Massachusetts Institute of Technology
6.857: Applied Cryptography and Security
Professors Ronald L. Rivest and Yael Tauman Kalai

Recitation 1
Feburary 4, 2022
TA: Lucas Camelo Sá

Recitation 1: Finite Fields

1 Fields: introduction

Definition 1.1 (Operation)**.** A binary *operation* on a set F is any function $g : F \times F \to F$.

In other words, operations map each pair of elements from F to a third element. This is just a more formal definition of our traditional understanding of an arithmetic operation: addition maps $(3, 2)$ to 5, multiplication maps $(3, 2)$ to 6, etc.

As a matter of fact, fields are (informally) sets coupled with operations that behave analogously to addition and multiplication. This structure enables us to perform sequences of invertible arithmetic operations on the underlying set – which we will eventually use for our cryptographic purposes.

Definition 1.2 (Field)**.** A *field* is a triple $(F, +, *)$ of an arbitrary *set* F coupled with two operations $+$ (*addition*) and $*$ (*multiplication*), which together satisfy:

1. **(Associativity):** $(a + b) + c = a + (b + c)$ and $(a * b) * c = a * (b * c)$ for every $a, b, c \in F$.
2. **(Commutativity):** $a + b = b + a$ and $a * b = b * a$ for every $a, b \in F$.
3. **(Identity elements):** There exist elements 0 and 1 such that $a + 0 = a$ and $a * 1 = a$ for every $a \in F$.
4. **(Additive inverses):** For any $a \in F$, there exists an element $-a \in F$ such that $a + (-a) = 0$.
5. **(Multiplicative inverses):** For any $a \neq 0 \in F$, there exists an element $a^{-1} \in F$ such that $a * a^{-1} = 1$.
6. **(Distribution law):** $(a + b) * c = a * c + b * c$ for every $a, b, c \in F$.

Examples $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$**.** The sets of rational, real, and complex numbers – coupled with their standard operations of addition/multiplication – are fields (verify this!).

The number of elements of a field is called its *order*. For the rest of the handout, we will work on finite fields (i.e., fields of finite order n). Alternatively, these are called *Galois Fields*.

Property 1.1 (Order of a field)**.** *Let F be a field of order n – then, n is the power of a prime. In other words, there exists a prime number p and integer m such that $n = p^m$.*

Property 1.2 (Uniqueness)**.** *For each prime number p and positive integer m, there exists a unique field of order p^m. This is referred to as $GF(p^m)$, the Galois Field of order p^m.*

Exercises. These exercises can be solved by combining the properties of a field.

1. Show that $0 * a = 0$ for every $a \in F$.
2. Show that if $ab = 0$, then either $a = 0$ or $b = 0$.
3. Show that the inverse of each element is unique (addition and multiplication separately).
4. Let F be a finite field of order n. Show that there exists $m \leq n$ such that $m \times 1 = 0$ (i.e., 1 summed to itself m times). Then show that $m \times a = 0$ for every $a \in F$.
5. (Fermat's little theorem*). If a field F has order n, then $a^{n-1} = 1$ for every $a \neq 0$ in F.

2 Constructing a Field

2.1 Fields of order p

GF(p) = $\mathbb{Z}_p$, i.e., the field of order p, is the field of remainder classes modulo p. Recall from modular arithmetic, that every non-zero remainder modulo p has an inverse. This is not true for remainder classes modulo n, where n is composite. So constructing fields of size p^m $(m > 1)$ will require more work.

2.2 Fields of order p^m

Recall the definition of a real-valued polynomial $P(x)$: it is a function $P(x)$ that maps x to $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_n, a_{n-1}, \cdots, a_1, a_0$ are P's coefficients and n is its degree.

Definition 2.1 (Polynomial ring)**.** Let F be a field. $F[X]$ is the set of all polynomials with coefficients in F.

Because F is a field, we can add and multiply polynomials in $F(x)$ just like we would with regular polynomials. More than that: we can perform polynomial division!

Example. Consider the following polynomials in $\mathbb{Z}_2[X]$ (i.e., coefficients are the binary remainders modulo 2): $H(x) = x^2 + x + 1$ and $Q(x) = x^2 + 1$. Then $H(x) + Q(x) = 2x^2 + x + 2 = x$ and $H(x)Q(x) = x^4 + x^3 + 2x^2 + x + 1 = x^4 + x^3 + x + 1$ (recall that $0 \equiv 2$ in $\mathbb{Z}_2$).

Division of polynomials. Let P and H be polynomials with coefficients in F. Then, there exist unique polynomials Q, R in $F[x]$, with R's degree strictly less than H's, such that:

$$P(x) = H(x)Q(x) + R(x)$$

Q and R are called quotient and remainder, respectively. Because of this, we can now view polynomials modulo H, just as we did in modular arithmetic.

Constructing a field. $(GF(p^m))$ Let H be an irreducible polynomial in $\mathbb{Z}_p(X)$ of degree m. Then the set of polynomials modulo H is a finite field of order p^m.

Example. Again in $\mathbb{Z}_2$, consider the irreducible polynomial $F(x) = x^8 + x^4 + x^3 + x + 1$. GL($2^8$) consists of polynomials from $\mathbb{Z}_2[X]$ modulo F. Let $H(x) = x^5 + x^3$ and $Q(x) = x^5 + x^2$. Then $H(x) + Q(x) = x^3 + x^2$ and $H(x)Q(x) = x^{10} + x^8 + x^7 + x^5 = x^2 F(x) + x^8 + x^7 - x^6 - x^3 - x^2 = x^8 + x^7 + x^6 + x^3 + x^2$.

If you think of the elements of GF(2^8) as binary vectors, this results in a procedure to add and multiply 8-bit vectors (and obtain other 8-bit vectors). Multiplication and addition work just like for real numbers, but without carrying. In particular, addition is equivalent to bitwise-xor.

Example. Add and multiply 00001110 and 00100100 in GF(2^8).
Answer. Sum: 00101010. Product: 111001110.