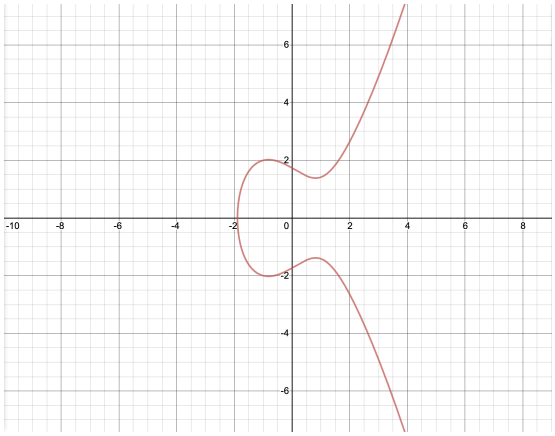
THREE PERSON DIFFIE-HELLMAN KEY EXCHANGE

JOSH ZEITLIN

Abstract. In this paper, we will introduce the theory of Elliptic Curves. We will start by studying the group law. Afterwards, we will look at torsion points and the properties that they have. Then, we will study the applications of the theory of elliptic curves within the field of cryptography where we will examine the Elliptic Curve Discrete Logarithm Problem which asks us to find some integer n such that given points on the Elliptic Curve Q and P $Q = nP$, the analogue of the Discrete Log Problem in $\mathbb{Z}/p\mathbb{Z}$. Then we will solve the Elliptic Curve Diffie-Hellman which is essentially the same as it is in $\mathbb{F}_p^\times$. Finally, we will extend the Elliptic Curve Diffie-Hellman by using the Weil-Pairing which allows a Key-Exchange between 3 persons rather than just 2.

1. Preliminary Definitions

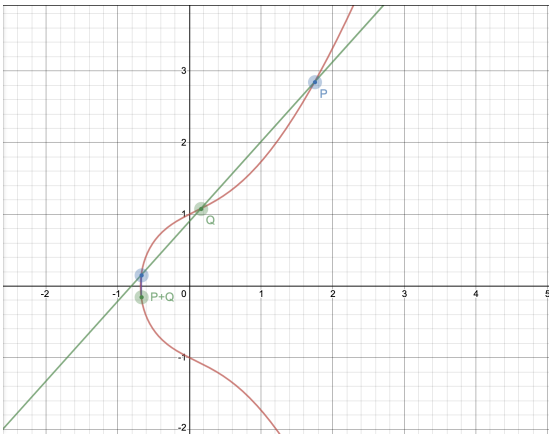
Definition 1.1. *Elliptic Curve:* An elliptic curve over a field is a set of solutions to any equation of the form $y^2 = x^3 + ax + b$ (this is known as Weierstrass form) together with a point at infinity denoted by ϑ.
One of the criterion of the elliptic curve is that the discriminant, denoted by Δ, satisfies $\Delta \neq 0$ where $\Delta = 4a^3 + 27b^2$.
The graph of an elliptic curve over the field $\mathbb{R}$ (the real numbers) should look like this:



The points on an elliptic curve form a group under addition; however, the algorithm to compute the sum of two points on an elliptic curve is not as simple as addition in $\mathbb{R}$ or $\mathbb{F}_p^\times$.

Definition 1.2. *The sum of two points on an elliptic curve:* To take the sum of two points on an elliptic curve, we draw a line through the two points we would like to add. Then we find the third point of intersection and reflect it over the x-axis. That point is then the sum. To make this easier to visualize:

Date: October 16, 2019.



More generally, an algorithm to compute the sum of the two points on an elliptic curve would go as follows,

(1) Select two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
(2) Then take the line defined by the equation $L : y = (\frac{y_1 - y_2}{x_1 - x_2}) \cdot x + (y_1 - x_1((\frac{y_1 - y_2}{x_1 - x_2})))$
(3) Next, find the point of intersection of L and the elliptic curve E, the point that is not P or Q
(4) Now, negate the y-coordinate of the point you find
(5) So $P \oplus Q = (x_3, -y_3)$ where x_3 and y_3 are the coordinates of the third point of intersection of L and E.

