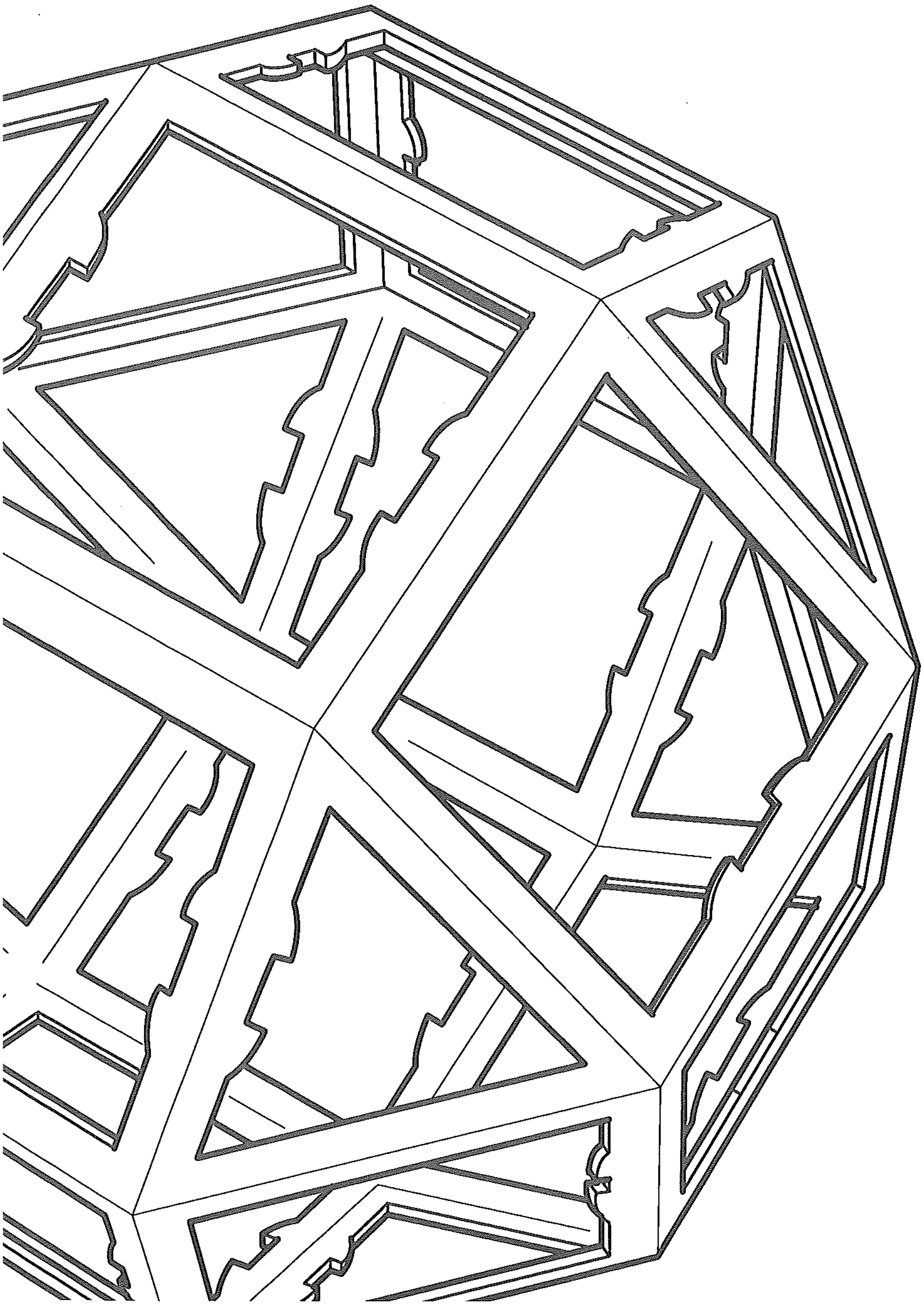
Department of Mathematics and Statistics
College of Engineering

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Summer Research Project

The Properties of Elliptic Curves Containing Singularities over the Field Z_p

By Alastair David Jamieson-Lane



09

The Properties of Elliptic Curves Containing Singularities Over the Field $\mathbb{Z}_P$

Alastair David Jamieson-Lane

February 4, 2009

Abstract

The study of elliptic curves is an important part of modern cryptography. In this report we consider the properties of singular elliptic curves over the field $\mathbb{Z}_p$, showing that they can always be factorized, that their equations always take a given form and that there are always $p + 1 \pm 1$ points satisfying this equation over the field $\mathbb{Z}_p$.

Keywords: Elliptic curves; modular arithmetic;mod; singular;

1 Introduction

This report looks into the various properties of elliptic curves, with a particular focus on trying to count the number of points on elliptic curves in $\mathbb{Z}_p$ and investigating the properties of singular elliptic curves. The study of elliptic curves is an important part of modern cryptography, particularly with referance to the "Discrete Logarithm Problem", which is used for ElGamal and Diffie-Hellman encryption [2, Sec. 7.5]. Finding a computationally fast method for calculating the number of points on an elliptic curve would have a variety of advantages in the field of cryptography. Efficient algorithms for calculating the number of points have been investigated, such as the SEA algorithm [4] and the use of a Gaussian Normal basis [7], however all require significant amounts of computer time, and are limited in there capabilities. Such algorithms are well outside the scope of this report. The first section of this report gives a precise definition of an elliptic curve, before examining it's group function, its relationship to the DLP, and some standard equations pertaining to individual elliptic curves. Section two uses an original proof to count the number of points on a singular elliptic curves. Section three uses a change of variables to rewrite an equation for a singular elliptic curve into another form, and considers the implications of this further. In section four we look at several questions raised by our previous investigations before going on to prove that all elliptic curves must take the form suggested in section 3, and that all curves of this form can be factorized. Finally we consider briefly weather it would be possible to make a singular elliptic curve into a group by simply removing the singularity.

