I-sage-ny Days 123

1 Exercises

1.1 Curve of a Given Order

Working over the field $\mathbb{F}_p$ with $p = 65537$ find an elliptic curve $E/\mathbb{F}_p$ with order $n = 65500$.

1.2 Identifying Supersingular Curves

Using the prime $p = 2^{127} - 1$, one of the following two curves $E/\mathbb{F}_p : y^2 = x^3 + a_i x + b_i$ is supersingular.

```
a1 = 170141183460469231731687303715884105666
b1 = 170141183460469231731687303715884105639

a2 = 170141183460469231731687303715884105683
b2 = 170141183460469231731687303715884105615
```

Can you identify which of these curves is supersingular? Can you do this without counting the number of points on the curve?

1.3 Computing the Torsion Basis

The curve $E/\mathbb{F}_{p^2} : y^2 = x^3 + x$ with $p = 2303761531$ is supersingular. Can you find a basis (P, Q) of the 20123-torsion?

1.4 A Secret Degree

The following two points on the curve $E/\mathbb{F}_{p^2} : y^2 = x^3 + x$ with $p = 167$ have been mapped through an isogeny $\varphi : E \to E'$ of unknown degree with codomain $E' : y^2 = y^2 = x^3 + 157x + 58i$. Given these points and their images: $R = \varphi(P)$ and $S = \varphi(Q)$, can you recover $\deg(\varphi)$?

```
P = (41*i + 72, 53*i + 72)
Q = (7*i + 104, 22*i + 99)
R = (88*i + 98, 162*i + 154)
S = (134*i + 45, 96*i + 114)
```

1.5 A Secret Isogeny

The curve $E/\mathbb{F}_{p^2} : y^2 = x^3 + x$ with $p = 1141139$ is ℓ-isogenous to one of the following curves:

- $E_1 : y^2 = x^3 + (834063i + 506039)x + 814755i + 999217$
- $E_2 : y^2 = x^3 + (529927i + 524019)x + 243345 * i + 662636$

Can you:

1. Identify which of E_1 or E_2 is isogenous to E
2. Can you identify the degree of the isogeny?
3. Can you compute the kernel generator of the isogeny?

1.6 SIDH is Dead, but it's a Good Place to Start

Using $e_a = 13$ and $e_b = 7$ with $p = 2^{e_a} \cdot 3^{e_b} - 1$ with the familiar field $\mathbb{F}_{p^2}$ with the modulus $x^2 + 1$, can you implement the SIDH key-exchange?

Using the following generators:

```
# Points of order 2^a
P2 = (7324352*i + 16002048, 6332233*i + 11123712)
Q2 = (16562304*i + 6975702, 177793*i + 12015269)

# Points of order 3^b
```

```
P3 = (7070938*i + 9209910, 11043714*i + 13024486)
Q3 = (11816278*i + 9737191, 9489901*i + 13040098)
```

and the following secret keys:

```
secret_alice = 6668
secret_bob = 1052
```

Can you compute the j-invariant of the shared secret?

Bonus Challenge.

Now do the same, but with the NIST level one parameters: $e_a = 216$ and $e_b = 137$.

1.7 Walking around the CSIDH (Part One)

Using the prime $p = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 - 1$ and the elliptic curve $E/\mathbb{F}_p : y^2 = x^3 + x$ compute the j-invariant of the public key obtained from the exponent vector $e = [0, 1, 0, 1, 1, 0, 1]$.

1.8 Walking around the CSIDH (Part Two)

Using the same starting data as above, we now allow the private exponent to have negative values. Can you compute the j-invariant of the codomain curve from the exponent vector: $e = [2, 0, -3, 5, -1, -3, 0]$.

Bonus Challenge.

Now do the same, but with the CSIDH parameters. Try implementing a full key exchange. For convenience, the CSIDH-512 prime is made of the following factors:

```
# CSIDH-512 parameters
ells = [3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
        71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139,
        149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223,
        227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,
        307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 587]
p = 4*prod(ells) - 1
```