Now, in order to double a point on E we add a point to itself we add $P \oplus P$. We take the line tangent to P on E and then find the intersection point on the graph, negate the y-coordinate and we are done. The formula for the slope of the line comes from a simple calculus problem of applying implicit differentiation to both sides of the equation of the elliptic curve equation in Weierstrass form. The slope of the line is $m = \frac{3x_1^2 + a}{2y_1}$. Similarly, to find the intercept of that line just plug in the coordinates of $P = (x_1, y_1)$ to get $b = y_1 - \frac{3x_1^2}{2y_1} \cdot x_1$. This result is trivial.

Definition 1.3. *The point at infinity* In an elliptic curve we define the point at infinity to be the point that results in summing any two points with the same x coordinate, i.e., $P = (x_1, y_1) \oplus P' = (x_1, -y_1)$. The point at order infinity is denoted by ϑ

By adding the point at infinity this acts as an identity and then an elliptic curve forms a group under addition. And $P^{-1} = P' \in E$ such that $P' \oplus P = \vartheta$. Let's make this idea more formal and then prove it.

Theorem 1.4. *$(E(\mathbb{F}), +)$ is a group where $\mathbb{F}$ is a group under addition.*

Proof. In order to prove this theorem, we must prove that all of the group axioms hold. First, we must prove closure. The sum of two points on an elliptic curve is either ϑ or another point on the elliptic curve. Similarly, $\vartheta + P \in E = P$. Next, by definition we have that ϑ is the identity. We also have that inverses have to be true, because $\forall P \in E(\mathbb{F}) \exists P'$ s.t. $P \oplus P' = \vartheta$. Because ϑ lies on all vertical lines we get that if $P = (x_1, y_1) \in E(\mathbb{F})$, then $P' = (x_1, -y_1)$ which is also in $E(\mathbb{F})$. Lastly, we must show associativity. Associativity is very easy to show, but it is very tedious. So this proof is left as an exercise for the reader as we have to do a lot of continuous addition. ∎

Definition 1.5. *n-torsion points* An n-torsion point on an elliptic curve is a point P such that $nP = \vartheta$. The set of all n-torsion points is denoted by $E[n]$.

We can show that this is a group with the following theorem.

Theorem 1.6. *The set $E[n]$ forms a group under addition on Elliptic Curves. More generally, the set of n-torsion points in any group forms a subgroup under the associated operation where in any group the set of n-torsion points are the points $g \in G$ s.t. $g \cdot n = e$ where e is the identity. This set of points is similarly denoted as $G[n]$.*

Proof. Because we know that $E(\mathbb{F})$ is a group under addition it suffices to show that $G[n]$ is a group for any other group G.

So again, let's show that the group axioms hold.

First, ϑ or e, the identity in any group is obviously an n torsion points as $e+\cdots+e = e\cdot n = e$. So because we have $e \in G[n]$ which is already $e \in G$ we have that the identity is in $G[n]$.

Next, let's show that closure holds given $g, h \in G[n]$

$$\begin{gathered} n \cdot g = e \\ n \cdot h = e \\ n \cdot h + n \cdot g = e + e = e = n(g + h) \end{gathered}$$

Hence $g + h \in G[n]$ is also an n-torsion point. Now we have to show inverses which is easy, because g is an n-torsion point if and only if g^{-1} is, seen here. If g is an n-torsion point then

$$n(g + g^{-1}) = n(e) = e = g(n) + g^{-1}(n) = g^{-1} \cdot n$$

So g^{-1} is also an n-torsion point. Then if g^{-1} is an n-torsion point then:

$$n(g + g^{-1}) = n(e) = e = g(n) + g^{-1}(n) = g \cdot n$$

Hence g is an n-torsion point as well. ∎

Similarly, we can also prove that the set of n-torsion points, $E[n]$ is a vector space. This notion of defining $E[n]$ as a vector space will be very useful later on when working with the Weil Pairing.

