Todo list

Geometric group law 3
Fix formatting here 4
Introduce what p-adics look like here? 5
Prove this! 6
″p-adic comment″ 6
Describe computation of lifts 6
more on reduction mod p 6
Prove this is a homomorphism 6

Chapter 1

Background

1.1 Introduction to Elliptic Curves

Definition 1.1. 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[1] is non-zero. This equation is called a **Weierstrass equation**.

When $\operatorname{char}(K) \neq 2, 3$, we can change variables to arrive at the simplified Weierstrass equation:

$$E : y^2 = x^3 + ax + b$$

where $a, b \in K$.

Definition 1.2. 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 $E(L)$.

An elliptic curve can be defined over any field K, but in cryptography we generally restrict K to be a finite field F_q where $q = p^n$, for p prime and $n \in \mathbb{Z}_{>0}$. In this paper we will restrict ourselves even further to prime fields $\mathbb{F}_p$ where $p \neq 2, 3$, and to an infinite field $\mathbb{Q}_p$ (the p-adics), which have

[1] If you must know,

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$$

characteristic 0. This means we will always be able to use the simplified equation given in the first definition above.

Definition 1.3. 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.

1.1.1 The group law

Describe geometric group law and how it motivates algebraic one. Possibly add figures to motivate this.

Definition 1.4. Let $E(K)$ be an elliptic curve over a field K with $char(K) \neq 2, 3$ defined by $y^3 = x^3ax + b$ with point at infinity $\mathcal{O}$. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be points on $E(K)$. Then:

1. (Identity.) $\mathcal{O} + P = P$ and $P + \mathcal{O} = P$.
2. (Additive inverses.) The additive inverse of P, denoted $-P$, is in $E(K)$, and $P + (-P) = \mathcal{O}$.
3. (Point Doubling.) If P is not its own inverse, then $P + P = 2P = (x_{2P}, y_{2P})$ where
$$x_{2P} = N^2 - 2x_P,$$
$$y_{2P} = N(x_P - x_{2P}) - y_P,$$
$$N = \frac{3x_P^2 + a}{2y_P}.$$
4. (Point Addition.) If $P \neq Q$ and $P \neq -Q$ then $P + Q = R = (x_R, y_R)$ where
$$x_R = M^2 - x_P - x_Q,$$
$$y_R = M * (x_P - x_R) - y_P,$$
$$M = \frac{y_Q - y_P}{x_Q - x_P}.$$

$E(K)$ is an abelian group under this group law.

Notation. Let P be a point on an elliptic curve. We use the notation $[n]P$ to denote scalar multiplication of P by a non-zero integer n. In other words,

$$[n]P = P + P + ... + P \text{ (n times)}.$$

1.1.2 Projective space and projective coordinates

1.1.3 The Elliptic Curve Discrete Logarithm Problem

The interesting thing about elliptic curves with regards to cryptography is that their structure can be used to construct a ”one-way” function.[2] A one-way function is one that is easy to perform but hard to undo (i.e., it is difficult to retrieve the input, given an output).

Definition 1.5 (Elliptic Curve Discrete Logarithm Problem)**.** Let E be an elliptic curve over a finite field $\mathbb{F}_q$, and let P be a point on E. Suppose we have a point Q on E that is some scalar multiple of P, i.e.,

$$[n]P = Q, \quad n \in \mathbb{N}.$$

The **elliptic curve discrete logarithm problem** (ECDLP) is to determine the natural number n, given E, P and Q.

On the other hand, the problem of determining $[n]P$ given n and P is not hard. One simple (to describe) way to do this is by using successive squaring.

Definition 1.6 (Successive Squaring for Elliptic Curves)**.** . Suppose we have an elliptic curve $E(K)$, a point $P \in E(K)$ and a nonnegative integer n. We can compute $[n]P$ recursively by calling SuccessiveSquare(n, P). The analogue of squaring for elliptic curves is doubling.

SuccessiveSquare(nonnegative integer m, point on elliptic curve Q):

Fix formatting here

1. If m = 0, return $\mathcal{O}$.

2. If m = 1, return Q.

3. If n is even, return $[m/2](2Q)$ by calling SuccessiveSquare$(n/2, 2Q)$.

[2] In this case one-way is in quotes because the problem is only hard in certain cases, and there is no guarantee that there is not some clever way to render the general problem easy.

4. If n is odd, return $[(m-1)/2](2Q)$ by calling SuccessiveSquare($(m-1)/2, 2Q)$ and add Q.

This asymptotic run-time of this algorithm is $O(\log n)$, a considerable improvement on brute force computation of $P + P + P + ...$ which takes $O(n)$ time. There are even faster algorithms for this computation that we do not describe here.

1.2 Formal Power Series

Definition 1.7.

1.3 Formal Logarithm

1.4 The p-adics

The p-adics $\mathbb{Q}_p$ are an alternate completion of the rationals $\mathbb{Q}$, with respect to the p-adic absolute value.[3] They will be useful in our discussion of solving ECDLP for curves of trace one.

Introduce what p-adics look like here?

Definition 1.8. 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 $\text{ord}_p(a)$.

Definition 1.9. For a prime p, we define a function $|.|_p : \mathbb{Q} \to \mathbb{Q}_{\geq 0}$ where for $a \in \mathbb{Q}$:

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

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

Proposition 1.10. *The p-adic absolute value is a norm on $\mathbb{Q}$, and induces a metric*

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

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

Proof.

