1. INTRODUCTION

This home assignment will be a very brief and informal introduction to both finite fields and elliptic curves over such.

My hope is that you, after completing this assignment, will be able to read and understand the modern applications of elliptic curves to codes (which, in fact, often use general algebraic curves over finite fields), cryptography and integer factorization. Needless to say, if you want to become an expert, you will need to know substantially more not only of number theory (including fields) and algebraic curve theory, but also some basic computer science stuff.

Anyway, I hope this will be a perfect start.

2. FINITE FIELDS

A finite field is exactly what it sounds like: a finite set $F$ which is also equipped with a field structure, i.e., there is an abelian group structure $(F, +, 0)$, a commutative ring structure $(F, +, 0, \cdot, 1)$ such that every $a \in F$ with $a \neq 0$ is invertible, meaning that for each $a \in F$ there is a (unique) $a^{-1}$ such that $aa^{-1} = a^{-1}a = 1$. Well, you all know this!

Now, the prime example, and in a sense the only one, is the ring $F_p := \mathbb{Z}/p\mathbb{Z}$, for $p$ a rational prime. In fact, we have the following theorem:

**Theorem 2.1.** Every finite field $F$ is isomorphic to a (finite) field extension of a field $F_p$, with $\#F = p^n$ for some $n \geq 1$.

**Theorem 2.2.** Every finite field extension $F \supset F_p$ is a finite field of $q := p^n$ elements, $n \geq 2$.

This may sound like an obvious theorem (and it is in a sense) but the construction is both nice and familiar and so I give you:

**Exercise 2.1.** Prove the above theorem by using the technique from the notes.

**Exercise 2.2.** Prove Theorem 2.1 by completing the following steps:

---

1 I'm sure some of you already are experts on this so in that case, you only have to be experts on the other topics.
Step 1: Prove that every finite field has characteristic $p$ for some prime $p$;
Step 2: Prove (by using Step 1, for instance) that every finite field includes a prime subfield $\mathbb{F}_p$ (see the Lecture notes);
Step 3: Deduce Theorem 2.1 from Step 2 and Theorem 2.2.

Note. I want to be perfectly clear on one thing: a field extension $\mathbb{F}_{p^n}$ is not equal to $\mathbb{Z}/p^n\mathbb{Z}$. It suffices to consider $\mathbb{Z}/2^2\mathbb{Z}$ to realize that this is not even a field as there is a zero divisor (namely, 2).

Also, every finite field satisfies $\# \mathbb{F} = p^n$ for some prime $p$ and $n > 0$. Hence, for instance, there is no field with six elements.

Since each finite field $\mathbb{F}$ is a field, everything you are allowed to do algebraically in $\mathbb{Q}$ (or any other field) is allowed in the finite field case also. Therefore, solving equations by factorizing polynomials, linear algebra, etc, is (in principle) perfectly legal. There are some subtle points where one has to be careful, especially in the case of characteristic two, but this need not worry us unless we plan to divide things by $p$ (as this is zero for $\mathbb{F}_p$).

Exercise 2.3. Use the previous exercise to construct a field of 9 elements and present the multiplication table. Note that every pair of fields of $p^n$ elements are isomorphic, so the field you construct is the field of nine elements, no matter how you constructed it.

Exercise 2.4. How many elements are there in a $k$-dimensional vector space $V_k$ over $\mathbb{F}_q$, $q := p^n$? How many $\ell$-dimensional linear subspaces are there in $V_k$?

Exercise 2.5. Solve the following (systems of) equations for all $p$:
(a) $z^2 + 5z + 6$;
(b) $z^3 + z + 2$;
(c) $z^4 - 10z^3 + 9z + 7$;
(d) \[
\begin{bmatrix}
2 & 1 & z \\
-2 & 1 & 2 \\
-3 & -1 & 1
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z
\end{bmatrix} =
\begin{bmatrix}
1 \\
-2a \\
-1
\end{bmatrix},
\text{ for all } a \in \mathbb{F}_p.
\]
(Start with taking $a = 0$ for simplicity.)

