Finite Fields and Generators

A **field** is simply a set $\mathbb{F}$ which contains numerical elements that are subject to the familiar addition and multiplication operations. Several different types of fields exist; for example, $\mathbb{R}$, the field of real numbers, and $\mathbb{Q}$, the field of rational numbers, or $\mathbb{C}$, the field of complex numbers. A generic field is usually denoted $\mathbb{F}$.

**Finite Fields**

Cryptography utilizes primarily **finite fields**, nearly exclusively composed of integers. The most notable exception to this are the *Gaussian numbers* of the form $a + bi$ which are complex numbers with integer real and imaginary parts. Finite fields are defined as follows:

\[
\begin{align*}
(\mathbb{Z}/n\mathbb{Z}) &= \mathbb{Z}_n \text{ the set of integers modulo } n \\
(\mathbb{Z}/p\mathbb{Z}) &= \mathbb{Z}_p \text{ the set of integers modulo a prime } p
\end{align*}
\]

Since cryptography is concerned with the solution of diophantine equations, the finite fields utilized are primarily integer based, and are denoted by the symbol for the field of integers, $\mathbb{Z}$.

A finite field $\mathbb{F}_n$ contains exactly $n$ elements, of which there are $n - 1$ nonzero elements. An extension of $\mathbb{Z}_n$ is the **multiplicative group** of $\mathbb{Z}_n$, written $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}_n^*$, and consisting of the following elements:

\[a \in \mathbb{Z}_n^* \text{ such that } \gcd(a, n) = 1\]

in other words, $\mathbb{Z}_n^*$ contains the elements coprime to $n$.

Finite fields form an **abelian group** with respect to multiplication, defined by the following properties:

- The product of two nonzero elements is nonzero $(ab = c | c \neq 0)$
- The associative law holds $(ab) c = a (bc)$
- The commutative law holds $(ab = ba)$
- There is an identity element $(I \cdot a = a)$
- Any nonzero element has an inverse $(a \cdot a^{-1} = 1)$
A subscript following the symbol for the field represents the set of integers modulo \( n \), and these integers run from 0 to \( n - 1 \) as represented by the example below

\[
\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}
\]

The multiplicative order of \( \mathbb{Z}_n \) is represented \( \mathbb{Z}_n^* \) and consists of all elements \( a \in \mathbb{Z}_n \) such that \( \gcd(a, n) = 1 \). An example for \( \mathbb{Z}_{12} \) is given below

\[
\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}
\]

If \( p \) is prime, the set \( \mathbb{Z}_p^* \) consists of all integers \( a \) such that \( 1 \leq a \leq p \). For example

<table>
<thead>
<tr>
<th>Composite ( n )</th>
<th>Prime ( p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z}_{11} ) = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}</td>
<td>( \mathbb{Z}_{11}^* ) = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}</td>
</tr>
<tr>
<td>( \mathbb{Z}_{9}^* ) = {1, 2, 4, 5, 7, 8}</td>
<td>( \mathbb{Z}_{11}^* ) = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}</td>
</tr>
</tbody>
</table>

**Generators**

Every finite field has a generator. A generator \( g \) is capable of generating all of the elements in the set \( \mathbb{Z}_n^* \) by exponentiating the generator \( g \mod n \). Assuming \( g \) is a generator of \( \mathbb{Z}_n^* \), then \( \mathbb{Z}_n^* \) contains the elements \( g^i \mod n \) for the range \( 0 \leq i \leq \phi(n) - 1 \). If \( \mathbb{Z}_n^* \) has a generator, then \( \mathbb{Z}_n \) is said to be cyclic.

The total number of generators is given by

\[
\phi(\phi(n))
\]

**Examples**

For \( n = p = 13 \) (Prime)

\[
\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}
\]

\[
\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}
\]

Total number of generators \( \phi(\phi(13)) = \phi(12) = 4 \) generators
Let \( g = 2 \), then \( g = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\} \), \( g = 2 \) is a generator

Since \( g = 2 \) is a generator, check if \( \text{gcd}(i, p - 1) = 1 \)
\[ 2^2 = 4, \quad \text{and} \quad i = 2, \quad \text{gcd}(2, 12) = 2 \neq 1, \quad \text{therefore,} \quad 4 \text{ is not a generator} \]
\[ 2^3 = 8, \quad \text{and} \quad i = 3, \quad \text{gcd}(3, 12) = 3 \neq 1, \quad \text{therefore,} \quad 4 \text{ is not a generator} \]

Let \( g = 6 \), then \( g = \{6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1\} \), \( g = 6 \) is a generator
Let \( g = 7 \), then \( g = \{7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1\} \), \( g = 7 \) is a generator
Let \( g = 11 \), then \( g = \{11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1\} \), \( g = 11 \) is a generator

There are a total of 4 generators, \((2, 6, 7, 11)\) as predicted by the formula \( \phi(\phi(n)) \).

For \( n = 10 \) (Composite)

\[ \mathbb{Z}_n = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \]
\[ \mathbb{Z}_n^* = \{1, 3, 7, 9\} \]

Total number of generators \( \phi(\phi(10)) = \phi(4) = 2 \) generators

Let \( g = 3 \), then \( g = \{3, 9, 7, 1, 3, 9, 7, 1, 3\} \), \( g = 3 \) is a generator
Let \( g = 7 \), then \( g = \{7, 9, 3, 1, 7, 9, 3, 1, 7\} \), \( g = 7 \) is a generator

There are a total of 2 generators \((3, 7, )\) as predicted by the formula \( \phi(\phi(n)) \).