1.1 What is an elliptic curve?

Elliptic curves equate a second degree polynomial of one variable to a third degree polynomial of another over some field $\mathbb{F}$. They are usually written as $y^2 = x^3 + bx + c$, a form which can generally be reached through an appropriate linear change of variables that preserves all major properties of the curve. We will go through an example of one such change of variables later in the report. Figure 1 depicts a representation of two example elliptic curves over the real numbers:

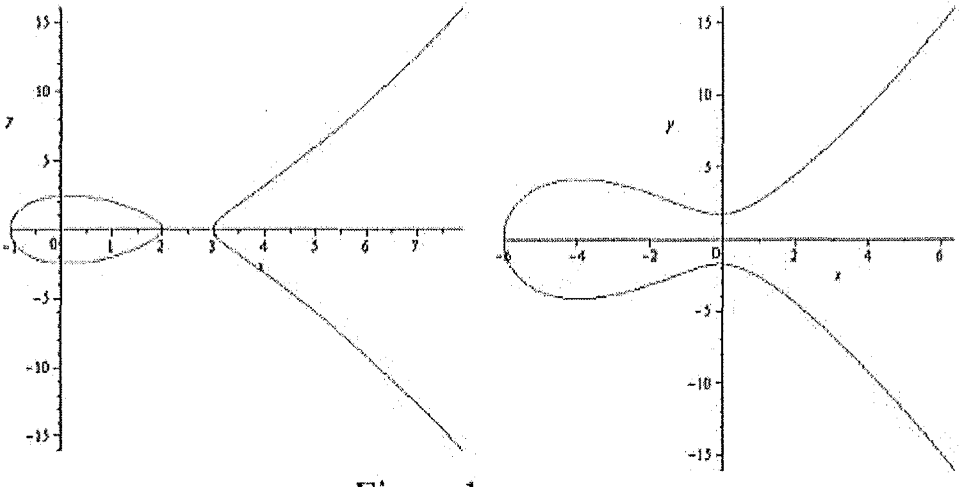


Figure 1

Elliptic curves can be defined over the real numbers, complex numbers, Modular field, or in fact any field, as all fields have both a an addition and a multiplication operation. An elliptic curve $\mathcal{E}$ is said to be the set of all points within a field $\mathbb{F}$ that satisfies the equation $y^2 = f(x)$ with the addition of a point at infinity, where $f(x)$ is some cubic function of x, that is

$$\mathcal{E} := \{(x, y) \in \mathbb{F} | (y^2 = f(x)) \cup \infty\}.$$

This construction is incredibly useful for cryptography, particulary when defined over the field $\mathbb{Z}_p$, where $\mathbb{Z}_p$ denotes the field of integers modulo p. The field of integers modulo p is the set of integers k satisfying $0 \leq k < p$, with the usual modulo addition and multiplication rules, and the additional rule that a and b are considered equal as long as $a - b$ is some multiple of p.

Example 1 On the field $\mathbb{Z}_7$ 5+4=9=2, also $\mathbb{Z}_7$ $5 \times 4 = 20 = 6 = -1$. Of note is the fact that $5 \times 3 = 15 = 1$, hence it can be said that $5^{-1} = 3$.

For our modula arithmetic to work properly we require that p be prime. This allows all numbers (except zero) to have a multiplicative inverse and also prevents such bizarre behavior as $(x - 3) \times (x - 45) = (x - 24)^2 \text{mod} 147$ (the particular importance of this example will become apparent later). Also, for the sake of simplicity, I will assume that $p > 3$ for the rest of this report. Elliptic curves can be defined over the fields $\mathbb{Z}_2$ and $\mathbb{Z}_3$, however several of the proofs in this report depend on 2 and 3 having well defined inverses, thus we will avoid these fields.

Some elliptic curves contain a "singularity", or "repeated root". When drawn over the real numbers a "singularity" is represented as the graph crossing itself. Singularities are points that have "multiplicity". Having a square factor on the right hand side of your elliptic curve will result in a singularity at that point.

Example 2 The curve $y^2 = x(x + 1)^2$ has a singularity at the point $(-1, 0)$.

It is impossible to take a tangent line at a singularity, because the singularity will either be a isolated point where there is no definable tangent, or a crossing point, where there are two equally valid tangent lines.

1.2 A Few Specifics

It is important here that we clarify a few specific details for later on in the report. Often in other articles "elliptic curves" will be spoken of only referring to curves of the given description of that are non singular. This is important to those texts so that elliptic curves can always be referred to as a group. Here I speak of both non singular and singular elliptic curves. What I refer to here as singular elliptic curves would be discounted completely in other texts.

I also often refer to a linear change of variables. Here I refer to a change of variables that does not effect the j invariant, Discriminant, number of points, or relationship between the points for an elliptic curve under the group operation (to be described later). A change of variables may scale or transpose any variable in such a way as to not change these properties. One such change of variables would for instance be setting $y' = 3y + 2$, or some such other linear transformation.

Another important concept is that of "isomorphism". Two groups are consider isomorphic if there is some renaming of variables such that the elements of the group relate to one another the same way under there standard group operation.

Example 3 N, S, E and W can be renamed $\triangle, \bigtriangledown, \triangleright$ and $\triangleleft$ respectively. The two sets $\{N, S, E, W\}$ and $\{\triangle, \bigtriangledown, \triangleright, \triangleleft\}$ can be considered Isomorphic.

For a more rigorous definition of Isomorphism please refer to [6, chapter 6].

1.3 DLP

The use of elliptic curve in cryptography is based upon what is known as the DLP, or discrete logarithm problem.

The DLP takes the form $3^\kappa = 81, \kappa =?$. In the real numbers this type of question can be easily solved by taking logarithms of each side, however when working in other groups it becomes very difficult. For instance, raising 3^6 in the field $\mathbb{Z}_7$ gives 1, which can be (relatively) easily calculated. Trying to compute κ for $5^\kappa \mathsf{mod} 17 = 2$ is much more computationally difficult, and generally requires an exhaustive search of all powers of 5. The DLP is most easily used over finite cyclic groups such $\mathbb{Z}_p$ under multiplication. These are used because all cyclic groups have an element α such that all group elements are powers of α, thus meaning that κ is defined for all elements (they all have a discrete logarithm base α). Any finite group however can be effectively used for the DLP. If using a non-cyclic group the only disadvantage is that not all elements will have a defined discrete logarithm. Because of the way the DLP is constructed this is not a significant problem.

