Algebraic Number Theory, a Computational Approach

William Stein

June 8, 2019

Chapter 1

Elliptic Curves, Galois Representations, and L-functions

This chapter is about elliptic curves and the central role they play in algebraic number theory. Our approach will be less systematic and more a survey than most of the rest of this book. The goal is to give you a glimpse of the forefront of research by assuming many basic facts that can be found in other books (see, e.g., [Sil92]).

1.1 Groups Attached to Elliptic Curves

Definition 1.1.1 (Elliptic Curve)**.** An *elliptic curve* over a field K is a genus one curve E defined over K equipped with a distinguished point $\mathcal{O} \in E(K)$. Here $E(K)$ is the set of all points on E defined over K.

We will not define *genus* in this book, except to note that a nonsingular curve over K has genus one if and only if over $\overline{K}$ it can be realized as a nonsingular plane cubic curve.[1] Moreover, one can show (using the Riemann-Roch formula) that over any field a genus one curve with a rational point can always be defined by a projective cubic equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

[1] For a detailed and technical explanation of genus see [Har77, Ch. II.8] or [LE06, Ch. 7.3]

In this form the distinguished point $\mathcal{O}$ is $(X : Y : Z) = (0 : 1 : 0)$. Note that $\mathcal{O}$ is the only point on the curve with $Z = 0$. So we can consider the rest of the curve in the affine coordinates by projecting onto the affine plane defined by $Z \neq 0$. This gives the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

Thus one often presents an elliptic curve by giving a *Weierstrass equation* (1.1), though there are significant computational advantages to other equations for curves (e.g., Edwards coordinates – see work of Bernstein and Lange in [BL07]).

Exercise 1.1.2. Look up the Riemann-Roch theorem in a book on algebraic curves (e.g. [Har77, LE06]).

1. Write it down in your own words.

2. Let E be an elliptic curve over a field K. Use the Riemann-Roch theorem to deduce that the natural map

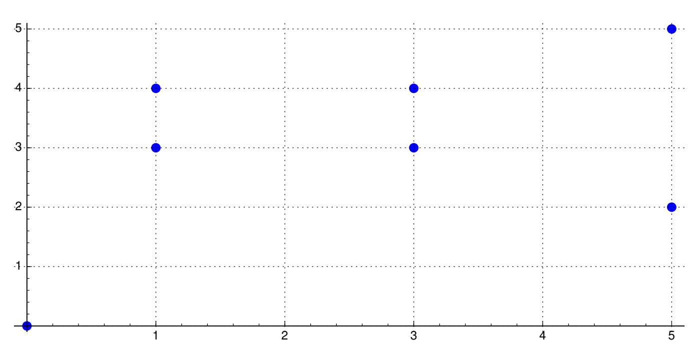
   $$E(K) \to \mathrm{Pic}^0(E/K)$$

   is an isomorphism.

Using Sage we plot an elliptic curve over the finite field $\mathbb{F}_7$ and an elliptic curve defined over $\mathbb{Q}$.

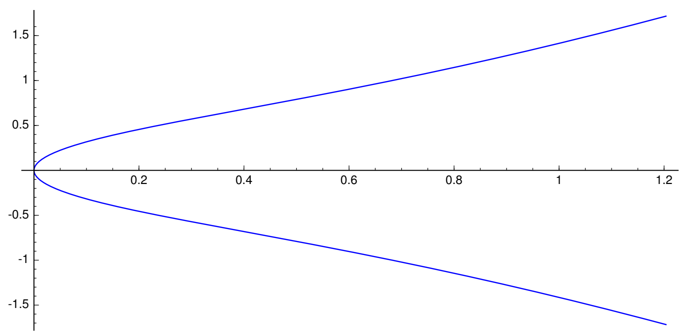
```
E = EllipticCurve(GF(7), [1,0])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x over
Finite Field of size 7
```



```
E = EllipticCurve([1,0])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x over
Rational Field
```



Note that both plots above are of the affine equation $y^2 = x^3 + x$, and do not include the distinguished point $\mathcal{O}$, which lies at infinity.

