Elliptic Curves for Primality Testing

Leo Toueg, 20062982

April 27, 2022

Contents

Abstract

There currently exist many algorithms that determine the primality of a number. However, there are two classes of such algorithms. Some of them are deterministic, others probabilistic. A deterministic algorithm is an algorithm that, given a particular input, will always produce the same output. In our case, probabilistic prime-proving algorithms return whether a given integer is prime, with an associated probability, or whether it is not prime. In this paper, we will look at how elliptic curves can be used for primality proving. First, we will go over elliptic curves, then the primality proving algorithms.

1 Introduction

Mathematicians have been studying prime numbers since the abstraction of numbers in the study of mathematics. Determining whether or not a number is prime is not an easy task. Interestingly, for thousands of years, the largest known prime number was 8191. As number theory progressed, finding the newest largest prime became a challenge to mathematicians. Nowadays, there exist various algorithms that determine the primality of a number, both probabilistically and deterministically. In this paper, I will go over the building blocks that paved the way for two such algorithms. We will introduce the Elliptic Curve Primality Proving Algorithm (ECPP), as well as the Goldwasser-Killian (GK) algorithm. We will assume no prior knowledge on elliptic curves. We will therefore begin with a historical introduction of elliptic curves, by showing one of their earliest appearances in number theory. We will look at one of the first significant connections between elliptic curves and number theory. This introduction will motivate an intuition for finding points on elliptic curves, considered over finite fields. We will introduce Hasse's Theorem, which will allow us to put bounds on the number of points of an elliptic curve, considered over a finite field of characteristic p, where p is a prime.

2 Elliptic Curves

An Elliptic Curve is an equation of the form $Y^2 = X^3 + aX + b$, where the cubic polynomial in the right hand side has a non-zero discriminant and a, b are elements in a field (If the field's characteristic is different from 2 and 3, then any cubic plane algebraic curve can be expressed as above after a change of variables). Over the last few decades, elliptic curves have been very useful, even being used to solve Fermat's Last Theorem. In this section, we will introduce an elliptic curve by looking at an instance of the congruent number problem.

2.1 Congruent Number Problem

Definition 2.1 (Congruent number)**.** A number n is **congruent** if it is a positive integer that is equal to the area of a right angled triangle with three rational number sides.

For example, 6 is a congruent number (triangle with sides 3, 4 and 5 has an area of 6). The congruent number problem is still a generally open question in mathematics.

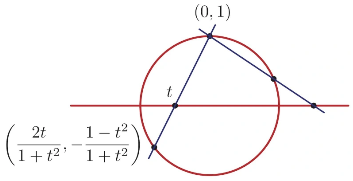

Figure 1: Finding rational points on a circle

There is still no general algorithm that determines whether a number is congruent or not. However, Fermat proved that no square number can be congruent, a result which surprisingly implies that there are no rational points on a certain class of Elliptic Curves. We will not look at Fermat's proof of this theorem, as it is out of the scope of this paper. For the purposes of our introduction to Elliptic Curves, let us consider the congruent number problem for $n = 1$.

Theorem 1 (Fermat)**.** There are no triangle with rational side lengths such that the area of the triangle is 1. That is, 1 is not a congruent number.

Proof. We begin with a right angled triangle with integer side lengths a, b and c satisfying $a^2 + b^2 = c^2$. We can re-scale this triangle, expressing it as: $a^2/c^2 + b^2/c^2 = 1$. Let $x = a/c$ and $y = a/b$. Our previous relation then becomes $x^2 + y^2 = 1$, or the equation for the unit circle.To find all rational points on the circle, we can take any known rational point, such as (0,1), and draw a line with rational slope t from this point. This line would intersect the circle at another rational point. Any point on a line passing through (0,1) and intersecting the unit circle satisfies the following two equations:

$$y = t(x + 1) \tag{1}$$

$$x^2 + y^2 = 1 \tag{2}$$

Solving for x and y we find all rational points on the unit circle.