2. Elliptic Curve Discrete Log Problem

Now that we have discussed n-torsion points and multiples of points on elliptic curves we can introduce the Elliptic Curve Discrete Logarithm Problem, abbreviated as the ECDLP. Recall the discrete logarithm problem which was the basis of the Diffie-Hellman Key Exchange in $\mathbb{F}_p^\times$:

Definition 2.1. *The Discrete Logarithm Problem:* The Discrete Logarithm Problem is the problem to take some prime number p and some primitive root $g \in \mathbb{F}_p^\times$ and some other $h \in \mathbb{F}_p^\times$ to find some x such that:

$$h \equiv g^x \mod p$$

Now, let's rigorously define the Elliptic Curve Discrete Log Problem.

Definition 2.2. *ECDLP:* Let $E(\mathbb{F}_p)$ be some Elliptic Curve defined over the Galois Field $\mathbb{F}_p$ where $p \in \mathbb{Z}$ is a prime. Let $P, Q \in E(\mathbb{F}_p)$ then the goal of the ECDLP is to find some n such that $Q = n \cdot P$. This is analogous to $\mathbb{F}_p^\times$ where we write

$$n = \log_P(Q)$$

Now the log function here is not well-defined because we could select some point that is indeed not a multiple of P and we would not get a value. However, when using the log function in Cryptography with Elliptic Curves it is always in a context such that the problem is solvable, but not always easily.

Remark 2.3. One other difficulty when dealing with the logarithm function for elliptic curves is that there can be more than one value. For example, look at the n-torsion points we discussed earlier. If $P \in E(\mathbb{F})$ and P satisfies $P \in E(\mathbb{F})[n]$ then $P \in E(\mathbb{F})[2n]$ and $E(\mathbb{F})[3n]$ and $E(\mathbb{F})[kn] \forall k \in \mathbb{Z}$.

However, because we are going to be working with finite fields, like $\mathbb{F}_p$ we can easily get around this. Now, in order to remedy this problem we must calculate the smallest $k \in \mathbb{Z}$ such that $i - j = k$ and $i \cdot P = j \cdot P$ $P \in E(\mathbb{F})[k]$.

Hence we define all of our solutions to the $Q = nP$ has n of the form $n' + c \cdot k$ where n' is our first and simplest solution. This makes $\log_P(Q) = n' \in \mathbb{Z}/k\mathbb{Z}$

We can also see that given two points $Q, R \in E(\mathbb{F}_p)$ we get $\log_P(Q+R) = \log_P(Q) + \log_P(R)$ so the $\log_P$ function is additive. We can formalize this with the following theorem:

Theorem 2.4. *The map:*

$$\log_P : E(\mathbb{F}_p) \to (\mathbb{Z}/k\mathbb{Z})$$

defines a homomorphism across the groups $E(\mathbb{F}_p)$ and $\mathbb{Z}/k\mathbb{Z}$.

This proof is left as an exercise for the reader.

3. Elliptic Curve Diffie-Hellman

Now, recall the Diffie-Hellman Key Exchange from cryptography in $\mathbb{F}_p^\times$. We get that Alice and Bob each start with a generator g of $\mathbb{F}_p^\times$. Now Alice chooses some arbitrary integer $a \in \mathbb{F}_p^\times$ and Bob chooses some other arbitrary integer $b \in \mathbb{F}_p^\times$.
Now, Alice computes

$$A = g^a \mod p$$

and Bob computes

$$B = g^b \mod p$$

Now, they publicly exchange A and B and then Alice computes

$$B^a \mod p \equiv (g^b)^a \mod p \equiv g^{ab} \mod p$$

and Bob computes

$$A^b \mod p \equiv (g^a)^b \mod p \equiv g^{ab} \mod p$$

So they both obtain the shared key $g^{ab} \mod p$. Now, the only way an eavesdropper whom we'll call Eve can crack this is by completing the Discrete Log Problem and similarly for Elliptic Curve Diffie-Hellman where Eve must solve the Elliptic Curve Discrete Log Problem in order to break the code.

