AWS_4_Elliptic_and_Hyperelliptic_Curves

March 5, 2026

1 Elliptic and Hyperelliptic curves

An elliptic curve can be created in Magma in several ways. See the handbook section Creation of an elliptic curve.

[0]:
```
P<x> := PolynomialRing(Rationals());

// to create the elliptic curve given in short Weierstrass form as y^2 = x^3 +␣
 ↪2x + 3, any one of the following commands can be used.
E := EllipticCurve([2,3]); E;
E := EllipticCurve(x^3+2*x+3); E;

// to create the elliptic curve given in long Weierstrass form as y^2 + 5 xy +␣
 ↪6 y = x^3 + 2x^2 + 3x + 4, any one of the following commands can be used.
E := EllipticCurve([5,2,6,3,4]); E;
E := EllipticCurve(x^3+2*x^2+3*x+4,5*x+6); E;
```

1.1 Question 1: Jacobi quartics

We are most familiar with elliptic curves written in short Weierstrass form:

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

but there are many other representations, each with their own unique properties. In this question, we will look at the Jacobi quartic representation:

$$Y^2 = rX^4 + sX^2 + 1.$$

This is a hyperelliptic curve $C_{r,s}$ of genus 1. With the specification of a point on the curve, it is an elliptic curve. Note that the projective point $(0 : 1 : 1)$ is on the curve $C_{r,s}$ for any r, s.

The magma intrinsic `EllipticCurve`can also take as input, a genus 1 curve C along with a specified point on C, and return the associated elliptic curve E in short Weierstrass form, along with a birational map $C \to E$.

1. Find a short Weierstrass model of the Jacobi quartic curve $C_{r,s}$ for $(r, s) = (2, -3)$.
2. Treat r, s as arbitrary parameters. This amounts to working in the function field `F(r,s) := FunctionField(Rationals(),2);`.Find a formula for a short Weierstrass model $E_{r,s}$ of $C_{r,s}$. Also find the map $C_{r,s} \to E_{r,s}$.

[0]:
```

```

1.2 Question 2: Separable quartics

More generally, any separable quartic polynomial $ax^4 + bx^3 + cx^2 + dx + e$ defines a hyperelliptic curve C of genus 1. The Jacobian of C is an elliptic curve E. The curve C is isomorphic to E over any field K such that $C(K) \neq \varphi$.

Starting from the polynomial $f(x) = 2x^4 + x^3 + x^2 + x + 2 \in \mathbb{Q}[x]$, construct the hyperelliptic curve C. Find a point on C, by extending the base field if necessary, and obtain a model of the elliptic curve $E = \mathrm{Jac}(C)$ over $\mathbb{Q}$. Find an isomorphism between C and E.

[1]:
```
P<x> := PolynomialRing(Rationals());
f := 2*x^4 + x^3 + x^2 + x + 2;
C := HyperellipticCurve(f);
Points(C,100); // searches for points on C with height up to 100
```

```
{@ @}
```

Alternately, the elliptic curve E can be found directly by using the `GenusOneModels` package in magma:

[2]:
```
C := GenusOneModel(2,[2,1,1,1,2]);
E := Jacobian(C); E;
```

```
Elliptic Curve defined by y^2 = x^3 + x^2 - 15*x - 12 over Rational Field
```

1.3 Question 3: Isogenies of elliptic curves

Let $E : y^2 = x^3 + x^2 - 15x - 12$ be the elliptic curve from the previous question.

1. Let $p = 2$. Consider the reduction of this elliptic curve E over $\mathbb{F}_p$. Using modular polynomials, find all elliptic curves over $\mathbb{F}_p$ that are ℓ-isogenous to E for some prime $\ell \leq 50$.
2. Repeat for all primes p of good reduction up to 50.
3. Suppose we want to find all primes $\ell \leq 50$ such that there exists an elliptic curve ℓ-isogenous to E over $\mathbb{Q}$. Modify your computation above to find all such primes ℓ, without using modular polynomials over $\mathbb{Q}$. Verify your result by checking with the magma intrinsic `IsogenousCurves`.

1.4 Question 4: Isogenies of hyperelliptic Jacobians

It is a harder problem to find isogenies of Jacobians of curves of genus > 1. For genus 2, the simplest possible isogenies are the so-called **Richelot isogenies**, with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

Consider the genus 2 hyperelliptic curve $C : y^2 = x(x^2 + 1)(x^2 - 2)$. In the isogeny graph of its Jacobian $\mathrm{Jac}(C)$, find the largest subgraph reachable by a sequence of **$\mathbb{Q}$-rational Richelot isogenies** starting from $\mathrm{Jac}(C)$.

[3]:
```
P<x> := PolynomialRing(Rationals());
f := x*(x^2-2)*(x^2+1);
C := HyperellipticCurve(f);
```

```
L := RichelotIsogenousSurfaces(C);
L;
```

```
[*
Hyperelliptic Curve defined by y^2 = -18*x^5 - 18*x^3 + 36*x over Rational Field
*]
```

Isogenous abelian varieties have the same L-function. In particular, for any prime p the **local Euler factors** of the L-function are the same. These are also called L**-polynomials**, and denoted $L_p(A,t)$ or $L_p(C,t)$ if $A = \mathrm{Jac}(C)$.

Do a sanity check, by verifying for each prime $p < 100$, that the L-polynomial $L_p(C,t)$ of all the isogenous curves you found above are equal. That is, each isogenous curve has the same number of points over any finite extension of $\mathbb{F}_p$ for any prime p.

1.5 Question 5: Isogenies and Endomorphisms over finite fields

For a nice curve $C/\mathbb{Q}$ and a prime p of good reduction, let C_p denote the reduced curve over $\mathbb{F}_p$. In characteristic p, there is always the Frobenius endomorphism Frob_p, which satisfies the L-polynomial $L_p(C,t) = L(C_p,t)$. Hence the endomorphism ring of the Jacobian $\mathrm{Jac}(C_p)$ is at least $\mathbb{Z}[\mathrm{Frob}_p]$.

Consider the genus 2 hyperelliptic curve $C : y^2 + xy = x^5 + x^2 + x$ over $\mathbb{Q}$. In this question, you will explore connections between isogenies in char 0 and those in positive characteristic.

1. The curve C has good reduction at the prime $p = 2$. By searching through all isomorphism classes of genus 2 hyperelliptic curves over $\mathbb{F}_2$, construct a list of isogenous curves to C_2 over $\mathbb{F}_2$.
2. Given that $\mathrm{End}(\mathrm{Jac}(C_2)) = \mathbb{Z}[\mathrm{Frob}_2]$, use your computations to conclude that there exist no genus 2 curve over $\mathbb{Q}$, whose Jacobian is connected to $\mathrm{Jac}(C)$ by an isogeny of 3-power degree (other than C itself, corresponding to the multiplication-by-3^n isogenies).
3. For what other primes $\ell \neq 3$, can you come to this conclusion?

[0]: