Primer on Finite Fields – Brice Minaud, MPRI 2.12.1

This is a quick summary/cheat sheet on the basics of finite fields, aimed at crypto students. \( \mathbb{P} \) is the set of prime numbers. Elements of \( \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \) are identified with \( \{0, \ldots, n-1\} \). Statements about equality and unicity are up to isomorphism.

Theorem 1. \( \mathbb{Z}_p \) for \( p \in \mathbb{P} \) is a field.

Proof. It suffices to show that non-zero elements are invertible. By Bézout’s identity, given \( x \in \{1, \ldots, p-1\} \), there exist \( y, z \in \mathbb{Z} \) such that \( xy + pz = \gcd(x, p) = 1 \). Hence \( xy = 1 \mod p \). Concretely, \( y \) can be computed using Euclid’s algorithm.

Theorem 2. Let \( \mathbb{F} \) be a finite field. There exist \( p \in \mathbb{P} \) (called the characteristic of \( \mathbb{F} \)) and \( n \in \mathbb{N} \) such that \( |\mathbb{F}| = p^n \).

Proof. Consider the additive subgroup generated by 1. Since \( \mathbb{F} \) is finite, this subgroup is cyclic, so it is isomorphic to \( \mathbb{Z}_k \) for some \( k \in \mathbb{N}^* \). If \( k \not\in \mathbb{P} \), there exist \( a, b \in \mathbb{Z}_k^* \) such that \( ab = 0 \), which implies they are not invertible, a contradiction. So \( k = p \in \mathbb{P} \) and \( \mathbb{F} \) contains \( \mathbb{Z}_p \) as a subfield. Since any field is a vector space over any subfield, it follows that \( |\mathbb{F}| = p^n \) for some \( n \).

Theorem 3. Let \( \mathbb{F} \) be a finite field of characteristic \( p \). The map \( F : x \mapsto x^p \) is an automorphism of \( \mathbb{F} \) over \( \mathbb{Z}_p \) (i.e. it leaves \( \mathbb{Z}_p \) fixed). It is called the Frobenius map.

Proof. The map \( F \) is clearly a morphism for multiplication. It suffices to show that \( (a + b)^p = ap + bp \) for \( a, b \in \mathbb{F} \). This can be done by writing out the expansion of \( (a + b)^p \) with the binomial coefficients, and noticing that all those coefficients vanish in \( \mathbb{Z}_p \), except the first and last.

Theorem 4. For all \( p \in \mathbb{P} \) and \( n \in \mathbb{N} \), there exists a unique field \( \mathbb{F} \) with \( |\mathbb{F}| = p^n \).

Proof. Let \( \mathbb{F} \) be the splitting field over \( \mathbb{Z}_p \) of the polynomial \( P(X) = X^{p^n} - X \). Let \( R \) denote the roots of \( P \) in \( \mathbb{F} \). The key point is that \( R \) is the set of fixed points of an automorphism (namely \( F^n \)), hence it is a field. It follows that \( \mathbb{F} = R \). On the other hand, \( P \) has a derivative of \(-1\), so it has distinct roots, and degree \( p^n \), so \( |R| = p^n \). This shows existence. Unicity essentially follows from the unicity of the splitting field.

Notation. The (unique) field of cardinality \( q = p^n \) is usually denoted by \( \mathbb{F}_q \), sometimes also \( \text{GF}(q) \) (for Galois Field). If \( p \in \mathbb{P} \), \( \mathbb{F}_p = \mathbb{Z}_p \).

Reminder. Let us recall two basic properties of polynomials over any field \( \mathbb{F} \).

- **Euclidian Division.** For all polynomials \( A, B \in \mathbb{F}[X] \) with \( B \neq 0 \), there exist unique polynomials \( Q, R \in \mathbb{F}[X] \) such that \( A = PQ + R \) and \( \deg(R) < \deg(Q) \) or \( R = 0 \). In particular, computing in \( \mathbb{F}[X] \) modulo some polynomial \( P \) amounts to considering the remainders in the division by \( P \).