Remark 1.1.3. The command `EllipticCurve` in `Sage` can take as input a list `[a4,a6]` of coefficients and returns an elliptic curve given by a Weirstrass equation with $a_1 = a_2 = a_3 = 0$ and a_4, a_6 as specified.

1.1.1 Abelian Groups Attached to Elliptic Curves

If E is an elliptic curve over K, then we give the set $E(K)$ of all K-rational points on E the structure of abelian group with identity element $\mathcal{O}$.[2] If we embed E in the projective plane, then this group is determined by the condition that three points sum to the zero element $\mathcal{O}$ if and only if they lie on a common line (some care needs to be taken when the points are not distinct). In our affine picture, a line will intersect the point at infinity if it is vertical, or equivalently if it of the form $x = a$ for some fixed $a \in K$.

Example 1.1.4. On the curve $y^2 = x^3 - 5x + 4$, we have $(0, 2) + (1, 0) = (3, 4)$. This is because $(0, 2)$, $(1, 0)$, and $(3, -4)$ are on a common line (given by the equation $y = 2 - 2x$) hence they sum to zero:

$$(0, 2) + (1, 0) + (3, -4) = \mathcal{O}.$$

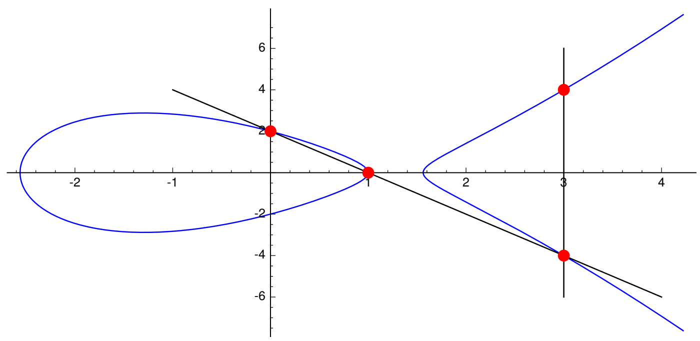
[2] As a reminder, we will not give rigorous proofs of any facts in this section. For a more detailed and technical explanation of the group structure for elliptic curves see [Sil92, Ch. III.2].

Notice $(3,4)$, $(3,-4)$, and $\mathcal{O}$ (the point at infinity on the curve) are also on a common line (given by $x=3$), so $(3,4) = -(3,-4)$. We can illustration this in `Sage`:

```
E = EllipticCurve([-5,4])
E(0,2) + E(1,0)
```

```
(3 : 4 : 1)
```

```
G += points ([(0,2) , (1,0) , (3,4) , (3,-4)],
pointsize=90 , color='red', zorder=10)
G += line ([(-1,4) , (4,-6)] , color='black')
G += line ([(3,-6) , (3,6)] , color='black')
G.show()
```



Iterating the group operation often leads quickly to very complicated points:

```
7*E(0,2)
```

```
(14100601873051200/48437552041038241 :
-170870044187066778452359 22/10660394576906522772066289 :
1)
```

Remark 1.1.5. In the previous example we saw that iterating the group operation led to points which used a lot of digits to write down. This notion can be made formal and is called the *height* of the point. The height function is used to prove the general Mordell-Weil theorem, see [Sil92, Ch. VIII.4]

Exercise 1.1.6. Let E be an elliptic curve given by a Weirstrass equation such as (1.1) with $a_1 = a_3 = 0$. Show that the points of order two are exactly the points on E with y-coordinate equal to 0.

[*Hint*: Recall that a point P has order 2 if $P + P + \mathcal{O} = \mathcal{O}$, which means the tangent line at P goes through the point at infinity.]

