We know that the roots of this equation if we subtract $\alpha t + \beta$ from both sides and multiply out and collect terms are our points t_1, t_2, and t_3, so we can rewrite the right hand side as

$$K \cdot (t - t_1)(t - t_2)(t - t_3) = (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (a\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + \ldots,$$

where K is some constant. If we multiply out the left hand side of the above equation and look at the coefficients of t^3 and t^2 we see

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}.$$

Using $\beta = s_1 - \alpha t_1$ we have a formula for t_3. To find the formula for the coordinates of $P_1 + P_2$ we draw the line through P_3 and the zero element, which in the t, s coordinate system is $(0, 0)$. Therefore the coordinates of $P_1 + P_2$ are $(-t_3, -s_3)$. Now notice that $s_1 \in p^{3\nu}R$, $\alpha \in p^{2\nu}R$ and $t_1 \in p^\nu R$. Therefore,

[3] These numbers are known as the p-integral rational numbers.

[4] R is clearly a ring because if $\alpha, \beta \in R$ then $\alpha \pm \beta, \alpha\beta \in R$.

$\beta \in p^{3\nu}R$, and the denominator of $t_1+t_2+t_3$ is a unit in R. We know from the equation above that $t_1+t_2+t_3 \in p^{3\nu}R$, and we also know $t_1, t_2 \in p^{\nu}R$, which means that $t_3 \in p^{\nu}R$. This means that if $P_1, P_2 \in p^{\nu}R$, then $P_3 \in p^{\nu}R$, and so $P_1 + P_2 \in p^{\nu}R$, so $C(p^{\nu})$ is closed under addition and taking negatives, and so it is a subgroup of $C(\mathbb{Q})$. Therefore,

$$-t_3 \equiv t_1 + t_2 \pmod{p^{3\nu}R}.$$

This means that we obtain a one-to-one homomorphism from $C(p^{\nu})$ to the quotient group $p^{\nu}R/p^{3\nu}R$, defined by

$$\frac{C(p^{\nu})}{C(p^{3\nu})} \to \frac{p^{\nu}R}{p^{3\nu}R},$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y}.$$

We now can show that if P is some point of finite order, then x and y have integer coefficients. We let P be some point of order m. Since $P \neq \mathcal{O}$, we know $m \neq 1$. Now let p be some prime, and suppose that $P \in C(p)$. Then $P = (x, y)$ is contained in some smaller group $C(p^{\nu})$ for some ν, with $P \notin C(p^{\nu+1})$. Suppose now that $p \nmid m$. If we apply the congruence

$$-t_3 \equiv t(P_1 + P_1) \equiv t_1 + t_1 \equiv t(P_1) + t(P_1) \pmod{p^{3\nu}R}.$$

m times, we get

$$t(mP) \equiv mt(P) \pmod{p^{3\nu}R}.$$

But notice that $mP = \mathcal{O}$, so $t(mP) = t(\mathcal{O}) = 0$. But since $p \nmid m$, m is a unit in R, so

$$0 \equiv t(P) \pmod{p^{3\nu}R}.$$

Therefore, $P \in C(p^{3\nu})$, which contradicts our assumption that it is not. Now suppose that $p|m$, say $m = pn$, and consider the point $P' = nP$. Clearly, P' has order p, and since $P \in C(p)$, then $P' \in C(p)$. Similarly to before, let $P' \in C(p^{\nu})$ but $P' \notin C(p^{\nu+1})$ for some ν. Then as before, we find that $pt(P') \equiv 0 \pmod{p^{3\nu=1}R}$, so $t(P') \equiv 0 \pmod{p^{3\nu-1}R}$. Clearly $3\nu - 1 \geq \nu + 1$, which contradicts that $P' \notin C(p^{\nu+1})$. Therefore, if $P = (x, y)$ is a point of finite order, $P \notin C(p)$ for all primes p, so the denominators of the x and y coordinates are not divisible by any prime, so they are 1, and $x, y \in \mathbb{Z}$. To finish the proof of the weaker version of the Nagell-Lutz theorem is easy, because if P has order two, $y = 0$ and we are done. If not, $2P \neq \mathcal{O}$. But we know that $2P$ also has finite order, so it has integer coordinates. We showed at the beginning of our proof in Lemma 3.10 that if P and $2P$ have integer coordinates then $y|D$, and this concludes the proof of the weaker version of the Nagell-Lutz Thoerem.

□

Let's now look at a few examples to see how the Nagell-Lutz Theorem works.

Example 3.11. Let E be defined as

$$E : y^2 = x^3 - 12x^2 - 128x + 1024.$$

By plugging in to our formula for D we see that $D = 17825792 = 2^{20} \cdot 17$, so we must check $y = 2, 2^2, 2^3, \dots, 2^{10}$, because y^2 must divide D. It is easy for us to see right away that $P = (0, -32)$ is a solution, because

$$(-32)^2 = x^3 - 12x^2 - 128x + 1024 \implies 1024 = x^3 - 12x^2 - 128x + 1024 \implies x = 0.$$

However, it is faster if we plug in the 10 possible y values into a computer program such as Maple that can quickly check for integer solutions. After doing this we can see that there are 3 integer solutions, giving the set of points

$$\{(0, -32), (16, 0), (0, 32), \mathcal{O}\}.$$

Example 3.12. Now let E be defined as

$$E : y^2 = x^3 - 28x^2 + 264x + 4096.$$

This curve has disciminant $D = -2^{22} \cdot 13^2$, so we must try more y values than last time. However, the procedure is the same, where we run a Maple program to check all of the possible y values such that $y^2|D$. If we do this we see that we get the set of points

$$\{(0, -64), (32, -128), (32, 128), (0, 64), \mathcal{O}\}.$$

Now we turn to the work of Mazur, who classified all of the possible structures for the torsion subgroups of elliptic curves. We begin with the statement of his theorem.

Theorem 3.13 (Mazur's Theorem)**.** *Let E be a nonsingular rational cubic curve, and suppose that $E(\mathbb{Q})$ contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \quad \textit{or} \quad m = 12.$$

More precisely, the set of all points of finite order in $E(\mathbb{Q})$ forms a subgroup which has one of the following two forms:

1. *A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.*
2. *The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$*

Remark 3.14. Notice that now that we have Mazur's Theorem it is easy to see that the points in Example 3.11 form a cyclic group isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and the curve in Example 3.12 has the subgroup of points of finite order isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Also, the curve in the last example in Section 3.1 has the subgroup $\mathbb{Z}2 \times \mathbb{Z}4$.

The proof of Mazur's theorem is beyond the scope of this paper; however, it is important to note the importance of this theorem. Before we discuss that, however, we need a definition.