Definition 3.1. *Elliptic Curve Diffie-Hellman* Take two people Alice and Bob who publicly exchange some elliptic curve over E over $\mathbb{F}_p$ so they both choose some $P \in E(\mathbb{F}_p)$.
Now, Alice will pick some integer a and Bob will pick some other integer b. Alice will compute

$$A = aP$$

and Bob will compute

$$B = bP$$

So Alice and Bob publicly exchange A and B. Now Eve can see both of these values, but will not be able to calculate a or b, because that will require taking $\log_P(B)$ and $\log_P(A)$ to find a and b which requires solving the elliptic curve discrete log problem.
So now, Alice will calculate

$$bA = b(aP)$$

and Bob will calculate

$$aB = a(bP)$$

This results in a shared key of abP which structurally speaking is very similar to the result we got in the regular Diffie-Hellman key exchange over $\mathbb{F}_p^\times$.

Now, we can introduce Elliptic Curve ElGamal.

Definition 3.2. *Elliptic Curve ElGamal:* First, Alice and Bob publicly exchange information and decide an elliptic curve E, a field to have it over, $\mathbb{F}_p$ and a point P on that curve.

Then, Alice chooses an arbitrary a which she will not tell *Bob* and then she calculates $A = aP$ and publishes that.

Bob chooses his cipher-text M that he wants to send to Alice and then he takes some number b and computes $B = bP$ and then $B' = M + bA$ to wit he publishes the pair (B, B').

To decrypt this Alice calculates $B' - aB$ to get M. This works, because $B' = M + bA - aB = M + baP - abP = M + baP - baP = M + \vartheta = M$

4. The Weil Pairing

In order to define a Weil Pairing we first must get familiar with a divisor of an elliptic curve.

Definition 4.1. *Divisor Function:* A divisor function of another function can be written as a summation of points multiplied by the exponents for their multiplicities and the order of their pole.

Example. Take the function $f(x) = \frac{\prod_i^k (x-r_i)^{m_i}}{\prod_i^h (x-q_i)^{n_i}}$ to wit the divisor function, denoted by $\operatorname{div}(f(x))$ is written as the formal sum

$$\operatorname{div}(f(x)) = (\textstyle\sum_i^k m_i[r_i]) - (\sum_i^h n_i[q_i]) = m_1[r_1] + m_2[r_2] + \cdots m_k[r_k] - n_1[q_1] - n_2[q_2] - \cdots - n_h[q_h]$$

Now we can also define a rational function of points $P = (x, y) \in E$, so in a similar manner we define a divisor of an elliptic curve.

Definition 4.2. *Divisor of an elliptic curve:* To define a divisor we write

$$\operatorname{div}(f) = \textstyle\sum_{P \in E} k_P \cdot P$$

Now, the degree of this divisor, denoted by $\deg(D)$ is the sum of those coefficients, or more formally $\sum k_P$. Now, the sum of a divisor on an elliptic curve is just $\sum n_k P$ (with no brackets), so a linear combination of the points on an elliptic curve.

Theorem 4.3. *Let D be a divisor on an Elliptic Curve E, written as*

$$D = \textstyle\sum n_k P$$

then D is a divisor of a rational function on an elliptic curve if and only if $\deg(D) = 0$ *and sum$(D) = \vartheta$, the point at infinity.*

Now, we can begin defining the Weil Pairing.