That the above condition—three points on a line sum to zero—defines an abelian group structure on $E(K)$ is not obvious. Depending on your perspective, the trickiest part is seeing that the operation satisfies the associative axiom. The best way to understand the group operation on $E(K)$ is to view $E(K)$ as being related to a class group. As a first observation, note that the ring

$$R = K[x, y]/(y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6))$$

is a Dedekind domain, so $\mathrm{Cl}(R)$ is defined, and every nonzero fractional ideal can be written uniquely in terms of prime ideals. When K is a perfect field, the prime ideals correspond to the Galois orbits of affine points of $E(\overline{K})$. Note that these do not include the point at infinity.

Let $\mathrm{Div}(E/K)$ be the free abelian group on the Galois orbits of points of $E(\overline{K})$, which as explained above is analogous to the group of fractional ideals of a number field (here we *do* include the point at infinity). We call the elements of $\mathrm{Div}(E/K)$ *divisors*. Let $\mathrm{Pic}(E/K)$ be the quotient of $\mathrm{Div}(E/K)$ by the *principal divisors*, i.e., the divisors associated to rational functions $f \in K(E)^*$ via

$$f \mapsto (f) = \sum_P \mathrm{Ord}_P(f)[P].$$

Here $K(E)$ is the fraction field of the ring R defined above. Note that the principal divisor associated to f is analogous to the principal fractional ideal associated to a nonzero element of a number field. The definition of $\mathrm{Ord}_P(f)$ is analogous to the "power of P that divides the principal ideal generated by f". Define the *class group* $\mathrm{Pic}(E/K)$ to be the quotient of the divisors by the principal divisors, so we have an exact sequence[3]:

reference text for this? Hartshorne abstract non-singular curves
or somewhere in Silverman Ch VIII? or an algebra text on valuations? or an exercise?

$$1 \to K(E)^*/K^* \to \mathrm{Div}(E/K) \to \mathrm{Pic}(E/K) \to 0.$$

A key difference between elliptic curves and algebraic number fields is that the principal divisors in the context of elliptic curves all have degree 0, i.e., the sum of the coefficients of the divisor (f) is always 0. This might be a familiar fact to you: the number of zeros of a nonzero rational function on a projective curve equals the number of poles, counted with multiplicity. If we let $\mathrm{Div}^0(E/K)$ denote the subgroup of divisors of degree 0, then we have an exact sequence

check grammar of footnote

$$1 \to K(E)^*/K^* \to \mathrm{Div}^0(E/K) \to \mathrm{Pic}^0(E/K) \to 0.$$

[3] The reason we use a 1 on the left of the sequence is that $K(E)^*/K^*$ is usually written in multiplicative notation and $\mathrm{Pic}(E/K)$ is written additively.

To connect this with the group law on $E(K)$, note that there is a natural map

$$E(K) \to \mathrm{Pic}^0(E/K), \qquad P \mapsto [P - \mathcal{O}].$$

Using the Riemann-Roch theorem, one can prove that this map is a bijection, which is moreover an isomorphism of abelian groups. Thus really when we discuss the group of K-rational points on an E, we are talking about the class group $\mathrm{Pic}^0(E/K)$.

Recall that we proved (Theorem **??**) that the class group $\mathrm{Cl}(\mathcal{O}_K)$ of a number field is finite. The group $\mathrm{Pic}^0(E/K) = E(K)$ of an elliptic curve can be either finite (e.g., for $y^2 + y = x^3 - x + 1$) or infinite (e.g., for $y^2 + y = x^3 - x$), and determining which is the case for any particular curve is one of the central unsolved problems in number theory.

The Mordell-Weil theorem (see Chapter **??**) asserts that if E is an elliptic curve over a number field K, then there is a nonnegative integer r, referred to as the *algebraic rank of* E, such that

$$E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus T, \tag{1.2}$$

where T is a finite group. This is similar to Dirichlet's unit theorem, which gives the structure of the unit group of the ring of integers of a number field. The main difference is that T need not be cyclic, and computing r appears to be much more difficult than just finding the number of real and complex roots of a polynomial!

