SUPERSINGULAR DOCUMENTATION

NADIR HAJOUJI

Given a prime $p < 15073$, the program can do the following:

- Find all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Compute the supersingular 2-isogeny graph.

1. Elements of $\mathbb{F}_{p^2}$

The class ElementFp2 will be used to represent and manipulate elements of $\mathbb{F}_{p^2}$.

Every element of $\mathbb{F}_{p^2}$ can be described as $a + b\sqrt{d}$ for some $a, b, d \in \mathbb{F}_p$ - here, d is assumed to be a nonsquare element. To construct an object that represents this element, use the class ElementFp2.

1.1. **Example.**

- Let $p = 193$, and $d = -11$. Note that d is a quadratic nonresidue mod p, so we can describe elements in $\mathbb{F}_{p^2}$ as $a + b\sqrt{-11}$.
- Let $u = 80 + 12\sqrt{-11} \in \mathbb{F}_{p^2}$. ElementFp2(193,-11,80,12) constructs an object that represents u:

```
>>> u = ElementFp2(193,-11,80,12)
>>> u
80+12 sqrt(-11)
```

- The coefficients a, b are treated as elements of $\mathbb{F}_p$, in the sense that they are deemed equal if and only if they are congruent mod p. This extends to elements of $\mathbb{F}_{p^2}$: if we define a "new" element $u_2 = (80 + 193) + (12 - 193)\sqrt{-11}$, the code will treate u, u_2 as equal:

```
>>> u2 = ElementFp2(193,-11,80+193,12-193)
>>> u == u2
True
```

- We can add and multiply elements of $\mathbb{F}_{p^2}$ using $+, *$:

```
>>> v = ElementFp2(193,-11,31,5)
>>> u+v
111+17 sqrt(-11)
```

```
>>> w = ElementFp2(193,-11,31,6)
>>> u*w
144+80 sqrt(-11)
```

- u.scale(n) returns the scalar multiple of u by the integer n. Note that n can be any (positive or negative) integer.

```
>>> u.scale(2)
160+24 sqrt(-11)
>>> u.scale(3)
47+36 sqrt(-11)
```

- We can also subtract/divide. Subtraction can be done directly using -:

```
>>> uplusv = u+v
>>> uplusv - v
80+12 sqrt(-11)
>>> uplusv - v == u
True
```

- To divide by an element w, say, we have to compute the multiplicative inverse of w and multiply by the inverse:

```
>>> utimesw = u*w
>>> winv = w.multInv()
>>> winv
166+192 sqrt(-11)
>>> utimesw*winv
80+12 sqrt(-11)
>>> utimesw*winv == u
True
```

- Finally, some elementary functions from Galois theory (Galois conjugate, norm, minimal polynomial) can be computed using u.conj(), u.norm(), u.minPoly('x').
  - Conjugates are straightforward: u.conj() represents the Galois conjugate of u as an element of $\mathbb{F}_{p^2}$.
  - The norm of u is computed by multiplying u and the conjugate of u, and returning **the first coordinate of the product**. Note that the output of u.norm() is an **integer**, not an element of $\mathbb{F}_{p^2}$.

```
>>> uconj = u.conj()
>>> uconj
80+181 sqrt(-11)
>>> u*uconj
71
>>> u.norm()
71
```

  - u.minPoly('x') returns a string that represents the minimal polynomial of u over the field $\mathbb{F}_p$, using 'x' as the variable.

```
>>> u.minPoly('x')
'x^2+33x+71'
```

2. Supersingular Elliptic Curves

Say we want information about supersingular curves in characteristic $p = 193$.

- We start by creating an object using the class supSingFp2:

```
>>> ss193 = supSingFp2(193)
>>> ss193
Data about supersingular curves in characteristic 193
```

- To obtain j-invariants of the supersingular curves, we use:

```
>>> ss193.js()
[42, 169, 80+181 sqrt(-11), 80+12 sqrt(-11), 114+151 sqrt(-11), 114+42 sqrt(-11)
, 119+13 sqrt(-11), 137+97 sqrt(-11), 119+180 sqrt(-11), 137+96 sqrt(-11), 148+1
05 sqrt(-11), 118+126 sqrt(-11), 148+88 sqrt(-11), 118+67 sqrt(-11), 17+51 sqrt(
-11), 17+142 sqrt(-11)]
```

Note that the output is a list of objects in the class ElementFp2.

