

ELLIPTIC CURVES IN MODERN CRYPTOGRAPHY

DANIELLE MACLENNAN

ABSTRACT. An investigation into elliptic curves and cryptography, and more importantly the merging of the two to create something that has a great impact on the security imperative to our everyday lives. After giving an overview of the necessary background information needed to understand the two areas, important properties of elliptic curves and their discrete logarithm problem are examined. This is related to the Diffie-Hellman Key Exchange, a widely used method of public key exchange, focusing on examples and why elliptic curve cryptography is of such advantage to the ciphering world.

1. INTRODUCTION

Cryptography is defined as the “science of secret writing” [2], i.e. the process and skill of communicating or deciphering secret messages, or ciphers. Historically, cryptography has mainly dealt with techniques for transmitting information or messages in a confidential manner so that a third party cannot read or understand it, even if they manage to obtain it through an insecure channel such as a public telephone line. These days however, cryptography is fundamental in our daily lives, providing effective tools to secure information about our email accounts or bank details, even protecting national security, and the use of mathematics is absolutely vital in the methods used.

Until recently, elliptic curves and the properties exhibited by them were only of major use deep in the core of mathematics, in areas such as topology, algebraic geometry and number theory. In fact, it was only in the mid 1980’s that elliptic curve cryptography was suggested by Victor Miller and Neal Koblitz. Now this method of secret transmission is a hotly investigated topic that is in use all over the world.

2. MATHEMATICAL BACKGROUND

2.1. Algebraically Closed Field. We define a field \mathbb{k} to be *algebraically closed* if every polynomial in $\mathbb{k}[x]$ has at least one root, i.e. if every polynomial with coefficients in \mathbb{k} has a least one root in \mathbb{k} . For example, \mathbb{C} is algebraically closed (this is the Fundamental Theorem of Algebra) but \mathbb{F}_3 is not, as $x^2 + 1$ is irreducible over this field.

We can also extend any field \mathbb{k} to its algebraic closure \mathbb{K} , where $\mathbb{k} \subseteq \mathbb{K}$ and the following conditions are satisfied:

- \mathbb{K} is algebraically closed, and
- if \mathbb{L} is a field such that $\mathbb{k} \subseteq \mathbb{L} \subseteq \mathbb{K}$ and \mathbb{L} is algebraically closed, then $\mathbb{L} = \mathbb{K}$.

2.2. Projective Space. In day-to-day mathematics we are used to working with vector spaces such as \mathbb{R}^n and \mathbb{C}^n - these are both examples of affine spaces. We define n-dimensional affine space over a field \mathbb{k} as

$$\mathbb{k}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{k}\}.$$

However, when working with an elliptic curve it is useful to add a “point at infinity” to it, which will act as the identity element when defining the group law. To do so we must work in projective space, a natural compactification of affine space.

Definition 2.1. Let \mathbb{k} be a field. The projective plane over \mathbb{k} is defined as

$$\mathbb{P}_{\mathbb{k}}^2 = (\mathbb{k}^3 \setminus \{(0, 0, 0)\}) / \sim$$

where $(x_0, y_0, z_0) \sim (x_1, y_1, z_1)$ if and only if there exists an $\alpha \in \mathbb{k}^\times = \mathbb{k} \setminus \{0\}$ such that $x_1 = \alpha x_0$, $y_1 = \alpha y_0$ and $z_1 = \alpha z_0$.

To remind ourselves that the points of $\mathbb{P}_{\mathbb{k}}^2$ are equivalence classes we write $(x_0 : y_0 : z_0)$ for the equivalence class of (x_0, y_0, z_0) in $\mathbb{P}_{\mathbb{k}}^2$.

More generally, projective n -dimensional space $\mathbb{P}_{\mathbb{k}}^n$ is defined as \mathbb{k}^{n+1} , minus the origin and modulo the relation

$$(a_0, \dots, a_n) \sim (b_0, \dots, b_n) \Leftrightarrow (a_0, \dots, a_n) = \lambda(b_0, \dots, b_n), \lambda \in \mathbb{k}^\times.$$

It is often useful to think of points in $\mathbb{P}_{\mathbb{k}}^n$ as being in one to one correspondence with lines through the origin in \mathbb{k}^{n+1} .

