Elliptic Curves and Torus Knots

Arielle Leitner

May 20, 2009

Abstract

In this paper, we present an overview of elliptic curves. We give an outline of the proof that an elliptic curve is isomorphic to a torus, and then prove our main theorem: the real points of an elliptic curve form either a (0,1) or a (0,2) torus link. We also showed that the set of curves with complex multiplication can yield curves with both types of link.

1 Introduction

Mathematicians have studied elliptic curves since the time of Diophantus. Most recently, they featured in Wiles' proof of Fermat's Last Theorem. There are many books written on the subject, two of which we reference (**?** and **?**). There are many perspectives from which to study an elliptic curve, and elliptic curves have many practical applications, including public key cryptography. In this paper, we offer a brief overview, show that an elliptic curve is a torus, and prove our main theorem: the real part of an elliptic curve forms either a (0,1) or a (0,2) torus link.

2 The Basics

It is best to begin by defining elliptic curve. An elliptic curve is a non-singluar projective cubic curve in two variables. An elliptic curve in generalized Weierstrass form over $\mathbb{C}$ is

$$y^2 + a_2xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We can rewrite an elliptic curve as a normalized Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

as we will explain shortly.

A curve is non-singular if its partial derivatives are not both equal to zero at any point on the curve. In other words, the curve always has a well defined tangent line. (For every point on the curve, either $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$, or both the partial derivatives are nonzero.) If the partials both vanish, the tangent line at P is not well defined. In the case of a cubic curve over $\mathbb{R}$, we mean that our curve does not have a cusp (for example, $y^2 = x^3$, as in the right of figure 1), or cross over itself (for example, $y^2 = x^2(x+1)$, as in the left of figure 1). There are two options for a non-singluar cubic curve: it may be all in one component,with one root ($y^2 = x^3 - 1$); or it may be in two components, with three real roots ($y^2 = x^3 - x$). See figure 2.

Now we will explain how to normalize an elliptic curve, as outlined by (**?**, Ch.2). Begin with the equation of an elliptic curve in Weierstrass form:

$$y^2 + a_2xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

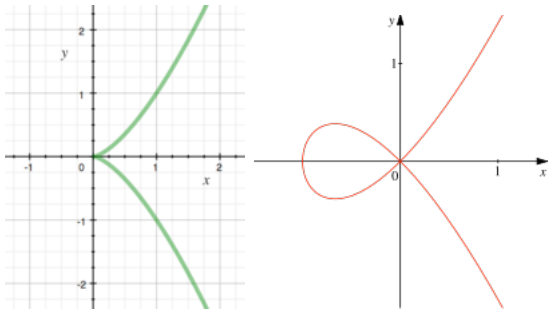
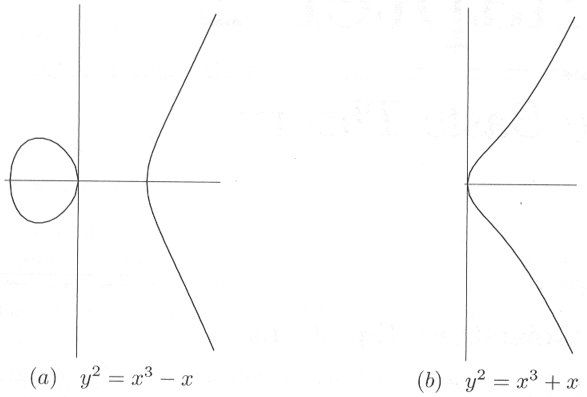


Figure 1: Singular Curves


$(a)\quad y^2 = x^3 - x$

$(b)\quad y^2 = x^3 + x$

Figure 2: Examples of non-singular curves.

If the characteristic of the field is not 2, divide by 2 and complete the square:

$$\left(y + \frac{a_1 x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 \frac{a_1 a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right)$$

Let $y_1 = y + \frac{a_1 x}{2} + \frac{a_3}{2}$. Then we can rewrite our curve with some new constants to get:

$$y_1^2 = x^3 + a_2' x^2 + a_4' x + a_6'.$$

Finally, if the characteristic of the field is also not 3, make the substitution $x_1 = x + \frac{a_2'}{3}$, and we have:

$$y_1^2 = x_1^3 + Ax_1 + B,$$

for some new constants A and B.

3 Projective Geometry

Just like Euclidean, or affine, geometry, projective geometry has its own set of axioms.

Definition 1. *Axioms for the projective plane:*
1. Any line contains two distinct points
2. Any two distinct lines intersect in a unique point
3. There exist at least four points, of which no three are collinear.

This seems just like Euclidean geometry, except for the fact that every pair of lines must intersect in a unique point. In Euclidean geometry, parallel lines do not intersect. In projective geometry, every pair of lines intersect.

Let's first define the projective line, $\mathbb{P}^1$, before we define the projective plane, $\mathbb{P}^2$. We define $\mathbb{P}^1$ to be the set of all directions in the affine plane. One way of describing this is as the set of all lines going through the origin. Lines through the origin are given by the equation $Ax = By$. We write $[A, B]$ to denote this line, where A and B are real and not both zero. However, two pairs $[A, B]$ and $[A', B']$ will give the same line if they are scalar multiples of each other. So, we can define $\mathbb{P}^1$ to be the set of all our lines modulo an equivalence relation: $[A, B] \sim [A', B']$ if $A = tA'$ and $B = tB', t \neq 0$, $t \in \mathbb{R}$. All the lines through the origin modulo this equivalence relation generate all the directions in the plane.

It is possible to construct the projective plane ($\mathbb{P}^2$) in at least two different ways. The first way is to define it as all the lines in the regular affine plane ($\mathbb{A}^2$), along with an extra "line at infinity", which is made up of all the "points at infinity" where the parallel lines were forced to intersect, by the axiom above. (All parallel lines of slope m in the affine plane will intersect at the point of infinity m in the projective plane, and so on for pairs of parallel lines in the affine plane of every slope.) In this way, we construct the projective plane as:

$$\mathbb{P}^2 \cong \mathbb{A}^2 \cup \{\text{the set of directions in } \mathbb{A}^2\} = \mathbb{A}^2 \cup \mathbb{P}^1. \tag{1}$$

It is straightforward to check that this construction of the projective plane satisfies the axioms in the definition. Every pair of non-parallel lines in the affine plane will intersect in a unique point, and every pair of lines that were parallel in the affine plane are now forced to intersect in a unique point in the projective plane. Thus every pair of lines will intersect in a unique point. We know that lines in $\mathbb{A}^2$ contain two distinct points, so the same line in $\mathbb{P}^2$ will also contain two distinct points. The projective line contains two distinct points, given $[x, y] \in \mathbb{P}^1$, with $x \neq 0$, then the point $[2x, y]$ will be different. So every line in in $\mathbb{A}^2 \cup \mathbb{P}^1$ contains two distinct points. To find four non-collinear points, of which no three are collinear, simply pick these points in $\mathbb{A}^2$, where they are already known to exist.

