ELLIPTIC CURVE CRYPTOGRAPHY

MAEVE COATES WELSH

Abstract. In this expository paper, we cover some basics of elliptic curves before proceeding to the main goal of the paper, which is to discuss the applications of these curves to the theory of cryptography. We primarily follow chapters 4 through 7 of Washington's Elliptic Curves: Number Theory and Cryptography [1] in the following manner: We start by proving Hasse's Theorem, and introduce the Discrete Logarithm Problem, along with several attacks and encryption methods that revolve around it. We then present some applications of elliptic curves to factorization problems.

Contents

1. Introduction

Elliptic curve cryptography largely relies on the algebraic structure of elliptic curves, usually over finite fields, and they are defined in the following way.

Definition 1.1 An **elliptic curve** E is a curve (usually) of the form $y^2 = x^3 + Ax + B$, where A and B are constant.

This equation is called the **Weierstrass equation**, and we will use it throughout the paper [2]. Let K be a field. If $A, B \in K$, we say that E is defined over K. We can look at the set of points of E defined over a field $L \supset K$, $E(L) = \{(x, y) \in L \times L | y^2 = x^3 + Ax + B\} \cup \{\infty\}$. Then, $E(L)$ can be given a group structure where the elements are points, and the operation is point addition. Notably, Mordell and Weil showed in 1928 that $E(K)$ is a finitely generated abelian group for any number field K [3] [4].
Let's briefly recall how the group structure is defined. Let E be the previous curve which is defined over the real numbers. Given two points P_1, and P_2, we define their sum in the following way:

Date: October 10, 2017.

Draw a line through P_1 and P_2, and let P_3' be the point where the line intersects E again, as in **Figure 1**. Then, reflect P_3' across the $x-$axis to obtain the point $P_3 = P_1 + P_2$. We can also find $2P_1 = P_1 + P_1$ by drawing the tangent line to the curve at P_1.

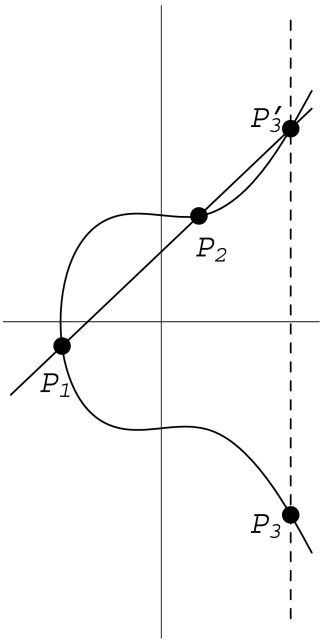

FIGURE 1. Point addition on elliptic curves [1].

The benefit of this structure to the field of cryptography is that point addition on elliptic curves is quite difficult and time consuming. Moreover, as we will see later, if we are given two points P and Q, and told that $kP = Q$, it is very hard and time-consuming to find k. Classical methods of solving this problem have faster specializations for certain groups, which means that for the problem to be hard, the group in question must be a large prime field. However, elliptic curve methods are equally difficult over prime groups and other similarly sized generic groups, and so they have no such specializations. Thus cryptography using elliptic curves is more efficient than using classical methods, because the elliptic curve variations of the classical methods offer more security over smaller groups. Solving this problem, which is called the **discrete logarithm problem**, is central to elliptic curve cryptography, and we will look at it more closely in Section 3.

Central to this problem are the **n-torsion** points of a curve, or the points in the set $E[n] = \{P \in E(\overline{K}) | nP = \infty\}$ where E is an elliptic curve over K. Here, $\overline{K}$ denotes the algebraic closure of K. Of course, when $K = \mathbb{F}_q$, where q is prime or a power of a prime, it follows that all points of E are torsion points for some n.

Additionally, the group structure of the curves gives rise to the following corollary of the Chinese Remainder Theorem:

Corollary 1.2. *For odd integers n_1, n_2 that are relatively prime, and an elliptic curve E defined over $\mathbb{Z}/n_1n_2\mathbb{Z}$, there exists a group isomorphism*

$$E(\mathbb{Z}/n_1n_2\mathbb{Z}) \cong E(\mathbb{Z}/n_1\mathbb{Z}) \oplus E(\mathbb{Z}/n_2\mathbb{Z}).$$

2. Hasse's Theorem

One incredibly useful theorem that occurs frequently in elliptic curve cryptography is **Hasse's Theorem**, which states that the order of the group of an elliptic curve over a finite field has both an upper and lower bound [5]. Notably, the bounds depend only on the finite field and not on the curve. However, this theorem takes some setup in order to prove it.

Definition 2.1. Let E be an elliptic curve defined over a field K. We define an elliptic curve **endomorphism** α as a homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ given by rational functions. This means that $\alpha(x, y) = (F_1(x, y), F_2(x, y))$ where F_1 and F_2 are rational functions.

