Chapter 2

Basic Operations

Overview

SQI$_{\text{SIGN}}$ involves the connection between two mathematical concepts that seem unrelated:

1) Isogenies between supersingular elliptic curves over finite fields
2) Maximal orders and ideals of quaternion algebras

Section 2.1 - Finite Fields

A field is a relatively well-equipped algebraic structure. As a review, we can build up to it from more fundamental structures

Abelian group

$$
\begin{tikzcd}
\text{Set} \arrow[r] & \text{Magma} \arrow[r] & \text{Semigroup} \arrow[r] & \text{Monoid} \arrow[d] \\
 & & \text{Abelian group} & \text{Group} \arrow[l]
\end{tikzcd}
$$

Field

$$\begin{tikzcd}
(S, +) \arrow[dr] & \\
a(b + c) = ab + ac \arrow[r] & (F, +, x) \\
(S \setminus \{0\}, x) \arrow[ur] &
\end{tikzcd}$$

Example

- An example is $\mathbb{Q}$, the rational numbers (set of fractions with integer numerator and denominator (den ≠ 0))
- Closure: Sum or multiplication of rational numbers is rational
- Associativity: A sequence of addition operations can be done in any order (similarly for multiplication)
- Identity: Additive identity: 0; Multiplicative identity: 1
- Inverse: Can simply negate a number to get its additive inverse; Can flip a fraction to get its multiplicative inverse (remember 0 is not included here)
- Commutativity: Can add or multiply two rationals in any order

Finite fields

We care about fields with a finite number of elements. All such fields are of prime power order (powers of a single prime). Specifically we care about F_p (operations are mod p) and F_{p^2} which both have characteristic p.

Ex. $F_p = (\mathbb{Z}_p, +, x)$ has characteristic p because $\underbrace{1 + 1 + 1 + \ldots + 1}_{\text{p times}} = 0 \pmod{p}$

We will consider p = 3 (mod 4)

Quadratic residue in F_p

- Useful for later definitions throughout the paper
- A number congruent to a perfect square: $b^2 = a \pmod p$
- Can test if ‘a’ is a perfect square in F_p by raising both sides by (p - 1) / 2
- $b^{p-1} = a^{(p-1)/2} \pmod p = 1 \pmod p$ (by Fermat’s little theorem)
- If this equation is not true, then ‘a’ wasn’t a perfect square to begin with

F_q for $q = p^2$

If F_p was analogous to the real numbers, then $F_{p\text{^}2}$ is analogous to the complex numbers. With $i^2 + 1 = 0$, elements of $F_{p\text{^}2}$ are of the form $a_0 + a_1 i$ for a_0, a_1 in F_p

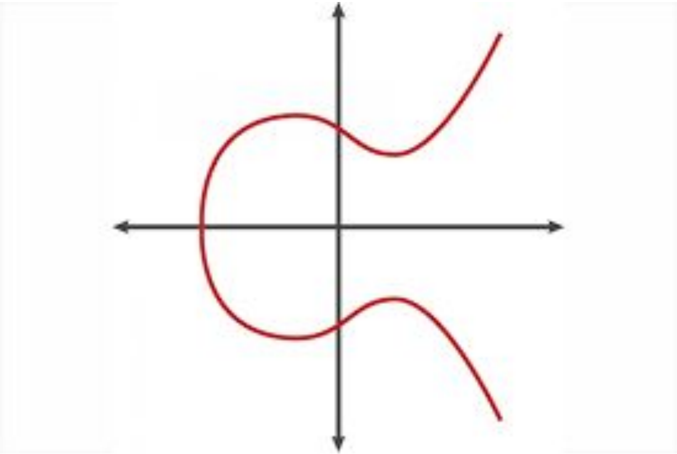
It's additive and multiplicative operations are the familiar ones when working with complex numbers. For instance, the multiplicative inverse of a + bi is:

$$\frac{1}{a + bi} \longrightarrow \frac{1}{a+ bi}\frac{(a-bi)}{(a-bi)} \longrightarrow \frac{a-bi}{a^2 + b^2}$$