Now let's define the projective plane a second way. Define the projective plane to be the set of all triples $[a, b, c]$, where a, b, c are real and not all zero. Let $\sim$ be an equivalence relation where $[a, b, c] \sim [a', b', c']$ if $[a', b', c'] = [ta, tb, tc]$ with $t \in \mathbb{R}$ and $t \neq 0$. Then $\mathbb{P}^2$ is the set of equivalence classes of triples, excluding $[0, 0, 0]$.

$$\mathbb{P}^2 = \frac{\{[a, b, c] : a, b, c \text{ are not all zero}\}}{\sim}$$

Proposition 1. *The two definitions described above are equivalent.*

Proof. To see this, construct the following pair of maps.

$$\mathbb{P}^2 \cong \frac{\{[a, b, c] : a, b, c \text{ are not all zero}\}}{\sim} \leftrightarrow \mathbb{A}^2 \cup \mathbb{P}^1$$

We first construct the map:

$$\phi_z : \frac{\{[a, b, c] : a, b, c \text{ are not all zero}\}}{\sim} \to \mathbb{A}^2 \cup \mathbb{P}^1$$

$$[a, b, c] \mapsto \begin{cases} \left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}^2 & \text{if } c \neq 0 \\ [a, b] \in \mathbb{P}^1 & \text{if } c = 0 \end{cases}$$

Now we construct the reverse map:

$$\psi_z : \mathbb{A}^2 \cup \mathbb{P}^1 \to \frac{\{[a,b,c] : a,b,c \text{ are not all zero}\}}{\sim}$$

$$(x,y) \in \mathbb{A}^2 \mapsto [x,y,1]$$
$$[A,B] \in \mathbb{P}^1 \mapsto [A,B,0]$$

First we will show these maps are well defined. Suppose $[a,b.c] \sim [d,e,f]$. Then $[d,e,f] = [ta,tb,tc]$. If $c = 0$, then $\phi_z([a,b,c]) = (\frac{a}{c}, \frac{b}{c})$, and $\phi_z([d,e,f]) = (\frac{ta}{tc}, \frac{tb}{tc}) = (\frac{a}{b}, \frac{b}{c})$. If $c \neq 0$, then $\phi_z([a,b,c]) = [A,B]$ and $\phi_z([d,e,f]) = [tA,tB] \sim [A,B]$. Also, if $[A,B] \sim [D,E] \in \mathbb{P}^1$, then $\psi_z([A,B]) = [A,B,0] \sim [D,E,0] = \psi_z([D,E])$.

We will show these two maps are inverses. If $c \neq 0$,

$$[a,b,c] \mapsto \left(\frac{a}{c}, \frac{b}{c}\right) \mapsto \left[\frac{a}{c}, \frac{b}{c}, 1\right] = [a,b,c].$$

If $c = 0$,

$$[a,b,c] \mapsto [a,b] \mapsto [a,b,0] = [a,b,c].$$

□

Why would we want to work with the projective plane as opposed to the regular affine plane? There are several useful consequences of working with projective geometry; perhaps the most remarkable of these is Bezout's theorem.

Definition 2. *A polynomial, F, is homogeneous of degree d, provided it satisfies*

$$F(tX,tY,tZ) = t^d F(X,Y,Z).$$

For example, the curve $C : X^2Y = ZY^2 + Z^3$ is homogenous of degree three.

Definition 3. *A projective curve C, is the set of solutions to a polynomial equation*

$$C : F(X,Y,Z) = 0,$$

where F is a non-constant homogeneous polynomial.

To see why this is useful, consider $[a,b,c] \sim [d,e,f] \in \mathbb{P}^2$. Substituting both pairs of coordinates into our curve, C, we have:

$$a^2b = cb^2 + c^3$$
$$(a^2b)t^3 = (cb^2 + c^3)t^3$$
$$(ta)^2(bt) = (ct)(bt)^2 + (ct)^3$$
$$d^2e = fe^2 + f^2.$$

So coordinates in the same equivalence class yield the same point on the curve.

Definition 4. *The degree of a curve is the degree of its defining polynomial.*

For example, the degrees of the curves $C_1 : X^2 + Y^2 - Z^2 = 0$ and $C_2 : Y^2Z - X^3 - XZ^2 = 0$ are 2 and 3, respectively.

Definition 5. *If C is a curve given by the equation $f(x,y) = 0$, then we can factor C into a product of irreducible polynomials*

$$f(x,y) = p_1(x,y)p_2(x,y)\cdots p_n(x,y).$$

Since $\mathbb{C}[x,y]$ is a unique factorization domain, every polynomial has a unique factorization into a product of this form. The components of the curve C are the curves $p_i(x,y)$. Two curves have no common components if their irreducible components are distinct.

For example, the curves $f(x) = x$ and $g(x) = x^2 + 1$ have no common components, but the curves $h(x) = x - 1$ and $k(x) = x^2 - 1$ have the common component $x - 1 = 0$.

Theorem 2 (Bezout)**.** *Let C_1 and C_2 be projective curves with no common components. Then the number of points in which C_1 and C_2 intersect is* $\deg(C_1) \cdot \deg(C_2)$.

Essentially, Bezout's theorem says that $C_1 \cap C_2$ consists of a finite set of points if the irreducible polynomials of C_1, C_2 are distinct. For a proof of Bezout's theorem, please see the appendix of **?** . It is important to note here that the points might not all be distinct. For example, the curves $y = 0$ and $y = x^2$ intersect only at $x = 0$, but this point is counted twice. The following definition is from (**?**, appendix).

Definition 6. *To each point, $P \in \mathbb{P}^2$ we assign a multiplicity, or intersection index $I(C_1 \cap C_2, P)$. This is a non-negative integer reflecting the extent to which C_1 and C_2 are tangent to one another at P or are not smooth at P. The intersection index has the following properties;*
1) If $P \notin C_1 \cap C_2$, then $I(C_1 \cap C_2, P) = 0$.
2) If $P \in C_1 \cap C_2$, if P is a non-singluar point of both C_1 and C_2, and if C_1 and C_2 have different tangent directions at P, then $I(C_1 \cap C_2, P) = 1$. We say C_1 and C_2 intersect transversally at P.
3) If $P \in C_1 \cap C_2$ and if C_1 and C_2 do not intersect transversally at P, then $I(C_1 \cap C_2, P) \geq 2$.