Definition 4.4. *The Weil Pairing*: Take two n-torsion points P, Q on an elliptic curve E. Now, define two rational functions on the elliptic curve E, R_P and R_Q such that their divisors are $\text{div}(R_P) = n[P] - n[\vartheta]$ and $\text{div}(R_Q) = n[Q] - n[\vartheta]$. Now, the Weil Pairing of two points P and Q is defined as

$$e_n(P, Q) = \frac{R_Q(Q+S)}{R_Q(S)} \Big/ \frac{R_Q(P-S)}{R_Q(-S)}$$

Now, let's take a look at several interesting properties of the Weil Pairing:

Theorem 4.5. *Properties of The Weil Pairing:*

(1) $e_n(P, P) = 1$
(2) $e_n(P, Q) = e_n(Q, P)^{-1}$
(3) e_n *is bilinear, i.e., given* $P, Q, R \in E[n]$ $e_n(P + R, Q) = e_n(P, Q) \cdot e_n(R, Q)$ *and similarly,* $e_n(P, Q + R) = e_n(P, Q) \cdot e_n(P, R)$
(4) $e_n(P, Q)^n = 1$, *i.e., it is an* n*-th root of unity given any two* n*-torsion points*
(5) *If,* $\forall Q \in E[m], e_m(P, Q) = 1$ *then* $P = \vartheta \in E[m]$.

Now, because $E[n]$ is a vector space as we proved earlier we can see that given two points $P_1, P_2 \in E[n]$ which form a basis of $E[n]$ and if we know the value of their Weil Pairing then we can calculate the value of any other Weil Pairing of element of $E[n]$.

To do so, because P_1 and P_2 form a basis for the n-torsion points we get $\forall P \in E[n] \exists a_P, b_P \in \mathbb{Z}/n\mathbb{Z}$ s.t. $P = a_P P_1 + b_P P_2$ and similarly for some $Q \in E[n] \exists a_Q, b_Q \in \mathbb{Z}/n\mathbb{Z}$ s.t. $Q = a_Q P_1 + b_Q P_2$.

So now, we can write $e_m(P, Q) = e_m(P_1, P_2)^{\det \begin{pmatrix} a_P & a_Q \\ b_P & b_Q \end{pmatrix}} = e_m(P_1, P_2)^{a_P b_Q - a_Q B_P}$, There are a couple of other efficient algorithms of calculating the Weil Pairing which I encourage you to look up; however, they will not be relevant for now.

One application of the Weil Pairing is that it can reduce the ECDLP in $E(\mathbb{F}_{p^k})$ to being equivalent to solving the Discrete Log Problem in $\mathbb{F}_{p^k}^\times$. To do this we use the MOV Algorithm written by Menezes, Okamoto, and Vanstone. First, however, we have to define the embedding degree.

Definition 4.6. *Embedding Degree:* Choose some elliptic curve E over $\mathbb{F}_p$ and choose some arbitrary $m \in \mathbb{Z}_{\geq 0}$ such that $p \nmid m$. Then the embedding degree of E with respect to m is defined to be the minimal value of k so that

$$E(\mathbb{F}_{p^k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Now, to set up the MOV algorithm we must take some point $P \in E(\mathbb{F}_p)$ such that P is a j-torsion point to wit j is a large prime greater than $\sqrt{p} + 1$.

Definition 4.7. MOV Algorithm

(1) Let $N = \#E(\mathbb{F}_{p^k})$
(2) Now take some point $\Theta \in E(\mathbb{F}_{p^k})$, but not in $E(\mathbb{F}_p)$
(3) Now, because P (the same P we described in our set up) is a j-torsion point we know that $E(\mathbb{F}_p)$ has a j-torsion point. So now, $j \mid \#E(\mathbb{F}_{p^k})$ then we can multiply Θ to get a new point $\frac{N}{j}\Theta$
(4) Then given your point P calculate the Weil Pairing in $\mathbb{F}_{p^k}^\times$ to get