Elliptic curves may be written in the form $y^2 = x^3 + Ax + B$, and so we can replace even powers of y with a polynomial in x, and odd powers of y with y times a polynomial in x. With some toggling, an endomorphism α as above may actually be written as $\alpha(x, y) = (f_1(x), yf_2(x))$ where f_1 and f_2 are rational functions. If $f_1(x) = \frac{p(x)}{q(x)}$ where p, q are polynomials, we define the **degree** of the endomorphism α to be $\deg(\alpha) = max\{\deg(p), \deg(q)\}$.

Definition 2.2 The **Frobenius Endomorphism** defined for an elliptic curve E over a finite field $\mathbb{F}_q$ is the map $\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ that sends a point (x, y) to the point (x^q, y^q). Clearly, $\deg(\phi_q) = q$.

The Frobenius endomorphism is not separable; however, the endomorphism $\phi_q - 1$ is, and we can use it to help prove Hasse's theorem by relating the order of the group of an elliptic curve to the degree of $\phi_q - 1$ in the following way.

Proposition 2.3. *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E defined over a field K. Then,* $\deg(\alpha) = |\ker(\alpha)|$.

Proof. Let $\alpha(x, y) = (f_1(x), yf_2(x))$ where f_1, f_2 are rational functions. Let $f_1(x) = \frac{p(x)}{q(x)}$. Then because α is separable, it follows that $f_1'(x) \neq 0$. Therefore $p'(x)q(x) - p(x)q'(x) \neq 0$. Consider the set $S = \{x \in \overline{K} | (p'q - q'p)(x) \cdot q(x) = 0\}$.
Because $p'(x)q(x) - p(x)q'(x) \neq 0$, S must be finite. Thus $\alpha(S)$ is finite, even though $f_1(x)$ obtains infinitely many distinct values as x ranges over $\overline{K}$. Therefore $\alpha(E(\overline{K}))$ is infinite. This allows us to find a point $(a, b) \in E(\overline{K})$ such that

1. $a, b \neq 0$ and $(a, b) \neq \infty$
2. $\deg(p(x) - aq(x)) = \deg(\alpha)$
3. $a \notin f_1(S)$
4. $(a, b) \in \alpha(E(\overline{K}))$.

Let $R = \{(x_1, y_1) \in E(\overline{K}) | \alpha(x_1, y_1) = (a, b)\}$. We claim that $|R| = \deg(\alpha)$. Consider some (x_1, y_1) in R. Then, $\frac{p(x_1)}{q(x_1)} = a$ and $y_1 f_2(x_1) = b$. (Because $(a, b) \neq \infty$, it follows that $q(x_1) \neq 0$.) This means that $f_2(x_1)$ is well defined, and because $b \neq 0$,

we see that $y_1 = \frac{b}{f_2(x_1)}$. So, x_1 determines y_1. Therefore the order of R is the order of the set $\{x|$ there exists $y \in \overline{K}$ such that $(x, y) \in R\}$.
We know that $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, and so we aim to show that these roots are all distinct. For contradiction, suppose that there exists a root x^* with multiplicity ≥ 2. Then, $p(x^*) - aq(x^*) = 0$ and $p'(x^*) - aq'(x^*) = 0$. We can rearrange these equations and multiply them to obtain $ap(x^*)q'(x^*) = ap'(x^*)q(x^*)$. Therefore, because $a \neq 0$, it follows that x^* is a root of $p'(x)q(x) - p(x)q'(x)$, and so $x^* \in S$. But $a = f_1(x^*)$, and so this implies $a \in f_1(S)$, which contradicts the restrictions on a. Therefore, $p(x) - aq(x)$ has exactly $\deg(\alpha)$ distinct roots. It follows that there are $\deg(\alpha)$ points (x_1, y_1) with $\alpha(x_1, y_1) = (a, b)$, so $|R| = \deg(\alpha)$. It is important to note that the assumptions on (a, b) were made to prove this for one point in $E(\overline{K})$. Because α is a homomorphism, the result then holds for any point in $E(\overline{K})$, including ∞. Thus $|\ker(\alpha)| = \deg(\alpha)$. □

We have related the degree of $\phi_q - 1$ to the size of the kernel, and now we can show that the kernel of this endomorphism is exactly the group $E(\mathbb{F}_q)$.

Proposition 2.4. *Let ϕ_q be the Frobenius endomorphism of an elliptic curve E defined over $\mathbb{F}_q$. Then,* $\ker(\phi_q - 1) = E(\mathbb{F}_q)$.

Proof. In $\overline{\mathbb{F}_q}$, $x^q =$ is the same condition as $x \in \mathbb{F}_q$, and similarly, $y^q = y$ is the same condition as $y \in \mathbb{F}_q$. Therefore the fixed points of ϕ_q are precisely those in $E(\mathbb{F}_q)$. It follows that the points $(x, y) \in E(\mathbb{F}_q)$ are exactly those such that $(\phi_q - 1)(x, y) = (x, y) - (x, y) = 0$. □

Lemma 2.5. *Let q be a prime, and let r and s be integers such that $gcd(s, q) = 1$. Let $a = q+1-\deg(\phi_q-1)$, where ϕ_q is the Frobenius endomorphism on some elliptic curve E over the finite field $\mathbb{F}_q$. Then,* $\deg(r\phi_q - s) = r^2q + s^2 - rsa$.