Exercise 2.6. If you were clever in the above exercises you used the fact that reduction modulo $p$ is a ring homomorphism, i.e., that

$$(\cdot) \downarrow : \mathbb{Q} \rightarrow \mathbb{F}_p, \quad a \downarrow \mapsto [a \pmod{p}], \quad \text{for } p \nmid c, \quad \text{where } a = \frac{b}{c},$$

is a ring homomorphism. Prove this!

In addition, prove that, by using that $(\cdot) \downarrow$ is a morphism of rings, you can solve the above equations first in $\mathbb{Q}$ and the reduce modulo $p$, assuming that $p$ is not inverted.

Note. Notice that one has to be careful when solving equations by reduction since there might be some subtle division present in the solving over $\mathbb{Q}$, which is not allowed modulo $p$. Such cases has to be dealt with separately.

---

2As an example of where one has to be careful I can mention that the definition of elliptic curves has to be modified for fields of characteristic two, for instance the field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

3No! Don’t even think about it. You cannot use the “square-root formula” for solving quadratic equations over finite fields.
3. Elliptic curves over finite fields

**Note.** Before we continue, we make the standing assumption that the characteristic of $\mathbb{F}_q$ is not two or three, i.e., that $q \neq 2^n, 3^n$ (except in Exercise 3.3, where we allow $p = 3$). Let’s ignore the deeper reason for this and simply say that if the characteristic were two or three we would need to have another definition of elliptic curve.

If the characteristic of the ground field ($\mathbb{F}_p$ in this case) is not two or three a cubic curve $\mathcal{C}$ over $\mathbb{Q}$ can be written in the Weierstrass normal form

$$y^2 = x^3 + ax + b,$$

for $a, b \in \mathbb{Q}$, and that the discriminant

$$\Delta_{\mathcal{C}} := 4a^3 + 27b^2,$$

is non-zero if and only if $\mathcal{C}$ is non-singular, that is, elliptic.

**Note.** If we wanted to allow characteristic 3, i.e., $q = 3^n$, in the definition above, we would have to put the equation in the Weierstrass form you know from the Lecture notes, namely,

$$(3.1)
\quad y^2 = x^3 + ax^2 + bx + c. $$

Wanting to work with $q = 2^n$ we would have accept the even more general form

$$y^2 + axy + by = x^3 + cx^2 + dx + e. $$

But for this assignment we tacitly assume that $p \neq 2, 3$, for simplicity. Also, to be perfectly accurate the discriminant above, as defined for the Weierstrass normal form we use here, should be

$$\Delta_{\mathcal{C}} = -16(4a^3 + 27b^2),$$

but for simplicity we ignore the factor $-16$ since the only thing we need the discriminant for here (now that $p \neq 2$) is to determine if $\Delta_{\mathcal{C}}$ is zero or not.

Now, exactly the same definition holds in the case when $\mathbb{Q}$ is replaced by $\mathbb{F}_p$ or $\mathbb{F}_q$, $q = p^n$.

**Exercise 3.1.** Derive the explicit equations for the group law in the case when the ground field is $\mathbb{F}_p$. This can be done with the reduction procedure described above, but beware of denominators!

Exactly as for the “characteristic zero case” we can form the group of $\mathbb{F}_q$-rational points:

$$\mathcal{C}(\mathbb{F}_q) = \{(u,v) \in \mathbb{F}_q^2 \mid v^2 = u^3 + au + b\}, \quad \text{for } q = p^n, n > 0. $$

That this is a group is almost obvious by what you already know. But notice that $\mathcal{C}(\mathbb{F}_q)$ is not a subgroup of $\mathcal{C}(\mathbb{F}_p)$ since it is not even a subset of $\mathcal{C}(\mathbb{F}_p)$. Instead, we have

$$\mathcal{C}(\mathbb{F}_p) \subset \mathcal{C}(\mathbb{F}_{p^2}) \quad \text{and} \quad \mathcal{C}(\mathbb{F}_p) \subset \mathcal{C}(\mathbb{F}_{p^{n+1}}),$$

which is in fact in perfect analogy with the zero characteristic case.

Also, we can homogenize equations to get projective curves over finite fields. This is completely obvious.