1.4 The Group Law

One such group that can be used for the DLP is that formed by an elliptic curve. In order for us to use the curve in such a manner we must first define the group operation. We denote the standard group operation for an elliptic curve as $\oplus$ (pronounced "oat", or "oh-plus"). For elliptic curves over the real numbers $\oplus$ is defined as follows:
-Step 1: Choose two points on your elliptic curve, P and Q.
-Step 2: Draw a straight line L through P and Q.
-Step 3: Find the point where L crosses your elliptic curve, label this R'. Reflect R' through the x axis, giving a point with the same x value, but the opposite y value. This point must be a solution to the curve, for we know that if (x,y) is a solution, so to must (x,-y), as +y and -y have the same square.

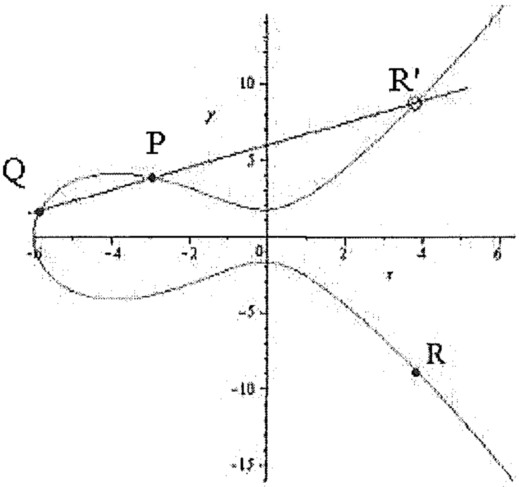


Figure 2

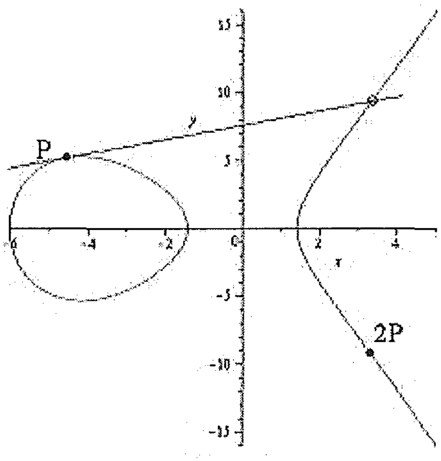


Figure 3

We now say that $R = P \oplus Q$.

There are several special cases that must be considered:
If P is directly above or below Q then the line will not cross the curve again. In this case we say $P \oplus Q = \infty$, and also that $P = -Q$.
If one of the points chosen is ∞ then we say $\infty \oplus P = P$. ∞ is the groups identity element.
If $P = Q$ then instead of drawing a line between the two points (which we can no longer do) we instead take a tangent to the elliptic curve at P. (see fig 3) In this case we can either write $P \oplus P = R$ or $2P = R$.

The $\oplus$ operator is currently defined geometrically over the real numbers, however when working over more abstract fields we will require a more abstract definition.

Definition 4 Let $\mathcal{E}$ be the set $\{(x, y) \in \mathbb{F} | (y^2 = x^3 + ax + b) \cup \infty\}$
Let P and Q both be elements of the set $\mathcal{E}$, written as (x_P, y_P) and (x_Q, y_Q) respectively, where x_P, y_P, x_Q and y_Q elements of $\mathbb{F}$. The *Sum* of P and Q, written as $P \oplus Q$ is the point $R \in \mathcal{E}$, written as (x_R, y_R) such that:
If $P = \infty$ then we define $P \oplus Q = \infty \oplus Q = Q = R$
If $Q = \infty$ then we define $P \oplus Q = P \oplus \infty = P = R$

If $x_P \neq x_Q$ then we define m as: $m = (y_P - y_Q) \times (x_P - x_Q)^{-1}$. then

$$x_R = m^2 - x_P - x_Q, \tag{1}$$

$$y_R = -y_P - m(x_R - x_P). \tag{2}$$

If $x_P = x_Q$ then either $y_P = y_Q$ or $y_P = -y_Q$. If $y_P = -y_Q$ then we define $P \oplus Q = \infty = R$. If $y_P = y_Q$ then $P = Q$ and we must compute the "tangent line" . The exact definition of a 'tangent line" on a generalized field is outside the scope of this paper, but can be found here: [5, chap3.1]. For now let us just consider the tangent on a generalized field to be a very close analogy to the tangent of a point over the real numbers. It can be computed in exactly the same way. First find the slope of the tangent line m:

$$m = (3x_P^2 + a) \times (2y_P)^{-1}$$

then calculate the x and y coordinates of R by

$$x_R = m^2 - 2x_P,$$

$$y_R = -y_P - m(x_R - x_P).$$

thus $P \oplus Q = P \oplus P = 2P = R$

We do not need to worry about weather $(2y_P) = 0$. This would require either $2 = 0$ or $y_P = 0$. If $y_P = 0$ then $y_P = -y_Q$, a case we have already considered. As always in this report we are assuming that we are not working in $\mathbb{Z}_2$, and thus can safely assume $2 \neq 0$. (definition of group function sourced from [8, page 58,59])

Now that $\oplus$ has been clearly defined it can be shown that the set of points $\mathcal{E}$ together with the operator $\oplus$ forms a group. ∞ is the groups identity element, all elements have an inverse under the group function (their mirror image through the x axis $(x, -y)$) and every possible pair of elements will add to give a third element of the group. The group operation is associative, and thus $(P \oplus Q) \oplus T = P \oplus (Q \oplus T)$. Associativity can be proved through exhaustively going through the algebra, or for an alternative geometric proof see [5, chap 5.6 prop 4]. In addition to these basic properties the set of points on an elliptic curve also have the additional property of being commutative, that is $P \oplus Q = Q \oplus P$, thus meaning that the curve forms what is known as an abelian group.

Because elliptic curves $\mathcal{E}$ defined over $\mathbb{Z}_p$ are finite abelian groups they are good candidates for the DLP. The difficulty in calculating κ for an elliptic curve is much greater then that of calculating κ for the real numbers, or even for a modular field. This is because $\oplus$ is much more complicated then multiplication, and hence harder to reverse. $\kappa P = T$ is not the kind of problem that is easily solved in your head. (See figure 4).