Proof. It can be shown, with some calculation, that $\deg(r\phi_q - s) = r^2 \deg(\phi_q) + s^2 \deg(-1) + rs(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1))$, and a proof can be found in the third chapter of Washington's Elliptic Curves: Number Theory and Cryptography [1]. Then, the result follows from the facts that $\deg(\phi_q) = q$ and $\deg(-1) = -1$. □

Theorem 2.6. *Hasse's Theorem* [5]. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then,* $-2\sqrt{q} + q + 1 \leq |E(\mathbb{F}_q)| \leq 2\sqrt{q} + q + 1$.

Proof. Let a be the same as in the previous lemma. Note that the lemma implies that $\deg(r\phi_q - s) \geq 0$ for all r, s such that $\gcd(s, q) = 1$. Consider the set $\{\frac{r}{s} | r, s \in \mathbb{Z}, \gcd(s, q) = 1\}$. This set is dense in $\mathbb{R}$, and so it follows that $qx^2 - ax + 1 \geq 0$ for all $x \in \mathbb{R}$. Therefore, the discriminant $a^2 - 4q$ must be less than or equal to 0. Thus it follows that $|a| \leq 2\sqrt{q}$.
Then, consider the endomorphism $\phi_q - 1$. It is well known that this is a separable endomorphism. By the previous propositions, $\deg(\phi_q - 1) = |\ker(\phi_q - 1)| = |E(\mathbb{F}_q)|$. Thus $a = q+1-|E(\mathbb{F}_q)|$, and it follows that $-2\sqrt{q}+q+1 \leq |E(\mathbb{F}_q)| \leq 2\sqrt{q}+q+1$. □

3. The Discrete Logarithm Problem

As we will see in the following section, cryptographic attacks using elliptic curves aim to solve the discrete logarithm problem:

Problem 3.1. *The Discrete Logarithm Problem. Let p be a prime, and let a, b*

be integers that are not divisible by p. Suppose it is known that there exists $k \in \mathbb{Z}$ such that $a^k \equiv b \bmod p$. Then, find k.

We can note that because k being a solution implies that $k + (p-1)$ is also a solution, it makes sense to solve for k modulo $p-1$ or a factor f of $p-1$ if $a^f \equiv 1 \bmod p$.
The group structure on elliptic curves allows an application of this problem to curves, as follows.

Problem 3.2 *The Discrete Logarithm Problem for Groups. Let G be a group, written multiplicatively, and let a, b be elements of G. Suppose it is known that there exists $k \in \mathbb{Z}$ such that $a^k = b$ in G. Then, find k.*

We can apply this to the group E^* generated by an elliptic curve E. Then, if we write E^* additively, we can rephrase the problem: Given points P, Q on E, suppose that there exists $k \in \mathbb{Z}$ such that $kP = Q$. Then, find k.
We usually let $N = |E^*|$, and assume N is known. Also for simplicity, we may assume P generates E^*.
One such approach to solving the Discrete Logarithm Problem is the Baby Step Giant Step attack, which is a computer algorithm. The algorithm requires around $\sqrt{N}$ steps and around $\sqrt{N}$ storage in order to solve the Discrete Logarithm Problem.

Method 3.3. *The Baby Step Giant Step Attack* [6].
Suppose we have P, Q on E as above, and $|E^*| = N$.

1. Fix some integer $m \geq \sqrt{N}$ and compute mP.
2. (The Baby Steps) Compute iP for $0 \leq i < m$ and store them in a list. We can do this by $iP = (i-1)P + P$.
3. (The Giant Steps) Compute $Q - jmP$ for $0 \leq j < m$ starting at $j = 0$ until we find some j such that $Q - jmP$ is a point in the stored list. We can do this by $Q - jmP = (-mP) + (Q - (j-1)mP)$.
4. Then for some i, j we have $i = Q - jmP$. So, $Q = kP$ where $k \equiv i + jm \bmod N$.

We can always find a match because $m \geq \sqrt{N}$ implies that we can assume $0 \leq k < m^2$. Let k^* be an integer in the interval $[0, m^2]$ such that $k^* + ml = k$. Then, $l = \frac{k-k^*}{m}$ implies $0 \leq l < m$. So, if $i = k^*$ and $j = l$, then we find that $Q - lmP = kP - lmP = k^*P$.
Note that we did not actually need to know the value of N. Instead, we can work just as well with an upper bound on N. Thus by Hasse's Theorem, we can use this method for elliptic curves over $\mathbb{F}_q$ because we have the upper bound $N < q+1+2\sqrt{q}$.
We can also improve this method by only computing iP in step 1. for $0 \leq i \leq \frac{m}{2}$, and storing the list of $\pm iP$ instead of just iP.