To motivate the definition of multiplicity, consider two curves $y = f(x)$ and $y = g(x)$. Suppose that there is some point a, where $f(a) = g(a)$, so that the curves intersect at a. Then $f(a) - g(a) = 0$, and $(x-a)|[f(x)-g(x)]$. We say that the multiplicity of the intersection at a is the highest power, n, such that

$$(x - a)^n |[f(x) - g(x)].$$

Figure 3 illustrates how a conic and a cubic intersect six times, and a cubic and a quintic intersect 15 times.

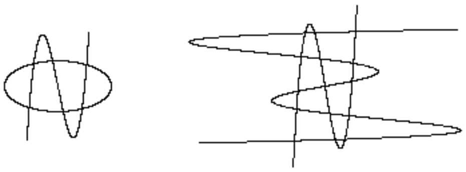


Figure 3: Examples of Bezout's Theorem.

Projective geometry provides us with a useful and necessary context for thinking about elliptic curves. Given an elliptic curve ($y^2 = x^3 + Ax + B$), we can homogenize it by multiplying every term by appropriate powers of z so that each term has degree three. This is our map ψ. We can also dehomogenize a curve, say with respect to z, by substituting 1 for z, as in our map ϕ. In this way, we can obtain a correspondence between projective curves and affine curves missing the points at infinity. We can think of the projective curve as all the affine parts "glued" together.

To demonstrate this a little better, let's compute an example. Suppose we want to study the affine curve

$$y^2 = x^3 - x.$$

We can transfer it to the projective plane by using the map ψ_z and homogenize the curve by multiplying every term by the appropriate power of Z. We have:

$$Y^2 Z = X^3 - XZ^2.$$

To find the point at infinity, we want to find the extra points we added in when we homogenized the curve. So, we use the map ϕ_z, and look at the second part of the map, when $Z = 0$. Then we have $X^3 = 0$, which gives us $[0, y, 0] \sim [0, 1, 0] \in \mathbb{P}^2$. So in the projective plane, we have :

$$Y^2 Z = X^3 - XZ^2 \subseteq \mathbb{P}^2 \cong (y^2 = x^3 - x \subseteq \mathbb{A}^2) \cup ([0, 1, 0] \subseteq \mathbb{P}^1) \subseteq \mathbb{A}^2 \cup \mathbb{P}^1 \cong \mathbb{P}^2.$$

When we transfered our curve from the affine plane to the projective plane through the process of homogenization, we added a point at infinity. The maps ψ_z and ϕ_z enabled us to find this point at infinity. We have now written our curve as a union of two parts corresponding to the first construction of the projective plane:

$$C \subseteq \mathbb{P}^2 \cong (C \cap \mathbb{A}^2) \cup (C \cap \mathbb{P}^1) \subseteq \mathbb{A}^2 \cup \mathbb{P}^1.$$

Proposition 3. *An elliptic curve has only one point at infinity.*

Proof. Begin by considering the normalized Weierstrass equation for an elliptic curve.

$$y^2 = x^3 + Ax + B \in \mathbb{A}^2.$$

Homogenize it by multiplying each term by the appropriate power of Z.

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \in \mathbb{P}^2.$$

The "points at infinity" will be the points where $Z = 0$. So, setting $Z = 0$, we have $X^3 = 0$. This gives us all triples of points $[0, y, 0] \cong [0, 1, 0] \in \mathbb{P}^2$, a single point.

What if we considered points where $X = 0$? Then we would have the curve $Y^2Z = BZ^3$. If $Y = 0$, then $Z = 0$ and we would have the point $[0, 0, 0] \notin \mathbb{P}^2$. So $Y \neq 0$. If $Z = 0$, then Y is free, and we have all triples of points $[0, y, 0] \sim [0, 1, 0] \in \mathbb{P}^2$, a single point. □

Considering Bezout's theorem with a line and a curve, every line will intersect an elliptic curve in three points. What if the line is vertical? Then it will intersect the elliptic curve in one or two points that are visible in the part of the curve lying in the affine plane. The third point of intersection is the "point at infinity" on the projective line, which lies infinitely far out on all vertical lines.

4 The Group Law on an Elliptic Curve

Perhaps one of the most interesting facts about elliptic curves is that the points on an elliptic curve form a group. This is not obvious, and requires proof. There are explicit formulas for adding points on an elliptic curve, that can be shown to satisfy the group axioms. However, we do not give them here; they can be found in (**?**, Ch.1) or (**?**, Ch.2). Instead, we will just present the basic idea.

From Bezout's theorem, we know that an elliptic curve and a line must intersect in $\deg(curve) \cdot \deg(line) = 3 \cdot 1 = 3$ points. There is a slight technicality here; if a line is tangent to a curve at a point, we say that the line intersects the curve twice (or three times) at that point. Figure 4 shows how to add points on an elliptic curve. To add points:
1. Start with two points on an elliptic curve, P and Q.
2. Draw the line between the points P and Q. It will intersect the curve in one more point, call it $P * Q$.

3. Now take the line through $P * Q$ and the identity point on the elliptic curve. This will intersect the curve in one more point, $P + Q$.
Since we count points with multiplicity, we may end up with a situation in which $P * Q = P$. In this case, proceed as outlined.

What if we want to add $P + P$? To start take the line tangent to the curve at P. This will intersect the curve in one more place, call it $P*P$. Take the line through $P*P$ and the identity to get $P+P$. Note that $P + P = -P$ and $P + P + P = O$, where O is the identity. If the identity is the point at infinity in a normalized curve, then the curve is symmetric about the x-axis, and the last step is a reflection across the x-axis. However, we could choose any point on the curve to be the identity, and it would satisfy the group law. The "point at infinity" is often chosen to be the identity. Since we are working in a group, there can only be one identity point.

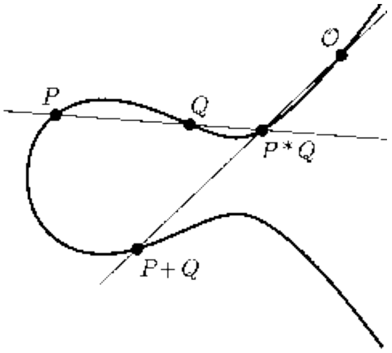


Figure 4: The Group Law.