**Exercise 3.2.** How many points are there in $\mathbb{P}^k_{\mathbb{F}_p}$?

A natural question is then: how many points are there on the curve $\mathcal{C} : y^2 = x^3 + ax + b$ over $\mathbb{F}_p$? Well, first of all, let me point out the obvious: since $\mathbb{F}_p$ is finite, there are only a finite number of points of $\mathcal{C}(\mathbb{F}_p), q = p^n$. This implies that $\mathcal{C}(\mathbb{F}_q)$ is a finite group for all powers $q$ of $p$. 


**Exercise 3.3.** Determine the number of $\mathbb{F}_p$-rational points on the following cubic curves over $\mathbb{F}_p$, $p = 3, 5, 7$. Furthermore, determine for which $p > 2$ the curve is elliptic, i.e., non-singular. Use the discriminant for this. The formula $(4a^3 + 27b^2)$ for the discriminant is applicable even when the characteristic is three (the $p = 3$ case) since in the examples below the coefficient of $x^2$ in (3.1) is zero.

- $y^2 = x^3$;
- $y^2 = x^3 + x + 1$;
- $y^2 = x^3 - 3x$;
- $y^2 = x^3 - 2x + 3$;
- $y^2 = x^3 + 5$;

There is an estimate of the number of $\mathbb{F}_p$-points on an elliptic curve due to Helmut Hasse (1898-1979):

**Theorem 3.1.** Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field with $q = p^n$. Then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$ 

**Exercise 3.4.** Use this to compare with your results above.

**Reducing curves modulo $p$.** Suppose that

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b, \quad a = \frac{a_n}{a_d}, \quad b = \frac{b_n}{b_d}, \quad p \not| a_d, b_d.$$ 

Recall that (2.1) is a ring morphism and we can reduce $E$ modulo $p$ by reducing the coefficients modulo $p$:

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b \quad \mapsto \quad E^1/\mathbb{F}_p : y^2 = x^3 + a^1x + b^1.$$ 

This curve $E^1$ is non-singular if and only if

$$\Delta_{E^1} = 4(a^1)^3 + 27(b^1)^2 \neq 0,$$

i.e., if and only if $p \not| \Delta_{E^1}$. Recall that we assume that $p \neq 2$.

**Note.** This is from now on a standing assumption: $E$ is non-singular, i.e., $p \not| \Delta_{E^1}$.

**Group structure.** We are now going to relate the group $E(\mathbb{Q})$ to the group $E^1(\mathbb{F}_p)$ of the reduced curve. To do this we will transform our curve $E/\mathbb{Q}$ to its projectivized version (which we denote the same)

$$E/\mathbb{Q} : \quad Y^2Z = X^3 + aXZ^2 + bZ^3.$$ 

First, let $[a : b : c]$ be a point in $\mathbb{P}^2(\mathbb{Q})$, i.e., $a, b, c \in \mathbb{Q}$. Then we can assume that at least one of $a, b, c$ is not divisible by $p$, since we can always clear denominators and then divide by the gcd$(a, b, c)$, the result representing the same point. So if $p|a, b, c$ the gcd$(a, b, c) > 1$ which by construction it is not. The homogeneous coordinates $[a : b : c]$ resulting from the above construction is called **normalized**. Hence every point in $\mathbb{P}^2(\mathbb{Q})$ has a (unique, up to sign) normalized representative.

Reducing a normalized point modulo $p$ thus yields a map:

$$(\cdot)^1 : \mathbb{P}^2(\mathbb{Q}) \rightarrow \mathbb{P}^2(\mathbb{F}_p), \quad [a, b, c] \mapsto [a^1, b^1, c^1].$$

Notice that, by passing to the projectivized version of $E$, we evade the awkward assumption that $p$ doesn’t divide the denominators of $a$ and $b$. In the affine case this cannot be ignored.

By the same procedure as for homogenized coordinates we can assume that the defining equation for $E$ is normalized. Indeed, multiplying with a common denominator and the
dividing with the greatest common divisor we get that the coefficients are integers and relatively prime.