4. Encryption

Here, we see how encryption using elliptic curves relies on the difficulty of solving the discrete logarithm problem.
Suppose person A wants to send a message to person B, and stop person C from reading it. Person A can encrypt the message, but in order to do this, they must

have an **encryption key**, which is a method for making some data or text unreadable, and person B must have a matching **decryption key**, which makes the encrypted data readable again, that person C must not have. In **symmetric encryption**, both keys are the same or one may be easily deduced from the other. Here, A and B need prior contact to establish the key. In **public key encryption**, B publishes a public encryption key, which A uses, and B also has a private decryption key which they use. However, public key encryption is usually slower, so it makes the most sense to use public key encryption to establish a key for symmetric encryption.
The Diffie-Hellman Key Exchange is a way for A and B to exchange a key for a symmetric encryption system over a public channel.

Method 4.1. *The Diffie-Hellman Key Exchange* [7].

1. A and B agree on an elliptic curve E over a finite field $\mathbb{F}_p$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_p)$, and a point P in $E(\mathbb{F}_p)$ such that the subgroup generated by P has a large order. Usually, E and P are chosen such that this order is a large prime.
2. A secretly chooses an integer $a \in \mathbb{Z}$ and computes $P_a = aP$. Then, A sends P_a to B.
3. B secretly chooses an integer $b \in \mathbb{Z}$ and computes $P_b = bP$. B sends P_b to A.
4. A computes $aP_b = abP$ and B computes $bP_a = baP$.
5. A and B use some publicly agreed upon method to get a key from abP. For example, they could choose the last 256 bits of the x coordinate of abP.

Person C only sees what passes through the public channels: E, $\mathbb{F}_p$, P, P_a, and P_b. Thus in order to find out the key that A and B have agreed on, C must solve the **Diffie-Hellman Problem**.

Problem 4.2. *The Diffie-Hellman Problem.* Given an elliptic curve E over a finite field $\mathbb{F}_p$, and points P, aP, and bP in $E(\mathbb{F}_p)$, compute abP.

If C can solve the discrete logarithm problem in $E(\mathbb{F}_p)$, then they can use P and aP to find a, or P and bP to find b. Then, they can find $a(bP) = b(aP) = abP$. However, it is unknown whether the Diffie-Hellman problem is solvable without using the discrete logarithm problem.

Elliptic curves also offer a way to authenticate a message, by "signing" it. The signature is then hard to replicate, and possible to validate by the receiving party. The **El Gamal Digital Signature** is one such way to do this.

Method 4.3. *The El Gamal Digital Signature* [8].

Suppose person A wants to sign a document and send it to person B without person C copying the signature. The signature must be verifiable, it must be possible to check that A signed it, and the signature must be tied to the specific document that A signed.

1. A first establishes a public key: an elliptic curve E over $\mathbb{F}_q$, and a point $P_A \in E(\mathbb{F}_q)$, where $|P_A| = N$. Then A chooses a secret integer a and computes $P_B = aP_A$. A also chooses a function $f : E(\mathbb{F}_q) \to \mathbb{Z}$ that has a large image, and few inputs for any given output. f is also made public.

2. A then represents the document as an integer m. If $m > N$, then choose a larger curve and start again. A chooses a random $k \in \mathbb{Z}$ such that k and N are relatively prime, and computes $R = kP_A$. Then, A computes $s \equiv k^{-1}(m - a \cdot f(R)) \bmod N$. The signed message is then the triple (m, R, s).

3. B gets A's public information, which is E, P_A, P_B, f, and (m, R, s). Then, B computes $V_1 = f(R)P_B + R$ and $V_2 = mP_A$. If $V_1 = V_2$, then the signature is validated.

Because $s \equiv k^{-1}(m - a \cdot f(R)) \bmod N$, it follows that there exists $z \in \mathbb{Z}$ such that $sk = m - q \cdot f(R) + zN$. Then,

$$\begin{aligned} skP_A &= (m - a \cdot f(R))P_A + zNP_A = (m - a(R))P_A + \infty \\ &\equiv (m - a \cdot f(R))P_A. \end{aligned}$$

Then we can see that

$$\begin{aligned} V_1 &= f(R)P_B + sR \\ &= f(R)aP_A + skP_A \\ &= f(R)aP_A + (m - a \cdot f(R))P_A \\ &= mP_A \\ &= V_2. \end{aligned}$$

Thus we see how the authentication comes from the equality $V_1 = V_2$.

C can try to use P_A and P_B to find a, in which case they can replicate A's signature. They can also use P_A and R to find k, which will allow them to find a because $ks \equiv m - a \cdot f(R) \bmod N$. Then, there are $\gcd(f(R), N)$ possibly solutions for a, if $f(R)$ and N are not relatively prime. If this number is small, C can check the different possibilities to see which works. In either case, C must solve the discrete logarithm problem.

Alternatively, C can try to produce a pair (R, s) such that $V_1 = V_2$, and C may do this for a different message n. C must find (R, s) such that $f(R)P_B + sR = mP_A$. If C chooses R first, then they must solve the discrete logarithm problem $sR = mP_A - f(R)P_B$. If they choose s first, then they must solve for R, but this turns out to be equally or more complex than solving for s.