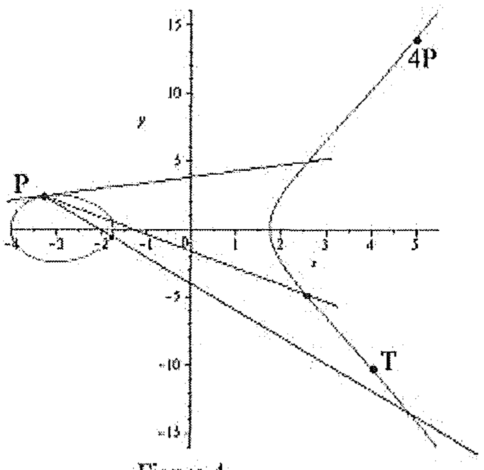


Figure 4

1.5 Order of Points and Curves

Unlike the group formed by multiplication on a modular field there is no guarantee that a point T on an elliptic curve is a multiple of a point P. This leads us to consider the idea of a points *order*. The smallest number λ, such that $\lambda P = \infty$ is said to be the order of a point, $|P|$. For non finite groups λ does not always exist, however every element P in a finite group G there exists some λ such that $\lambda P = I$ where I is the identity of the group.

Proof Consider the group element Q. It is clear that if we keep adding Q to itself within any finite group we will eventually run out of elements, and at some time there must find j and k such that $jQ = kQ$. Now, for all elements in our group there must be an inverse under the group operation, therefore $jQ \oplus -(jQ) = kQ \oplus -(jQ) = \infty = (k - j)Q$. Therefore there must exist some $\lambda = k - j$ such that $\lambda Q = \infty$.

Elliptic curves defined on $\mathbb{Z}_p$ are finite groups, therefore all points have a finite order. We want points of high order, so that we maximize the possible values of T for our DLP. We must avoid points of low order, for example points of the from (x,0) which have order 2 (See figure 5).

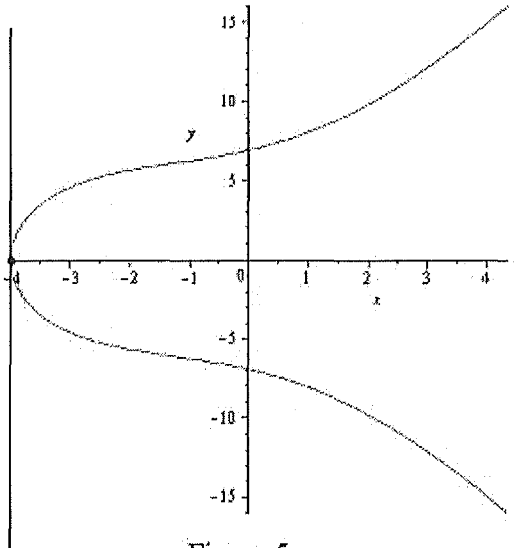


Figure 5

The total number of points on an entire curves is said to be the order of the curve $|\mathcal{E}|$. Lagrange's theorem ([6, Thrm. 7.1, page 137]) states that the order of any individual element in a group is a divisor of the total order of the group

Example 5 If an elliptic curve has twelve points, then the order of any given point must be 1,2,3,4,6 or 12.

It is helpful if we can calculate $|\mathcal{E}|$, because the order of $\mathcal{E}$ gives us information about the order of every single point, which we can then use to improve the efficiency of our cryptographic algorithms. Note, this concept of "order" makes no sense when spoken of over the real numbers, as there is a infinite number of points along the line. It does however make sense for $\mathcal{E}$ defined over the field $\mathbb{Z}_p$.

There is a formula given which can tell us the number of points of a given curve:

$$|\mathcal{E}| = 1 + \sum_{x\in\mathbb{F}} (\frac{f(x)}{\mathbb{F}} + 1), \tag{3}$$

where $f(x)$ denotes the cubic on the right hand side of the elliptic curve equation,$\mathbb{F}$ denotes the given field and $\frac{???}{\mathbb{F}}$ denotes the Legendre symbol. [1, page 1]

The Legendre symbol is defined by:
$\frac{v}{\mathbb{F}} = +1$ if there exists $z \in \mathbb{F}$ such that $v = z^2 \neq 0$
$\frac{v}{\mathbb{F}} = -1$ if there does not exist z $\in \mathbb{F}$ such that $v = z^2$
$\frac{v}{\mathbb{F}} = 0$ if $v = 0$ [9]

Example 6 Let us consider the Legendre symbol if it were to be taken over the real numbers.
For all $v > 0$ there exists z with the property that $z^2 = v$ therefore $\frac{v}{\mathbb{R}} = +1$ if $v > 0$.
For all $v < 0$ there does not exist z such that $z^2 = v$ therefore $\frac{v}{\mathbb{R}} = -1$ is $v < 0$.

Example 7 Over the complex numbers there exists z such that $z^2 = v$ for all v, $\frac{v}{\mathbb{R}} = +1$ for all $v \neq 0$

What Eqn.(3) is in effect saying is "take every possible x value. If your formula results in a square, add 2. If it results in a non square add nothing. If it results in 0, add 1." You end up going through manually and checking every single possible x value to determine if it gives you any y values. Finally, you add 1 on at the end to represent your ∞ point.

1.6 A Couple Important Quantities

Aside from a curves order there are two more quantities to note that are associated with a curve. There is the discriminant of a curve, and the j-

invariant. The discriminant of the curve, Δ, tells us the geometric shape of the curve if its equation were to be graphed over the real numbers and is written as $\Delta(\mathcal{E}) = -16(4a^3 + 27b^2)$, where $\mathcal{E} := y^2 = x^3 + ax + b$. Curves with positive discriminant have two disconnected pieces, when graphed over the real numbers. Curves with negative discriminant are represented as one continuous line when drawn over the real numbers. Curves with Discriminant 0 are singular, and thus have at least one point at which the tangent line can not be defined. (See figure 6, also referance [8, page 47,48]) It is important to note, that because the tangent line can not always be sensibly defined for singular graphs the $\oplus$ operation does not make sense. It is for this reason that singular curves are unable to form groups as non-singular curves can, and thus have limited use in the field of cryptography.