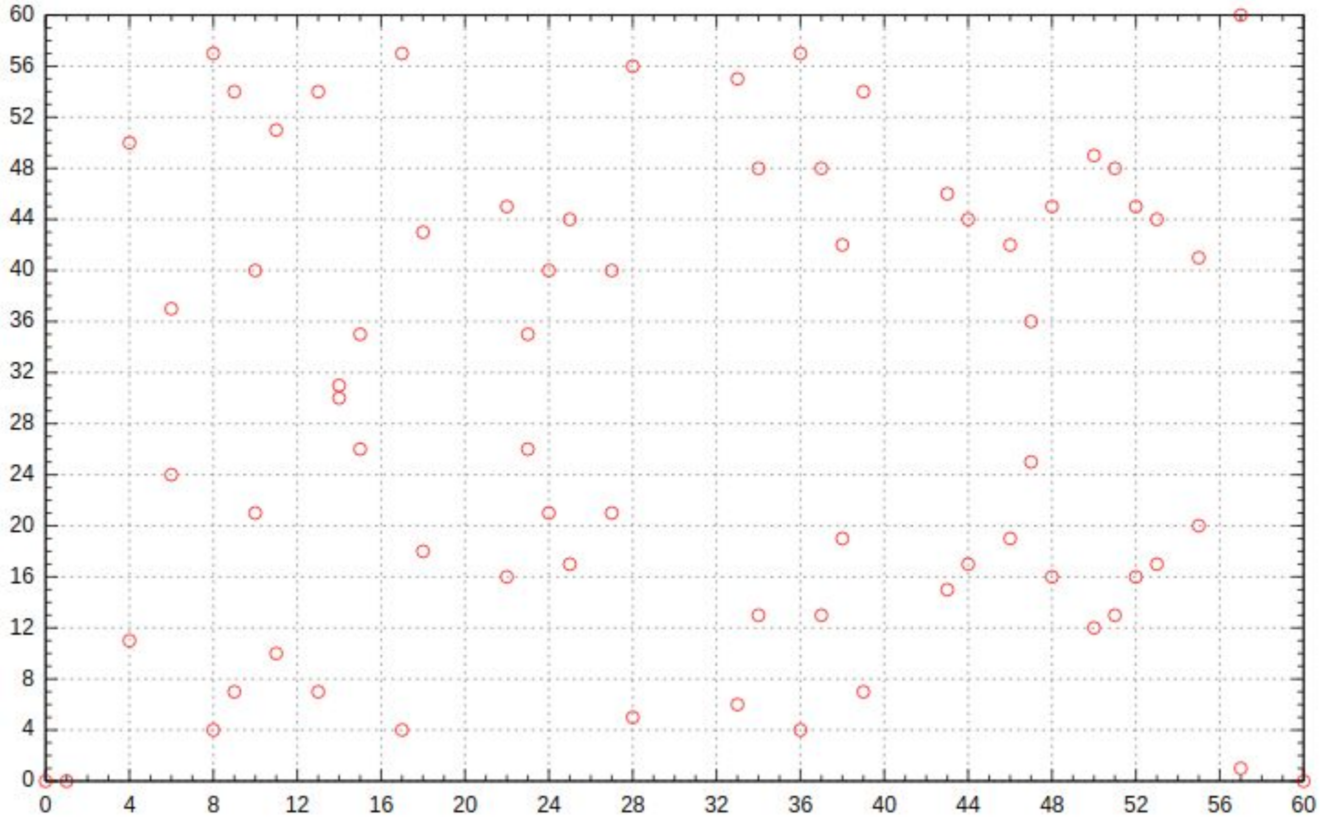
Section 2.2 - Elliptic Curves

- Montgomery elliptic curves are curves of the form: $By^2 = x^3 + Ax^2 + x$
- We also importantly consider a “point at infinity”, ∞, to be part of the curve
- Two curves are isomorphic if there is a bijective (one-to-one correspondence) mapping between them of the form $(x, y) \leftrightarrows (D(x + R), Cy)$
- They are “quadratic twists” of one another if $C = \sqrt{(B/B')}$ and are isomorphic if B/B' is a perfect square

Elliptic curve over the real numbers



An elliptic curve over the finite field, F_{61}



Supersingular meaning

If the number of solutions to the curve is congruent to 1 mod char(F_q), it is called supersingular.

Recall we care about p = 3 (mod 4) and $F_{p\hat{}2}$

In this case, if B = 1, the curve has exactly $(p + 1)^2$ points

Ex. B = 1, p = 7, $(7 + 1)^2$ = 64 mod 7 = 1 (mod 7) ✓

Group structure of elliptic curves

Collectively supplementing the points on the elliptic curve with a binary addition operation yields an abelian group!