$$x = (1 - t^2)/(t^2 - 1) \tag{3}$$

$$y = 2t/(t^2 + 1) \tag{4}$$

Now, recall that we are trying to find a rational side length right angled triangle with area 1. Since our triangle has sides a and b, the area of our triangle is $\frac{1}{2}ab$. Rewriting in terms of x and y, we find an expression for the area:

$$\begin{aligned}\frac{1}{2}ab &= \frac{1}{2}(cx)(cy)\\ &= \frac{1}{2}c^2xy\\ &= \frac{1}{2}c^2(\frac{1-t^2}{t^2+1})(\frac{2t}{t^2+1})\end{aligned}$$

Cancelling the 2 and the 1/2 , we know that the Left Hand Side is equal to 1, so:

$$1 = \frac{c^2(1-t^2)t}{t^2+1}$$

Rearranging:

$$(\frac{t^2+1}{c})^2 = t - t^3$$

Letting $X = -t$ and $Y = \dfrac{t^2+1}{c}$, we get the following:

$$Y^2 = X^3 - X$$

Note that $X^3 - X$ has non-zero discriminant. Thus $Y^2 = X^3 - X$ is an elliptic curve. Therefore, we have reduced the congruent number problem for n = 1 to finding rational solutions the elliptic curve $Y^2 = X^3 - X$. As it turns out, Fermat proved that this Elliptic Curve had no rational solutions other than (-1,0), (0,0), (1,0), and the point at infinity, using the method of descent. Now that we have introduced the notion of elliptic curves, we will begin a more formal discussion on elliptic curves.

2.2 Group operation on Elliptic Curves

We will start by defining the group operations on an elliptic curve. It can be shown that any line intersects an elliptic curve at 3 points, by Bezout's Theorem. So, we can take two points on the elliptic curve, say P and Q. Define a new point, by drawing a line through P and Q, intersecting the curve at a new point R. Reflecting this point across the x-axis defines addition. The group structure only holds if we include a point called the point at infinity, the identity element. It can be thought of geometrically as

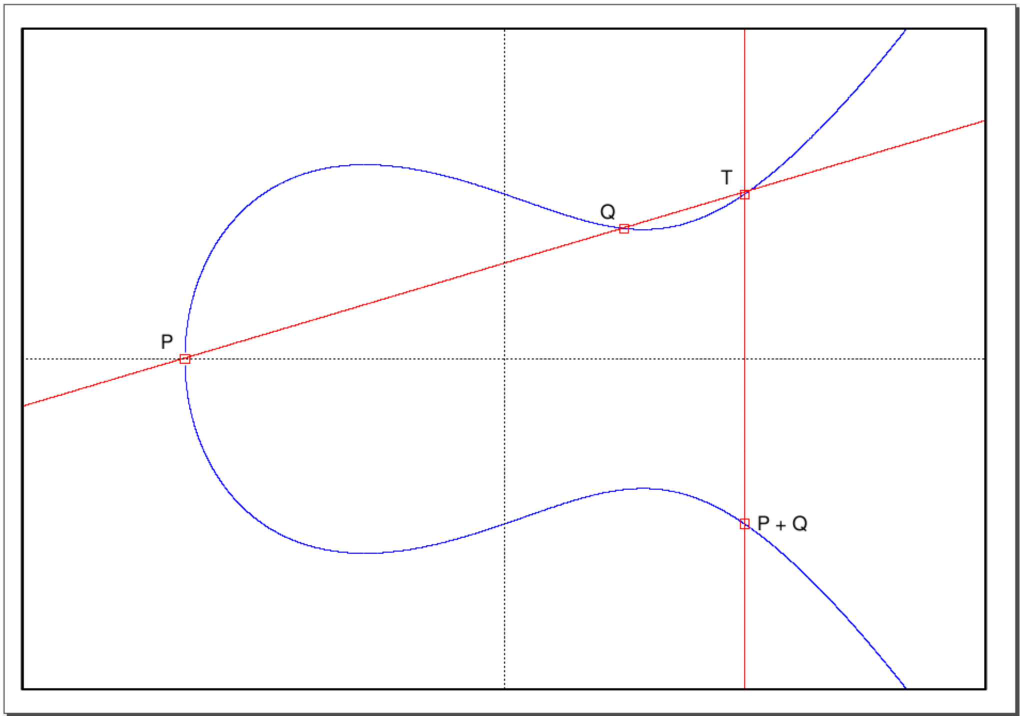

Figure 2: Elliptic Curve Group Law (Point Addition)

the result of adding two points that are vertically aligned, P and -P. For this reason, we have: P + (-P) = ∞. Defining addition formally:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