Definition 3.15. Let E be an elliptic curve. Then the *torsion subgroup* of E, E_{tor}, is defined as:

$$E_{tor} = \{P = (x, y) \in E(\mathbb{Q}) : \text{P has finite order}\},$$

Mazur's Theorem tells us that if an elliptic curve E has a torsion subgroup, it is isomorphic to one of the above groups. This theorem is important in proving Fermat's Last Theorem, and a contributing factor to Barry Mazur being awarded the National Medal of Science in 2011. A natural question one might ask following Mazur's Theorem is if there is then a way to classify *all* elliptic curves with these torsion subgroups. The answer is yes, and in fact, Kubert proposed a table before Mazur proved his result [6]. After Mazur's Theorem was proved, we then knew that Kubert's table was complete. Now we state a proposition from Kubert's work, and include his table.

Theorem 3.16 (Kubert's Boundedness Conjecture Over $\mathbb{Q}$)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Let T be a subgroup of $E_{tor}(\mathbb{Q})$. Then T is parameterizable.*

Table 1: *Parametrization of Torsion Structures* [6]

1. $\mathbf{0}$:$y^2 = x^3 + ax^2 + bx + c$;$\Delta_1(a, b, c) \neq 0$,
   $\Delta_1(a, b, c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.
2. $\mathbb{Z}/\mathbf{2}\mathbb{Z}$: $y^2 = x(x^2 + ax + b)$; $\Delta_1(a, b) \neq 0$, $\Delta_1(a, b) = a^2b^2 - 4b^3$.
3. $\mathbb{Z}/\mathbf{2}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $y^2 = x(x + r)(x + s)$, $r \neq 0 \neq s \neq r$.
4. $\mathbb{Z}/\mathbf{3}\mathbb{Z}$: $y^2 + a_1xy + a_3y = x^3$; $\Delta(a_1, a_3) = a_1^3a_3^3 - 27a_3^4 \neq 0$.

   The form $E(b, c)$ is used in all parametrizations below where $E(b, c) = y^2 + (1 - c)xy - by = x^3 - bx^2$, $(0, 0)$ is a torsion point of maximal order, $\Delta(b, c) = \alpha^4b^3 - 8\alpha^2b^4 - \alpha^3b^3 + 36\alpha b^4 + 16b^5 - 27b^4$, and $\alpha = 1 - c$.
5. $\mathbb{Z}/\mathbf{4}\mathbb{Z}$: $E(b, c)$, $c = 0$, $\Delta(b, c) = b^4(1 + 16b) \neq 0$.
6. $\mathbb{Z}/\mathbf{4}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b, c)$, $b = v^2 - \frac{1}{16}$, $v \neq 0, \pm\frac{1}{4}$, $c = 0$.
7. $\mathbb{Z}/\mathbf{8}\mathbb{Z}\times\mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b, c)$, $b = (2d-1)(d-1)$, $c = b/d$, $d = \alpha(8\alpha+2)/(8\alpha^2-1)$, $d(d - 1)(2d - 1)(8d^2 - 8d + 1) \neq 0$.
8. $\mathbb{Z}/\mathbf{8}\mathbb{Z}$: $E(b, c)$, $b = (2d - 1)(d - 1)$, $c = b/d$, $\Delta(b, c) \neq 0$.
9. $\mathbb{Z}/\mathbf{6}\mathbb{Z}$: $E(b, c)$, $b = c + c^2$, $\Delta(b, c) = c^6(c + 1)^3(9c + 1) \neq 0$.

10. $\mathbb{Z}/\mathbf{6}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b,c)$, $b = c + c^2$, $c = (10 - 2\alpha)/(\alpha^2 - 9)$, $\Delta(b,c) = c^6(c+1)^3(9c+1) \neq 0$.
11. $\mathbb{Z}/\mathbf{12}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = m + \tau$, $f = m/(1-\tau)$, $m = (3\tau - 3\tau^2 - 1)/(\tau - 1)$, $\Delta(b,c) \neq 0$.
12. $\mathbb{Z}/\mathbf{9}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f(f-1) + 1$, $\Delta(b,c) \neq 0$.
13. $\mathbb{Z}/\mathbf{5}\mathbb{Z}$: $E(b,c)$, $b = c$, $\Delta(b,c) = b^5(b^2 - 11b - 1) \neq 0$.
14. $\mathbb{Z}/\mathbf{10}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f^2/(f - (f-1)^2)$, $f \neq (f-1)^2$, $\Delta(b,c) \neq 0$.
15. $\mathbb{Z}/\mathbf{7}\mathbb{Z}$: $E(b,c)$, $b = d^3 - d^2$, $c = d^2 - d$, $\Delta(b,c) = d^7(d-1)^7(d^3 - 8d^2 + 5d + 1) \neq 0$.

We now have a table that paramaterizes *all* of the possible curves that have torsion subgroups. This is extremely powerful as we can now, simply by looking at the equation of a curve, determine if it has a torsion subgroup. Before we look further into the work of Kubert, and how it applies to our primality testing, we require a lemma.

Lemma 3.17. *If p is prime, then there are at most $p^2 - 1$ many points of order p on $E(\mathbb{F}_q)$, where q is prime, and $q \nmid \Delta_E$*

Proof. Here we will not prove the entire lemma, but rather simply show that for primes $p = 2, 3, 5$ or 7, we have an upper bound on the number of points of order p, we will need this in Section 4. We suppose for all cases that $E(\mathbb{F}_q) : y^2 = f(x) \pmod{q}$, with q prime, and P is a torsion point of order p. First consider $p = 2$. Then we know that $2P = \mathcal{O}$, so we have

$$P = -P \implies (x,y) = (x,-y) \implies 2y = 0, f(x)$$

However, we know that for fields a polynomial $f(x)$ has at most $\deg(f)$ roots[2], so we know that there are 3 possible solutions, or at most 3 points of order 2 over $\mathbb{F}_q$.

We now consider $p = 3$. We know that $3P = \mathcal{O}$ so

$$2P = -P \implies x_{2P} = \frac{x_1^4 - 2bx_1 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c} = x,$$

where we got x_{2P} from the doubling formula in Section 3.1. Again, we know that the equation $x_{2P} - x = 0$ is a polynomial of degree 4, so over $\mathbb{F}_q$ it has at most 4 roots. For each x value there are two possible y values, which means there are at most 8 points of order 3.

Next we have $p = 5$. If we do successive doublings of P we have $4P = -P$. As with the $p = 3$ case, plugging into the doubling formula gives an equation for x_{4P}, which we can easily see has order less than or equal to 16. Again there are 2 possible y values for each x value, so we get at most 32 points of order 5.

Finally consider $p = 7$. Notice that P has order 7 $\iff$ $8P = P$, so we can use the doubling formula again, giving a polynomial equation for the x coordinate of $8P$. It is easy to see that polynomial has order at most 32, which means at most 64 points of order 7. As we mentioned this proof does not show the stronger bound of $p^2 - 1$ for all primes p, but as the reader will see in Section 4, we simply need a bound for $p = 2, 3, 5$ or 7.