Example 1.1.7. `Sage` has algorithms which can compute this rank for us. For example we can compute the ranks of the curves $y^2 + y = x^3 - x + 1$ and $y^2 + y = x^3 - x$ respectively.

```
EllipticCurve([0,0,1,-1,1]).rank()
```

```
0
```

```
EllipticCurve([0,0,1,-1,0]).rank()
```

```
1
```

Also, if L/K is an arbitrary extension of fields, and E is an elliptic curve over K, then there is a natural inclusion homomorphism $E(K) \hookrightarrow E(L)$. Thus instead of just obtaining one group attached to an elliptic curve, we obtain a whole collection, one for each extension of L. Even more generally, if S/K is an arbitrary scheme, then $E(S)$ is a group, and the association

$S \mapsto E(S)$ defines a functor from the category of schemes to the category of groups. Thus each elliptic curve gives rise to map:

$$\{\text{Schemes over } K\} \longrightarrow \{\text{Abelian Groups}\}$$

Remark 1.1.8. Elliptic curves are not the only objects that induce a functor from schemes to groups. *Abelian varieties* are a larger class of schemes, which includes elliptic curves, that also induce such a functor. For more on Abelian varieties see [Mil86].

1.1.2 A Formula for Adding Points

We close this section with an explicit formula for adding two points in $E(K)$. If E is an elliptic curve over a field K, given by an equation $y^2 = x^3 + ax + b$, then we can compute the group addition using the following algorithm.

Algorithm 1.1.9 (Elliptic Curve Group Law)**.** Given $P_1, P_2 \in E(K)$, this algorithm computes the sum $R = P_1 + P_2 \in E(K)$.

1. [One Point $\mathcal{O}$] If $P_1 = \mathcal{O}$ set $R = P_2$ or if $P_2 = \mathcal{O}$ set $R = P_1$ and terminate. Otherwise write $P_i = (x_i, y_i)$.

2. [Negatives] If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \mathcal{O}$ and terminate.

3. [Compute λ] Set $\lambda = \begin{cases} (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2, \\ (y_1 - y_2)/(x_1 - x_2) & \text{otherwise.} \end{cases}$
   Note: If $y_1 = 0$ and $P_1 = P_2$, output $\mathcal{O}$ and terminate.

4. [Compute Sum] Then $R = \left(\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu\right)$, where $\nu = y_1 - \lambda x_1$ and x_3 is the x coordinate of R.

1.1.3 Other Groups

There are other abelian groups attached to elliptic curves, such as the torsion subgroup $E(K)_{\mathrm{tor}}$ of elements of $E(K)$ of finite order. The torsion subgroup is (isomorphic to) the group T that appeared in Equation (1.2) above). When K is a number field, there is a group called the Shafarevich-Tate group $\text{Ш}(E/K)$ attached to E, which plays a role similar to that of the class group of a number field (though it is an open problem to prove that $\text{Ш}(E/K)$ is finite in general). The definition of $\text{Ш}(E/K)$ involves Galois cohomology, so we wait until Chapter **??** to define it. There are also component groups attached to E, one for each prime of $\mathcal{O}_K$. These groups all come together in the Birch and Swinnerton-Dyer conjecture (see `http://wstein.org/books/bsd/`).

1.2 Galois Representations Attached to Elliptic Curves

Let E be an elliptic curve over a number field K. In this section we attach representations of $G_K = \mathrm{Gal}(\overline{K}/K)$ to E, and use them to define an L-function $L(E, s)$. This L-function is yet another generalization of the Riemann Zeta function, that is different from the L-functions attached to complex representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$, which we encountered before in Section **??**.