Thus it is the generally agreed upon that the security of this signature is very close to the security of discrete logarithms for $E(\mathbb{F}_q)$. While this is very useful, the method is unfortunately not very efficient because the message (m, R, s) is three times as long as the document m. There is a variant of the El Gamal digital signature that uses cryptographic hash functions to minimize the length of the message. However, not all elliptic curve encryption methods are based on the discrete logarithm problem. The Rivest-Shamir-Adleman system is the most famous public key cryptosystem, and it has an elliptic curve version, thanks to Koyama-Maurer-Okamoto-Vanstone, although it is not often used.

Method 4.4. *Classical RSA Encryption* [9].

Suppose Person A wants to send a message to person B, without person C reading the message.

1. B privately chooses distinct, large primes p, q and lets $n = pq$. B also chooses $e, d \in \mathbb{Z}$ such that $ed \equiv 1 \bmod (p-1)(q-1)$. Then B makes n and e public.

2. A encrypts their message as a number $m \bmod n$, and computes $c \equiv m^e \bmod n$. Then A sends c to B.

3. Then B computes $m \equiv c^d \bmod n$ to find m.

C only sees n, e, and c, so if C can factor n then they can find d. Then, finding d amounts to finding m. Therefore the harder it is to factor n, the more secure the cryptosystem is.

The following elliptic curve variant of the RSA encryption uses properties of **supersingular** curves, or curves E in characteristic p such that $E[p] = \{\infty\}$. These supersingular curves are central to elliptic curve cryptography, as they have several useful properties. For an elliptic curve E over $\mathbb{F}_{p^e}$ for some prime p and some $e \in \mathbb{Z}$, E is supersingular if and only if $q + 1 - |E(\mathbb{F}_{p^e})| \equiv 0 \bmod p$ if and only if $|E(\mathbb{F}_{p^e})| \equiv 1 \bmod p$. Moreover, if $p \geq 5$, then E is supersingular if and only if $|E(\mathbb{F}_p)| = p + 1$. It can also be shown that the curve E defined by $y^2 = x^3 + B$ over $\mathbb{F}_q$, where $b \in \mathbb{F}_q^x$, is supersingular if q is odd and $q \equiv 2 \bmod 3$. Proofs of these statements can be found in Chapter 4 of Washington's Elliptic Curves: Number Theory and Cryptography.

Method 4.5. *Koyama-Maurer-Okamoto-Vanstone Elliptic Curve RSA Encryption* [10].

Let the situation with A, B, and C be as before.

1. B privately chooses distinct, large primes p, q such that $p \equiv q \equiv 2 \bmod 3$, and finds $n = pq$. B also chooses integers e, d such that $ed \equiv 1 \bmod \operatorname{lcm}(p+1, q+1)$. Then, B makes n and e public.
2. A represents the message as 2 integers (m_1, m_2), which can be regarded as a point M. Then, M is a point on the elliptic curve E represented by $y^2 = x^3 + b \bmod n$, where $b = m_2^2 - m_1^3 \bmod n$. (However, A does not need to actually calculate b, because the point addition later does not use it.) Note that E is supersingular modulo p and q.
3. A calculates $R = (r_1, r_2) = eM$ on E, and sends R to B.
4. B calculates $dR = deM \equiv M \bmod n$ to find M.

The fact that $deM = M$ follows from the fact that E is supersingular modulo p and modulo q. Then, $|E(\mathbb{F}_p)| = p+1$ and $|E(\mathbb{F}_q)| = q+1$, and so $(p+1)M \equiv \infty \bmod p$ and $(q+1)M \equiv \infty \bmod q$. Recall that $ed \equiv 1 \bmod p+1$ and so $ed = 1 + k(p+1)$ for some $k \in \mathbb{Z}$. Then, it follows that

$$\begin{aligned} dR &= deM \\ &= (1 + k(p+1))M \\ &= M + k(p+1)M \\ &\equiv M + \infty \bmod p \\ &\equiv M \bmod p. \end{aligned}$$

Similarly, $dR \equiv M \bmod q$. Thus it follows that $dR \equiv M \bmod n$.
Here, C only sees n, e, and R. If C can factor $n = pq$, then they can find $d \equiv e^{-1} \bmod (p+1, q+1)$, and thus solve for M.
Suppose instead that C knows d but not how to factor n. C can do the following, and we claim that they will probably succeed in factoring n.

1. C finds integers v, m with v odd and $m \geq 1$ such that $ed - 1 \equiv 2^m v$.
2. C picks a random pair of integers $S = (s_1, s_2) \bmod n$. This a point on the

curve E' given by $y^2 = x^3 + (s_2^2 - s_1^3)$.

3. C calculates $S_0 = vS$. If $S_0 = \infty \bmod n$, then start from step 2 and choose a new S. If $S_0 = \infty \bmod p$ or q but not both, then $S_0 = (x_0, y_0)$ where $y_0 \equiv 0 \bmod p$ or $\bmod q$. Then, $gcd(y_i, n) = p$ or q, so C has factored n. Otherwise, C continues:

4. C computes $S_{i+1} = 2S_i$ for $i = 0, 1, 2, \ldots, m$. If C finds some i such that $S_{i+1} = \infty \bmod n$, then C returns to step 2 and chooses a new S. If C finds some i such that $S_{i+1} = \infty \bmod p$ or q but not both, then C has factored n, as in step 3.