□

Before we continue on to our own primality tests, let us introduce the current standards in elliptic curve factoring and primality testing.

3.3 Elliptic Curve Primality Tests and Factoring Algorithms

In this section we introduce primality tests and factoring algorithms that use the properties of elliptic curves we introduced above. The general idea of these methods is to assume N is prime, and then find a contradiciton by breaking down the group law. We begin with a primality test.

3.3.1 Goldwasser-Killian Test

The idea of the Goldwasser-Killian Test is to find an elliptic curve E with $m = |E(\mathbb{Z}/N\mathbb{Z})|$, where m has a large prime, or pseudo-prime, factor[5]. If q is such a factor, we assume q is prime, and look for a point P such that

$$\begin{gathered} P \in E(\mathbb{Z}/N\mathbb{Z}) \\ m \cdot P = O_E \\ (m/q) \cdot P \neq O_E \end{gathered}$$

If such a point P is found, we now need to prove that q is indeed prime, but we have now reduced the problem of proving N is prime to proving q is prime. So we can apply this recursively until we reach a number that can be factored with other algorithms. As stated before, if N is not prime, the algorithm can run forever, hence why it is more theoretical than applicable, but it will never give a false answer. If the algorithm determines N to be prime, the sequence of primes $N_0 = N, N_1 = q, \dots, N_i, \dots$, along with the curves E_i, and points P_i is called the primality certificate of N. Now let's state the formal algorithm from Cohen [1].

Algorithm 3.18 (Goldwasser-Killian)**.** [1] Let $N \neq 1$ be a positive integer coprime to 6. This algorithm will try to prove that N is prime. If N is not prime, the algorithm may detect it or may run indefinitely.

[5] Large meaning $q|m$ with $q > (\sqrt[4]{N} + 1)^2$

Step 1: Set $i = 0$ and $N = n_i$.

Step 2: If $n_i < 2^{30}$, trial divide n_i by the primes up to 2^{15}. If n_i is not prime, go to Step 9.

Step 3: Choose a and b randomly in $\mathbb{Z}/n_i\mathbb{Z}$ and check that $4a^3+27b^2 \in (\mathbb{Z}/n_i\mathbb{Z})*$. Let E be the elliptic curve with the equation $y^2 = x^3 + ax + b$.

Step 4: Compute $m = |E(\mathbb{Z}/n_i\mathbb{Z})|$. If this cannot be computed go to Step 9.

Step 5: Check that $m = 2q$, where q passes the Rabin-Miller Test. If not go back to Step 3.

Step 6: Choose a random $x \in \mathbb{Z}/n_i\mathbb{Z}$ until the Legendre-Jacobi Symbol $\left(\frac{x^3+ax+b}{n_i}\right)$ is equal to 0 or 1. Then compute $y^2 = x^3 + ax + b$. If this fails, go to Step 9.

Step 7: Compute $P_1 = m \cdot P$, and $P_2 = (m/q) \cdot P$, where P is the point found in Step 6. If the computations are not possible, then go to Step 9. Otherwise, check that $P_1 = \mathcal{O}$. If not, go to Step 9. Check if $P_2 = \mathcal{O}$, and if so, go back to Step 6.

Step 8: Set $i = i + 1$, and $n_i = q$, and go back to Step 2.

Step 9: If $i = 0$ then N is composite and stop the algorithm. If not, set $i = i - 1$ and go back to Step 3.

We reiterate again here that this algorithm is primarily theoretical, and not used for applications of primality testing. However, it does still indicate one of the ways elliptic curves can be used to prove the compositeness or primality of a number. In the next subsection we will introduce an elliptic curve factoring method that is very applicable, and we will show an example of factoring using the method.

3.3.2 Lenstra's Elliptic Curve Factoring Algorithm

Here we look into a factoring algorithm using elliptic curves developed by H.W. Lenstra which is one of the three most popular modern factoring methods along with the quadratic sieve and the number field sieve [1]. Before we state the algorithm, briefly recall the group law on elliptic curves. For an elliptic curve $E : y^2 = x^3 + ax + b$, the formula for a point $P_3 = P_1 + P_2$ is $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda x_3 + \nu$ where $\lambda = \frac{y_2-y_1}{x_2-x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Notice now, that these equations are obviously true in a field[6], but if we are working with E over $\mathbb{Z}/N\mathbb{Z}$, this may not always work, because $x_2 - x_1$ is not required to have an inverse. However, this is *exactly* what we want. If $x_2 - x_1$ does not have an inverse modulo N, then $\gcd(x_2 - x_1, N)$ is a non-trivial divisor of

[6] unless $x_2 = x_1$

N. Therefore, we will now consider E over $\mathbb{Z}/N\mathbb{Z}$, assuming N is prime, and look for a contradiction to that assumption. Now that we understand why this method provides a non-trivial factorization of N, we can turn our focus to the implementation of the algortihm.

Algorithm 3.19 (Lenstra's Elliptic Curve Algorithm)**.** [9] Let $N \geq 2$ be a number we wish to factor.

Step 1: Check $\gcd(6, N) \neq 1$. If so, we have a non-trivial factor. Also check that $N \neq m^r$ for some $r \geq 2$.

Step 2: Choose random point $P = (x_1, y_1)$ and integer a.

Step 3: Let $b = y_1^2 - x_1^3 - ax_1 \pmod N$, so

$$E : y^2 = x^3 + ax + b$$

where $P \in E$.

Step 4: Check $\gcd(4a^3 + 27b^2, N) = 1$. If it is N, go back to 2 and choose a new a, and if $1 < \gcd(4a^3 + 27b^2, N) < N$, it is a factor of N.

Step 5: Choose a number k which is a product of small primes, and compute $kP = \left(\frac{\alpha_k}{\delta_k^2}, \frac{\beta_k}{\delta_k^3}\right)$ by writing k in base 2 and adding up the terms modulo N.

Step 6: Compute $\gcd(\delta_k, N)$. If this is equal to 1, either choose a larger k, or a new a. If it $\gcd(\delta_k, N) = N$, choose a smaller k.

The crucial step in this algorithm is computing $kP \pmod N$, so let's look a little more closely at what is going on. The trick for computing kP is writing k in base 2 as $k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_r \cdot 2^r$. Then from our doubling formula, we need to compute

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

Here, if we cannot compute λ, we have a nontrivial factor of N, because $\gcd(y, N) \neq 1$. If we can compute λ, we do as follows all modulo N:

$$\begin{aligned} P_0 &= P \\ P_1 &= 2P_0 \\ P_2 &= 2P_1 = 2^2 P_0 \\ &\vdots \qquad \vdots \\ P_r &= 2P_{r-1} = 2^r P_0 \end{aligned}$$

Then we can compute kP simply by summing up the table. If we let k_iP indicate the i^{th} step in computing kP, then if we cannot compute kP, it's because $\gcd(x_i - x_{i-1}, N) \neq 1$ from the addition formula, and we can stop the algorithm here because we have a non-trivial factor of N [9]. The best way to see how the algorithm works is in practice with the example below.