- **Number of roots.** A corollary of Euclidian division is that \( \alpha \in \mathbb{F} \) is a root of \( P \in \mathbb{F}[X] \) iff \( (X - \alpha) \) divides \( P \). A corollary of the corollary is that the number of roots of a polynomial is upper-bounded by its degree.
Theorem 5. Let $\mathbb{F}$ be a finite field. The multiplicative group $(\mathbb{F}^*, \cdot)$ is cyclic.

Proof. Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ such that $|\mathbb{F}| = p^n - 1$. Let $d$ be a divisor of $k = p^n - 1$. Elements whose order divides $d$ are roots of $X^d - 1$, so there can be at most $d$ of them. This implies there can be at most one cyclic subgroup of order $d$, hence at most $\phi(d)$ elements of order exactly $d$ (where $\phi : d \mapsto |\{k : \gcd(k, d) = 1\}$ is Euler’s totient function). But each one of the $k$ elements of $\mathbb{F}^*$ must have some order $d | k$, and by a standard equality $\sum_{d | k} \phi(d) = k$, so in fact there are exactly $\phi(k)$ elements of order $k = |\mathbb{F}^*|$. \hfill \qed

Corollary 1. Let $\mathbb{F}$ be a finite field of characteristic $p$. Let $\alpha \in \mathbb{F}$ be a generator of the multiplicative group (called a primitive element). Let $P$ be the minimal polynomial of $\alpha$ over $\mathbb{Z}_p$ (monic polynomial of smallest degree in $\mathbb{Z}_p[X]$ such that $P(\alpha) = 0$). Then $\mathbb{F} \sim \mathbb{Z}_p[X]/P$.

Proof. Clearly, $\mathbb{Z}_p(\alpha)$ (the smallest field generated by the elements of $\mathbb{Z}_p$ and $\alpha$) is equal to $\mathbb{F}$. This implies that $\mathbb{F}$ is the splitting field of the minimal polynomial $P$ of $\alpha$. Because a minimal polynomial must be irreducible, this implies $\mathbb{F} \sim \mathbb{Z}_p[X]/P$. \hfill \qed

Thus, every finite field $\mathbb{F}_{p^n}$ can be constructed as $\mathbb{Z}_p[X]/P$, for some irreducible $P \in \mathbb{Z}_p[X]$ of degree $n$. This yields a concrete way to represent elements of $\mathbb{F}_{p^n}$: they are in bijection with the polynomials of $\mathbb{Z}_p[X]$ of degree strictly less than $n$. Field operations can be computed like in $\mathbb{Z}_p[X]$, followed by reduction mod $P$. Inverses can be computed using Euclid’s algorithm.

A few more random facts.

- In practice, $\mathbb{F}_{2^n}$ and $\mathbb{F}_p$ for $p \in \mathbb{P}$ are the most common finite fields in computer science. In $\mathbb{F}_{2^n}$, field operations are especially fast; addition is just a XOR.

- The polynomial $P$ used to represent $\mathbb{F}_{p^n}$ as $\mathbb{Z}_p[X]/P$ is not uniquely determined. Any minimal polynomial of a primitive element will do—and you can expect many, since the polynomial will have degree $n$, and there are $\phi(p^n - 1)$ primitive elements. Polynomials of this form are called primitive. There also exist irreducible polynomials that are not of this form.

- $\mathbb{F}_{p^n}$ is Galois over $\mathbb{Z}_p$. The Galois group is cyclic, generated by the Frobenius map $F$.

- $\mathbb{F}_{p^n}$ contains $\mathbb{F}_{p^d}$ for each $d | n$ as a subfield, and no other subfield. Indeed, $\mathbb{F}_{p^d}$ can be obtained as the fixed points of $F^d$. Conversely, if a subfield has cardinality $p^d$ for some $d$, since $\mathbb{F}_{p^n}$ is a vector space over it, $(p^d)^k = p^n$ for some $k$, so $d | n$. (This can also be seen as a consequence of the fundamental theorem of Galois theory.)

- For any $q = p^n$, $\mathbb{F}_{q^m} \sim \mathbb{F}_q[X]/P$ for some irreducible $P \in \mathbb{F}_q[X]$ of degree $m$ (as was the case for $n = 1$). In particular, $\mathbb{F}_q$ admits irreducible polynomials of every degree.