Recall that the order of $E(\mathbb{Z}_n)$ divides $ed - 1$, because $ed \equiv 1 \bmod (p+1)(q+1)$. Then, $S_m = (ed-1)S = edS - S$, which is the point ∞. This implies that each sequence of S_i's finds some i with $S_{i+1} = \infty \bmod p$ or q, or both.

Let k' be the highest power of 2 such that $2^{k'}$ divides $p+1$. For a random point $S \in E(\mathbb{F}_p)$, there is a $1/2$ chance that $2^{k'}$ divides $|S|$, which follows from the fact that $E(\mathbb{F}_p)$ is cyclic. Then, $S_{k'-1} = 2^{k'-1}vP \neq \infty \bmod p$, but $S_{k'} = 2^{k'}vP = \infty \bmod p$. If $2^{k'}$ doesn't divide $|S|$, then $S_{k'-1} = \infty \bmod p$. A similar result holds for q. Then, because $\bmod p$ and $\bmod q$ are independent, we can see that for at least half of the time, the sequence of S_i's reaches $\infty \bmod p$ at a different index than it does $\bmod q$. Thus C finds a factorization of n with this method for at least half of the choices for S, and so it is highly likely that they can factor n. Therefore, we can conclude that knowing d is computationally equivalent to knowing how to factor n.

5. Factorization of Integers

It comes as no surprise that elliptic curves can also be used to factor numbers of around 60 digits, and to find prime factors of around 20 to 30 digits for larger numbers. The method, which is thanks to Henrik Lenstra, is best introduced with an example.

Example 5.1. Suppose we want to factor 35. Let E be the elliptic curve $y^2 = x^3 + x - 1 \bmod 35$. Let P be the point $(1, 1)$ on E, and attempt to compute $9P$. By successive doubling, we find that

$$2P = (2, 2)$$
$$4P = (0, 22), \text{ and}$$
$$8P = (16, 19).$$

Then to find $9P$, we calculate $8P + P$. The slope of the line through P and $8P$ is $\frac{19-1}{16-1} = \frac{18}{15}$. We can't find 15^{-1} because $\gcd(15, 35) = 5 \neq 1$, and so we can't evaluate the slope. However, we have found that $5|35$, and so $35 = 5 \cdot 7$.

Then, $E(\mathbb{Z}/35\mathbb{Z}) \cong E(\mathbb{F}_5) \oplus E(\mathbb{F}_7)$. So, we can try to find the order of P in $E(\mathbb{F}_5)$ and $E(\mathbb{F}_7)$. We find that in $E(\mathbb{F}_5)$, $|P| = 9$, but in $E(\mathbb{F}_7)$, $|P| = 11$. So, we see why we couldn't calculate $9P$; it is an infinite point in $E(\mathbb{F}_5)$, but a finite point in $E(\mathbb{F}_7)$.

If instead we had found that the order of P in $E(\mathbb{F}_7)$ was 9, then this point would not have helped us find a factor of 35. However, the probability of this happening is fairly low, and so for large composite n, the most difficult part of this process is finding $k \in \mathbb{Z}$ such that $kP = \infty$ modulo a factor of n. So, if we work with enough elliptic curves, it is likely that we can find k for a point on one of them.

Method 5.2. *Elliptic Curve Factorization Method* [11].

The method for factoring some $n \in \mathbb{N}$ is as follows:

1. Choose $10 - 20$ elliptic curves over $E(\mathbb{Z}/n\mathbb{Z})$, and label them $E_i : y^2 = x^3 + A_i x + B_i$. Also choose a point $P_i (\bmod n)$ on each E_i. The most efficient way to do this is by choosing a random $A_i \in \mathbb{Z}/n\mathbb{Z}$, and a random pair of integers $u_i, v_i \in \mathbb{Z}/n\mathbb{Z}$. Then set $P_i = (u_i, v_i)$, and choose B_i such that $B_i = v_i^2 - u_i^3 - A_i u_i \bmod n$. Let E_i be the elliptic curve $y^2 = x^3 + A_i x + B_i \bmod n$. Then, we have our point P_i on E_i. (This is quicker than choosing A_i, B_i, and u_i, and trying to find v_i.)
2. Choose $C \in \mathbb{Z}$, where C is around 10^8, and compute $(C!)P_i$ on E_i for each i. This can be done recursively, so calculating $C!$ is not necessary. C must be this large because we are looking for primes that may be very large.
3. If step 2 fails because some slope calculated does not exist modulo n, then we will have found a factor of n.
4. If step 2 succeeds for all i, then increase C or choose new curves E_i and points P_i, and start over.

Note that steps 2 through 4 can be done in parallel, checking each curve E_i simultaneously, to increase efficiency.

Suppose that n is composite, and around 100 digits, and suppose that we have tested all primes up to 10^7 but have not found a prime factor of n. Then, the above method is very useful because it is very likely that n will have a prime factor less than 10^{40}.