Example 3.20. We will atempt to factor $N = 23 \cdot 31 \cdot 37 \cdot 47 = 1239907$. In Maple, we use the built in **mod** function and compute $2^i \cdot P \pmod{N}$. For this implementation, we only computed these values, and tested to see if the algorithm failed at this point, before needing to add up the 2-adic expansion of $k \cdot P$. We test this method with $a = 3$, $x_1 = 1$, $y_1 = 3$, and $k = 15$. However, our algorithm doesn't work, and we only find the trivial factor of 1239907, so we must go back and choose a new a[7]. We go back, and set $a = 4$, but again, this doesn't work. Now we go back, and set $a = 5$, and the algorithm works, finding 37!

In this chapter we learned about the current elliptic curve primality tests and factoring algorithms, and saw how the factoring algorithm works in practice. What one might wonder now, is why, if we have so much information on the forms of elliptic curves from the work of Kubert, Nagell, Lutz, and Mazur do we choose our curves randomly? Instead, is there a way to utilize our previous knowledge to better our tests for primality using elliptic curves? These questions are answered in the following chapter.

4 New Developments

In the previous chapters we obtained the basic theory of elliptic curves, including the theorems of Mazur, Nagell and Lutz, and Kubert. The theorem of Mazur confirms a conjecture of Kubert that his list of parametrizations of Torsion structures of elliptic curves is complete. In this chapter we use this classification of all torsion subgroups to develop a new variant of elliptic curve primality testing. We take points of known order, and seek to deduce non-primality of N by breaking down the group law modulo N. In 4.1 we begin with some lemmas to convert curves to a more usable form. Then in 4.2 we renormalize Kubert's table to apply our formulas in Weierstrass Normal Form, and in 4.3, we introduce our new primality tests, and a theorem about their effectiveness.

4.1 Alternative Representations of Elliptic Curves

Before we begin with new methods of primality testing we record different forms of elliptic curves in Weierstrass Form. Weierstrass equations come in various forms, each of which are easier to use for certain applications. For example, the form $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is more convenient for pure number theory, but we would like to have E in a different form that is easier

[7] For the method written in Maple we need to choose a new a here, but typically, we would try to add up the powers of 2 times P, and if that also worked, we would then choose a new a

to work with when testing for primality. We demonstrate the ability to move between representations of E in a series of lemmas.

Lemma 4.1. *If E is an elliptic curve of the form $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, with each $a_i \in F$, where char$(F) \neq 2$, then E can also be represented by*

$$E : y^2 + a_3y = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6,$$

and a point on E (x, y) corresponds to the point $(x, y + \frac{a_1x}{2})$.

Proof. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with point (x, y). We add and subtract $\frac{a_1^2x^2}{4}$ to the left hand side.

$$\implies y^2 + a_1xy + a_3y + \frac{a_1^2x^2}{4} - \frac{a_1^2x^2}{4} = (y + \frac{1}{2}a_1x)^2 - \frac{a_1^2x^2}{4} + a_3y = RHS.$$

Now we let $y = y - \frac{a_1x}{2}$, which gives

$$(y - \frac{a_1x}{2} + \frac{1}{2}a_1x)^2 - \frac{a_1^2x^2}{4} + a_3(y - \frac{a_1x}{2}) = y^2 + a_3y - \frac{1}{4}a_1x^2 - \frac{1}{2}a_1a_3x.$$

Moving the y independent term to the RHS we get

$$E : y^2 + a_3y = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6.$$

To complete the proof we simply update our point (x, y) by subsituting in for y. □

We will demonstrate how this looks with two examples.

Example 4.2. Let's look at the curve

$$E : y^2 + xy - 4y = x^3 - 4x^2.$$

Following the Lemma, we add and subtract $\frac{a_1^2x^2}{4} = \frac{x^2}{4}$ from both sides giving

$$y^2 + xy + \frac{x^2}{4} - \frac{x^2}{4} - 4y = x^3 - 4x^2$$

$$\implies (y - \frac{x}{2})^2 - \frac{x^2}{4} - 4y = x^3 - 4x^2$$

$$\implies (y - \frac{x}{2})^2 - 4y = x^3 - \frac{17}{4}x^2$$

We now substitute $y = y - \frac{x}{2}$ giving

$$(y - \frac{x}{2} + \frac{x}{2} + \frac{x^2}{4})^2 - 4(y - \frac{x}{2}) = RHS$$

$$\implies y^2 - 4y + 2x = RHS$$

$$\implies y^2 - 4y = x^3 - \frac{17}{4}x^2 - 2x$$

Example 4.3. Now consider

$$E : y^2 + 4xy = x^3.$$

Here we add and subtract $4x^2$ giving

$$y^2 + 4xy + 4x^2 - 4x^2 = x^3$$
$$\implies (y + 2x)^2 - 4x^2 = x^3.$$

Setting $y = y - 2x$ gives

$$y^2 = x^3 + 4x^2$$

and we are done.

Now we turn to the next step of getting E into a more usable form with the following Lemma.

Lemma 4.4. *If E is an elliptic curve of the form $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with each $a_i \in F$, and char$(F) \neq 2$, then E can be represented as*

$$\hat{E} : y^2 = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6 + \frac{1}{4}a_3^2.$$

Further, if $P = (x, y)$ is a point on E, then in the new representation of E, $\hat{E}$, $\hat{P} = (x, y - \frac{a_1x}{2} - \frac{a_3}{2})$.

Proof. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with point $P = (x, y)$. Then by the above lemma we know that E can be represented as $\hat{E} : y^2 + a_3y = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6$ with $\hat{P} = (x, y - \frac{a_1x}{2})$. Similarly to the last lemma, we will complete the square on the LHS. We add and subtract $\frac{a_3^2}{4}$ from the LHS, giving

$$y^2 + a_3y + \frac{a_3^2}{4} - \frac{a_3^2}{4} = (y + \frac{a_3}{2})^2 + a_3y - \frac{a_3^2}{4}$$

Letting $y = y - \frac{a_3}{2}$ gives

$$((y - \frac{a_3}{2}) + \frac{a_3}{2})^2 + a_3(y - \frac{a_3}{2}) - \frac{a_3^2}{4} = y^2 - \frac{1}{4}a_3^2.$$

We now add the y independent term to the RHS to get

$$y^2 = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6 + \frac{1}{4}a_3^2.$$

As before, we must apply the same subsitiution to $\hat{P}$ giving $\tilde{P} = (x, y - \frac{a_1x}{2} - \frac{a_3}{2})$. □

Again, let's illustrate the process with a few examples.