- The set of j-invariants can also be described as the zero set of a polynomial with coefficients in $\mathbb{F}_p$. The polynomial will have either linear or quadratic factors; we can either obtain the list of factors, or the full polynomial written as a product. In both cases, all polynomials are represented as strings.

To use these, a string needs to be chosen to represent the variable:

```
>>> ss193.jPolyFacs('j')
['j-42', 'j-169', 'j^2+33j+71', 'j^2+158j+169', 'j^2+148j+1', 'j^2+112j+99', 'j^
2+90j+166', 'j^2+150j+192', 'j^2+159j+143']
>>> ss193.jPoly('j')
'(j-42)(j-169)(j^2+33j+71)(j^2+158j+169)(j^2+148j+1)(j^2+112j+99)(j^2+90j+166)(j
^2+150j+192)(j^2+159j+143)'
```

- The 2-isogeny graph was computed to obtain the j-invariants. To obtain the adjacency matrix of the 2-isogeny graph:

```
ss193.twoIsogMat()
[[0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0], [1, 0, 0, 0, 1, 1, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0], [1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0], [1, 0, 0,
 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0], [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0,
 0, 0, 0], [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0], [0, 0, 1, 0, 0, 0,
0, 0, 2, 0, 0, 0, 0, 0, 0, 0], [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0],
 [0, 0, 0, 1, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0], [0, 0, 0, 1, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 1, 0, 1], [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0], [0, 0, 0,
 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0], [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0,
 0, 0, 1], [0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0], [0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 1, 0, 0, 0, 0, 1], [0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0]]
```

- If we want explicit models of the supersingular curves, we can use:

```
>>> ss193.fgs()
[(133, 190), (136, 158), (164+1 sqrt(-11), 15+17 sqrt(-11)), (164+192 sqrt(-11),
 15+176 sqrt(-11)), (160+118 sqrt(-11), 99+99 sqrt(-11)), (160+75 sqrt(-11), 99+
94 sqrt(-11)), (3+14 sqrt(-11), 103+41 sqrt(-11)), (49+4 sqrt(-11), 114+116 sqrt
(-11)), (3+179 sqrt(-11), 103+152 sqrt(-11)), (49+189 sqrt(-11), 114+77 sqrt(-11
)), (130+48 sqrt(-11), 95+97 sqrt(-11)), (188+146 sqrt(-11), 187+68 sqrt(-11)),
(130+145 sqrt(-11), 95+96 sqrt(-11)), (188+47 sqrt(-11), 187+125 sqrt(-11)), (44
+72 sqrt(-11), 55+63 sqrt(-11)), (44+121 sqrt(-11), 55+130 sqrt(-11))]
```

Each of the pairs (f, g) represents an equation:

$$y^2 = x^3 + fx + g$$

describing a supersingular elliptic curve.

Note that the coefficients f, g are elements of $\mathbb{F}_{p^2}$.

3. Algorithm

To do the computations, we use a specialized version of **Algorithm 2** from the paper *Computing Modular Polynomials* by Denis Charles and Kristin Lauter (ChaLau).

- The original algorithm in (ChaLau) works for any pair of primes p, ℓ.
- Our program assumes that $p < 15073$ and that $\ell = 2$.

By making these restrictions, we enjoy the following:

- In the general algorithm, steps (2) and (3) involve computing a Hilbert polynomial and finding a root of the Hilbert polynomial. By restricting to $p < 15073$, we can essentially skip these steps, as the Hilbert polynomial we need will be a linear, and its root is well-known.
- In the general algorithm, step (5) requires us to find all ℓ-torsion points on a given elliptic curve. When $\ell > 2$, this can require a substantial amount of work; however, when $\ell = 2$, we simply need to solve a quadratic equation in $\mathbb{F}_{p^2}$.

Our simplified algorithm basically boils down to doing the following:

- Find a d from the list:

$$-1, -3, -2, -7, -11, -19, -43, -67, -163$$

which is a nonsquare in $\mathbb{F}_p$. The prime $p = 15073$ is smallest with the property that all of those elements are squares; so by taking $p < 15073$, at least one of those elements is guaranteed to be a nonsquare. Once we have d, we can do the following:
  - Describe elements of $\mathbb{F}_{p^2}$ as $a + b\sqrt{-d}$.
  - We can find a model of an elliptic curve with integer coefficients whose reduction mod p is guaranteed to be supersingular.