Prove this!

Explain why we don't really detailed proofs of Cauchy sequences etc

Definition 1.11. 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.

1.4.1 Computing lifts and reducing modulo p

Since $\mathbb{Q}_p$ is a field with characteristic 0, we can talk about elliptic curves over the p-adics, and all of the theory we built up in the previous sections applies.

Describe computation of lifts

Going the other way is simple. We define a map from $E(\mathbb{Q}_p)$ to $\tilde{E}(\mathbb{F}_p)$ by reducing a point modulo p, i.e, extracting its a_0 term.

more on reduction mod p

1.4.2 More about elliptic curves over $\mathbb{Q}_p$

Definition 1.12. Let $E(\mathbb{Q}_p)$ be an elliptic curve. The group $E_1(\mathbb{Q}_p)$ is defined to be:

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} = \mathcal{O}\}.$$

In words, E_1 is the set of points on E that reduce modulo p to $\mathcal{O}$. This leads naturally to the following proposition:

Proposition 1.13.

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \simeq E(\mathbb{F}_p).$$

Proof. Define a map $r : E(\mathbb{Q}_p) \to E(F_p)$ where $r(P) = \tilde{P}$. By definition, the kernel of this map is $E_1(\mathbb{Q}_p)$. The result follows from the First Isomorphism Theorem.

Prove this is a homomorphism

Definition 1.14. The subgroup E_n (for $n \in N$) of $E(\mathbb{Q}_p)$ is defined:

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \mathrm{ord}_p(x_P) \leq -2n\} \cup \{\mathcal{O}\},$$

where x_P is the x-coordinate of P.

[3] The standard completion of $\mathbb{Q}$, of course, is $\mathbb{R}$ with respect to the familiar absolute value

Chapter 2

Discrete Logarithm on Elliptic Curves of Trace One

In this section we will see that elliptic curves of trace one should not be used for cryptography, because there is a subexponential algorithm for solving the ECDLP in this case. This algorithm was initially proposed by Nigel Smart in [Sma99].

Recall that if E is an elliptic curve over a field $\mathbb{F}_q$, then having trace one means that:

$$\#E(\mathbb{F}_p) = p.$$

In words, the number of group elements is the same as the number of elements in the underlying prime field.

Throughout this section, we will work with a toy example so that the computations can be shown in full.

Example (Setup)**.** Let E be defined over F_7 by the equation:

$$y^2 = x^3 + 6x + 5.$$

This is an elliptic curve because the discriminant $\Delta = -16(4 \cdot 6^3 + 27 \cdot 5^2) = -24624 \neq 0$.[1]

[1] The equation for the discriminant simplifies to

$$\Delta = -16(4a^3 + 27b^2)$$

for $E(K)$ with with char(K)$\neq 2, 3$. Here char($\mathbb{F}_7$) = 7.

The points satisfying E are:

$$\begin{array}{llll} \mathcal{O} & (2,2) & (2,5) & (3,1) \\ (3,6) & (4,3) & (4,4). & \end{array}$$

E has 7 points, so it has trace one.
Now let $\tilde{P} = (2,5)$ and $\tilde{Q} = (4,3)$. Suppose we know that

$$[n]\tilde{P} = \tilde{Q}$$

for some natural number n (this is indeed the case). How can we solve the discrete log problem and determine n?

We do not have a (known) direct way of computing logarithms in $\mathbb{F}_p$, but we do have a way in the p-adics Q_p.

Example (Computation of lifts)**.** We compute the lifts of $\tilde{P}$ and $\tilde{Q}$ in $E(\mathbb{F}_7)$ to P and Q in $E(\mathbb{Q}_7)$.
We know $\tilde{P} = (2,5)$ and we want to solve for $P = (x,y)$. We choose $x = 2$. We want to solve for the first two coefficients a_0 and a_1 of the p-adic expansion of $y = a_0 + a_1 p + ...$ Since y must reduce to 5, we let $a_0 = 5$.We use our formula for a_1:

$$a_1 = -\frac{f(2,5)}{7*(2*5)} = \frac{5^2 - 2^3 - 6*2 - 5}{70} = 0?$$

COMMENT : Is this wrong, or is it the anomalous case Smart mentioned?
Using a similar method, we determine that $Q =$. TODO

Example (Scalar multiplication by p)**.** We compute [7]P and [7]Q. TODO

Remark. $E_1(\mathbb{Q}_p)$ can be defined in this way as well. EXPLAIN WHY.
QUESTION: $E_0(\mathbb{Q}_p)$ is the same as $E(\mathbb{Q}_p$?

Definition 2.1. For E an elliptic curve over $\mathbb{Q}_p$, we define $\hat{E}(p\mathbb{Z}_p)$ to be the set $p\mathbb{Z}_p$ with addition law:

$$x \oplus y = F(x,y) \text{ for all } x, y \in p\mathbb{Z}_p,$$

where F is the formal power series:

$$F(x,y) = x + y - ...$$

TODO : figure out what this is in the simplified case

Bibliography

[Gou93] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, 1993. An introduction.

[HMV04] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Professional Computing. Springer-Verlag, New York, 2004.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sma99] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.