Example 4.5. We will continue with the curve from the first example above, which now looks like

$$E : y^2 - 4y = x^3 - \frac{17}{4}x^2 - 2x,$$

with point $P = (0, 0)$. Following the proof of the Lemma we add and subtract 4 from the left hand side giving

$$y^2 - 4y + 4 - 4 = RHS$$

Factoring gives

$$(y - 2)^2 = x^3 - \frac{17}{4}x^2 - 2x + 4.$$

We now let $y = y + 2$, and see that

$$(y + 2 - 2)^2 = x^3 - \frac{17}{4}x^2 - 2x + 4$$

$$\implies y^2 = x^3 - \frac{17}{4}x^2 - 2x + 4.$$

We now update our point to get $\hat{P} = (0, -2)$, which we can clearly see is a solution of our new curve.

Example 4.6. In our second example let's consider the curve

$$E : y^2 - y = x^3 - x^2,$$

with point $P = (0, 0)$. In this case we add and subtract $1/4$ from the left hand side giving

$$y^2 - y + \frac{1}{4} - \frac{1}{4} = x^3 - x^2$$

$$\implies (y - \frac{1}{2})^2 = x^3 - x^2 + \frac{1}{4}.$$

We set $y = y + \frac{1}{2}$, which gives

$$(y + \frac{1}{2} - \frac{1}{2})^2 = RHS$$

$$\implies y^2 = x^3 - x^2 + \frac{1}{4}$$

We now keep track of P, updating as in the statement of the Lemma to get $\hat{P} = (0, -\frac{1}{2})$

4.2 Generalization of Kubert's Table to Weierstrass Normal Form

We begin our work on development of a new primaility test by first generalizing Kubert's classification of torsion structures of elliptic curves to Weierstrass Normal form, so we can use the well defined doubling points formula. To convert the table we use the process from Section 4.1 as well as completing the square and keeping track of substitutions. The analogous table is listed below.

Theorem 4.7 (Generalization of Kubert's Boundedness Conjecture Over $\mathbb{Q}$)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Let T be a subgroup of $E_{tor}(\mathbb{Q})$. Then T is parameterizable in Weierstrass Normal Form.*

Table 2: *Parametrization of Torsion Structures in Weierstrass Normal Form*

1. $\mathbf{0}$:$y^2 = x^3 + ax^2 + bx + c$;$\Delta_1(a,b,c) \neq 0$, $\Delta_1(a,b,c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

2. $\mathbb{Z}/\mathbf{2}\mathbb{Z}$: $y^2 = x(x^2 + ax + b)$; $\Delta_1(a,b) \neq 0$, $\Delta_1(a,b) = a^2b^2 - 4b^3$.

3. $\mathbb{Z}/\mathbf{2}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $y^2 = x(x+r)(x+s)$, $r \neq 0 \neq s \neq r$.

4. $\mathbb{Z}/\mathbf{3}\mathbb{Z}$: $y^2 = x^3 + \alpha x^2 + \beta x + \gamma$ where $\beta \neq \frac{128\alpha^2}{27}$ and $\gamma = \frac{\beta}{2}$

   The form $E(b,c)$ is used in all parametrizations below where $E(b,c) : y^2 = x^3 + 4[(1-c)^2 - 4b]x^2 - 128b(1-c)x + 1024b^2$, $(0, -32b)$ is a torsion point of maximal order, $\Delta(b,c) = -4\alpha^3\gamma + \alpha^2\beta^2 + 18\alpha\beta\gamma - 4\beta^3 - 27\gamma^2$ where $\alpha = 4[(1-c)^2 - 4b]$, $\beta = -128b(1-c)$, and $\gamma = 1024b^2$.

5. $\mathbb{Z}/\mathbf{4}\mathbb{Z}$: $E(b,c)$, $c = 0$, $\Delta(b,c) \neq 0$.

6. $\mathbb{Z}/\mathbf{4}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b,c)$, $b = v^2 - \frac{1}{16}$, $v \neq 0, \pm\frac{1}{4}$, $c = 0$.

7. $\mathbb{Z}/\mathbf{8}\mathbb{Z}\times\mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b,c)$, $b = (2d-1)(d-1)$, $c = b/d$, $d = \alpha(8\alpha+2)/(8\alpha^2-1)$, $d(d-1)(2d-1)(8d^2 - 8d + 1) \neq 0$.

8. $\mathbb{Z}/\mathbf{8}\mathbb{Z}$: $E(b,c)$, $b = (2d-1)(d-1)$, $c = b/d$, $\Delta(b,c) \neq 0$.

9. $\mathbb{Z}/\mathbf{6}\mathbb{Z}$: $E(b,c)$, $b = c + c^2$, $\Delta(b,c) = c^6(c+1)^3(9c+1) \neq 0$.

10. $\mathbb{Z}/\mathbf{6}\mathbb{Z} \times \mathbb{Z}/\mathbf{2}\mathbb{Z}$: $E(b,c)$, $b = c + c^2$, $c = (10 - 2\alpha)/(\alpha^2 - 9)$, $\Delta(b,c) \neq 0$.

11. $\mathbb{Z}/\mathbf{12}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = m + \tau$, $f = m/(1-\tau)$, $m = (3\tau - 3\tau^2 - 1)/(\tau - 1)$, $\Delta(b,c) \neq 0$.

12. $\mathbb{Z}/\mathbf{9}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f(f-1) + 1$, $\Delta(b,c) \neq 0$.

13. $\mathbb{Z}/\mathbf{5}\mathbb{Z}$: $E(b,c)$, $b = c$, $\Delta(b,c) \neq 0$.

14. $\mathbb{Z}/\mathbf{10}\mathbb{Z}$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f^2/(f - (f-1)^2)$, $f \neq (f-1)^2$, $\Delta(b,c) \neq 0$.

15. $\mathbb{Z}/\mathbf{7}\mathbb{Z}$: $E(b,c)$, $b = d^3 - d^2$, $c = d^2 - d$, $\Delta(b,c) \neq 0$.

Clearly Kubert's table looks a bit more complicated in Weierstrass Normal Form, but from above, we have explicit formulas for doubling points once a curve is in Weierstrass Normal Form. This makes it extremely easy computationally to compute $2P$, $4P$, $8P$, ..., which we can use to test N for primality as follows. We assume N is prime, and that all of our group laws will hold, and look for a contradiction. We can take the torsion point of maximal order and compute multiples for curves from our table until we find a contradiction and have proved N is composite, or are satisfied with the probability that N is prime.