We can also write this as

$$\mathbb{P}_{\mathbb{k}}^n = \mathbb{k}^n \sqcup \mathbb{P}_{\mathbb{k}}^{n-1}.$$

To justify this, consider a point $(a_0 : \dots : a_n)$. As this is actually an equivalence class, if $a_n \neq 0$ then we can use the relation \sim to divide through by a_n , giving us

$$(a_0 : \dots : a_n) = \left(\frac{a_0}{a_n}, \frac{a_1}{a_n}, \dots, 1\right),$$

a point in \mathbb{k}^n . If $a_n = 0$, we have $(a_0 : \dots : a_{n-1} : 0)$, and

$$\{(a_0 : \dots : a_{n-1}, 0) \mid a_0, \dots, a_{n-1} \in \mathbb{k}\} \simeq \mathbb{P}_{\mathbb{k}}^{n-1}.$$

2.3. Points at infinity. As mentioned earlier it is useful to add a point at infinity to an elliptic curve. To understand where this comes from, consider the following:

If $(x : y : z)$ is a point in $\mathbb{P}_{\mathbb{k}}^2$ with $z \neq 0$ then we can divide through by z to get $(x : y : z) = (\frac{x}{z} : \frac{y}{z} : 1)$. These are the “finite” points in $\mathbb{P}_{\mathbb{k}}^2$.

Otherwise, $z = 0$ and we have

$$(x : y : 0) = \lim_{z \rightarrow 0} (x : y : z) = \lim_{t \rightarrow \infty} (x : y : \frac{1}{t}) = \lim_{t \rightarrow \infty} (xt : yt : 1).$$

So the x and y coordinates will tend to ∞ , and for this reason the points $(x : y : 0)$ are called the “points at infinity” of $\mathbb{P}_{\mathbb{k}}^2$.

3. CRYPTOGRAPHICAL BACKGROUND

There are two forms of cyptrography, secret-key (also known as symmetric) and public-key (also known as asymmetric) [3]. We will use the standard notation of Alice wanting to send a message to Bob, and an eavesdropper Eve trying to intercept and understand the message.

3.1. Secret-key Cryptography. This is the oldest and fastest type of cryptography, based around the sharing of some secret key between the people who would like to communicate. This secret key is used both in the encryption process by the sender of the message to compute the ciphertext or code, and by the receiver to decrypt the message back to cleartext, hence the name symmetric. A current standardized method of this type is called the AES symmetric-key cryptosystem.

A simple example of a secret-key system is obtained by substituting 1 for A, 2 for B, ..., 26 for Z. Say Alice wishes to send Bob the message “Leave the country now”, she would note that L is represented by 12, E by 5, etc and send the message

$$\begin{array}{cccc} 12 & 5 & 1 & 21 & 5 \\ & 20 & 8 & 5 & \\ 3 & 15 & 21 & 14 & 20 & 18 & 25 \\ & 14 & 15 & 23. & \end{array}$$

When Bob receives the message, he simply has to use the same key to convert the message back to cleartext and then get himself to the nearest airport as fast as he can. However, if Eve reads the message she has no way of deciphering the message unless she knows the secret key.

The advantages of secret-key cryptography is that as decryption is simply the reversal of manipulations on bits of the message, it is very fast. The main disadvantage is that a secret-key must be shared beforehand in a secure way and kept private, which is tricky in a large network.

3.2. Public-key Cryptography. This materialized in the late 1970’s and is based around one-way functions, i.e. functions whose inverses cannot be computed in any reasonable amount of time. Elliptic curve cryptography is one of the main examples of public-key cryptography. Other widely used methods of public-key cryptography are modifications of the RSA cryptosystem, which is dependent on the idea that while it is relatively easy to generate two large primes P and Q (1024-bit being a typical size for reasonable security) it is nearly impossible to factorise their product PQ .

Public-key cryptography is much slower than secret-key cryptography, and therefore is most commonly used alongside it, for example as a method to exchange a secret key or for enabling signatures for authentication.

4. ELLIPTIC CURVES

Elliptic curves have been fundamental in areas of mathematics such as algebraic geometry, number theory and topology for many decades. Now they are vital in public-key cryptography (see Remark 5.1), and some think they could even replace cryptography methods based on integer factorization, such as RSA and DSA. They were proposed for applications in cryptography due to their fast group law and because so far no subexponential attack on their discrete logarithm problem is known.