  Note that this takes care of steps 1-3 in **Algorithm 2**.
- If $d \in \{-1, -2, -3, -7\}$, then we can obtain a model of the form $y^2 = x(x^2+ax+b)$. For other values of d, the elliptic curve over $\mathbb{Z}$ does not have 2-torsion in characteristic 0, but does in characteristic p. When we have d of this type, the model we obtain in step 1 will be a Weierstrass equation of the form:

$$y^2 = x^3 + fx + g$$

Our first task is finding a root of $x^3 + fx + g$ in $\mathbb{Z}/p\mathbb{Z}$, and doing a change of variable so that the equation has the form:

$$y^2 = x(x^2 + ax + b)$$

- Once we have a supersingular curve of the form:

$$y^2 = x(x^2 + ax + b)$$

we do a simplified version of **Algorithm 1** that will allow us to obtain up to 3 new models of the same form representing new supersingular curves:
  - First, note that the equation:

  $$y^2 = x(x^2 - 2ax + (a^2 - 4b))$$

  represents a different supersingular curve.
  - The original curve actually admits two more equations of this form: to find them, we solve the quadratic $x^2 + ax + b$ to obtain two roots r_1, r_2. By moving r_1, r_2 to 0, we obtain two new equations (that represent the original curve):

  $$y^2 = x(x^2 + a_i x + b_i)$$

  and for each of these two equations, we use 2-isogenies to obtain two other curves:

  $$y^2 = x(x^2 - 2a_i x + (a_i^2 - 4b_i))$$

So, starting from the original (a, b), we obtain 3 new pairs (a, b). Now, we take each of the new pairs and repeat the process; we will eventually find every supersingular curve and every 2-isogeny by doing this process.

4. Proofs

The proof that the algorithm works can be found in the paper (ChaLau)

In the implementation, we implicitly exploited the following fact: *All of the necessary computations can be done without ever leaving* $\mathbb{F}_{p^2}$*.* In the program, we solve quadratic equations with coefficients in $\mathbb{F}_{p^2}$, without worrying about whether the roots exist or not - we *know* they exist because of part (2) in the following theorem:

Theorem 4.1. *Let $p > 3$ be a prime and let $j \in \mathbb{F}_{p^2}$ be a supersingular j-invariant. Assume $j \neq 0, 1728$.*

1. *There are precisely two elliptic curves $E_1, E_2/\mathbb{F}_{p^2}$ (up to $\mathbb{F}_{p^2}$-isomorphism) with j-invariant equal to j.*
2. *Both E_1, E_2 have full 2-torsion defined over $\mathbb{F}_{p^2}$.*
3. *Exactly one of E_1, E_2 has a 3-torsion point in $\mathbb{F}_{p^2}$.*
4. *Let ℓ be a prime factor of $p+1$. Exactly one of E_1, E_2 has full ℓ-torsion defined over $\mathbb{F}_{p^2}$.*

The algorithm computes the 2-isogeny graph; the theorem says that the 2-isogeny graph can be computed over $\mathbb{F}_{p^2}$. In this section, we will prove this theorem, as it does not appear to be widely known.

The first claim is well-known: in fact if K is any field and $j \in K$, the number of isomorphism classes of elliptic curves over K with that j-invariant is precisely equal to the number of elements in $K^\times/K^{\times 2}$. Since $\mathbb{F}_{p^2}$ is a finite field of odd characteristic, $K^\times/K^{\times 2}$ contains two elements. This fact does not require E to be supersingular.

In fact, if $E/\mathbb{F}_q$ is given by an equation:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

for some a_2, a_4, a_6, and d is any nonsquare in $\mathbb{F}_q$, then we can obtain the equation of the other elliptic curve with equal j-invariant:

$$dy^2 = x^3 + a_2x^2 + a_4x + a_6$$

Given $E/\mathbb{F}_q$, we will write E^{-1} to denote an elliptic curve which is not isomorphic to E over $\mathbb{F}_q$, but which has the same j-invariant.

We will need the following elementary facts about E^{-1}:

- $E(\mathbb{F}_q)[2] \cong E^{-1}(\mathbb{F}_q)[2]$.
- $|E(\mathbb{F}_q)| + |E^{-1}(\mathbb{F}_q)| = 2q + 2$.