Where λ is the slope of the line connecting points P and Q, given by:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

If P is not distinct from Q, or P=Q, then finding the slope of the line connecting P to Q is simply the tangent line to the curve at that point. Hence, to find the value of λ in this case we must take the derivative of the EC, using implicit differentiation:

$$\frac{dy}{dx}(y^2 = x^3 + ax + b)$$
$$2y\frac{dy}{dx} = 3x^2 + a$$
$$\frac{dy}{dx}(x_1, y_1) = \frac{3x_1^2 + a}{2y_1} = \lambda$$

To summarize, we get the following group operation:

$$P + Q = R = ((\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1)$$
$$2P = ((\frac{3x_1^2 + a}{2y_1})^2 - 2x_1, \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1)$$

Under these operations, rational points on an elliptic curve form an abelian group, along with the point at infinity O, serving as the identity element. Summarizing the results is the following theorem:

Theorem 2.1. Let E be an elliptic curve over a field K. Further, let

$$E(K) := \{(x, y) \in K \times K \mid Y^2 = X^3 + aX + b\} \cup \{O\}$$

be the set of K-rational points on E. Then $(E(K), +, O)$ is an abelian group.

Observe that if $P = (x_1, y_1), Q = (x_2, y_2) \in E(K)$, then $\lambda \in K$ and $R = P + Q = (x_3, -y_3) \in E(K)$. This means the addition is well-defined on E(K). Now that we have a group structure on elliptic curves, we will consider them over finite fields, over the modulus of some prime p. In this context, the points P and Q have coordinates modulo p and the group operations are the ones previously defined. But how do we find the points in the group of an elliptic curve modulus p? Since values for x in the formula for the elliptic curve can only be integers in $\mathbb{F}_p$, we can create a table enumerating the value of y^2 for each value $x \leq p - 1$, and see if these values have square roots. However, the problem of finding whether or not a given number has a square root in $\mathbb{F}_p$ is not easy. Naturally, one question we can ask ourselves is: how many points are there on a given elliptic curve? This brings us to the next section, where we introduce Hasse's Theorem.

2.3 Elliptic Curves and Number theory

As we have seen in this paper, the set of rational points on an elliptic curve over $\mathbb{Q}$ defines an abelian group. Of course, if an elliptic curve is defined over a finite field, the number of points on it is also finite. While in general, the number of points that lie on an elliptic curve is rather difficult to compute, there is a theorem which has been developed to give an algorithm for computing that exact number of points on an elliptic curve over finite fields.

Theorem 2.2 (Hasse's Theorem). [1] Let $\mathbb{F}_q$ be a finite field (i.e. *the* finite field with q elements, where q is a power of some prime p) and E be an elliptic curve over $\mathbb{F}_q$. Then the number of rational points on E satisfies

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

Here, $E(\mathbb{F}_q)$ denotes the number of points on the curve E over $\mathbb{F}_q$. But there are some algorithms used to compute the exact number of points on a given elliptic curve. For example, one of them is Schoof's algorithm. The implications of Hasse's theorem are deep, extending well beyond the realm of elliptic curves. Indeed, it is equivalent to the determination of the absolute value of the roots of the local zeta-function of E. As such, the proof escapes the scope of this paper, however the reader is encouraged to familiarize themselves with it. We can now start looking at primality proving algorithms.

3 Primality Proving Algorithms

Primality Proving algorithms are a class of algorithms that seek to determine whether or not a given number is prime. There are two types of such algorithms. The first type determines with certainty whether or not the input is prime. The second returns either: a guarantee of the compositeness of the input, or the primality of the input associated with a certain probability. In this section, we will look at both the Goldwasser-Killian (GK) and Elliptic Curve Primality Proving (ECPP) algorithms.