4.1. What is an elliptic curve? Formally, an elliptic curve over a field \mathbb{k} is a projective non-singular algebraic curve of genus 1. Any elliptic curve can be regarded as a subset of the projective plane, $\mathbb{P}_{\mathbb{k}}^2$ - the set of solutions $(X : Y : Z)$ of the homogeneous equation

$$ZY^2 = X^3 + AXZ^2 + BZ^3$$

where A and B are constants in \mathbb{k} . We define $E(\mathbb{k})$ to be the set of points in E over \mathbb{k} , and it is clear that $E(\mathbb{k}) \subset \mathbb{P}_{\mathbb{k}}^2 = \mathbb{k}^2 \sqcup \mathbb{P}_{\mathbb{k}}^1$. In fact, E intersects the line $\mathbb{P}_{\mathbb{k}}^1 = \{(X : Y : 0) \in \mathbb{P}_{\mathbb{k}}^2\}$ at

only one point, as from the above equation $Z = 0 \Rightarrow X = 0$, and since the origin is not in the projective plane $Y \neq 0$. We can then assume that $Y = 1$, and hence

$$E(\mathbb{k}) \cap \mathbb{P}_{\mathbb{k}}^1 = (0 : 1 : 0) := \infty.$$

So if we let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ we can write

$$E(\mathbb{k}) = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Thus we obtain the Weierstrass equation for an elliptic curve, $y^2 = x^3 + Ax + B$, which is a subset of affine space and will be used several times later in the paper.

4.2. The Group Law. Addition of points on an elliptic curve is not as straightforward as the addition of points in, for example, \mathbb{R}^2 . Instead, we have to draw a line through the two points, find where it intersects the elliptic curve for the third time and reflect this point of intersection in the x -axis to obtain the sum of the original two points.

It is possible to define a law of addition for points on an elliptic curve in this way so that they form an abelian group, as shown below.

Theorem 4.1. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E . We define their sum $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*

(1) *If $x_1 \neq x_2$, then*

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

where

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

(2) *If $x_1 = x_2$ but $y_1 \neq y_2$, then*

$$P_1 + P_2 = \infty.$$

(3) *If $P_1 = P_2$ and $y_1 \neq 0$, then*

$$\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

where

$$m = \frac{3x_1^2 + A}{2y_1}.$$

(4) *If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.*

Also, we define

$$P + \infty = P$$

for all points P on E (including ∞).

Proof. (Adapted from [4].)

(1) First let's assume that $P_1 \neq P_2$, that neither point is ∞ , and that $x_1 \neq x_2$. If we draw the line L connecting the two points, L will have the equation

$$y = m(x - x_1) + y_1$$

where

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

To find the point where the line intersects E again, say $P'_3 = (x'_3, y'_3)$, we can substitute to get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

which can be rearranged into the form

$$0 = x^3 - m^2x^2 + \dots$$

The three roots of this cubic correspond to the three points of intersection of L and E . Note that if we have a cubic polynomial $x^3 + ax^2 + bx + c$ with roots r, s , and t , then

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \dots$$

i.e. $r + s + t = -a$. Since in this case we already know x_1 and x_2 to be two of the roots we can see that $m^2 = x_1 + x_2 + x'_3$, which we can rearrange to give

$$x'_3 = m^2 - x_1 - x_2, \quad y'_3 = m(x'_3 - x_1) + y_1.$$

Now to reflect this point across the x -axis all we need to do is change the sign of the y -coordinate giving us $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

- (2) Now take P_1 and P_2 as above but this time let $x_1 = x_2$. If $y_1 \neq y_2$ then the line joining P_1 and P_2 is vertical and hence intersects E at ∞ . It is conventional to think of ∞ being at the top *and* at the bottom of the y -axis, as if the ends of the y -axis are wrapping around and meeting - this may be easier to think of if you visualise a finite field rather than a field such as the real numbers. We can relate this to $\mathbb{P}_{\mathbb{k}}^2 = \mathbb{k}^2 \sqcup \mathbb{P}_{\mathbb{k}}^1$ by noting that both ends of the y -axis have the same slope, and hence give the same point in $\mathbb{P}_{\mathbb{k}}^1 \subset \mathbb{P}_{\mathbb{k}}^2$, ∞ . This means that when we reflect ∞ in the y -axis we just get ∞ again, and hence

$$P_1 + P_2 = \infty.$$

- (3) This time lets consider the case where $P_1 = P_2 = (x_1, y_1)$. When two points are very close together on a curve the line between them is approximately a tangent, and so we take the line L through these two coinciding points to be the tangent line at this point. We can use partial differentiation with respect to x to find the gradient m :