4.3 New Tests for Primality

In the previous sections we worked to convert elliptic curves into forms that we said would make it easier for them to be exploited to prove compositeness or primality of a number we wish to test, say N. In this section we develop new tests, that make use of our extensive previous knowledge of the torsion subgroups of elliptic curves, and the points on those curves. We begin with a theorem.

Theorem 4.8. *Suppose that $E/\mathbb{Q}$ is an elliptic curve with integer coefficients, $\gcd(N, \Delta_E) = 1$, where Δ_E is the discriminant, and suppose that $M_E(N)$ is*

$$M_E(N) = \#\left\{(x,y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : y^2 \equiv f(x) \pmod{n}\right\}.$$

1. *If $M_E(N) + 1 \not\equiv 0 \pmod{N_{tor}}$, then N is composite, where N_{tor} indicates the order of E_{tor}.*

2. *If point P has finite order m in $E(\mathbb{Q})$ but $\{P, 2P, 3P, \ldots, mP\}$ has less than m points in $\mathbb{Z}/N\mathbb{Z}$, then N is composite.*

3. *If $N + 1 - 2\sqrt{N} < M_E(N) < N + 1 + 2\sqrt{N}$ does not hold, then N is composite.*

4. *If there are more than $p^2 - 1$ points with order p on $E \pmod{N}$, where p is prime, then N is composite.*

Before we can prove this theorem we need a few theorems. First we need Lagrange's Theorem[8][2].

Theorem 4.9 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$ and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.*

Lagrange's theorem gives rise to an important Corollary for the proof of our theorem.

[8] For a proof of Lagrange's Theorem see Dummit and Foote

Corollary 4.10. *If G is a finite group and $x \in G$, then the order of x divides the order of G.*

Proof. Recall that the order of an element is the order of the subgroup generated by that element, so we simply apply Lagrange's Theorem to the subgroup generated by the element. □

Now we require the following theorem on the reduction of $E \pmod{p}$, where p is prime.

Theorem 4.11. *Let the group E_{tor} be defined as:*

$$E_{tor} = \{P = (x, y) \in E(\mathbb{Q}) | P \textit{ has finite order}\},$$

and the reduction modulo p map be defined as:

$$(x, y) \mapsto (\bar{x} = x \pmod{p}, \bar{y} = y \pmod{p}) \in \bar{E}(\mathbb{F}_p).$$

Then the reduction modulo p map $E_{tor} \mapsto \bar{E}(\mathbb{F}_p)$ is an injective homomorphism.

Proof. To show that the reduction modulo p map is we seek to show that it is a well defined map and

$$\overline{P_1 + P_2 + P_3} = \bar{P_1} + \bar{P_2} + \bar{P_3}.[2]$$

Clearly this map is well defined, because by the Nagell-Lutz Theorem, if P has finite order, then it has integer coordinates, and E has integer coefficients. To show that $\overline{P_1 + P_2 + P_3} = \bar{P_1} + \bar{P_2} + \bar{P_3}$ we need that $P_1 + P_2 + P_3 = \mathcal{O} \implies \bar{P_1} + \bar{P_2} + \bar{P_3} = \mathcal{O}$. We have a few different cases, first consder all points equal to $\mathcal{O}$. Then clearly $\mathcal{O} + \mathcal{O} + \mathcal{O} = \mathcal{O} \implies \bar{\mathcal{O}} + \bar{\mathcal{O}} + \bar{\mathcal{O}} = \mathcal{O}$. Now consider if only one of the points is equal to $\mathcal{O}$. Suppose $P_1 = \mathcal{O}$, then $\bar{P_1} = \mathcal{O}$, and we have

$$\mathcal{O} + P_2 + P_3 = \mathcal{O} \implies P_2 = -P_3,$$

so if negativity is preserved, then $\bar{P_1} + \bar{P_2} + \bar{P_3} = \mathcal{O}$[3]. However, $\overline{-P} = \overline{(x, -y)} = (\bar{x}, \overline{-y}) = -\bar{P}$, so negativity is preserved, and $\bar{P_1} + \bar{P_2} + \bar{P_3} = \mathcal{O}$. Next, we have all points not equal to $\mathcal{O}$. All points P_1, P_2, and P_3 have integer coordinates, and thus can be reduced modulo p.

Suppose that $P_1 + P_2 + P_3 = \mathcal{O}$, so they are all on a line, say $y = \lambda x + \nu$. From Section 3.1 we have $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = -\lambda x_3 - \nu$. By the Nagell-Lutz theorem, we have that x_1, x_2, x_3, y_3, and a are integers, and therefore, λ and $\nu \in \mathbb{Z}$, so they can be reduced modulo p. So we have

$$x^3 + ax^2 + bx + c - (\lambda x - \nu) = (x - x_1)(x - x_2)(x - x_3)$$
$$\implies x^3 + \bar{a}x^2 + \bar{b}x + \bar{c} - (\bar{\lambda}x - \bar{\nu}) = (x - \bar{x_1})(x - \bar{x_2})(x - \bar{x_3}).$$

Also, $\bar{\lambda}\bar{x_1} - \bar{n}u = \bar{y_1}$ and similarly for x_2 and x_3. Therefore, the line $y = \bar{\lambda}x + \bar{\nu}$ intersects $\bar{P_1}, \bar{P_2}, \bar{P_3}$, meaning that $\bar{P_1} + \bar{P_2} + \bar{P_3} = \mathcal{O}$[3]. Now we have that it is a homomorphism, it is easy to see that it is injective because clearly no integer point would be reduced to the identity, because that would mean it was reduced to infinity modulo p.

□

Example 4.12. In this example we will demonstrate the reduction modulo p map. Consider the curve

$$E : y^2 = x^3 - 176x^2 + 3072x + 147456,$$

which we know from Table 2 has a torsion subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The points of finite order on this curve are the set

$$S = \{(0, -384), (192, 1152), (48, 0), (192, -1152), (0, 384), \mathcal{O}\}.$$

The resultant points with E reduced over primes such that $p \nmid \Delta_E$ are shown below.

$\pmod{p}$	$S \pmod{p}$
$\pmod{5}$	$\{(0, -4), (2, 2), (3, 0), (2, -2), (0, 4), \mathcal{O}\}$
$\pmod{23}$	$\{(0, -16), (8, 2), (2, 0), (8, -2), (0, 16), \mathcal{O}\}$
$\pmod{167}$	$\{(0, -50), (25, 150), (48, 0), (25, -150), (0, -50), \mathcal{O}\}$
$\pmod{293}$	$\{(0, -91), (192, 273), (48, 0), (192, -273), (0, 91), \mathcal{O}\}$

Notice that for each prime we have always have 6 distinct points. However, if we try to reduce our set S modulo 36, we find that we get the set

$$\bar{S} = \{(0, -24), (12, 0), (12, 0), (12, 0), (0, 24), \mathcal{O}\},$$

which clearly does not have 6 distinct points. This is what we are exploiting in our test.