There is a natural action of G_K on the points of $E(\overline{K})$. Given a point $P = (a, b) \in E(\overline{K})$ we define $\sigma(P)$ to be the point $(\sigma(a), \sigma(b))$. Since E is defined over K the point $\sigma(P)$ will again lie on E so the action is well defined. Note that the group structure on E is defined by algebraic formulas with coefficients in K. It follows that the action commutes with point addition meaning that $\sigma(P + Q) = \sigma(P) + \sigma(Q)$. Now fix an integer n. From what we have seen, the subgroup

$$E[n] = \{P \in E(\overline{K}) \colon nP = \mathcal{O}\}$$

is invariant under the action of G_K. We thus obtain a homomorphism

$$\overline{\rho}_{E,n} \colon G_K \to \mathrm{Aut}(E[n]).$$

Warning 1.2.1. Though the action of G_K leaves the group $E[n]$ fixed, it may act non-trivially on individual elements! Otherwise $\overline{\rho}_{E,n}$ would not be very interesting.

For any positive integer n, the group $E[n]$ is isomorphic as an abstract abelian group to $(\mathbb{Z}/n\mathbb{Z})^2$. There are various related ways to see why this is true. One is to use the Weierstrass $\wp$-theory to parametrize $E(\mathbb{C})$ by the complex numbers, i.e., to find an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where Λ is a lattice in $\mathbb{C}$ and the isomorphism is given by $z \mapsto (\wp(z), \wp'(z))$ with respect to an appropriate choice of coordinates on $E(\mathbb{C})$. It is then an easy exercise to verify that $(\mathbb{C}/\Lambda)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. For a detailed and rigorous walk through of this method see [DS05, Ch. 1.4].

Another way to understand $E[n]$ is to use the fact that $E(\mathbb{C})_{\mathrm{tor}}$ is isomorphic to the quotient

$$H_1(E(\mathbb{C}), \mathbb{Q})/H_1(E(\mathbb{C}), \mathbb{Z})$$

of homology groups and that the homology of a curve of genus g is isomorphic to $\mathbb{Z}^{2g}$. Then we have a non-canonical isomorphism

$$E[n] \approx (\mathbb{Q}/\mathbb{Z})^2[n] = (\mathbb{Z}/n\mathbb{Z})^2.$$

Technically the previous arguments have shown $E(\mathbb{C})[n] \approx (\mathbb{Z}/n\mathbb{Z})^2$. However, our definition of $E[n]$ used points in $E(\overline{K})$. So we need to show the points $E(\mathbb{C})[n]$ are actually defined over $\overline{K}$. Note that $E(\mathbb{C})[n]$ is finite and invariant under $\mathrm{Aut}(\mathbb{C}/\overline{K})$ for the same reason as $E[n]$ was invariant under $\mathrm{Gal}(\overline{K}/K)$ (point addition is defined by algebraic formulas with coefficients in K). It follows that $E(\mathbb{C})[n]$ is indeed defined over $E(\overline{K})$ so the arguments above show that $E[n] \approx (\mathbb{Z}/n\mathbb{Z})^2$.

Remark 1.2.2. Notice that the arguments above used many analytic facts about geometry over $\mathbb{C}$ (e.g. homology, analytic structure) in order to prove algebraic facts (e.g. the number of torsion points) about $E(\overline{K})$. This is part of a more general concept called the *Lefschetz principle* which generally relates geometry over an algebraically closed field of characteristic 0 to geometry over $\mathbb{C}$. For more on this see [Sil92, Ch. VI.6].

Remark 1.2.3. In fact, if p is a prime that does not divide n then $E[n] \approx (\mathbb{Z}/n\mathbb{Z})^2$ over fields of characteristic p. However, the methods we used above do not apply to the case of positive characteristic. Another method is to show the multiplication by n map is separable and has degree n^2. For a detailed proof see [Sil92, Cor. III.6.4].

Exercise 1.2.4. Let E be an elliptic curve defined over a number field K. Fix an integer n and consider the extension of K given by

$$K(E[n]) = K(\{a, b\colon (a, b) \in E[n]\}).$$

Show that $K(E[n])/K$ is a finite Galois extension.

Hint: By the arguments above $\#E[n] = n^2$ which shows the extension is finite. Next recall that $E[n]$ is left invariant by the action of $\mathrm{Gal}(\overline{K}/K)$. What can you say about the embeddings from $K(E[n])$ into $\overline{K}$ which leave K fixed?