There is another useful theorem due to Mordell:

Theorem 4. *Let E be an elliptic curve. The the group of rational points on the curve, $E(\mathbb{Q})$, is a finitely generated abelian group.*

A rational point is a point where both coordinates are rational. An abelian group, G, is called finitely generated if there are finitely many elements $x_1, x_2, ..., x_r \in G$, such that every element of G can be written $g = n_1x_1 + n_2x_2 + \cdots + n_rx_r$, where $n_i \in \mathbb{Z}$. In other words, there is some finite list of elements in G, such that every element in G can be written as an integer linear combination of these elements. Actually this gives us some important information about the structure of the group. The Fundamental Theorem of Finitely Generated Abelian Groups as stated in **?** is the following:

Theorem 5. *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}/({p_1}^{k_1}\mathbb{Z}) \times \mathbb{Z}/({p_2}^{k_2}\mathbb{Z}) \times \cdots \times \mathbb{Z}/({p_n}^{k_n}\mathbb{Z}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

where the p_i are primes, not necessarily distinct, and the k_i are positive integers. The direct product is unique except for a possible rearrangement of the factors, that is, the number of factors (called the Betti number of G) of $\mathbb{Z}$ is unique and the prime powers ${p_i}^{k_i}$ are unique. The Betti number, or number of factors, r, is more commonly called the rank of an elliptic curve.

For example, the curve $y^2 = x^3 - x$ has rank 0. As is shown in **?** the group of rational points on this curve is:

$$E(\mathbb{Q}) = \{O, (0,0), (1,0), (-1,0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

5 An Elliptic Curve is a Torus

The group law on an elliptic curve is the same as the group law on a torus generated by a lattice. The proof is long and detailed, and can be found in (**?**, Ch.9). We give the basic details here. A lattice is an additive subgroup of $\mathbb{C}$ of the form $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}, \text{ and } \omega_1, \omega_2 \in \mathbb{C}\}$. We are interested in lattices because $\mathbb{C}/L$ is a torus. To see this, imagine a lattice on the complex plane, i.e., $(w_1, w_2 \in \mathbb{C})$. Just looking at one "fundamental parallelogram" gives us a picture of everything in $\mathbb{C}/L$. Now, since we are looking at $\mathbb{C}/L$, we can imagine gluing the bottom and top of the parallelogram to form a tube, and then gluing the edges of the tube together to form a torus.

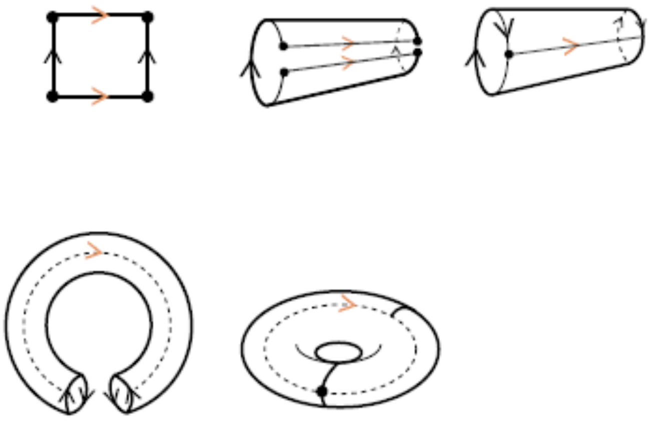


Figure 5: Constructing a Torus.

To show the correspondence between a lattice and an elliptic curve, we need to introduce a meromorphic function, called the Weierstrass $\wp$-function, $\wp(z)$. A meromorphic function is a function of the form $f(z) = \dfrac{g(z)}{h(z)}$, where g, h are entire functions with $h(z) \neq 0$. An entire function is a function that is differentiable everywhere in the domain. So a meromorphic function will only have finite-order, isolated poles and zeros, and no essential singularities in its domain. Here we have the Weierstrass function:

$$\wp(z) = \wp(z;L) = \frac{1}{z^2} + \sum_{\omega\in L, w\neq 0}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Since all the terms in the Weierstrass function are squared, $\wp(z) = \wp(-z)$.

Proposition 6. *(1) $\wp(z)$ is meromorphic on $\mathbb{C}$, (2) is doubly periodic, (3) and every doubly periodic function for L is a rational function of $\wp$ and its derivative, $\wp'$.*

In other words, every doubly periodic function on L, can be written as a ratio of polynomials of $\wp$ and $\wp'$.

Proof. To prove (1), note that a limit of analytic functions is analytic, so $\wp(z)$ is analytic for $z \notin L$. If $z \in L$, then the sum of the terms for $\omega \neq z$ is analytic near z, and the term $\dfrac{1}{(z-\omega)^2}$ causes $\wp$ to have a double pole at z.
To prove (2), we want to show that $\wp(z+\omega) = \wp(z)$, for all $\omega \in L$. Begin by differentiating $\wp(z)$ term by term to get :

$$\wp'(z) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3}.$$

Notice $\omega = 0$ is included in the sum. The sum converges absolutely when $z \notin L$, and changing z to $z+\omega$ shifts the terms in the sum. So, $\wp'(z+\omega) = \wp'(z)$. Thus, there is some constant, c_ω such that $\wp(z+\omega) - \wp(z) = c_\omega$, for all $z \notin L$. Put $z = \frac{\omega}{2}$, and $c_\omega = \wp(-\omega/2) - \wp(\omega/2) = 0$, since $\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$.

As a result of the function being doubly periodic, it assumes exactly the same values on corresponding points on the opposite side of the "fundamental parallelogram." So the Weierstrass $\wp$ function is still well defined even when the opposing sides of the parallelogram are identified. However, when we make this identification, and glue the corresponding edges, we have a torus. So the torus is the natural domain of the Weierstrass $\wp$ function, or any doubly periodic complex function, and $\wp(Z)$ is well defined on $\mathbb{C}/L$.

The proof of (3) can be found in **?**. □

After proving a few more theorems and lemmas, one can show the following.

Theorem 7. *The following map is an isomorphism of groups.*

$$\begin{aligned} \phi : \mathbb{C}/L &\to E(\mathbb{C}) \\ z &\mapsto [\wp(z), \wp\prime(z), 1] \\ 0 &\mapsto [0, 1, 0] \end{aligned}$$

where [0,1,0] is the point at infinity on the elliptic curve.

$E(\mathbb{C})$ is the group of complex points of the elliptic curve. Every lattice generates an elliptic curve.