3.1 Goldwasser-Killian

Before introducing the test, we will need the following theorem, which fixes an elliptic curve in Weierstrass form $Y^2 = X^3 + aX + b$, where a and b are in a finite ring $\mathbb{F}_n$ such that the parameters define a proper Elliptic Curve:

Theorem 3.1. Let n, a, b be integers such that $gcd(4a^3 - 27b^2, n) = 1$. If there is a prime q such that $q \geq \sqrt{n} + 2\sqrt[4]{n} + 1$, and a point M on an elliptic curve $Y^2 = X^3 + aX + b$ over the ring $\mathbb{F}_n$, different from the point at infinity, such that qM is defined and $qM = \infty$, then n is prime.

Proof. Suppose that there is a prime divisor of n. Then there must be some prime divisor r of n with $r \leq \sqrt{n}$. Consider the projection of the elliptic curve E into $\mathbb{Z}/\text{r}\mathbb{Z}$, denoted $\overline{E}$. Since $gcd(4a^3 - 27x^2, n) = 1$, then $4a^3 - 27b^2 \not\equiv 0 \ mod(r)$. Also, r is prime, so $\overline{E}$ gives a group. Consider the projection of the point M onto $\overline{E}$, demoted M_r, where

[1] proof: J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag

$M_r = M \bmod r$. Since $qM = \infty$ in E, $qM_r = \infty$ in $\overline{E}$. So, the order of M_r divides q. We also set M != ∞ in E, so $M_r! = \infty$ in $\overline{E}$. Therefore the order of $M_r! = 1$, and thus the order of M_r is exactly q. We can apply Hasse's Theorem to the number of points in $\overline{E}$, and use the fact $r \leq \sqrt{n}$, to get:

$$|E(\mathbb{Z}/r\mathbb{Z})| \leq r + 2\sqrt{r} + 1 \leq \sqrt{n} + 2\sqrt[4]{n} + 1.$$

By our initial hypothesis, q is greater than the right hand side of the inequality. Hence the order of M_r is greater than the order of the group. This is clearly a contradiction. So, n must be a prime.

3.2 GK Algorithm

In order to use this theorem, one must find a suitable elliptic curve with $|E(\mathbb{Z}/r\mathbb{Z})| = 2q$ where q passes a probabilistic primality test (such as Miller-Rabin). However, one can now vary through many elliptic curves until finding a group of this form. One also needs to find an $M \in E$ such that $qM = \infty$. Notice that since $|E(\mathbb{Z}/r\mathbb{Z})| = 2q$, when q is prime there is an element $x \in E$ of order q. Thus, approximately half of the elements have order q. Once an elliptic curve with 2q points and an $M \in E$ are found such that $qM = \infty$, it is shown that n is prime if q is prime. Notice that for large n, if n is prime, by Hasse's Theorem, $n + 1 - 2\sqrt{n} \leq 2q \leq n + 2\sqrt{n} + 1 \implies q \approx \frac{n}{2}$. This means the prime to be checked is approximately halved on each iteration. The test can be used to find a chain of likely primes$n > q_1 > q_2 > ... > q_n$, and once some q_i is small enough that is is a known prime, or can be proven to be prime using another method, the whole chain of number is proven to be prime. Unfortunately, this method is unpractical due to the amount of time it takes to find a curve fitting the proper criteria, but over time this is getting easier with computers.

3.3 ECPP

The ECPP algorithm comes in four parts:

- Generate Curve(p)
- Find-Point(p,q,(a,b))
- Prove-Prime(p)
- Check-Prime(certificate)

3.3.1 Generate Curve(p)

1. Randomly select $a, b \in \mathbb{F}_n$ such that $gcd(4a^3+27b^2, n) = 1, p+1-\lfloor\sqrt{p} \leq |E_{(a,b)}| \leq p+1+\lfloor\sqrt{p}$ and $|E_{(a,b)}|$ is even. There exists a nice probabilistic proof that assures the distribution of curves satisfying these properties is almost normal, and there also exists an efficient algorithm for computing $|E_{(a,b)}|$, the number of rational points on the elliptic curve E defined by a and b.
2. Set $q = \frac{|E_{(a,b)}|}{2}$ If q is divisible by 2 or 3, retry step 1.