Recall from Hasse's Theorem that for an elliptic curve over $\mathbb{F}_p$, we have that

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

It turns out that each integer in that interval occurs as the order of some elliptic curve E. So, if $n = pq$, for simplicity, we can look at $E(\mathbb{Z}/n\mathbb{Z})$ as a curve modulo p and modulo q. If C is a reasonable size, then the density of **C-smooth integers**, or integers that have only prime factors less than or equal to C, in the interval is high enough, and the distribution of the orders of random curves is sufficiently uniform such that it is likely for us to find a curve E with $C-$smooth order when we choose the initial 10-20 curves. Moreover, a point P on E is likely to be such that $(C!)P \equiv \infty \bmod p$, and unlikely that $(C!)(P \bmod q) \equiv \infty \bmod q$. If this does happen, we can simply choose a smaller C. This is why the method works.

Cryptography nowadays mainly uses values of n such that $n = pq$ where p, q are primes of more than 75 digits. In these cases, other factorization methods such as the **quadratic sieve** and the **number field sieve** are more efficient [12] [13]. However, the elliptic curve method is sometimes used to find smaller primes in intermediate steps in these methods.

A closely related question is that of proving that large numbers are prime. The following proposition introduces one such method, and is thanks to Pocklington and Lehmer [14] [15].

Proposition 5.3. *Let $n > 1$ be an integer, and let $n - 1 = rs$ for some $r, s \in \mathbb{Z}$ with $r \geq \sqrt{n}$. Then, suppose that for each prime l dividing r, there exists $a_l \in \mathbb{Z}$*

such that $a_l^{n-1} \equiv 1 \mod n$ *and* $\gcd(a_l^{\frac{n-1}{l}}, n) = 1$. *Then,* n *is prime.*

Proof. Let l^e be the highest power of l dividing r, and let p be a prime factor of n. Let $b \equiv a_l^{\frac{n-1}{l}} \mod p$. Then, we see that

$$\begin{aligned} b^{l^e} &\equiv a_l^{n-1} \\ &\equiv 1 \mod p, \text{ and} \\ b^{l^{e-1}} &\equiv a_l^{\frac{n-1}{l}} \\ &\not\equiv 1 \mod p \end{aligned}$$

because $\gcd(a_l^{\frac{n-1}{l}} - 1, n) = 1$. So, the order of b in $\mathbb{Z}/p\mathbb{Z}$ is l^e, and so $l^e | p-1$. This is true for each prime l that divides r, and so we see that in fact $r|p-1$. Then, $p, r \geq \sqrt{n}$ implies that n has no prime factors less than $\sqrt{n}$, and so n must be prime. □

However, this method relies on being able to find enough factors of $n-1$ to find $r \geq \sqrt{n}$ such that we know all prime factors of r. Goldwasser and Kilian improved it by using elliptic curves [16]. Because $|(\mathbb{Z}/n\mathbb{Z})^\times| = n-1$ for prime n, if we look at elliptic curves over $\mathbb{Z}/n\mathbb{Z}$, we can replace $n-1$ with a different group order near n. (Recall, this is a consequence of Hasse's Theorem, as in the Elliptic Curve Factorization Method.) Moreover, we have enough possible elliptic curves such that we can find one where the order can be partially factored.

Theorem 5.4. *Let* $n > 1$ *be an integer, and let* E *be an elliptic curve modulo* n. *Suppose there exist distinct primes* $l_1, \ldots, l_k$ *and finite points* $P_1, \ldots, P_k \in E(\mathbb{Z}/n\mathbb{Z})$ *such that*

1. $l_i P_i \equiv \infty \mod n$ *for* $1 \leq i \leq k$
2. $\Pi_{i=1}^k l_i > (n^{\frac{1}{4}} + 1)^2$.

Then n *is prime.*

Proof. Let p be a prime factor of n, and write $n = p^e m$ where e is the highest power of p dividing n. Then, it follows that

$$E(\mathbb{Z}/n\mathbb{Z}) \cong E(\mathbb{Z}/p^e\mathbb{Z}) \oplus E(\mathbb{Z}/m\mathbb{Z}).$$

Then, each P_i is finite in $E(\mathbb{Z}/n\mathbb{Z})$, so it is also finite modulo p^e in $E(\mathbb{Z}/p^e\mathbb{Z})$. We can then reduce P_i to obtain a finite point $P_{i,p} \equiv P_i \mod p$ in $E(\mathbb{F}_p)$.
Because $l_i P_i \equiv \infty \mod n$, it follows that $l_i P_i \equiv \infty$ modulo every factor of n, and so $P_{i,p}$ has order l_i in $E(\mathbb{F}_p)$. Thus l_i divides the order of $E(\mathbb{F}_p)$ for all i. Therefore $\Pi_{i=1}^k l_i$ divides the order of $E(\mathbb{F}_p)$. Thus, with Hasse's Theorem, we have that

$$(n^{\frac{1}{4}} + 1)^2 < \Pi_{i=1}^k l_i \leq |E(\mathbb{F}_p)| < p + 1 + 2\sqrt{p} = (p^{\frac{1}{2}} + 1)^2$$

and it follows that $p > \sqrt{n}$. Then, as in the previous proposition, n is prime. □

We demonstrate an application of this with an example.