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

If $y_1 \neq 0$ then the equation of L is, as before,

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

which can again be rearranged into the form

$$0 = x^3 - m^2x^2 + \dots$$

Although this time we only have one root, x_1 , it is a double root as L is a tangent to E , hence we find the third point of intersection $P'_3 = (x'_3, y'_3)$ where

$$x'_3 = m^2 - 2x_1, \quad y'_3 = m(x'_3 - x_1) + y_1,$$

and we can flip this in the x -axis to obtain $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

- (4) Finally, if $P_1 = P_2$ and $y_1 = 0$, then the line is vertical and we set $P_1 + P_2 = \infty$ as before.

To show that $P + \infty = P$, notice that the line through P and ∞ is a vertical line that intersects E again at the reflection of P in the x -axis. \square

This addition of points satisfies

- Associativity
- Existence of inverse (denoted $-P$)
- Existence of identity (∞)
- Commutativity

and so the points on E form an additive abelian group with ∞ as the identity element.

4.3. Repeated Addition of Points. If P is a point on an elliptic curve and $k \in \mathbb{N}$, then

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

If k is an integer less than 0, then

$$kP = \underbrace{(-P) + (-P) + \dots + (-P)}_{-k \text{ times}}.$$

If k is very large, which it almost always will be in cryptography (see later for justification), then repeatedly adding P to itself is very inefficient. Instead, we use a method called *successive doubling*. For example, to find $23P$ we would calculate

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P, \quad 16P = 8P + 8P, \quad 23P = 16P + 4P + 2P + P.$$

Even though the size of the coordinates will rapidly increase with successive doubling, the fields worked over in cryptography are usually finite and so we can reduce the coordinates using modulo arithmetic. Thus, they remain fairly small and manageable.

4.4. Elliptic Curves over Finite Fields. Finite fields are the most common fields to work over in cryptography. If \mathbb{F} is a finite field and E is an elliptic curve defined over \mathbb{F} , it is obvious that $E(\mathbb{F})$ is a finite group, as for any point $(x, y) \in E(\mathbb{F})$ there are only a finite number of choices for each x and y . Many properties of this group, especially its order, are important in several contexts. To count how many points are in $E(\mathbb{F})$, and hence find its order, we go through all possible values of x , calculate y^2 from the equation of the elliptic curve and see if there is a square root of this number in the finite field.

For example if E is defined by the curve $y^2 = x^3 + x + 1$ over \mathbb{F}_5 :

x	y^2	y	Points
0	1	± 1	$(0, 1), (0, 4)$
1	3	—	—
2	$11 \equiv 1 \pmod{5}$	± 1	$(2, 1), (2, 4)$
3	$31 \equiv 1 \pmod{5}$	± 1	$(3, 1), (3, 4)$
4	$69 \equiv 4 \pmod{5}$	± 2	$(4, 2), (4, 3)$
∞		∞	∞

Note that none of the elements in \mathbb{F}_5 are congruent to 3 when they are squared. As there are 9 points, the order of $E(\mathbb{F}_5)$ is 9.

4.5. The Order of a Point. Let $P \in E(\mathbb{F}_q)$ where q is a prime power. The order of P is the smallest positive integer k such that

$$kP = \infty.$$

Note that if k is the order of P and $nP = \infty$ then $k \mid n$. Also, by Lagrange's Theorem, the order of a point P must divide the order of the group $E(\mathbb{F}_q)$.

5. THE DISCRETE LOGARITHM PROBLEM

Let G be any group, written multiplicatively, and let $a, b \in G$. If we know that there exists some integer k such that $a^k = b$, then the classical discrete logarithm problem is to find k .

We are most concerned with the case where $G = E(\mathbb{F}_q)$, and as G is an additive group we can rewrite the discrete logarithm problem as

$$kA = B$$

where A and B are points on the elliptic curve defined by E and k is once again an integer.