Finally, we need Hasse's Theorem.

Theorem 4.13 (Hasse's Theorem)**.** *[8] Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

or equivalently

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

We will not give a proof of Hasse's Theorem here as it is beyond the scope of this thesis, but Silverman gives a complete proof in his book.[8] Now we can prove Theorem 4.8 quite easily.

Proof of Theorem 4.8.

1. Let P be a point of maximum order, say $\text{ord}_E(p) = d$. We know from the corollary to Lagrange's Theorem that the order of an element must divide the order of the group. We also know from Theorem 4.11 that the reduction $\pmod{p}$ map is injective, so $d|N_{tor}$. Now we simply notice that

   $$N_{tor} = 1 + \#\left\{(x, y) \in \mathbb{Z}/n\mathbb{Z} : y^2 = x^3 + Ax^2 + Bx + C \equiv 0 \pmod{N}\right\},$$

   where the 1 is from the point at infinity, finishing the proof of the first case.

2. Suppose contrary to the statement of the second part of the theorem that $\{P, 2P, 3P, \ldots, mP\}$ has less than m points. Then $iP \equiv kP \pmod{N}$ for some i and k, and so N is composite.

3. If $N+1-2\sqrt{N} < M_E(N) < N+1+2\sqrt{N}$ is not true, then this violates Hasse's Thoerem, so N is composite.

4. By lemma 3.17, there are at most p^2-1 many points of order p for primes p on $E(\mathbb{F}_N)$, with N prime; so if this fails, we know that N is not prime.

This concludes the proof of Theorem 4.8 □

Now let's show how this might work with a simple example.

Example 4.14. We will try to prove that $n = 9$ is composite using this simple test in order to illustrate what is going on. We choose the curve $E : y^2 = x^3 - 12x^2 - 128x + 1024$, which we get from our generalization of Kubert's table with a $\mathbb{Z}/4\mathbb{Z}$ torsion subgroup. We see that $\Delta_E = 17825792$, $\gcd(\Delta_E, 9) = 1$. We know from Kubert that the point $P = (0, -32)$ is a point of maximal order, so $\text{ord}_E(P) = 4$. However, if we reduce $E \pmod{9}$, we get $E : y^2 = x^3 + 6x^2 + 7x + 7$. We see all the possibilities for x in the table below.

$x \pmod{9}$	$x^2 \pmod{9}$	$x^3 + 6x^2 + 7x + 7 \pmod{8}$
0	0	7
1	1	3
2	4	8
3	0	1
4	7	6
5	7	2
6	0	4
7	4	0
8	1	5

The quadratic residues $\pmod{9}$ are 0, 1, 4, and 7 so from the table we see that there are 9 possible solutions, and one point at infinity. But $4 \nmid 10$, so $n = 9$ is composite.

Example 4.15. We will now try to prove 39 is composite. We choose the curve from $\mathbb{Z}/5\mathbb{Z}$ in our generalization of Kubert's with $b = 1$. This gives

$$E : y^2 = x^3 - 16x^2 + 1024,$$

with discriminant $\Delta_E = -11534336 = -2^{20} \cdot 11$. We see easily that $\gcd(\Delta_E, 39) = 1$, and know from our table that $P = (0, -32)$ is a point of order 5. Now using maple we check to see how many solutions there are to

$$y^2 \equiv x^3 - 16x^2 + 1024 \pmod{39},$$

and find that there are 36 integer solutions. If we add the one point at infinity we get a total of 37, but notice that $37 \nmid \Delta_E$, so we conclude that 39 is composite.

Example 4.16. We can use the curve $E : y^2 = x^3 - 16x^2 + 2560x + 25600$, which from our generlization of Kubert's Table we know to have a torsion subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$, to prove that 1729, one of the Carmichael Numbers, is composite. We find the discriminant is $\Delta_E = -101580800000$, and $\gcd(1729, \Delta_E) = 1$. We use Maple again to find that there are 4104 solutions, plus one point at infinity, giving 4105. This means that 1729 passes the first test of Theorem 4.8, as clearly $5|4105$, but notice that $1729 + 1 + 2\sqrt{1729} < 1814 < 4104 = M_E(N)$, so we know by condition 3 that 1729 is composite. Notice how simple and quickly we could do this, whereas if we tried to use some of the most basic primality tests from Section 2 we might have concluded incorrectly that 1729 was prime.

Example 4.17. Finally we will show that the Carmichael Number 15841 is composite using the curve $E : y^2 = x^3 + 32x^2 + 5376x + 50176$ with torsion subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$. The discriminant of this curve is $\Delta_E = -511079088128$, and $\gcd(15841, \Delta_E) = 1$, so we can use our test. We count solutions using Maple, and find that there are 17316 solutions, plus one point at infinity, but $5 \nmid 17317$, so we know that 15841 is composite. We also can use our third condition to prove 15841 is composite, so our test detects the compositeness of 15841 in two ways, whereas many simple primality tests miss it entirely.

Remark 4.18. Computationally we begin to have difficulty counting solutions for numbers over about 10,000. This is one of the aspects in which this test needs to be further developed for it to be implemented efficiently, as the focus of primality testing is on numbers significantly larger than 10,000.

A natural question that we might ask now that we have seen how this compositeness test works is how often we expect it to fail? We know from our generalization of Kubert's Table that $(0, -32b)$ is a torsion point of maximal order on 11 different curves. Let's consider the family of curves with a torsion subgroup isomorphic to $\mathbb{Z}/k\mathbb{Z}$ where $k \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. Then we know that a point P of maximal order has coordinates $(0, -32b)$. We also know that $(k-1)P = -P$ so that $P + (k-1)P = \mathcal{O}$. Therefore, if

$$P \equiv (k-1)P \pmod{N},$$

where N is an integer, then the test will detect that N is composite. So for each curve we have the condition that $64b \equiv 0 \pmod{N}$ with $\gcd(N, \Delta_E) = 1$ implies compositeness. But we know that there are infinitely many b such that $N|b$, so all that is left is for us to find curves with the discriminant condition met. So it would seem extremely unlikely for us to miss a composite number with this test. However, we can go further as the following theorem shows.

Theorem 4.19. *If N is a composite number, then Theorem 4.8 will always detect it.*

Proof. For simplicity assume now that N is squarefree, such that $N = q_1 q_2 \dots q_t$, where all the q_i are distinct primes. Choose $E : y^2 = f(x)$ such that $\mathbb{Z}/p\mathbb{Z} \subseteq E_{tor}(\mathbb{Q})$, where $p \in \{2, 3, 5, 7\}$, and $\gcd(N, \Delta_E) = 1$. For each $1 \leq i \leq t$ define

$$M_i := \#E(\mathbb{F}_{q_i}).$$

We know that $p|N_i$ for all i, because the order of an element divides the order of the group by the corollary to Theorem 4.9, so define

$$M_i^* := M_i - 1 = \#\{(x,y) \pmod{q_i} : y^2 \equiv f(x) \pmod{q_i}\}.$$

By the Chinese Remainder Theorem, there will be $M_1^* M_2^* \dots M_t^*$ many solutions modulo $q_1 q_2 \dots q_t$.