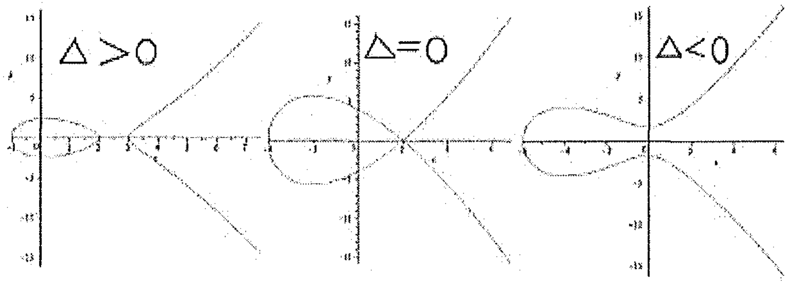


Figure 6

The second important variable associated with $\mathcal{E}$ is it's j-invariant. This is a value which will stay the same under any change of variables. It is defined as

$$j(\mathcal{E}) = \frac{1728(4a)^3}{-16(4a^3 + 27b^2)}. \tag{4}$$

For any elliptic curve on an algebraically closed field two elliptic curves having the same j invariant is enough to prove that there is some linear change of variables that takes one to the other, and thus that they are isomorphic. j is undefined for singular elliptic curves. [8, page 50]

2 Order of Singular Elliptic Curves

In this section we will use an original proof to find the number of points over a singular elliptic curve.

The general formula for the number of points on an elliptic curve that is able to be factorized, over the field $\mathbb{Z}_p$ is

$$|\mathcal{E}| = p + 1 + \sum_{x=0\ldots p-1} \frac{(kx-a)(jx-b)(lx-c)}{\mathbb{Z}_p}. \tag{5}$$

This is simply a rearrangement of Eqn. (3).
The Legendre symbol is completely multiplicative in its first argument, that is $\frac{mn}{\mathbb{R}} = \frac{m}{\mathbb{R}} \times \frac{n}{\mathbb{R}}$. Because of this the case of a singular factorized curve yields interesting results:

$$p+1+ \sum_{x=0\ldots p-1} \frac{(kx-a)(jx-b)^2}{\mathbb{Z}_p} = p+1+ \sum_{x=0\ldots p-1} \frac{(kx-a)}{\mathbb{Z}_p} \times \frac{(jx-b)^2}{\mathbb{Z}_p}, \tag{6}$$

It can be seen that $\frac{(jx-b)^2}{\mathbb{Z}_p}$ will always be $+1$, except when $jx - b = 0$. When $jx-b = 0$ we find $\frac{(jx-b)^2}{\mathbb{Z}_p} = 0$, thus the value corresponding to $jx-b = 0$ must be removed from our sum. This greatly simplifies our expression for $|\mathcal{E}|$. We now have

$$|\mathcal{E}| = p + 1 + \sum_{x=0\ldots p-1, jx-b\neq 0} \frac{(kx-a)}{\mathbb{Z}_p}. \tag{7}$$

let $kx - a = \omega$. It can be seen that for all x there exists some ω satisfying $kx - a = \omega$. Simply rearrangement will give $x = k^{-1}(\omega + a)$, thus it can be seen that for all ω there exists x. The function taking x to ω is a bijection. Thus, as we know that as x spans the set of all possible values in $\mathbb{Z}_p$, so too must ω. If we replace the expression $kx - a$ in our equation with ω, and then sum for all values of ω instead of x, we will get the same result. We are summing up over the same values but in a different order. Thus:

$$\sum_{x=0\ldots p-1, j-b\neq 0} \frac{(kx-a)}{\mathbb{Z}_p} = \sum_{\omega=0\ldots p-1, jk^{-1}(\omega+a)-b\neq 0} \frac{\omega}{\mathbb{Z}_p}. \tag{8}$$

Before we can continue with our proof, we will need to prove the following lemma:

Lemma 8 *Exactly half of the elements of the set* $\mathbb{Z}_p \setminus \{0\}$ *are Square.*

Proof We will first show that every square in $\mathbb{Z}_p$, other then zero, has two distinct roots. Let $r^2 = s^2$. Let t be an element in our field such that$s = r - t$. This results in:

$$r^2 = s^2 = (r-t)^2 = r^2 - 2rt + t^2$$

because every element in our field must have an additive inverse we can say $0 = 2rt - t^2$ therefore $+2rt = t^2$. Now we must consider two possible cases, either $t = 0$ or $t \neq 0$. If $t \neq 0$ then t^{-1} exists and thus:$2rtt^{-1} = t^2t^{-1}$ therefore $2r = t$. This value of t leads to the conclusion $s = r - 2r = -r$. The other case to consider is $t = 0$. In that case $s = r - 0 = r$
Thus for any square number s^2 there are two possible roots, $+r$ and $-r$. Next we must prove that these two roots are distinct. If $+r = -r$ then $(+r) + (-r) = 2r = 0$ This would only be possible if either 2=0 or $r = 0$. Recall that we assumed $p > 3$ at the beginning of this report, thus $2 \neq 0$. Also the case where $r = 0$ can be ignored because 0 was discounted at the beginning of this lemma. Thus $+r \neq -r$.

Because every non-zero square has two *distinct* roots, there must be exactly twice as many roots as squares. Therefore the number of squares must be exactly half the number of possible non-zero roots. Therefore half of all non-zero elements in a finite field must be square.

With this Lemma we are able to state that $\sum_{\omega=0\ldots p-1} \frac{\omega}{\mathbb{Z}_p} = 0$, as we are summing over $\frac{p-1}{2}$ square terms, $\frac{p-1}{2}$ non square terms and a single 0 term. Thus perfect cancelation occurs and our sum totals to zero. Now, to finally complete our equation:

$$|\mathcal{E}| = p+1+ \sum_{\omega=0\ldots p-1, jk^{-1}(\omega+a)-b\neq 0} \frac{\omega}{\mathbb{Z}_p} = p+1+ \sum_{\omega=0\ldots p-1} \frac{\omega}{\mathbb{Z}_p} - (\frac{\omega}{\mathbb{Z}_p})_{jk^{-1}(\omega+a)-b=0}$$

$$|\mathcal{E}| = p + 1 + 0 - \frac{kbj^{-1} - a}{\mathbb{Z}_p} \tag{9}$$

Now, assuming that $kbj^{-1} - a \neq 0$ we have $|E| = p + 1 \mp 1$. If $kbj^{-1} - a = 0$ then our equation must is of the form $y^2 = (kx - a)^3$.