$$p = e_j(P, \tfrac{N}{j}\Theta)$$

$$q = e_j(Q, \tfrac{N}{j}\Theta)$$

(5) So now we have that $q = p^n \mod p^k$. This is because we can write the two Weil Pairings in terms of their basis, P_1 and P_2 such that $P = a_P P_1 + b_P P_2$ and $\frac{N}{j}\Theta = a_{\frac{N}{j}\Theta} P_1 + b_{\frac{N}{j}\Theta} P_2$ such that $e_j(P, \frac{N}{j}\Theta) = e_j(P_1, P_2)^{a_P b_{\frac{N}{j}\Theta} - a_{\frac{N}{j}\Theta} b_P}$ and $e_j(Q, \frac{N}{j}\Theta) = e_j(nP, \frac{N}{j}\Theta) = e_j(P_1, P_2)^{a_{nP} b_{\frac{N}{j}\Theta} - b_{nP} a_{\frac{N}{j}\Theta}}$

(6) Now we can use Pohlig-Hellman or some other algorithm to solve $q = p^n \mod p^k$ and then we have n and have solved the ECDLP

5. The Modified Weil Pairing

The Weil Pairing can be quite problematic in cryptography because it is usually rendered useless because in Elliptic Curve cryptography we usually want to deal with pairs of points like cP and kP, that are each multiples of each other or have some sort of common point that they are a multiple of and we know that $e_n(c \cdot P, d \cdot P) = 1$.
To fix this define

$$\phi : E[m] \to E[m]$$

such that $\phi(P) \neq a \cdot P$ where $a \in \mathbb{Z}$. So now we can calculate

$$e_m(cP, \phi(dP)) = e_m(cP, d\phi(P)) = e_m(P, \phi(P))^{cd}$$

Now, let's define j to be some prime greater than 2. Given some Elliptic Curve E we can take some j-torsion point P and define a function $\phi : E \to E$.

Definition 5.1. Now, ϕ is a *j-distortion map* for the point P if $\phi(nP) = n\phi(P) \forall n \in \mathbb{N}$ and the Weil Pairing of the points P and $\phi(P)$ is a primitive root of unity.

Now from this we can define the modified Weil Pairing which is denoted by $\hat{e}_n$ to help us more with cryptography where we can take an elliptic curve E and a j-torsion point.

Definition 5.2. Relative to some map $\phi : E \to E$ we can get

$$\hat{e}_j(P_0, P_1) = e_j(P_0, \phi(P_1))$$

and our two points $P_1 = aP$ and $P_2 = bP$ are each separate multiples of P.

6. Tripartite Diffie-Hellman Key Exchange

Using the power of the Weil pairing we can now extended the Diffie-Hellman to three people. So now, assume we have three people trying to talk to each other, Alice, Bob and Charlie. So starting from the same point at which Alice chooses some integer a, Bob chooses some integer b and Charlie chooses some integer c. They each publicly decide on some point P on an elliptic curve $E(\mathbb{F}_r)$ such that P is a j-torsion point to wit Alice computes

$$A = aP$$

and Bob computes

$$B = bP$$

and the Charlie computes

$$C = cP$$

Now, each of the three of them publish A, B and C. Using the Weil Pairing, Alice will then compute

$$\hat{e}_n(B, C)^a$$

then Bob computes

$$\hat{e}_n(B,C)^b$$

and Charlie computes

$$\hat{e}_n(A,B)^c$$

Now, we have that Alice's value is $\hat{e}_n(bP,cP)^a = \hat{e}_n(P,P)^{abc}$, similarly we can see that this is also the case for Bob's value and Charlie's value. Hence the shared value for Alice, Bob and Charlie is

$$\hat{e}_n(P,P)^{abc}$$

Now, we can show that this system is secure, because the security relies on Eve being able to solve the ECDLP. Because if Eve can solve the ECDLP she can easily find a, b and c.