Case 1 ($t \equiv 0 \pmod 2$)**.** $N = q_1 q_2 \dots q_t$, so then

$$\#E(\mathbb{F}_N) = M_1^* M_2^* \dots M_t^* + 1,$$

where the one is from the point at infinity. But notice, each $M_i^* \equiv -1 \pmod p$, so then we have

$$M_1^* M_2^* \dots M_t^* + 1 \equiv (-1)^t + 1 \equiv 2 \pmod p \implies p \nmid \#E(\mathbb{F}_N)$$

as long as $p \neq 2$, so N is composite.

Case 2 ($t \equiv 1 \pmod 2$)**.** Notice here that modulo q_1 we have $p-1$ many points of order p, and similarly for $q_2, q_3, \dots q_t$. Therefore, modulo $q_1 q_2 \dots q_t$ we have $(p-1)^t$ many points of order p. But we know that $t \geq 3$, because if not N would be prime, which means there are at least $(p-1)^3$ many points of order p modulo $q_1 q_2 \dots q_t$. For $p > 3$, $(p-1)^3 > p^2 - 1$, so we know that N is composite.

□

Remark 4.20. Notice that in this proof we did not address two cases: first, that N is not square free, and second, that N is a prime power. However, these cases do not worry us, because if N is not square free, say $N = q_1^{a_1} q_2^{a_2} \dots q_t^{a_t}$, then we can set $n_i = q_i^{a_i}$, and use the Chinese Remainder Theorem with $N = n_1 n_2 \dots n_t$. If N is a prime power, say $N = q^a$, then notice that if x is a solution to $y^2 = f(x) \pmod q$, then so is $x + q, x + 2q, \dots$, so the number of solutions explodes.

Remark 4.21. If $p = 5$ earlier we showed that there are at most 32 points of order 5. However, for $t = 3$, $(5-1)^3 = 64 > 32$, so we are still over the bound. Similarly for $p = 7$, we get $6^3 = 216 > 64$.

Remark 4.22. One thing to notice is that for the first case we said nothing about when $p = 2$, and for the second, nothing about $p = 2, 3$. However, this does not matter because we still showed that the test will work for $p = 5$ and 7 for both cases. Also, for the second case, it could easily be that $(3-1)^t > 3^2 - 1$, it is just not necessary. What this proof shows is that it is more likely to detect compositeness if we use curves with torsion subgroups isomorphic to $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$, something to keep in mind if we tried to implement this test efficiently.

Remark 4.23. The power of this theorem can not be understated, as we have shown that we can detect *all* composite numbers while only ever having to divide by 2, 3, 5, or 7.

The beauty of this test is the utilization of previous study of elliptic curves to minimize the computional difficulty, however, we still have a handful of difficult tasks if we were to implement this test effectively. The primary issuee comes with counting solutions as we remarked earlier in this section. In reality we would be using this test for extremely large numbers, so it would be necessary to find a more efficient way to count solutions. Work has been done in this area, although it is beyond the scope of this thesis. What we can say, however, is that there are theoretical point counting algortihms which run in polynomial time in the logarithm of p, and have been able to count the points on an elliptic curve over a 200 digit prime[1]. For more on point counting algorithms one can look into the work of Schoof, Elkies, and Atkins, specifically Schoof's 1995 article "Counting points on elliptic curves over finite fields"[7]. The work done on this is rather incredible to be able to reduce the problem of point counting to polynomial time in the logarithm of p, and makes us believe that our test can be practical if implemented correctly.

5 Concluding Remarks

In this thesis we introduced the importance of primality testing and factoring algorithms in Section 2.1, and used the rest of Section 2 to cover basic number theory and the beginnnings of primality testing and factoring algorithms. We began in Section 2.2 by proving Fermat's Little Theorem and demonstrating how it could be used for a very basic test for compositeness. In Section 2.3 we described the more advanced Rabin-Miller test, which is often used as a first step before plugging a number N into the more advanced tests from later in the thesis. Finally Section 2.4 described Pollard's $p-1$ Method, which has the structure that many of the more advanced tests try to mimic. In Section 3 we began by describing the group law and doubling points formula. We then defined the discriminant of a curve, and finally have the statement of the Mordell-Weil Theorem. In Section 3.2 we focus on the work of Mazur, Nagell-Lutz, and Kubert, which fully classifies the possible torsion structures as well as categorizes *all* elliptic curves based on their torsion subgroups. Finally in Section 3.3 we describe the Goldwasser-Killian Test, a current elliptic curve primality test, and then follow by describing Lenstra's elliptic curve factoring algorithm, one of the methods in use today.

Section 4 is where we developed our own contributions. We began by proving that an elliptic curve E in one Weierstrass form can be easily converted to another Weierstrass form that may be more preferable for certain applications. In Section 4.2 we applied the work of Section 4.1 to generalize Kubert's classification of elliptic curves to a more usable form in terms of primality testing. Section 4.3, however, is where the most interesting developments were proven. We began with Theorem 4.8, a new primality test with 4 separate conditions to test that utilize our previous knowledge of elliptic curves and their torsion structures. Most importantly though is Theorem 4.19, which shows that our primality test detects *all* composite integers, and further, in the proof of Theorem 4.19 we noticed that we can detect any composite integer without ever having to divide by more than 7. With more time we would next look into setting up our test for efficient implementation, which includes finding better ways to count the number of points on an elliptic curve, and attempt to quantify the expected run time of our test using computational algebraic number theory.

References

[1] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 2011.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra Third Edition.* John Wiley and Sons, Inc., Hoboken, NJ, 2004.

[3] Michael Galperin. Torsion points of elliptic curves. `http://math.uchicago.edu/~may/REU2013/REUPapers/Galperin.pdf`. [Online: Accessed 5 Feb 2017].

[4] W.R. Alford; Andrew Granville; and Carl Pomerance. There are infinitely many carmichael numbers. *Annals of Mathematics*, 139:703–722, 1994.

[5] J. S. Kraft and L. C. Washington. *An Introduction to Number Theory with Cryptography.* CRC Press, 2014.

[6] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, s3-33(2):193–237, 1976.

[7] René Schoof. Counting points on elliptic curves over finite fields. *Journal de thorie des nombres de Bordeaux*, 7(1):219–254, 1995.

[8] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[9] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer-Verlag, 1992.