Theorem 9 *All curves of the from* $(kx-a)(jx-b)^2$ *have* $p + 1 \mp 1$ *points (assuming* $jx - b \neq kx - a$*). All curves of the from* $(kx-a)^3$ *have* $p+1$ *points.*

3 Writing singular curves using an equation in a different form

3.1 Change of form

Elliptic curves are not generally written with the right hand side of the equation factorized. Most equations relating to elliptic curves assume that they are not factorized. (One such equation is that of the j invariant). As such, having information about singular curves in there factorized form is of limited use. It would be most useful to have a general form for singular curves for several reasons. Firstly, anyone wanting to do cryptography will know which curves to steer clear of. Secondly, given what we know about the order of singular elliptic curves we may be able to find some use for them further down the track, for instance, can we transform them into some form of non-singular curve while still retaining the same number of points?
It is obvious that all curves of the form: $y^2 = (kx-a)(mx-b)^2$, are singular, as they contain the repeated root $x = bm^{-1}$, however this is not the standard form in which elliptic curves are presented- a curve could very easily factorize to this form and be completely unrecognisably in any other.
The general form used for elliptic curves on a modular field by both Silverman and Deuring (and presumably most others) is $y^2 = x^3 + sx + t$. All elliptic curves can be written in this form through some linear change of variables, as long as the prime base is greater then 3 [8, 47–51]. We must make two further assumptions for this change of variables to work. Firstly, that our singular curve can be full factorized (it may be possible to have singular curves that can not be factorized, in which case they will not be represented by this change of variables). Secondly we must assume that k is a square on the field we are working in.

So, now our task is to find a suitable linear change of variables such that:

$$y^2 = (kx-a)(mx-b)^2 \equiv y^2 = x^3 + sx + t$$

The first step in this is to remove the k and m terms from the equation. This can be done by defining: $a' = a \times k^{-1}$ and $b' = b \times m^{-1}$ Both multiples are then pulled out the front of the equation:$y^2 = m^2k(x-a')(x-b')^2$. The m and k terms can now be removed by setting $y' = y \times m^{-1}\sqrt{k^{-1}}$ Thus: $y'^2 = (x-a')(x-b')^2$. Now we will expand our factorization:

$$y'^2 = x^3 - (2b' + a')x^2 + (b'^2 + 2a'b')x - a'b'^2.$$

In order to remove our x^2 term from the equation we will need to use the change of variables $x' = x - g$. This results in the equation

$$x'^3 + sx' + t = (x-g)^3 + s(x-g) + t = x^3 - 3gx^2 + 3g^2x + g^3 + sx - sg + t$$

Now, by matching coefficients we will be able to determine s, g and t and hence determine an appropriate change of variables. For the sake of easy notation we will now drop the ' from both a and b. First let us match the x^2 coefficients:

$$-3gx^2 = -(2b+a)x^2 \longrightarrow g = 3^{-1}(2b+a)$$

With this information we are then able to calculate s.

$$3g^2x + sx = (b^2 + 2ab)x \longrightarrow 3^{-1}(2b+a)^2 + s = b^2 + 2ab$$

$$\longrightarrow 3s = 3b^2 + 6ab - (2b+a)^2 = 3b^2 + 6ab - (4b^2 + 4ab + a^2) = -(b^2 - 2ab + a^2).$$

Thus we can conclude that

$$s = -3^{-1}(b-a)^2.$$

Now that we have both s and g we can substitute their values into the constant terms in order to calculate t:

$$-g^3 - sg + t = -ab^2 = -3^{-3}(2b+a)^3 + 3^{-1}(2b+a)3^{-1}(b-a) + t$$

Now, multiplying through by 27, and rearranging to make t the subject we get: $27t = -27ab^2 + (2b+a)^3 - 3(2b+a)(b-a)^2$
$= -27ab^2 + (8b^3 + 12ab^2 + 6a^2b + a^3) - 3(b-a)(2b^2 - ab - a^2)$
$= -27ab^2 + 8b^3 + 12ab^2 + 6a^2b + a^3 - 6b^3 - 3 + 3ab^2 + 3a^2b + 6ab^2 - 3a^2b - a^3$.
By using lots of cancelation we are able to simplify that to

$$2b^3 - 6ab^2 + 6a^2b - 2a^3 = 2(b-a)^3 \therefore t = 2 \times 27^{-1}(b-a)^3$$

This gives us the final result:

$$y^2 = x^3 + 3^{-1}(b-a)^2x + 2 \times 27^{-1}(b-a)^3 \tag{10}$$

Normally we would like to calculate the J-invariant of the elliptic curve, to determine whether or not our two elliptic curves are isomorphic, however this invariant is not defined for singular curves, and thus can not help confirm our change of variables.

3.2 The *Twist* Function

It is interesting to note the similarities between Eqn. (10) and that of the M. Deuring "twist" operation [3, page 2]. The *twist* operation takes two inputs, first, an elliptic curve Φ defined over $\mathbb{F}$, second some arbitrary non 0 element c of $\mathbb{F}$. A curve Φ with $p+1+t$ points is transformed into a different curve Ψ with $p+1\pm t$ points using the *twist* operation. Assuming $c \neq 1$ these two curves will not be isomorphic.