**Exercise 3.5.** Suppose \( E / \mathbb{Q} \) is an elliptic curve (or an algebraic curve) with homogeneous, normalized defining equation \( F(X,Y,Z) \). Prove that (3.2) induces a reduction modulo \( p \) on \( E / \mathbb{Q} \), i.e., we have a commutative diagram:

\[
\begin{array}{ccc}
P^2(\mathbb{Q}) & \xrightarrow{(\cdot)^1} & P^2(\mathbb{F}_p) \\
\text{restr.}_\mathcal{E} & & \text{restr.}_\mathcal{E} \\
P^2(\mathcal{E}(\mathbb{Q})) & \xrightarrow{(\cdot)^1} & \mathcal{E}(\mathcal{E}_{\mathbb{F}_p})
\end{array}
\]

where the map in the bottom row is a map of sets, and the vertical ones are the restriction maps to \( E \) and \( E_{\mathbb{F}_p} \), respectively.

We want to show that \( \mathcal{E}(\mathbb{Q}) \xrightarrow{(\cdot)^1} \mathcal{E}_{\mathbb{F}_p} \) is a morphism of groups. To do this we need to have an intersection theory of lines and cubics in \( P^2(\mathbb{F}_p) \). That is, we need to know that the number of intersection points of \( L \) with \( \mathcal{E}_{\mathbb{F}_p} \) is always three, counting multiplicities. This is not immediate by the fact that we work in projective space and Bézout’s theorem\footnote{That says that the number of intersections of two projective (algebraic) curves of degree \( n \) and \( m \) is \( nm \) counting multiplicities.}, since this is only valid for algebraically closed fields and \( \mathbb{F}_p \) is not algebraically closed (such fields are always infinite!).

Therefore, we circumvent this with the following proposition.

**Proposition 3.2.** Let \( \mathcal{C} / \mathbb{Q} \) be an algebraic curve over \( \mathbb{Q} \) and \( L / \mathbb{Q} \) a line over \( \mathbb{Q} \) and assume that the points of intersection in \( \mathbb{C} \) are rational, i.e.,

\[
L \cap \mathcal{C} = \{ p_1^{m_1}, \ldots, p_n^{m_n} \}, \text{ with } p_i \in \mathbb{Q} \text{ and } n := \deg(\mathcal{C}),
\]

where \( m_i \) are the multiplicities. Assume further \( F_{\mathbb{F}_p}(X,Y,0) \neq 0 \), where \( F(X,Y,Z) \) is the normalized defining equation for \( \mathcal{C} \). Then

\[
L_{\mathbb{F}_p} \cap \mathcal{C}_{\mathbb{F}_p} = \{ (p_1^{m_1})^{m_1}, \ldots, (p_n^{m_n})^{m_n} \}.
\]

That \( F_{\mathbb{F}_p}(X,Y,0) \neq 0 \) means that not every coefficient of the normalized \( F(X,Y,0) \) is divisible by \( p \).

**Proof.** The proof will consist of a series of exercises.

**Exercise 3.6.** We divide the proof into three steps.

**Step 1:** Show that if the intersection points \( p_i \) of \( \mathcal{C} \) and \( Z = 0 \) are \( p_i = [a_i,b_i,0] \), we have

\[
F(X,Y,0) = c \prod_{i=1}^n (b_iX - a_iY), \text{ with } p \nmid c.
\]

**Step 2:** Show that reduction of \( F(X,Y,0) \) modulo \( p \) then gives the right number of intersection points for \( L_{\mathbb{F}_p} \cap \mathcal{C}_{\mathbb{F}_p} \).

**Step 3:** Show that for each relatively prime triple \( (a,b,c) \) there is an integer \( 3 \times 3 \)-matrix

\[
\begin{pmatrix}
D_1 & D_2 & D_3 \\
D_4 & D_5 & D_6 \\
a & b & c
\end{pmatrix}
\]
of determinant one, transforming the general normalized line \( L: aX + bY + cZ = 0 \) to a line at infinity \( Z' = 0 \). Deduce from this that reduction modulo \( p \) is well-defined, thereby finishing the proof. □

As a corollary of this proposition we get the result we want:

**Theorem 3.3.** The map \( \mathcal{E}(\mathbb{Q}) \to \mathcal{E}^1(\mathbb{F}_p) \) sending \( 0 \) to \( 0 \) is a morphism of groups.