Now we need to work the other way, and show that every elliptic curve generates a lattice. Let $y^2 = 4x^3 - Ax - B$ be an elliptic curve over $\mathbb{C}$. We want to use this curve to find generators A, B corresponding to this curve that generate the lattice L. Define the Eisenstein series for $k \geq 3$:

$$G_k(L) = \sum_{\omega \in L, \omega \neq 0} \omega^{-k}.$$

This sum can be shown to converge, see (**?**, p.263). It is also shown in **?** that

$$\wp'(z) = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Setting $g_2 = 60G_4$ and $g_3 = 140G_6$ gives

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

So the points $(\wp(z), \wp'(z))$ lie on the curve

$$y^2 = 4x^3 - g_2x - g_3.$$

So we have our lattice generators $A = g_2(L)$ and $B = g_3(L)$.

The last thing left to do is to figure out how to generate a lattice, given an elliptic curve.

Definition 7. *To compute the arithmetic-geometric mean, denoted $M(a, b)$, the following algorithm is used.*

$$\begin{aligned} a_0 &= a, b_0 = b \\ a_n &= \frac{1}{2}(a_{n-1} + b_{n-1}) \\ b_n &= \sqrt{a_{n-1}b_{n-1}} \end{aligned}$$

It is shown in **?** *that* $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ *which we call* $M(a, b)$.

For a curve with three real roots, e_1, e_2, e_3, we can generate our lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ by

$$\omega_1 = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \text{ and } \omega_2 = \frac{\pi i}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})}.$$

Using GP PARI, it is easy to compute examples. The curve $y^2 = x^3 - x$ has three real roots, and has a lattice generated by $\omega_1 = 2.62205...$ and $\omega_2 = i\omega_1$.

Lattices may be defined similarly for curves with only one real root. Let $e' = \sqrt{3{e_1}^2 - \frac{1}{4}g_2}$. Then:

$$\omega_1 = \frac{2\pi}{M(\sqrt{4e'}, \sqrt{2e' + 3e_1})}\ , \omega_2 = \frac{-\omega_1}{2} + \frac{\pi i}{M(\sqrt{4e'}, \sqrt{2e' - 3e_1})}.$$

For example, the curve $y^2 = x^3 + 1$ has only one real root, and a lattice generated by $\omega_1 = 4.2065...$ and $\omega_2 = -2.1032... + i(1.21432...)$.

The important point is that if a curve has three real roots, then our parallelogram is a rectangle. If we have only one real root, we can still normalize one of the lattice generators to be real, but the other will be complex, giving us a parallelogram.

6 Mapping the Real Part of an Elliptic Curve to a Torus

Our main theorem shows what happens to the real part of the elliptic curve when we perform the group isomorphism between $E(\mathbb{C})$ and $\mathbb{C}/L$, by mapping the points of the elliptic curve to points on the torus.

Theorem 8. *The real part of an elliptic curve is either a (0,1) or a (0,2) torus link.*

First let's give some background on torus links, which may be found in **?**. We'll start with torus knots, which are links with a single component or closed curve. A torus knot is a knot that lies on the surface of a torus. We denote it by (p, q), where p, q are relatively prime. The integer p is the number of times the thread is looped through the hole of the torus, and q is the number of revolutions the string makes around the torus before the ends are joined. For example the well known trefoil knot is a $(3, 2)$ torus knot, because it loops 3 times around the hole of the torus, and travels twice around before the ends are joined. Note that (p, q) and (q, p) knots are equivalent, since the "hole" of a torus is not well defined. That is, we have two different ways to glue the "fundamental parallelogram" into a torus when we start with the planar diagram. In terms of the parallelogram, p and q count the number of crossings on the two edges. For a torus link, p and q need not be relatively prime. A torus link will have $\gcd(p, q)$ components, or closed curves. When $(p, q) = 1$, there is a single component and the link is a knot. Our Theorem says that the real points on an elliptic curve will either be mapped to the unknot, (which is a loop around the torus once), or to two parallel unknotted loops.

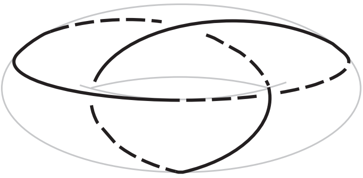


Figure 6: A (3,2) trefoil.

The next step to prove the theorem is to determine how the real points of an elliptic curve are mapped from our normalized elliptic curve to a lattice. The real points of an elliptic curve are the points that we see when we look at the graph of an elliptic curve in the plane. We define an elliptic curve over the complex numbers, but we would need to be able to visualize 4 dimensional space to see how this actually works. Recall that we can normalize an elliptic curve to the form $y^2 = x^3 + Ax + B$. To determine where the real points get mapped to, we wrote several programs in GP PARI to generate and test random elliptic curves. The programs are given in the appendix. We found that there are two cases. This following may be found in (**?**, Ch.9).

Proposition 9. *Let E be an elliptic curve. If E has three real roots (two components), then the real points of the elliptic curve get mapped to the line $y = 0$, the bottom of the parallelogram, and also to a line midway up the parallelogram, parallel to the base, $y = (1/2)\mathrm{Im}(\omega_2)$. This forms a (0,2) torus link. If the curve has only one component (one real root) the real points get mapped to the bottom of the parallelogram. This is the (0,1) torus knot.*

Here we are using the notation $y = \mathrm{Im}(\omega_2)$ to denote a line midway up the parallelogram and parallel to the bottom. Recall that when there are three real roots, ω_2 is purely imaginary. So we have a horizontal line intersecting the y-axis at ω_2. Figure 7 illustrates the two possibilities for the fundamental parallelogram, with the real points drawn in bold.

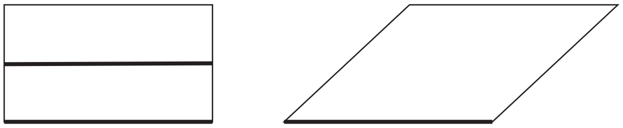


Figure 7: The two "fundamental parallelograms".