Theorem 10 *Given the curve $\Phi := y^2 = x^3 + ax + b$, the twist of Φ, Ψ is defined as $\Psi := y^2 + x^3 + axc^2 + bc^3$. If c is square then Ψ has $p+1+t$ points, just like Φ. If c is non-square then Ψ has $p+1-t$ points. [?]*

Proof $|\Phi| = 1+p+\sum_{x\in\mathbb{F}}(\frac{f(x)}{\mathbb{F}}) = p+1+t$. let $\hat{\Psi} := y^2 = c^3(\hat{x}^3 + a\hat{x} + b)$, thus $|\hat{\Psi}| = 1+p+\sum_{\hat{x}\in\mathbb{F}}(\frac{c^3\times f(\hat{x})}{\mathbb{F}})$. Because the Legendre symbol is completely multiplicative in its first argument (see 2) we can say

$$\sum_{\hat{x}\in\mathbb{F}}(\frac{c^3\times f(\hat{x})}{\mathbb{F}}) = \frac{c^3}{\mathbb{F}} \times \sum_{\hat{x}\in\mathbb{F}}(\frac{f(\hat{x})}{\mathbb{F}}) = \frac{c}{\mathbb{F}} \times \frac{c^2}{\mathbb{F}} \times \sum_{\hat{x}\in\mathbb{F}}(\frac{f(\hat{x})}{\mathbb{F}})$$

thus because $\frac{c^2}{\mathbb{F}} = 1$ we have: $|\hat{\Psi}| = 1+p\mp\sum_{\hat{x}\in\mathbb{F}}(\frac{f(\hat{x})}{\mathbb{F}})$ where $\mp$ is determined by $\frac{c}{\mathbb{F}}$.

From $\hat{\Psi}$ we can get to Ψ by defining $x = c\hat{x}$, thus absorbing several of the c terms. Thus: $\Psi := y^2 = c^3(\hat{x}^3 + a\hat{x} + b) = c^3\hat{x}^3 + c^3a\hat{x} + c^3b = x^3 + c^2ax + c^3b$ and $|\Psi| = p+1\pm t$

Because the *twist* operation allows us to take a curve with a known number of points $(p+1+t)$ and change it to one with $p+1\mp t$ points through a simple transformation I had hoped that we would be able to go from a singular curve, and change into a non singular one, with a known number of points. This would be useful, as the resulting curve could be used for cryptography because it was non singular, but would also have a well defined number of points. Unfortunately this doesn't work. This is because the *twist* of a curve has discriminant proportional to the discriminant of the original curve. Since all singular curves have discriminate 0, the twist operation will still always result in a discriminant of 0, and hence a singular curve. We show that the discriminant of a *twist*ed elliptic curve is proportional to that of the original by simply looking at the relevant formulas:

$\Phi := y^2 = x^3 + ax + b,$
$\Psi := y^2 = x^3 + c^2ax + c^3b,$
$\Delta(\Phi) = -16(4a^3 + 27b^2).$
Where Ψ is the *twist* of Φ

By simply substituting our new values into the discriminant equation we get:

$$\Delta(\Psi) = -16(4(c^2a)^3 + 27(c^3b)^2).$$

$$\Delta(\Psi) = -16c^6(4a^3 + 27b^2).$$

The discriminant of the twist is thus proportional to the discriminant of the original elliptic curve, thus singular curves can not be twisted into non singular ones, as the *twist* must necessarily have discriminant 0.

4 Questions Raised

Given the above formula for a singular elliptic curve, several question come to mind about what this implies. Is this form of elliptic curve always singular? Do all singular curves take this form? Is the cubic on x always able to be factorized, or do there exist singular curves with no proper factorization in the field $\mathbb{Z}_p$?

4.1 On the possibility of non-singular curves of this form

The first question can be answered easily by calculating the discriminant: let $\Upsilon := y^2 = x^3 - 3^{-1}\delta^2 x + 2 \times 27^{-1}\delta^3$, be the general form of the curve we have found.

$$\Delta(\Upsilon) = -16(4a^3 + 27b^2) = -16(4 \times -3^{-3}\delta^{2\times 3} + 27 \times 2^2 \times 27^{-2}\delta^{3\times 2})$$

$$= -16(-4 \times 27^{-1}\delta^6 + 4 \times 27^{-1}\delta^6) = 0$$

Hence all elliptic curves of the form Υ must be singular.

4.2 On the possibility of singular curves of other forms

The second question- weather or not all singular elliptic curves must take this form - will need a little more work. In our rearrangement of variables we only proved that all factorisable elliptic curves with square k could take this form, this does not preclude the existence of other singular curves that do not take this form. We will return then to our standard formula for all elliptic curves. Let Ω be any singular elliptic curve, written as $\Omega := y^2 = x^3 + \alpha x + \beta$ with the property $\Delta(\Omega) = 0$
It can be shown that all possible Ω must be equivalent to Υ.
First, we use the property $\delta(\Omega) = 0$ to find a relationship between α and β.

$$\delta(\Omega) = 0 = -16(4\alpha^3 + 27\beta^2) \therefore -27\beta^2 = 4\alpha^3$$

$$4\alpha^3 \times (-3)^{-3} = \beta^2 \therefore \beta = -3^{-1} \times 2\alpha\sqrt{-3^{-1}\alpha}$$

Now, for the expression under the square root sign to be square it is necessary that $\alpha = -q^2 3^{-1}$. Substituting this relation into our expression gives:

$$\Omega := y^2 = x^3 + \alpha x + \beta = x^3 - 3^{-1}q^2 x - 3^{-1} \times 2\alpha\sqrt{-3^{-1}\alpha}$$

$$\Omega := x^3 - 3^{-1}q^2 x - 3^{-1} \times 2 \times -q^2 3^{-1}\sqrt{3^{-2}q^2} = x^3 - 3^{-1}q^2 x + 3^{-3} \times 2 \times q^3,$$

Therefore $\Omega = \Upsilon$ as needed.
Thus it has been shown that all curves of the form Υ are singular, and all singular curves take this form.

4.3 On the possibility of factorization

The final question we are considering here is weather or not all possible singular curves are able to be factorized. We have a formula for all singular curves. Because no linear change of variables affects an equations ability to be factorized all we have to do is find a general factorization for our general equation.

$$\Upsilon := y^2 = x^3 - 3^{-1}\delta^2 x + 2 \times 27^{-1}\delta^3.$$

Working with 27^{-1} in the middle of our formula causes trouble, so to make our jobs easier, we should start by bringing this out the front.

$$y^2 = 27^{-1}(27x^3 - 9\delta^2 x + 2 \times \delta^3).$$

Now, using Maple to give us a quick hand we can determine that

$$27^{-1}(27x^3 - 9\delta^2 x + 2 \times \delta^3) = 27^{-1}(2\delta + 3x)(\delta - 3x)^2.$$

Thus it is shown that all curves of the form Υ can be factorized, therefore all singular curves can be factorized. This is a very useful result, as many of our previous results ran on the assumption that the singular curve in question could be factorized .