**Exercise 3.7.** Prove the theorem using the foregoing proposition. *Hint:* Use the geometric definition of the group law on \( \mathcal{E}(\mathbb{Q}) \) and reduce modulo \( p \).

Now, let \( \text{Fin}(\mathcal{E}) \) be the subset of \( \mathcal{E}(\mathbb{Q}) \) of elements of finite order, i.e.,

\[
\text{Fin}(\mathcal{E}) := \bigcup_N N = \{ p \in \mathcal{E}(\mathbb{Q}) \mid Np = 0, \text{ for some } N < \infty \}.
\]

**Exercise 3.8.** Prove that \( \text{Fin}(\mathcal{E}) \) is a subgroup of \( \mathcal{E}(\mathbb{Q}) \).

This means that \( \cdot \rangle \) restricts to give a group morphism

\[
(\cdot) \rightarrow \mathcal{E}^1(\mathbb{F}_p).
\]

**Exercise 3.9.** Prove that this morphism is an injection. As a result \( \text{Fin}(\mathcal{E}) \) can be considered as subgroup of \( \mathcal{E}^1(\mathbb{F}_p) \).

This is a rather remarkable result! As an application let me show the following simple example:

**Example 3.1.** Let \( \mathcal{E}/\mathbb{Q} : y^2 = x^3 + 3 \). This has discriminant \( \Delta = 243 = 3^5 \) and so for \( p \geq 5 \) we have a group morphism

\[
\text{Fin}(\mathcal{E}) \to \mathcal{E}^1(\mathbb{F}_p).
\]

It is easy to check by explicit calculation (do this!) that

\[
\#\mathcal{E}^1(\mathbb{F}_5) = 6, \quad \#\mathcal{E}^1(\mathbb{F}_7) = 13.
\]

The conclusion of the above exercise is that \( \text{Fin}(\mathcal{E}) \) has to be a subgroup of both \( \mathcal{E}^1(\mathbb{F}_5) \) and \( \mathcal{E}^1(\mathbb{F}_7) \). However, since 6 and 13 share no common factors there can be no group being a subgroup of both \( \mathcal{E}(\mathbb{F}_5) \) and \( \mathcal{E}(\mathbb{F}_7) \), since the order of a subgroup divides the order of the group (or you could, in this case, argue that since 13 is prime it \( \mathcal{E}(\mathbb{F}_7) \) have no non-trivial subgroups at all). Hence we see that \( \text{Fin}(\mathcal{E}) \) has to be \( \{0\} \).

Therefore, reduction modulo primes can tell us very much on the structure of the characteristic zero case, \( \mathcal{E}(\mathbb{Q}) \).

This is a often an extremely viable and fruitful approach in algebraic geometry: proving things in \( \mathbb{F}_p \) (or characteristic \( p \)) where things might be simpler, and hope to be able to “lift” the result to characteristic zero (\( \mathbb{C} \), for instance) where the actual geometry lives.

Below is another indication of the power of this approach.

4. **ZETA FUNCTIONS AND THE WEIL CONJECTURES**

This ending section, being both the end of this home assignment and the end of the course, should simply be thought of as an orientation to something that every mathematician should have seen at least once in his or her lifetime. Thus there are no exercises here.

In the 1930’s and 1940’s, primarily when being in prison for desertion, André Weil studied the number of solutions to systems of polynomial equations over finite fields, or in
the terminology of algebraic geometry, the number of points of varieties defined over finite fields. In this study he made some remarkable and very deep conjectures concerning this number of points.

But let us take it from the beginning. Put \( \mathcal{F} := \{ F_i(z) \in \mathbb{F}_p[z] \mid i \in I \} \) where \( I \) is some (finite, say) index set and \( z = (z_1, \ldots, z_n) \) indeterminates.

Recall that if all the \( F_i \)'s were polynomials over some field \( K \), then the intersection of the zero sets \( Z(F_i) \) in \( \mathbb{A}_K^n \) of all the \( F_i \)'s was the “total zero set”, i.e., the common zeros of all these polynomials in \( \mathbb{A}_K^n \).