4.1. **3-torsion.**

Let $p > 3$ be a prime, q a power of p, and $E/\mathbb{F}_q$ an elliptic curve given by:

$$y^2 = x^3 + fx + g$$

Let $T : \mathbb{F}_q[x]$ be the polynomial:

$$T(x) = 3x^4 + 6fx^2 + 12gx - f^2$$

Lemma 4.2. *Let $P_0 = (x_0, y_0) \in E(\mathbb{F}_q)$. Then P_0 is a point of order 3 if and only if $T(x_0) = 0$.*

Proof. P_0 has order 3 if and only if $2P_0 = -P_0$ if and only if $x(2P_0) = x(-P_0)$. Setting $x(2P_0) = x_0$ and simplifying the expression shows $x(2P_0) = x_0$ if and only if $T(x) = 0$. □

Lemma 4.3. *Suppose E has at least one 3-torsion point defined over $\mathbb{F}_q$. Then exactly one of the following is true:*

(1) *Every 3-torsion point of E is defined over $\mathbb{F}_q$.*
(2) *$E(\mathbb{F}_q)$ contains a 3-torsion point, $E^{-1}(\mathbb{F}_q)$ contains a 3-torsion point and the full 3-torsion subgroup of E is defined over $\mathbb{F}_{q^2}$.*
(3) *$E^{-1}(\mathbb{F}_q)$ does not contain a 3-torsion point, and the full 3-torsion subgroup of E is defined over $\mathbb{F}_{q^3}$.*

Proof. Since E has at least one 3-torsion point, the polynomial $T(x)$ has at least one linear factor. Let $T_0(x)$ be the other factor of degree 3.

(1) If $T_0(x)$ splits completely, then every 3-torsion point has x-coordinate in $\mathbb{F}_q$. Thus every 3-torsion point either lies on $E(\mathbb{F}_q)$ or $E^{-1}(\mathbb{F}_q)$.

Suppose $E(\mathbb{F}_q), E^{-1}(\mathbb{F}_q)$ both contain a 3-torsion point, say P_0, P_1. Then $P_0 + P_1$ is a 3-torsion point, so it lives in $E(\mathbb{F}_q) \cup E^{-1}(\mathbb{F}_q)$. Say $P_0 + P_1 \in E(\mathbb{F}_q)$. Then $P_1 = (P_0 + P_1) - P_0 \in E(\mathbb{F}_q)$, so $P_1 \in E(\mathbb{F}_q) \cap E^{-1}(\mathbb{F}_q)$.

But that means P_1 has order 2, which means P_1 is not a nontrivial point of order 3; this is a contradiction. Thus, every point of order 3 lies in $E(\mathbb{F}_q)$ if $T_0(x)$ splits completely. Furthermore, $E^{-1}(\mathbb{F}_q)$ contains no 3-torsion points.

(2) If $T_0(x)$ factors into a linear polynomial and an irreducible quadratic, then there are precisely two pairs of 3-torsion points with x-coordinate in $\mathbb{F}_q$, say $\pm P_0, \pm P_1$. These 3-torsion points lie on $E(\mathbb{F}_q) \cup E^{-1}(\mathbb{F}_q)$.

Now, if $\pm P_0, \pm P_1 \in E(\mathbb{F}_q)$, then $E(\mathbb{F}_q)$ contains 4 nontrivial points of order 3, and the 3-torsion subgroup contains 5 elements when we include the origin. This is impossible, because the size of the 3-torsion subgroup must be a power of 3.

Thus, we must have $\pm P_0 \in E(\mathbb{F}_q)$ and $\pm P_1 E^{-1}(\mathbb{F}_q)$, so each of E, E^{-1} contains a nontrivial 3-torsion point over $\mathbb{F}_q$. Furthermore, $T_0(x)$ splits completely over $\mathbb{F}_{q^2}$, so we have all 3-torsion points in $E(\mathbb{F}_{q^2})$ by the previous point.

(3) Finally, $T_0(x)$ might be irreducible. In that case, the splitting field of $T_0(x)$ is $\mathbb{F}_{q^3}$, so we can obtain all 3-torsion points in $E(\mathbb{F}_{q^3})$

□

4.2. **Proof of theorem.** Let $E/\mathbb{F}_{p^2}$ be an elliptic curve, with $j(E) \neq 0, 1728$. We start by showing that if $E/\mathbb{F}_{p^2}$ is supersingular, then $|E(\mathbb{F}_{p^2})|$ is either equal to $(p+1)^2$ or $(p-1)^2$. By the Weil conjectures, $(p-1)^2 \leq |E(\mathbb{F}_{p^2})| \leq (p+1)^2$. In order for E to be supersingular,

$$|E(\mathbb{F}_{p^2})| \equiv p^2 + 1 \pmod{p}$$

Combining the previous two facts shows that $|E(\mathbb{F}_{p^2})| \in \{p^2+1, p^2 \pm p + 1, p^2 \pm 2p + 1\}$, so there are 5 possibilities for $|E(\mathbb{F}_{p^2})|$. If $p \equiv 1 \pmod{12}$, then Theorem 4.2 in (Sch) says this doesn't happen. When $p \not\equiv 1 \pmod{12}$, there *are* curves with cardinality p^2+1 and $p^2 \pm p + 1$, but they are twists of the curves with $j = 0, 1728$.