Remark 5.1. While adding a point on an elliptic curve to itself several times is relatively straightforward, reversing the process and computing the discrete logarithms appear to be much more difficult and time consuming. In fact, it is the difficulty of the discrete logarithm problem that elliptic curve cryptography relies upon. This can be increased by using points and working over fields with large order.

6. DIFFIE-HELLMAN KEY EXCHANGE

The computation of discrete logarithms was merely a matter of interest to most of the mathematical world until 1976, when Diffie and Hellman published their seminar paper “New Directions in Cryptography” [1], which describes a method of public key exchange for the multiplicative group of a finite prime field. The Diffie-Hellman Key Exchange can also be used over the group defined by an elliptic curve over any finite field, as demonstrated below:

- (1) Alice and Bob agree on an elliptic curve E over a finite field \mathbb{F}_q , and a point $P \in E(\mathbb{F}_q)$. This information is public.
- (2) Alice chooses a secret integer a , then computes aP and sends it to Bob.
- (3) Bob chooses a secret integer b , computes bP and sends it to Alice.
- (4) Alice and Bob can then both calculate abP .

However, an eavesdropper, Eve, will have to compute abP only knowing P , aP and bP in $E(\mathbb{F}_q)$. If Eve can solve discrete logs in this field, she can use P and aP to find a , which she can then multiply to bP to get abP , so it is essential that the elliptic curve, point and field are chosen so that the discrete logarithm problem is hard. It is not yet known whether or not there is some other way of computing abP without using discrete logs [4].

7. EXAMPLES

In all of these examples, we will let $A = B = 1$ in the Weierstrass equation for an elliptic curve, hence we are working with E defined by $y^2 = x^3 + x + 1$.

7.1. Easy - E over \mathbb{F}_3 . The points in $E(\mathbb{F}_3)$ are, working modulo 3,

x	y^2	y	Points
0	1	± 1	$(0, 1), (0, 2)$
1	0	0	$(1, 0)$
2	2	—	—
∞		∞	∞

i.e. $|E(\mathbb{F}_3)| = 4$. Both $(0, 1)$ and $(0, 2)$ have order 4, $(1, 0)$ has order 2, and ∞ of course has order 1.

Suppose we propose the discrete logarithm problem for E over \mathbb{F}_3 of

$$k(0, 2) = (0, 1).$$

This can be solved easily. Since the order of $(0, 2)$ is only 4, we can simply use brute force to go through the arithmetic of calculating $k(0, 2)$ for $k = 0, 1, 2, 3$.

$$0(0, 1) = \infty.$$

$$1(0, 1) = (0, 1).$$

To find $2(0, 1)$ we use Part 3 of Theorem 4.1 to calculate

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{1}{2} = 1 \times 2^{-1} \equiv 1 \times 2 = 2$$

and then

$$x_3 = m^2 - 2x_1 = 2^2 - 0 = 4 \equiv 1 \pmod{3}$$

$$y_3 = m(x_1 - x_3) - y_1 = 2(0 - 1) - 1 \equiv 0 \pmod{3}$$

Hence $2(0, 1) = (1, 0)$.

As $3(0, 1) = 2(0, 1) + (0, 1) = (1, 0) + (0, 1)$ we use Part 1 of Theorem 4.1:

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1}{-1} \equiv 2$$

so that

$$x_3 = m^2 - x_1 - x_2 = 2^2 - 1 - 0 = 3 \equiv 0 \pmod{3}$$

$$y_3 = m(x_1 - x_3) - y_1 = 2(1 - 0) - 0 = 2$$

Therefore $3(0, 1) = (0, 2)$, and thus the discrete logarithm is solved with $k = 3$.

Although the arithmetic involved in this can take some time to do by hand, it would take seconds with a computer and the correct software, hence any secret message using this discrete logarithm problem would be completely unsafe from eavesdroppers. In fact, in the case of the Diffie-Hellman key exchange where Eve will know $(0, 1)$, $a(0, 1)$ and $b(0, 1)$ where a and b could be the same, it should be trivial to calculate $ab(0, 1)$, as there are only 4 elements in $E(\mathbb{F}_3)$, one of which is the identity element ∞ and one of which is $(0, 1)$.