The final assumption that was previously made and needs explanation is the assumption that k was square, and thus could be removed via a suitable change of variables on y (beginning of 3). With this factorization of our singular curve we can see that no problem arises. The x coefficients from each bracket come out the front of our equation giving $3^3 \times 27^{-1}(3^{-1} \times 2\delta + x)(3^{-1} \times \delta - x)^2$. Any form of singular equation must have k such that it can be transformed to this form under a liner change of variables. As can be seen, the factor out the front is canceled completely, thus all Singular curves can be written in a factorized form where the x coefficients are 1.

5 The Group $\mathcal{S}$

So, we have the following rather interesting results regarding singular curves.
- All singular curves have form Υ, all curves of this form are singular
- All singular curves can be fully factorized.
- All singular curves have order $p + 1 \pm 1$.

However, singular curves are not able to be used in cryptography. It is clear that the singularity is what causes singular curves to be unsuitable for cryptography, and so the logical question to ask is "can we easily get rid of the singularity?"
Let D denote the singular point $(3^{-1}\delta, 0)$ on the curve

$$\Upsilon := y^2 = x^3 - 3^{-1}\delta^2 x + 2 \times 27^{-1}\delta^3 = 27^{-1}(2\delta + 3x)(\delta - 3x)^2$$

. The question "is does the set $\mathcal{S} = \{\{(x, y) \in \mathbb{F}|\Upsilon\} \cup \{\infty\} \setminus \{D\}\}$ form a group under the operation $\oplus$?" The biggest issue to consider when removing elements from a group is that the group will no longer be closed. It is important to note that what we are removing D is not actually a group, however it is still important to consider issues of closure. Does there exist some P and Q in $\mathcal{S}$ such that $P \oplus Q = D$, where D is not in $\mathcal{S}$? I will prove here that there exists no such P,Q.

Proof Let P,Q be points that are solutions to the equation Υ on the field $\mathbb{F}$, such that $P = (x_P, y_P), Q = (x_Q, y_Q)$. We then find the equation for the line passing through both points to be $y = m(x - x_P) + y_P$. This line will cross the curve when:

$$27^{-1}(2\delta + 3x)(\delta - 3x)^2 = y^2 = m^2(x - x_P)^2 + 2my_P(x - x_P) + y_P^2. \quad (11)$$

For $P \oplus Q = D$ it is necessary that $x = x_D = 3^{-1}\delta$ and $y = y_D = 0$. Substituting these values into Eqn (2) gives $y_D = -y_P - m(x_D - x_P)$ therefore $y_P = -m(3^{-1}\delta - x_P)$

Substituting into Eqn.(11) gives:
$0 = m^2(3^{-1}\delta - x_P)^2 - 2m^2(3^{-1}\delta - x_P)^2 + (3^{-1}2\delta + x_P)(3^{-1}\delta - x_P)^2$
Now assuming that $x_P \neq 3^{-1}\delta$ we can divide through by $(3^{-1}\delta - x_P)^2$, thus leading to: $m^2 = (3^{-1}2\delta + x_P)$

Eqn. (1) states that $x_D = m^2 - x_P - x_Q$. Substitution gives gives $3^{-1}\delta = 3^{-1}2\delta + x_P - x_P - x_Q$ therefore $x_Q = 3^{-1}\delta$. If our previous assumption that $x_P \neq 3^{-1}\delta$ is correct then Q=D, however if it isn't correct then $P = D$, either way there can be no two points in $\mathcal{S}$ such that $P \oplus Q = D$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}$.

It would be good to prove that the set $\mathcal{S}$, with the operator $\oplus$ formed a group, however it still remains to be proved that the operator remains associative. All proofs of this that I have read stipulate that the curve must be non-singular, although hopefully the removal of the singular point is enough to get these proofs to work. This must be rigorously proved before $\mathcal{S}$ can be considered a group, although initial investigations are positive.

Calculating $|\mathcal{S}|$ is much easier then calculating $|\mathcal{E}|$ for a generalized elliptic curve, hence suggesting $\mathcal{S}$ is possibly more suitable for cryptography, however there are several issues which must be considered:

- Is the operator $\oplus$ associative over $\mathcal{S}$?
- Is $\mathcal{S}$ isomorphic to some group that we already have?
- Are there any obvious fast algorithm for solving the DLP on $\mathcal{S}$.

IF all of these issues can be overcome then we will have a mathematical object very well suited for use with the DLP, and thus useful in the field of cryptography.

6 Conclusion

In this report we have covered the basic arithmetic of elliptic curves as well as their application to cryptography through the DLP. Although it is non-singular curves that are used in cryptography we here considered their singular counterparts. We found original proofs showing that singular curves over a finite field have $p + 1 \pm 1$ points, and proved that all singular curves can take the form Υ. We then considered weather the set of non singular points over a singular curve can be used to form a group, and thus allow us to use singular curves for cryptography.

References

[1] Ahmet Tekcan Betül Gezer and Osama Bizim, *The number of rational points on elliptic curves and circles over a finite field*, 1.

[2] Jahannes A. Buchmann, *Introduction to cryptography*, 1999.

[3] Thomas A. Schmidt Erkay Savaş and Çetin K. Koç, *generating elliptic curves of prime order*, 2.

[4] Mireille Fouquet and François Morain, *Isogeny volcanoes and the sea algorithm*, ANTS-V: Proceedings of the 5th International Symposium on Algorithmic Number Theory (London, UK), Springer-Verlag, 2002.

[5] William Fulton, *Algebraic curves, an introduction to algebraic geometry*, 2008 (originally published 1969.

[6] Joseph A. Gallian, *Contemporary abstract algebra*, 2002.

[7] Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park, Jae Heon Kim, and Sang Geun Hahn, *Fast elliptic curve point counting using gaussian normal basis*, ANTS-V: Proceedings of the 5th International Symposium on Algorithmic Number Theory (London, UK), Springer-Verlag, 2002, pp. 292–307.

[8] Joseph H. Silverman, *The arithmatic of elliptic curves*, 1986.

[9] Eric W. Weisstein, *Legendre symbol from mathworld a wolfram web resource.*