Example 1.2.5. Consider the case when $n = 2$. From Exercise 1.1.6 we know that the points in $E[2]$ are exactly the points with y-coordinate 0. Let E be the elliptic curve given by $E : y^2 = x^3 + x + 1$. If $y = 0$ then x has to be a root of the polynomial $x^3 + x + 1$, so the points in $E[2]$ are defined over the splitting field of $x^3 + x + 1$. We can compute these points in `Sage`.

```
E = EllipticCurve([1,1]); E
```

```
Elliptic Curve defined by y^2 = x^3 + x + 1 over
Rational Field
```

```
R.<x> = QQ[]; R
```

```
Univariate Polynomial Ring in x over Rational Field
```

```
f = x^3 + x + 1
K.<a> = NumberField(f)
M.<b> = K.galois_closure(); M
```

```
Number Field in b with defining polynomial
x^6 + 6*x^4 + 9*x^2 + 31
```

```
F = E.change_ring(M)
T = F.torsion_subgroup(); T
```

```
Torsion Subgroup isomorphic to Z/2 + Z/2 associated
to the Elliptic Curve defined by y^2 = x^3 + x + 1
over Number Field in b with defining polynomial
x^6 + 6*x^4 + 9*x^2 + 31
```

```
T.gens()
```

```
((1/18*b^4 + 5/18*b^2 + 1/2*b + 2/9 : 0 : 1),
(1/18*b^4 + 5/18*b^2 - 1/2*b + 2/9 : 0 : 1))
```

Note that this matches with what we expected: we computed two generators for $E[2]$ (the output of the last cell) corresponding to two generators of $(\mathbb{Z}/2\mathbb{Z})^2$.

If $n = p$ is a prime, then upon chosing a basis for the two-dimensional $\mathbb{F}_p$-vector space $E[p]$, we obtain an isomorphism $\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. We thus obtain a mod p Galois representation

$$\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p).$$

This representation $\overline{\rho}_{E,p}$ is continuous if $\mathrm{GL}_2(\mathbb{F}_p)$ is endowed with the discrete topology, because the field $K(E[p])$ is a Galois extension of K of finite degree by Exercise 1.2.4.

In order to attach an L-function to E, one could try to embed $\mathrm{GL}_2(\mathbb{F}_p)$ into $\mathrm{GL}_2(\mathbb{C})$ and use the construction of Artin L-functions from Section **??**.

Unfortunately, this approach is doomed in general, since $\mathrm{GL}_2(\mathbb{F}_p)$ frequently does not embed in $\mathrm{GL}_2(\mathbb{C})$. The following Sage session shows that for $p = 5, 7$, there are no 2-dimensional irreducible representations of $\mathrm{GL}_2(\mathbb{F}_p)$, so $\mathrm{GL}_2(\mathbb{F}_p)$ does not embed in $\mathrm{GL}_2(\mathbb{C})$. The notation in the output below is `[degree of rep, number of times it occurs]`.

```
GL(2,GF(2)).gap().CharacterTable().CharacterDegrees()
```

```
[ [ 1, 2 ], [ 2, 1 ] ]
```

```
GL(2,GF(3)).gap().CharacterTable().CharacterDegrees()
```

```
[ [ 1, 2 ], [ 2, 3 ], [ 3, 2 ], [ 4, 1 ] ]
```

```
GL(2,GF(5)).gap().CharacterTable().CharacterDegrees()
```

```
[ [ 1, 4 ], [ 4, 10 ], [ 5, 4 ], [ 6, 6 ] ]
```

```
GL(2,GF(7)).gap().CharacterTable().CharacterDegrees()
```

```
[ [ 1, 6 ], [ 6, 21 ], [ 7, 6 ], [ 8, 15 ] ]
```

Instead of using the complex numbers, we use the *p-adic numbers* [4], as follows. For each power p^m of p, we have defined a homomorphism

$$\overline{\rho}_{E,p^m} : G_K \to \mathrm{Aut}(E[p^m]) \approx \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}).$$