Example 5.5. Let $n = 31$, and look at elliptic curves modulo 31 until we find one with an order divisible by a prime l slightly larger than $(31^{\frac{1}{4}} + 1)^2$. We find

the curve E, $y^2 = x^3 + 3x + 19 \bmod 31$, with $l = 17$. We can check the order of the curves we look at by considering curves where we know a point. Here, the point $(2, 8)$ is on E and the Baby Step, Giant Step method shows that the order of $(2, 8)$ is $34 = 17 \cdot 2$. Then, we can take the point $P = 2(2, 8) = (28, 18)$, and so $|P| = 17$. Then, by the previous theorem, 31 is prime.

6. More Elliptic Curve Cryptography

Elliptic curve cryptography has been popular with the U.S. National Institute of Standards and Technology, whose Suite B recommended algorithms include the Diffie-Hellman public key exchange, and the **Elliptic Curve Digital Signature Algorithm**, which is a variant of the El Gamal Digital Signature Algorithm [17]. Additionally, there are several more attacks, such as the **Pollig-Hellman Method**, which relies on the knowledge of the prime factorization of the order of a point in $E(\mathbb{F}_q)$, and the **Menezes-Okamoto-Vanstone Attack**, which uses a pairing on elliptic curves called the **Weil Pairing** to transform the discrete logarithm problem over $E(\mathbb{F}_q)$ into one over $\mathbb{F}_{q^m}^{\times}$ [18] [19] [20]. There are also other encryption systems based on elliptic curves, such as the **Elliptic Curve Integrated Encryption Scheme**, which incorporates symmetric encryption functions [21].

Acknowledgments

It is a pleasure to thank my mentor, Anthony Santiago Chaves, without whom this paper would not be possible, for his indispensable patience and guidance this summer. I would also like to thank Dr. Peter May, the University of Chicago Math Department, and everyone else who made this REU possible.

References

[1] L. Washington. Elliptic Curves: Number Theory and Cryptography. Taylor Francis Group, LLC. 2008.
[2] K. Weierstrass. "Math. Werke" (1,2). Mayer Mller. 1894 - 1895.
[3] L. J. Mordell. "On the rational solutions of the indeterminate equations of the third and fourth degrees". Proc Cam. Phil. Soc. 21. pp. 179 - 192. 1922.
[4] A. Weil. "L'arithmetique sur les courbes algebriques". Acta Mathematica. 52 (1). pp. 281 - 315. 1928.
[5] H. Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkorper. I, II III". Crelle's Journal. (175). 1936.
[6] D. Shanks. "Class number, a theory of factorization and genera." In Proc. Symp. Pure Math. 20. pp. 415 - 440. AMS. 1971.
[7] W. Diffie; M. Hellman. "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6). pp. 644 - 654. 1976.
[8] T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". IEEE Trans Inf Theory. 31 (4): 469 - 472. 1985.
[9] R. Rivest; A. Shamir; L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. 21 (2). pp. 120 - 126. 1978.
[10] K. Koyama; U. M. Maurer; T. Okamoto; S. A. Vanstone. "New public-key schemes based on elliptic curves over the ring Zn." Proc. of Crypto. 1991.
[11] H. Lenstra. "Factoring integers with elliptic curves". Annals of Mathematics. 126. pp. 649 - 673. 1987.
[12] C. Pomerance. Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory, Part I. Math. Centre Tract 154. pp 89 - 139. 1982.
[13] C. Pomerance. "A Tale of Two Sieves". Notices of the AMS. 43 (12). pp. 1473 - 1485. 1996.
[14] H. C. Pocklington. "The determination of the prime or composite nature of large numbers by Fermat's theorem". Proc Cam. Phil. Soc. 18. pp. 29 - 30. 1914 - 1916.

[15] D. H. Lehmer.. "Tests for primality by the converse of Fermat's theorem". Bull. Amer. Math. Soc. 33 (3). pp. 327 - 340. 1927.
[16] S. Goldwasser; J. Kilian. "Almost all primes can be quickly certified." STOC 86 Proc. of the 18th Annual ACM Symposium on Theory of Computing. pp. 316 - 329. 1986.
[17] "FIPS PUB 186-1. Digital Signature Standard (DSS). 1998.
[18] S. Pohlig; M. Hellman. "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance". IEEE Transactions on Information Theory (24). pp. 106 - 110. 1978.
[19] A. Menezes; T. Okamoto; S. A. Vanstone. "Reducing elliptic curve logarithms to logarithms in a finite field". IEEE Transactions on Information Theory. 39. pp. 1639 - 1646. 1993.
[20] A. Weil. "Sur les fonctions algbriques corps de constantes fini". Les Comptes rendus de l'Acadmie des sciences. 210. pp. 592 - 594. 1940.
[21] V. Shoup. A proposal for an ISO standard for public key encryption, Version 2.1. 2001.