Proof. First we will do the rectangular case, when E has three real roots. We have $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\omega_1 \in \mathbb{R}$ and $\omega_2 \in i\mathbb{R}$. Then we have $(\wp(z), \wp\prime(z)) \in E(\mathbb{R})$, when $z = t\omega_2$ with $0 \leq t < 1$, and also when $z = (1/2)\omega_1 + t\omega_2$, with $0 \leq t < 1$. Where does this come from? If z is real and the lattice, L, is preserved under complex conjugation, then conjugating the defining expression for $\wp(z)$ leaves it unchanged, so $\wp$ maps reals to reals. To see the second part, conjugate $z = (1/2)\omega_1 + t\omega_2$ to get $z = -(1/2)\omega_1 + t\omega_2$, which is equivalent to z modulo L. The defining expression for $\wp(z)$ is again unchanged, so $\wp$ maps reals to reals. In particular, the real points will be mapped either to a line on the bottom of the parallelogram, or to a line on the bottom of the parallelogram and another line half way up and parallel to the bottom of the parallelogram.

To see the torus knots, simply fold the fundamental parallelogram into a torus. □

This proof answers our question for a standard choice of our lattice generators ω_1, ω_2, corresponding to a normalized curve. Now the question is what would happen if our lattice generators were not normalized? To examine this, we look at an operation called homothety. Two lattices, L, L' are said to be homothetic if $L = \lambda L'$, where $\lambda \in \mathbb{C}$. Points on our lattice get mapped:

$$\lambda : z \mapsto \lambda z, \text{ where } (x, y) = x + iy = z.$$

Now let's consider points on a line. If lines cannot be made to wrap more times around the torus under homothety, then the lattice we start with does not matter, because we'll get the same curve on the torus.

Lemma 10. *The number of times that a line intersects the parallelogram does not change under homothety. In other words, the torus link formed by the real part of the elliptic curve does not change under homothety.*

Proof. Let's start with some points on the line $y = mx + b$, and then apply homothety. Set $\lambda = (s + it)$. Then we have:
$\lambda(x + i(mx + b)) = (s + it)(x + i(mx + b)) = (x(s - tm) + b) + i(x(sm + t) + b) = u + iv.$
We want to write v as $v = nu + c$, with $n, c \in \mathbb{R}$. Then we will have shown that lines get mapped to lines under homothety. Take $n = \dfrac{sm + t}{s - tm}$, and $c = (1 - n)b$. Then we will have $v = nu + c$.

To see that the number of times the line wraps around does not change, consider a line that passes through the points $a\omega_1 + 0\omega_2$ and $b\omega_1 + \omega_2$, with $a, b \in \mathbb{R} \cap [0, 1]$, where we have picked our points to be on the bottom and top of the fundamental parallelogram respectively. Then $a\omega_1 + 0$ represents a point on the bottom of the parallelogram that is some fraction of the distance between 0 and ω_1. Under homothety, we would map to $\lambda(a\omega_1 + 0\omega_2) = a\lambda\omega_1 + 0$ and $\lambda(b\omega_1 + \omega_2) = b\lambda\omega_1 + \lambda\omega_2$. So the end points of our line stay the same proportion of the distance along the top and bottom of the parallelogram, leaving the number of times our line wraps around the torus unchanged. □

Here is an alternate version of the first part of the proof, that lines get mapped to lines. Homothety can also be thought of as a linear map in $\mathbb{R}^2$.

Proof. Let $\lambda = s + it, z = x + iy$. Then $\lambda z = sx - ty + i(tx + sy)$. So we have the map:

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \lambda \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} s & -t \\ t & s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

□

Note that we do not even need this much to figure out what happens to our curves under homothety. The lines that we have are the ones on the bottom of the parallelogram and half way up. It is clear that homothety maps points on the perimeter of the parallelogram to points on the perimeter of the parallelogram, so the line on the bottom of the parallelogram will get mapped to a line on the bottom of the parallelogram. In the case with three real roots, (recall that this condition generates a rectangular lattice with ω_2 purely imaginary), we will also have a line half way up, $y = \frac{1}{2}\text{Im}(\omega_2)$. Under homethety this line gets mapped to $y = \lambda\omega_1 x + \lambda\frac{1}{2}w_2$, a line half way up and parallel to the bottom of the parallelogram.

7 Complex Multiplication

We also studied elliptic curves with complex multiplication. An endomorphism is a homomorphism of a group, G, to itself. The endomorphisms of a group can be shown to form a ring under composition of homomorphisms, see **?**.

Definition 8. *An elliptic curve is said to have complex multiplication if its endomorphism ring is strictly larger than $\mathbb{Z}$.*

On an elliptic curve, we can always construct an endomorphism by "multiplying" the points on the curve by some $n \in \mathbb{Z}$, i.e., adding a point to itself n times. If $n < 0$, we add the inverse of a point n times. So, $\mathbb{Z} \subseteq \text{End}(E)$. If a curve has complex multiplication, then it has other endomorphisms besides multiplication by the integers. The proof of the next theorem is essentially from (**?**, Ch.10).

Lemma 11. *Let G be a group. If $\phi : G \to G$ is an isomorphism and $\psi : G \to G$ is a homomorphism, then $\phi^{-1} \circ \psi \circ \phi$ is a homomorphism.*

Proof. We want to show that for $a, b \in G$, $(\phi^{-1} \circ \psi \circ \phi)(a \cdot b) = (\phi^{-1} \circ \psi \circ \phi)(a) \cdot (\phi^{-1} \circ \psi \circ \phi)(b)$. Since ϕ is an isomorphism and ψ is a homomorphism:

$$\begin{aligned} (\phi^{-1} \circ \psi \circ \phi)(a \cdot b) &= (\phi^{-1}(\psi(\phi(a \cdot b)))) \\ &= (\phi^{-1}(\psi(\phi(a) \cdot \phi(b))) \\ &= (\phi^{-1}(\psi(\phi(a)) \cdot \psi(\phi(b))) \\ &= (\phi^{-1}(\psi(\phi(a))) \cdot \phi^{-1}(\psi(\phi(b))). \end{aligned}$$