3. Since we need q to be prime, we run a probabilistic primality test on q. If we find that q is composite, then retry from step 1. If q does not return composite, then q is a probable prime. The case where the probable prime turns out to be composite is addressed in the analysis.

4. Return (a,b), q

We have now selected the EC that we will use to test the primality of n. Our next objective is to find a point L on $E_{(a,b)}$ such that $qL = 0$.

3.3.2 Find-Point(p,q,(a,b))

1. Randomly select $x \in \mathbb{F}_p$ until $x^3 + ax + b$ is a quadratic residue.

2. Compute the square root of $x^3 + ax + b$ and set y to be one of the square roots. Let $L = (x, y)$ a point on $E_{(a,b)}$ over the field $\mathbb{F}_p$

3. If $qL \neq 0$, retry from step 1

4. Return L

3.3.3 Prove-Prime(p)

1. Let $i = 0, p_0 = p$ and define a number Low $= \max(2^{\log p^{\frac{C}{\log\log\log p}}}, 37)$ to be the lower bound for values p_i that we will test, where C is some constant such that a deterministic prime testing algorithm will run in polynomial time in step 3.

2. While $p_i <$ Low:

   (a) Run algorithm 1 with input parameter p_i to find an elliptic curve $E_{(a,b)}$ and another prime $p_i + 1$

   (b) Run algorithm 2 Find-Point with input $(p_i, p_i{+}1, (a, b))$ and set output equal to L

   (c) Set $i = i + 1$

   (d) If any of the p_i is divisible by 2 or 3, or if $i \geq (\log p)^{\log\log p}$, break the loop and retry from step 1

3. Use a deterministic algorithm to test if p_i is prime. If p_i is not prime, retry from step 1.

4. Return the prime certificate, along with corresponding elliptic curves and Points, then proceed to certificate-checking Algorithm.

3.3.4 Check-Prime(certificate)

1. Reject if $p_i > \max(2^{\log p^{\frac{C}{\log \log \log p}}}, 37)$
2. Use a near-polynomial time deterministic algorithm to test if p_i is prime. If it is not prime, reject it.
3. For each j from 0 to i-1 inclusive, reject if any of the following assertions fail:
   (a) $2 \not| p_j$
   (b) $2 \not| p_j$
   (c) $gcd(4(a_j)^3 + 27(b_j)^2, p_j) = 1$
   (d) $p_(j + 1) > (\sqrt[4]{n} + 1)^2$
   (e) $L_j \neq 0$
   (f) $p_(j + 1)L_j = 0$
4. Accept p_0 as prime.

We conclude this paper with a discussion and analysis on ECPP.

3.3.5 ECPP Analysis

The overall approach to the ECPP is to recduce the question of the primality of p to the question of primality of a smaller prime q, where $q \leq \frac{p}{2} + o(p)$. This results in a chain of primes, called a prime certificate, with p_0 small enough to be checked manually. It is for this reason that we define the value Low as the lower bound on q since we are only interested in finding primes q small enough that it is easy to check its primality. The Generate-Curve Algorithm generates a random elliptic curve with order 2q where q is a probable prime determined by a probabilistic primality testing algorithm. To do so, we randomly select $a, b \in \mathbb{F}_p$ until the necessary conditions hold. The Find-Point Algorithm takes a curve found in the Generate-Curve, and finds a point such that the order of the point is q. This is done by randomly selecting values for L. This is effective because about half the points will have order q. Lastly, the Prove-Prime algorithm generates a chain of primes, forming a certificate for the prime we are interested in proving. This algorithm repeats and terminates whenever one of the primes in the chain is small enough to be deterministically proven. Since the q generated by the Generate-Curve is only probably prime, there may be cases where q is composite. In 3.3.3, we handled this case, since if i becomes too large, then the loop breaks and tries a different elliptic curve. We can therefore set a bound on the number of elliptic curves to test before we conclude with a very high probability that p is in fact composite.

4 References

[1] Schoof, R. (2008). Four primality testing algorithms. arXiv preprint arXiv:0801.3840.
[2] Goldwasser, S., Kilian, J. (1999). Primality testing using elliptic curves. Journal of the ACM (JACM), 46(4), 450-472.