7.2. Moderate - E over \mathbb{F}_{11} . The points in $E(\mathbb{F}_{11})$ are

x	y^2	y	Points
0	1	1, 10	$(0, 1), (0, 10)$
1	3	5, 6	$(1, 5), (1, 6)$
2	0	0	$(2, 0)$
3	9	3, 8	$(3, 3), (3, 8)$
4	3	5, 6	$(4, 5), (4, 6)$
5	10	—	—
6	3	5, 6	$(3, 5), (3, 6)$
7	10	—	—
8	4	2, 9	$(8, 2), (8, 9)$
9	2	—	—
10	10	—	—
∞	∞	∞	∞

and so $E(\mathbb{F}_{11})$ has order 14.

Working modulo 11 is already harder and much more time consuming to do by hand, though it probably wouldn't make much difference to a computer.

Consider the point $(3, 8)$. If we chose the discrete logarithm problem

$$k(3, 8) = (6, 5)$$

Eve would have to do roughly 4 times as many calculations as in the previous example, which would take approximately 4 times as long (for this discrete logarithm problem she would actually only have to do 5 calculations, but as the order of the group is 14 and she doesn't know that the order of the point is 7 she could have to do any number of calculations up to 13).

7.3. Difficult - E over \mathbb{F}_{1093} . Consider the discrete logarithm problem

$$k(0, 1) = (413, 959).$$

It can be shown that the order of $(0, 1)$ is 1067.

$$0(0, 1) = \infty$$

$$1(0, 1) = (0, 1)$$

To calculate $2(0, 1)$, we find

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{1}{2} = 1 \times 2^{-1} \equiv 547 \pmod{1093}$$

and then

$$x_3 = m^2 - 2x_1 = 547^2 - 0 \equiv 820 \pmod{1093}$$

$$y_3 = m(x_1 - x_3) - y_1 = 547(0 - 820) - 1 \equiv 682 \pmod{1093}$$

So $2(0, 1) = (820, 682)$.

These calculations are already far too difficult and lengthy for it to be sensible to do them by hand, and even on a computer they can take quite a while.

For $3(0, 1)$, we get

$$m = \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{681}{820} \equiv 538 \pmod{1093}$$

so that

$$x_3 = m^2 - x_1 - x_2 \equiv 72 \pmod{1093}$$

$$y_3 = m(x_1 - x_3) - y_1 \equiv 611 \pmod{1093}$$

Hence $3(0, 1) = (72, 611)$.

It is already clear that by increasing the order of the finite field that we are working over and the order of the point we are repeatedly adding the discrete logarithm problem is going to take a lot longer to solve, even if we were to use successive doubling. Here, k could be any integer up to 1075, which is 1072 more than example 1 and 1065 more than in example too, so a lot more calculations will have to be done. The arithmetic is more tricky too, which will add to how long it would take to find a solution.

7.4. Secure. We have looked at elliptic curves over finite fields up to an order of 1093, and found even then that increasing the field order by a couple of bits makes the discrete logarithm problem computationally harder and time consuming. In elliptic curve cryptosystems used today, $E(\mathbb{F})$ usually have an order of about 256-bits. Although there are many attacks known for the discrete logarithm problem that would greatly increase the probability of solving the previous examples, such as the MOV attack and Pollard's Rho Method, they stand little chance against groups of such high order [4].

8. ADVANTAGES OF ELLIPTIC CURVE CRYPTOGRAPHY

The main advantage of an elliptic curve cryptosystem is that they provide the same level of security as other cryptosystems while using fewer bits. To have the same security as that provided by a 2048-bit RSA it is estimated that we could use an elliptic curve equal to a multiple of a prime of approximately 256-bits. They offer great increases in speed in many situations, and also require smaller chip size, less power consumption, etc.

REFERENCES

- [1] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 143–180. Westview, Boulder, CO, 1982.
- [2] The Columbia Encyclopedia. *Cryptography*, 2008. 6th edition, Columbia University Press.
- [3] Gerhard Frey and Tanja Lange. Introduction to public-key cryptography. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 547–572. Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [4] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

DEPARTMENT OF MATHEMATICS, GLASGOW UNIVERSITY, GLASGOW G12 8QW, SCOTLAND.
E-mail address: 0506460m@student.gla.ac.uk