So $\phi^{-1} \circ \psi \circ \phi$ is a homomorphism. □

Theorem 12. *Let E be an elliptic curve over $\mathbb{C}$ corresponding to the lattice L. Then:*

$$\text{End}(E) \cong \{\beta \in \mathbb{C} | \beta L \subseteq L\}.$$

Proof. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the lattice corresponding to E. Let α be an endomorphism of E. Then α is a homomorphism from $E(\mathbb{C})$ to $E(\mathbb{C})$, and α is given by rational functions (see **?**):

$$\alpha(x, y) = (R(x), S(y))$$

for rational functions R, S. Recall the isomorphism ϕ from our map between an elliptic curve and a torus. Then the map

$$\tilde{\alpha}(z) = \phi^{-1}(\alpha(\phi(z)))$$

is a homomorphism from $\mathbb{C}/L$ to $\mathbb{C}/L$. If we consider only a sufficiently small neighborhood U of $z = 0$, we have an analytic map from U to $\mathbb{C}$ (since by taking a small enough neighborhood we can avoid any poles from our homomorphism of rational functions), with

$$\tilde{\alpha}(z_1 + z_2) \equiv \tilde{\alpha}(z_1) + \tilde{\alpha}(z_2) \pmod{L}$$

for all $z_1 z_2 \in U$. By subtracting the appropriate element of L, we may assume $\tilde{\alpha}(0) = 0$. Since

$$\begin{aligned}\tilde{\alpha}(z_1 + z_2) \equiv \tilde{\alpha}(z_1) + \tilde{\alpha}(z_2) \pmod{L} &\Rightarrow \tilde{\alpha}(z_1) = \tilde{\alpha}(z_2) - \omega \\ &\Rightarrow \omega = \tilde{\alpha}(0) \equiv 0 \pmod{L}.\end{aligned}$$

By continuity, $\tilde{\alpha}(z)$ is near zero whenever z is near zero. If U is small enough, we can assume that

$$\tilde{\alpha}(z_1 + z_2) = \tilde{\alpha}(z_1) + \tilde{\alpha}(z_2)$$

for all $z_1, z_2 \in U$. Both sides are near zero, so they may differ only by $0 \in L$. So, for $z \in U$, we have

$$\begin{aligned}\tilde{\alpha}'(z) &= \lim_{h\to 0} \frac{\tilde{\alpha}(z+h) - \tilde{\alpha}(z)}{h} \\ &= \lim_{h\to 0} \frac{\tilde{\alpha}(z) + \tilde{\alpha}(h) - \tilde{\alpha}(z)}{h} \\ &= \lim_{h\to 0} \frac{\tilde{\alpha}(h) - \tilde{\alpha}(0)}{h} = \tilde{\alpha}'(0).\end{aligned}$$

Let $\beta = \tilde{\alpha}'(0)$. Since $\tilde{\alpha}'(z) = \beta$ for all $z \in U$, we must have that $\tilde{\alpha}(z) = \beta z$ for all $z \in U$. Now take an arbitrary $z \in \mathbb{Z}$. Then there exists some $n \in \mathbb{Z}$ with $z/n \in U$. Thus,

$$\tilde{\alpha}(z) \equiv n\tilde{\alpha}(z/n) = n(\beta z/n) = \beta z \pmod{L},$$

so our endomorphism $\tilde{\alpha}$ is given by multiplication by β. Since $\tilde{\alpha}(L) \subseteq L$, we have also that $\beta L \subseteq L$.

Thus far, we have shown that endomorphisms are given by numbers β. Now we will show that all β's give endomorphisms. Take $\beta \in \mathbb{C}$ satisfying $\beta L \subseteq L$. We have the homomorphism:

$$\beta : \mathbb{C}/L \to \mathbb{C}/L.$$

We want to show that the corresponding map on E is given by rational functions in x, y. The functions $\wp(\beta z)$ and $\wp'(\beta z)$ are doubly periodic with respect to L, since $\beta L \subseteq L$. By proposition **??**, there are rational functions, R, S such that

$$\wp(\beta z) = R(\wp(z)) \text{ and } \wp'(\beta z) = \wp'(z)S(\wp(z)).$$

So multiplication by β on $\mathbb{C}/L$ corresponds to the map

$$(x, y) \mapsto (R(x), yS(x))$$

on E. This is what it means for β to be an endomorphism on E. □

Now let's compute an example of a curve that does have complex multiplication. That is, we want to find an endomorphism of the group of points on a curve that is not multiplication by some element of $\mathbb{Z}$. For example, we can argue that the curve $y^2 = 4x^3 - 4x$, has complex multiplication. This curve is generated by the lattice $\omega_1 = 2.622057...$ and $\omega_2 = i\omega_1$. This is a square lattice, so rotation by $\frac{\pi}{2}$ sends L back to itself. In other words, $iL = L$. By putting this into our expression for the Weierstrass -$\wp$ function, we have:

$$\begin{aligned}\wp(iz) &= \frac{1}{(iz)^2} + \sum_{\omega\neq 0} \left(\frac{1}{(iz-\omega)^2} - \frac{1}{\omega^2} \right) \\ &= \frac{1}{(iz)^2} + \sum_{i\omega\neq 0} \left(\frac{1}{(iz-i\omega)^2} - \frac{1}{i\omega^2} \right) \\ &= -\wp(z).\end{aligned}$$

Differentiating, $\wp'(iz) = i\wp'(z)$. So we have the endomorphism given by:

$$i(x, y) = (-x, iy).$$

To check that this is actually an endomorphism, take a point (x, y) on our curve. Substitute as prescribed by the homomorphism:

$$-iy^3 = (iy)^3 = 4(-x)^2 - 4(-x) = 4x^2 + 4x = i(4(ix)^2 - 4(ix)).$$

So our map sends points on the curve to points on the curve, since we have mapped to a reflection across the x-axis. If a curve has complex multiplication, and its endomorphism ring is larger than $\mathbb{Z}$, then what could the endomorphism ring be?

Definition 9. *Let $K = \mathbb{Q}(\sqrt{-d}) = \{a + b\sqrt{-d}|a, b \in \mathbb{Q}\}$. Then K is an imaginary quadratic field.*

The following is shown in (**?**, Ch.10).

Theorem 13. *Let K be an imaginary quadratic field. Let $\tau \in \mathbb{C}$. Then an elliptic curve $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ has complex multiplication by some subring in K if and only if $\tau \in K$.*

In other words, the endomorphism ring of an elliptic curve is either $\mathbb{Z}$ or a subring in an imaginary quadratic field. Another question we wanted to answer was whether curves that have complex multiplication correspond to $(0, 1)$ or $(0, 2)$ torus links. Earlier in this section, we saw a curve with complex multiplication that had three real roots, and thus gives a $(0, 1)$ torus link. It turns out that the curve $y^2 = x^3 + 1$ has complex multiplication by $(x, y) \mapsto (\frac{-1+\sqrt{-3}}{2}x, -y)$. As we also saw before, this curve has only one real root, and corresponds to a $(0, 2)$ torus link. So, curves with complex multiplication can have either type of real link.

References

C.C. Adams, *The Knot Book.* American Mathematical Society, 2004.

J.B. Fraleigh. *A First Course in Abstract Algebra.* 7th edition. Pearson Education, Inc. New York, NY, 2003.

