Chapter 1

Introduction

1.1 What is an elliptic curve?

An elliptic curve is wisdom. [1]

This is another page of my amazing thesis.

This is another page of my amazing thesis!!

Chapter 2

Elliptic Curve Basics

Definition 2.1. Let K be a field. An **elliptic curve** E **over** K is defined by an equation:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and the **discriminant** Δ is non-zero. This equation is called a **Weierstrass equation**.

Definition 2.2. With K and E defined as above, the set of **L-rational points** on E for any extension L of K is the set of pairs $(x, y) \in L \times L$ that satisfy E, together with $\mathcal{O}$, the point at infinity.

The set of L-rational points is denoted $E(L)$.

Definition 2.3. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The **trace of Frobenius** t is defined by:

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

where $\#E(\mathbb{F}_q)$ is the number of elements in $E(\mathbb{F}_q)$.

Remark. The trace of Frobenius is equal to one if and only if $E(\mathbb{F}_q)$ has exactly q elements. This has important implications for cryptography, as we will see.

Chapter 3

Formal Power Series and Formal Logarithm

3.1 Formal Power Series

Definition 3.1.

3.2 Formal Logarithm

Hello

Chapter 4

P-adic numbers

4.1 The p-adics

Definition 4.1. For a rational number a and a prime number p, separate out all factors of p from a and write:

$$a = p^r \frac{m}{n}$$

where r, m and n are integers, and p does not divide m or n. The exponent r is called the **p-adic ordinal** of a, denoted $\mathrm{ord}_p(a)$.

Definition 4.2. For a prime p, we define a function $|.|_p : \mathbb{Q} \to \mathbb{Q}_{\geq 0}$ where for $a \in \mathbb{Q}$:

$$|a|_p = \begin{cases} p^{-\mathrm{ord}_p(a)} & a \neq 0 \\ 0 & a = 0. \end{cases}$$

The function $|.|_p$ is called the **p-adic absolute value**.

Proposition 4.3. *The p-adic absolute value is a norm on $\mathbb{Q}$, and induces a metric*

$$d_p(a,\ b) = |a - b|_p$$

for $a, b \in \mathbb{Q}$.

Definition 4.4. A p-adic number a is called a **p-adic integer** if $ord_p(a) \geq 0$. The set of all p-adic integers is denoted $\mathbb{Z}_p$.

Remark. A p-adic integer is always of the form

$$a_0 + a_1 p + a_2 p^2 + ...,$$

i.e., all powers of p are non-negative.

Bibliography

[1] Fake Person. *A Book*. 1992.