We combine together all of these representations (for all $m \geq 1$) using the inverse limit. Recall that the p-adic numbers are

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^m\mathbb{Z},$$

which is the set of all compatible choices of integers modulo p^m for all m. We obtain a (continuous) homomorphism

$$\rho_{E,p} : G_K \to \mathrm{Aut}(\varprojlim E[p^m]) \cong \mathrm{GL}_2(\mathbb{Z}_p),$$

where $\mathbb{Z}_p$ is the ring of p-adic integers. The composition of this homomorphism with the reduction map $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$ is the representation $\overline{\rho}_{E,p}$, which we defined above, which is why we denoted it by $\overline{\rho}_{E,p}$.

[4] For a review of p-adic numbers and p-adic analysis see [Kob96].

Exercise 1.2.6. Let E be the elliptic curve $y^2 = x^3 + x + 1$. Let $E[2]$ be the group of points of order dividing 2 on E. Let

$$\overline{\rho}_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[2])$$

be the mod 2 Galois representation associated to E.

1. Find the fixed field K of $\ker(\overline{\rho}_{E,2})$.

2. Is $\overline{\rho}_{E,2}$ surjective?

3. Find the group $\mathrm{Gal}(K/\mathbb{Q})$.

4. Which primes are ramified in K?

5. Let I be an inertia group above 2, which is one of the ramified primes. Determine $E[2]^I$ explicitly for your choice of I. What is the characteristic polynomial of Frob_2 acting on $E[2]^I$.

6. What is the characteristic polynomial of Frob_3 acting on $E[2]$?

We next try to mimic the construction of $L(\rho, s)$ from Section **??** in the context of a p-adic Galois representation $\rho_{E,p}$.

Definition 1.2.7 (Tate module)**.** The *p-adic Tate module of E* is

$$T_p(E) = \varprojlim E[p^n].$$

Let M be the fixed field of $\ker(\rho_{E,p})$. The image of $\rho_{E,p}$ is infinite, so M is an infinite extension of K. Fortunately, one can prove that M is ramified at only finitely many primes (the primes of *bad reduction* for E and p—see [ST68]). If ℓ is a prime of K, let D_ℓ be a choice of decomposition group for some prime $\mathfrak{p}$ of M lying over ℓ, and let I_ℓ be the inertia group. We haven't defined inertia and decomposition groups for infinite Galois extensions, but the definitions are almost the same: choose a prime of $\mathcal{O}_M$ over ℓ, and let D_ℓ be the subgroup of $\mathrm{Gal}(M/K)$ that leaves $\mathfrak{p}$ invariant. Then the submodule $T_p(E)^{I_\ell}$ of inertia invariants is a module for D_ℓ and the characteristic polynomial $F_\ell(x)$ of Frob_ℓ on $T_p(E)^{I_\ell}$ is well defined (since inertia acts trivially). Let $R_\ell(x)$ be the polynomial obtained by reversing the coefficients of $F_\ell(x)$. One can prove that $R_\ell(x) \in \mathbb{Z}[x]$ and that $R_\ell(x)$, for $\ell \neq p$ does not depend on the choice of p. Define $R_\ell(x)$ for $\ell = p$ using a different prime $q \neq p$, so the definition of $R_\ell(x)$ does not depend on the choice of p.

Definition 1.2.8. The L-series of E is

$$L(E,s) = \prod_{\ell} \frac{1}{R_\ell(\ell^{-s})}.$$

A prime $\mathfrak{p}$ of $\mathcal{O}_K$ is a prime of *good reduction* for E if there is an equation for E such that $E \mod \mathfrak{p}$ is an elliptic curve over the field $\mathcal{O}_K/\mathfrak{p}$. If $K = \mathbb{Q}$ and ℓ is a prime of good reduction for E, then one can show that that $R_\ell(\ell^{-s}) = 1 - a_\ell \ell^{-s} + \ell^{1-2s}$, where $a_\ell = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$ and $\tilde{E}$ is the reduction of a local minimal model for E modulo ℓ. (There is a similar statement for $K \neq \mathbb{Q}$.)

