6.857 R01 Notes
Spring 2016

1 Intro
These are the notes for the first recitation of 6.857. They borrow heavily from Prof. Rivest’s past 6.857 lecture notes on finite fields.

2 Groups and Finite Fields
This section will deal with groups and fields.

2.1 Groups
Definition 1 A group is a set $G$ equipped with a function $\cdot : G \times G \to G$ (i.e. for $a,b$ in $G$, $a \cdot b$ is also in $G$; sometimes we just write $ab$ instead of $a \cdot b$) such that the following properties hold:

- $\forall a,b,c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- There exists an identity element $e \in G$ such that $\forall a \in G : a \cdot e = e \cdot a = a$
- $\forall a \in G, \exists$ an inverse $a' \in G$ such that: $a \cdot a' = a' \cdot a = e$

In addition, if for all $a,b$ in $G$ it is true that $ab = ba$, then we call $G$ a commutative (or abelian) group.

It is easy to prove that the identity element $e$ is unique. Also, $\forall a \in G$ the inverse $a'$ is also unique (Hint: use proof by contradiction)

2.2 Finite Fields
Definition 2 A finite field $F$ is a system $(S, +, \cdot)$ where $S$ is a finite set and $+, \cdot$ are binary operations on $S$, such that the following properties hold:

- $(S, +)$ is an abelian group with 0 being the identity element. Therefore:
• ∀ \(a,b,c \in S\) : \((a+b)+c=a+(b+c)\)
• ∀ \(a \in S\) : \(a+0=0+a=a\)
• ∀ \(a \in S\), \(\exists\) an inverse \((-a) \in G\) such that: \(a+(-a)=(-a)+a=0\)
• ∀ \(a,b \in S\) : \(a+b=b+a\)

**In addition** (here \(S^* = S - 0\)):
• \((S^*, ·)\) is an abelian group with \(1\) being the identity element.
• ∀ \(a,b,c \in S\) : \((a \cdot b) \cdot c=a \cdot (b \cdot c)\)
• ∀ \(a \in S\) : \(a \cdot 1=1 \cdot a=a\)
• ∀ \(a \in S^*\), \(\exists\) an inverse \(a^{-1} \in G\) such that: \(a \cdot a^{-1}=a^{-1} \cdot a=1\)
• ∀ \(a,b \in S\) : \(a \cdot b=b \cdot a\)

**Finally:**
• ∀ \(a,b,c \in S\) : \((a+b) \cdot c=a \cdot c+b \cdot c\)

It can be proven using the properties of fields that \(0 \cdot g = g \cdot 0 = 0\) for all \(g \in F\).

A simple example of a finite field is \(\mathbb{Z}_2 = \{0, 1\}\). Addition in this field is just XOR (i.e. \(0 + 0 = 1 + 1 = 0\) and \(1 + 0 = 0 + 1 = 1\)). Multiplication is like AND (i.e \(1 \cdot 1 = 1\) and \(0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0\)). You can check that all the properties of finite fields are satisfied in \(\mathbb{Z}_2\).

Another example of a finite field is \(\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}\) which is the set of residues modulo a prime number \(p\).

Solving linear equations in finite fields is very intuitive.

Specifically if we want to solve \(a \cdot x + b = 0\) where \(a \neq 0\) then we proceed as follows:

\[
a \cdot x + b = 0 \Rightarrow (a \cdot x + b) + (-b) = 0 + (-b) = -b \Rightarrow a \cdot x + (b + (-b)) = -b \Rightarrow a \cdot x + 0 = -b \Rightarrow a \cdot x = -b \Rightarrow a^{-1}(a \cdot x) = a^{-1}(-b) \Rightarrow (a^{-1}a) \cdot x = a^{-1}(-b) \Rightarrow 1 \cdot x = a^{-1}(-b) \Rightarrow x = a^{-1}(-b)
\]

which is what one would expect.
2.3 Existence of Finite Fields

Theorem 1 (Galois) For all primes $p$ and for all positive integers $n$ there exists a unique finite field with $p^n$ elements.

We call this field $GF(p^n)$. Of special interest to cryptography is the case where $p=2$. The field $GF(2^8)$ is used in the Advanced Encryption Standard (to be covered later in the term).

Next, we describe what $GF(2^k)$ looks like for general $k$.

Definition 3 $GF(2^k) = \{a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + a_0 : a_i \in \mathbb{Z}_2\}$ where $\mathbb{Z}_2 = \{0, 1\}$ is the finite field with 2 elements.

Each element in $GF(2^k)$ is simply a polynomial of degree $\leq k - 1$ with coefficients in $\mathbb{Z}_2 = \{0, 1\}$. We can represent an element $g = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + a_0$ in $GF(2^k)$ simply by its coefficients. I.e. we can write $g = a_{k-1}a_{k-2}...a_1a_0$.

A simple example is $GF(2^2) = \{0, 1, x, x + 1\}$

2.4 Addition in $GF(2^k)$

Addition in $GF(2^k)$ is simply the addition of the coefficients of the respective polynomials. For example, in $GF(2^2)$ we get $(x + 1) + x = 1$ (using the coefficient notation this can be written as $11 + 10 = 01$ which is bitwise XOR). Therefore the additive inverse of any element $g$ in $GF(2^k)$ is $g$ itself (because $g + g = 0$; check this yourself as an exercise).

2.5 Multiplication in $GF(2^k)$

Multiplication in $GF(2^k)$ involves two steps. The first step is to multiply the two polynomials normally using $\mathbb{Z}_2$ arithmetic. The resulting polynomial may have degree $\geq k$ which is obviously not an element of $GF(2^k)$. We must then divide by an irreducible polynomial of degree $k$ and the result will then be an element of $GF(2^k)$.

For example, in $GF(2^2)$, the irreducible polynomial we use is $x^2 + x + 1$. Therefore $(x + 1) \cdot (x + 1) = (x^2 + 1)mod(x^2 + x + 1) = x$. In $GF(2^8)$ the irreducible polynomial we use in the AES is $x^8 + x^4 + x^3 + x + 1$. 
3 Fermat’s Theorem for Finite Fields

Theorem 2 For all elements $g$ in a finite field $F$ (where $F$ has $n$ elements) the following equalities hold:

- $g + g + g + ... + g = 0$
  \( \underbrace{n \text{ times}} \)

- $g \cdot g \cdot g \cdot ... \cdot g = 1$ when $g \neq 0$
  \( \underbrace{n - 1 \text{ times}} \)