Some of the claims we are making will not apply to those curves; however, when that happens, it is because there is a j-invariant that appears on more than 2 isomorphism classes of elliptic curve. The point is, there may be 2 or 4 curves for which the claims fail, but there exist 2 for which they claims hold.

For the proof, we simply need to know that for all super singular j's, there exist $E, E^{-1}/\mathbb{F}_{p^2}$ with cardinalities $(p \pm 1)^2$.

(1) Since p is odd, $(p \pm 1)^2$ is even. Thus, both E, E^{-1} must have at least one two torsion point. Similarly, since $p > 3$, exactly one of $p+1, p-1$ is divisible by 3, so exactly one of E, E^{-1} has a point of order 3.

We now need to show that the curves actually have full 2/3 torsion.

(2) WLOG assume E has a point of order 3 and E^{-1} does not. Then either E has full 3-torsion defined over $\mathbb{F}_{p^2}$, or the 3-torsion subgroup of E is defined over $\mathbb{F}_{(p^2)^3} = \mathbb{F}_{p^6}$.

Here's the key point: for any supersingular j in $\mathbb{F}_{p^2}$, there is an elliptic curve $E/\mathbb{F}_{p^2}$ that has full 3-torsion over $\mathbb{F}_{p^6}$.

This includes elliptic curves with $j = 0, 1728$.

(3) Let $E_1, E_2/\mathbb{F}_{p^2}$ be supersingular curves, and assume that E_1, E_2 have 3-torsion points in $\mathbb{F}_{p^2}$. (If they don't, replace them by E_1^{-1}).

Then:

- There is an isogeny $E_1 \to E_2$ of degree 3^r, for some r, defined over $\mathbb{F}_{p^6}$.
- Since 3^r is odd, the 2-torsion subgroups of $E_1(\mathbb{F}_{p^6}), E_2(\mathbb{F}_{p^6})$ are isomorphic.

Upshot: If E_1, E_2 are any pair of supersingular elliptic curves over $\mathbb{F}_{p^2}$, then the 2-torsion of E_1, E_2 coincide over $\mathbb{F}_{p^6}$.

(4) Every supersingular curve over $\mathbb{F}_{p^2}$ has at least one 2-torsion point. If $E/\mathbb{F}_q$ has at least one 2-torsion point, then the 2-torsion subgroup does not change after passing to an extension of odd degree.

Therefore, the 2-torsion subgroups of all supersingular curves coincide over $\mathbb{F}_{p^2}$.

(5) Finally, let $E_0/\mathbb{F}_p$ be a supersingular elliptic curve. Then E_0 has at least one 2-torsion point over $\mathbb{F}_p$, and necessarily has all 2-torsion points over $\mathbb{F}_{p^2}$.

Thus, *every* supersingular elliptic curve has full 2-torsion in $\mathbb{F}_{p^2}$.

(6) Let ℓ be a prime factor of $p+1$, and let $E_0/\mathbb{F}_p$ be a supersingular curve. We've already proven the result for $\ell = 2$, so we may assume ℓ is odd. Then $E_0(\mathbb{F}_p), E_0^{-1(\mathbb{F}_p)}$ both contain points of order ℓ. Those points generate disjoint subgroups in $E_0(\mathbb{F}_{p^2})$, so they can be obtained to generate the full ℓ-torsion group.

Now, if $E/\mathbb{F}_{p^2}$ is any other supersingular curve, there is an isogeny $E \to E_0$ of degree 2^r for some r, which is defined over $\mathbb{F}_{p^2}$. Thus, the ℓ-torsion subgroup of E is isomorphic to the ℓ-torsion subgroup of E_0- so E contains full ℓ-torsion in $\mathbb{F}_{p^2}$.

References

Denis Charles and Kristin Lauter. Computing modular polynomials, 2004.

Schoof, R.; *Nonsingular Plane Cubic Curves over Finite Fields*, J. Combinatorial Theory, **46**, 2, 183-208, 1987.