J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

L. Washington. *Elliptic Curves: Number Theory and Cryptography.* 2nd edition. Chapman and Hall, Boca Raton, Florida, 2008.

8 Appendix: GP PARI Code

Here is the GP PARI code I wrote to map points on an elliptic curve to points on a torus. The first program allows the user to choose an elliptic curve to map. It prints the output in the PARI window as the coordinates of the points on the torus.

```
{print("please enter the vector of coefficients for an elliptic curve in Weierstrass normal form");
L=input();
print("please input the length of the interval you would like to map");
Int=input();
print("please input the distance between the points you would like to use for mapping");
step=input();
E=ellinit(L);
W=E[15];
if(imag(E[14][3])!=0,
         forstep(x=E[14][1],Int,step,y=ellordinate(E,x)[1];
                                     w=[x,y];          /*MAP WITH ONE ROOT*/
                                     z=ellpointtoz(E,w);
                                     a=real(z);
                                     if(imag(z)==W,b=0,
                                                 if(floor(imag(z)*10^10)/10^10==0,
                                                        b=0, b=imag(z))
                                                        );
                                     print([a,b])
                                     );
                         ,
         first=min(E[14][1],min(E[14][2],E[14][3]));    /*ORDERING ROOTS */
         third=max(E[14][1],max(E[14][2],E[14][3]));
         if((E[14][1]!=first)*(E[14][1]!=third),second=E[14][1],
                 if((E[14][2]!=first)*(E[14][2]!=third),
                           second=E[14][2],second=E[14][3]));
         forstep(x=first,second,step,y=ellordinate(E,x)[1]; w=[x,y];
                                z=ellpointtoz(E,w);       /*MAPPING FIRST PART*/
                                a=real(z);
                                b=imag(z);
                                print([a,b])
                                );
          forstep(x=third,third+Int,step,y=ellordinate(E,x)[1];
                                w=[x,y];          /*MAP SECOND COMPONENT*/
                                z=ellpointtoz(E,w);
                                a=real(z);
                                if(imag(z)==W,b=0,
                                                if(floor(imag(z)*10^10)/10^10==0,
                                                             b=0, b=imag(z))
                                                             );
                                 print([a,b])
                                 );
);
print("w/2 is ", W/2);
}
```

The second program generates m random elliptic curves, with random coefficients chosen from $[0, n] \cap \mathbb{Z}$. It writes the output to two files. The "curvepoints" file gives the point on the torus that each point on the elliptic curve was mapped to. The "curvesfancy" file gives the equation of the lines on the torus that the points got mapped to. Both files also offer additional information about each randomly generated curve.

```
{
print("please input a bound on the range you would like to choose coefficients from");
n=input();
print("please input the number of curves you would like to create");
m=input();
print("please input the step size you would like to use for mapping");
step=input();
for(i=1,m,
         if(Mod(random(n),2)==1,A=1,A=-1);  /*GENERATE A RANDOM CURVE*/
         a=random(n)*A;
         if(Mod(random(n),2)==1,B=1,B=-1);
         b=random(n)*B;
         if(Mod(random(n),2)==1,C=1,C=-1);
         c=random(n)*C;
         if(Mod(random(n),2)==1,D=1,D=-1);
         d=random(n)*D;
         if(Mod(random(n),2)==1,F=1,F=-1);
         f=random(n)*F;
         L=[a,b,c,d,f];
         E=ellinit(L);
         W=E[16];
         write("curvepoints","");
         write("curvepoints","");
         write("curvepoints","Here is curve number "i" :",L);
         write("curvesfancy","");
         write("curvesfancy","");
         write("curvesfancy","Here is curve number "i" :",L);
         write("curvesfancy","The roots are:",E[14]);
         write("curvesfancy","The lattice is:",E[15],",",E[16]);
         if(real(E[16])==0,write("curvesfancy","W2 is purely imaginary"),
                          write("curvesfancy","W2 is complex"));
if(imag(E[14][3])!=0,write("curvepoints","This curve has only one real root");
write("curvesfancy","This curve has only one real root");
          forstep(x=E[14][1],E[14][1]+10,step,y=ellordinate(E,x)[1];
                  w=[x,y];
                  z=ellpointtoz(E,w);
                  j=real(z);                 /*MAP ONE ROOT */
                  if(imag(z)==W,k=0,
                            if(floor(imag(z)*10^10)/10^10==0, k=0,
                                     k=imag(z))      /*MAP ZERO POINTS TO ZERO */
                                     );
                   if(k==0,count=count+1);
                   ints=ints+1;
                   write("curvepoints",[j,k])
          );
          if(count==ints, write("curvesfancy", "Second componet, y=",0));
                  ,
         write("curvepoints","The roots are:",E[14]);
         write("curvepoints","The lattice is:",E[15],",",E[16]);
         first=min(E[14][1],min(E[14][2],E[14][3]));       /*ORDERING ROOTS */
         third=max(E[14][1],max(E[14][2],E[14][3]));
         if((E[14][1]!=first)*(E[14][1]!=third),second=E[14][1],
                   if((E[14][2]!=first)*(E[14][2]!=third),
                             second=E[14][2],second=E[14][3]));
         write("curvepoints","First Componet");
         count=0;  ints=0;
         forstep(x=first,second,step,y=ellordinate(E,x)[1];
         w=[x,y];z=ellpointtoz(E,w);
                   j=real(z);                /*MAP FIRST COMPONENT */
                   k=imag(z);
                   write("curvepoints",[j,k]);
                   ints=ints+1;
                   if(floor(k*10^10)/10^10==floor(imag(W/2)*10^10)/10^10,
                          count=count+1,);
         );
         if(count==ints,write("curvesfancy", "First Componet: y=", W/2));
         write("curvepoints","Second Componet");
         count=0; ints=0;
         forstep(x=third,third+10,step,y=ellordinate(E,x)[1];
                  w=[x,y];
                  z=ellpointtoz(E,w);
                  j=real(z);                 /*MAP SECOND COMPONENT */
                  if(imag(z)==W,k=0,
                            if(floor(imag(z)*10^10)/10^10==0, k=0,
                                     k=imag(z))      /*MAP ZERO POINTS TO ZERO */
                                     );
                   if(k==0,count=count+1);
                   ints=ints+1;
                   write("curvepoints",[j,k])
          );
          if(count==ints, write("curvesfancy", "Second componet, y=",0));
);
write("curvepoints","w/2 is ", W/2);
write("curvesfancy","w/2 is ", W/2);)
}
```