One can prove using fairly general techniques that the product expression for $L(E,s)$ defines a holomorphic function in some right half plane of $\mathbb{C}$, i.e., the product converges for all s with $\Re(s) > \alpha$, for some real number α.

Recall that the Artin L-function from Section **??** (see Equation **??**) extended to meromorphic function on the entire complex plane and Artin conjectured that the L-function of any continuous representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ also extends to a meromorphic function on $\mathbb{C}$. We could ask the same question for the L-functions attached to elliptic curves. However, we will instead ask for something stronger:

Does the L-function $L(E,s)$ attached to an elliptic curve E extends to a holomorphic function on $\mathbb{C}$?

This question was one of the central topics in number theory in the late 1990s and early 2000s. An amazing fact is that the question has been answered in the affirmative.

Theorem 1.2.9. *The function $L(E,s)$ extends to a holomorphic function on all $\mathbb{C}$.*

This is a corollary to the modularity theorem described in the next section, see Corollary 1.2.11.

1.2.1 Modularity of Elliptic Curves over $\mathbb{Q}$

Fix an elliptic curve E over $\mathbb{Q}$. In this section we will explain what it means for E to be modular, and note the connection with Conjecture 1.2.9 from the previous section.

First, we give the general definition of modular form (of weight 2). The complex *upper half plane* is $\mathfrak{h} = \{z \in \mathbb{C} : \Im(z) > 0\}$. A *cuspidal modular form* f of level N (of weight 2) is a holomorphic function $f : \mathfrak{h} \to \mathbb{C}$ such that

$\lim_{z\to i\infty} f(z) = 0$ and for every integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with determinant 1 and $c \equiv 0 \pmod N$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-2} f(z).$$

For each prime number ℓ of good reduction, let $a_\ell = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$. If ℓ is a prime of bad reduction let $a_\ell = 0, 1, -1$, depending on how singular the reduction $\tilde{E}$ of E is over $\mathbb{F}_\ell$. If $\tilde{E}$ has a cusp, then $a_\ell = 0$, and $a_\ell = 1$ or -1 if $\tilde{E}$ has a node; in particular, let $a_\ell = 1$ if and only if the tangents at the cusp are defined over $\mathbb{F}_\ell$.

Extend the definition of the a_ℓ to a_n for all positive integers n as follows. If $\gcd(n, m) = 1$ let $a_{nm} = a_n \cdot a_m$. If p^r is a power of a prime p of good reduction, let

$$a_{p^r} = a_{p^{r-1}} \cdot a_p \; - \; p \cdot a_{p^{r-2}}.$$

If p is a prime of bad reduction let $a_{p^r} = (a_p)^r$.

Attach to E the function

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i z}.$$

It is an extremely deep theorem that $f_E(z)$ is actually a cuspidal modular form, and not just some random function.

The following theorem is called the modularity theorem for elliptic curves over $\mathbb{Q}$. Before it was proved it was known as the Taniyama-Shimura-Weil conjecture.

Theorem 1.2.10 (Wiles, Brueil, Conrad, Diamond, Taylor)**.** *Every elliptic curve over $\mathbb{Q}$ is modular, i.e, the function $f_E(z)$ is a cuspidal modular form.*

Corollary 1.2.11 (Hecke)**.** *If E is an elliptic curve over $\mathbb{Q}$, then the L-function $L(E, s)$ has an analytic continuous to the whole complex plane.*

For an excellent introduction to the modularity theorem and its many forms, see [DS05].

Bibliography

[BL07] Daniel J Bernstein and Tanja Lange, *Inverted edwards coordinates*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer, 2007, pp. 20–27.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Kob96] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, Springer New York, 1996.

[LE06] Q. Liu and R.Q. Erne, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, OUP Oxford, 2006.

[Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[ST68] J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, `http://wstein.org/papers/bib/Serre-Tate-Good_Reduction_of_Abelian_Varieties.pdf`.