However, breaking the 3 person Diffie-Hellman also has another angle to it. Eve has $\hat{e}_n(P,P)$ and knows aP so she can find $\hat{e}_n(aP,P) = \hat{e}_n(P,P)^a$. Hence Eve can recover a if she uses some algorithm to solve the Discrete Logarithm Problem in the field that the elliptic curve is over, $\mathbb{F}_q$.

7. Bibliography

(1) Atkin, A. O. L. and Morain, F. "Elliptic Curves and Primality Proving." Math. Comput. 61, 29-68, 1993.
(2) Cassels, J. W. S. Lectures on Elliptic Curves. New York: Cambridge University Press, 1991.
(3) Cremona, J. E. Algorithms for Modular Elliptic Curves, 2nd ed. Cambridge, England: Cambridge University Press, 1997.
(4) Cremona, J. E. "Elliptic Curve Data." https://modular.fas.harvard.edu/cremona/ INDEX.htm.
(5) Du Val, P. Elliptic Functions and Elliptic Curves. Cambridge, England: Cambridge University Press, 1973.
(6) Fermigier, S. "Collection of Links on Research Articles on Elliptic Curves and Related Topics." https://www.fermigier.com/fermigier/elliptic.html.en.
(7) Gebel, J.; Pethő, A.; and Zimmer, H. G. "Computing Integral Points on Elliptic Curves." Acta Arith. 68, 171-192, 1994.
(8) Hartshorne, R. Algebraic Geometry. New York: Springer-Verlag, 1999.
(9) Ireland, K. and Rosen, M. "Elliptic Curves." Ch. 18 in A Classical Introduction to Modern Number Theory, 2nd ed. New York: Springer-Verlag, pp. 297-318, 1990.
(10) Joye, M. "Some Interesting References on Elliptic Curves." https://www. geocities.com/MarcJoye/biblio_ell.html.
(11) Katz, N. M. and Mazur, B. Arithmetic Moduli of Elliptic Curves. Princeton, NJ: Princeton University Press, 1985.
(12) Knapp, A. W. Elliptic Curves. Princeton, NJ: Princeton University Press, 1992.
(13) Koblitz, N. Introduction to Elliptic Curves and Modular Forms. New York: Springer-Verlag, 1993.
(14) Lang, S. Elliptic Curves: Diophantine Analysis. Berlin: Springer-Verlag, 1978.
(15) Mazur, B. and Tate, J. "Points of Order 13 on Elliptic Curves." Invent. Math. 22, 41-49, 1973/74.
(16) McKean, H. and Moll, V. Elliptic Curves: Function Theory, Geometry, Arithmetic. Cambridge, England: Cambridge University Press, 1999.

(17) Riesel, H. "Elliptic Curves." Appendix 7 in Prime Numbers and Computer Methods for Factorization, 2nd ed. Boston, MA: Birkhäuser, pp. 317-326, 1994.
(18) Silverman, J. H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986.
(19) Silverman, J. H. The Arithmetic of Elliptic Curves II. New York: Springer-Verlag, 1994.
(20) Silverman, J. H. and Tate, J. T. Rational Points on Elliptic Curves. New York: Springer-Verlag, 1992.
(21) Stillwell, J. "Elliptic Curves." Amer. Math. Monthly 102, 831-837, 1995.
(22) Stroeker, R. J. and Tzanakis, N. "Solving Elliptic Diophantine Equations by Estimating Linear Forms in Elliptic Logarithms." Acta Arith. 67, 177-196, 1994.
(23) Swinnerton-Dyer, H. P. F. "Correction to: 'On 1-adic Representations and Congruences for Coefficients of Modular Forms.' " In Modular Functions of One Variable, Vol. 4, Proc. Internat. Summer School for Theoret. Phys., Univ. Antwerp, Antwerp, RUCA, July-Aug. 1972. Berlin: Springer-Verlag, 1975.
(24) Weisstein, E. W. "Books about Elliptic Curves." https://www.ericweisstein .com/ encyclopedias/ books/EllipticCurves.html.

Email address: jzeitlin36@gmail.com