In our present case \( K = \mathbb{F}_q \), \( q = p^n \), and so we seek to count
\[
\#Z(\mathcal{F}) = \#( \cap_{i \in I} Z(F_i) ) = \# \{ p \in \mathbb{A}^{\infty}_{\mathbb{F}_q} \mid F_i(p) = 0, \quad \forall i \in I \}.
\]

The way Weil approached this is as follows. Let \( V := Z(\mathcal{F}) \), and introduce the following function (notice the clash of notation, but it can’t be helped; both are classical):
\[
Z(V/\mathbb{F}_q, t) := \exp \left( \sum_{\ell=1}^{\infty} \frac{\#(V(\mathbb{F}_q^\ell)) t^\ell}{\ell} \right),
\]
where \( V(q^\ell) \) denotes the set of \( q^\ell \)-rational points of \( V \), i.e., the set of \( (a_1, \ldots, b_n), a_i \in \mathbb{F}_q \), such that \( F_i(a_1, \ldots, a_n) = 0 \) for all \( F_i \in \mathcal{F} \).

This (generating) function \( Z(V/\mathbb{F}_q, t) \) is called the Hasse–Weil zeta function.

Knowing the zeta function we can recover \( \#(V(\mathbb{F}_q)) \) by
\[
\#(V(\mathbb{F}_q)) = \left. \frac{1}{(\ell-1)!} \frac{d\ell}{dt} \log(Z(V/\mathbb{F}_q^\ell), t) \right|_{t=0}.
\]

Now, in 1949 Weil made the following conjectures concerning this.

**Theorem 4.1** (Weil conjectures). Let \( \mathbb{F}_q \) be a field with \( q \) elements and \( V/\mathbb{F}_q \) a smooth \( n \)-dimensional projective variety (think: zero set in projective space). Then Weil conjectured:

**Rat:** \( Z(V/\mathbb{F}_q, t) \in \mathbb{Q}(t) \), i.e.,
\[
Z(V/\mathbb{F}_q, t) = \frac{K(t)}{L(t)}, \quad K(t), L(t) \in \mathbb{Q}[t];
\]

**Func:** There is an integer \( \varepsilon \) connected to the topology of \( V \) such that
\[
Z(V/\mathbb{F}_q, (q^\ast t)^{-1}) = \pm q^{\frac{\varepsilon}{2}} t^{\frac{\varepsilon}{2}} Z(V/\mathbb{F}_q, t);
\]

**Rie:** There is a factorization
\[
Z(V/\mathbb{F}_q, t) = \frac{K_1(t)K_2(t) \cdots K_{2n-1}(t)}{(1-t)K_2(t) \cdots K_{2n-2}(t)(1-q^\ast t)}, \quad K_i(t) \in \mathbb{Z}[t],
\]
and for each \( 1 \leq i \leq 2n-1 \) there is a factorization over \( \mathbb{C} \) as
\[
K_i(t) = \prod_j (1 - a_{ij} t), \quad \text{with} \quad |a_{ij}| = q^z, \quad a_{ij} \in \mathbb{C}.
\]

The designations **Rat, Func, Rie** refer to the parts “Rationality”, “Functional relation” and “Riemann Hypothesis”.

Weil himself proved the conjectures for elliptic curves and so called **abelian varieties** (higher-dimensional analogues of elliptic curves in that they are varieties with a group structure). In 1960 Bernard Dwork (1923–1998) proved the general rationality conjecture as stated above and within a few years the general functional equation was settled by the joint force of a score of people, most notably Alexander Grothendieck (born 1928; I urge
you to look him up on the internet; he is extremely fascinating!) and Micheal Artin (born 1934).

Then, finally, in 1972, Pierre Deligne (born 1944; look him up also!) proved the last, and hardest part, the Riemann hypothesis for varieties. The reason for calling it a Riemann hypothesis, lies in the fact that

\[
Z(V/\mathbb{F}_q,q^{-s}) = 0 \implies |q^s| = \sqrt{q}, \quad \text{so} \quad \Re(s) = \frac{1}{2}.
\]

This conjecture, now theorem, is one of the absolute deepest results of the last century, connecting algebraic geometry, topology and number theory. A mere mortal like myself will never be able to understand the full depth and profoundness of this theorem (in fact, I don’t know much more than what I’ve here conveyed to you). Hopefully some of you are.