Lecture 4: Finite Fields (PART 1)

PART 1: Groups, Rings, and Fields

Theoretical Underpinnings of Modern Cryptography

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

January 23, 2017
11:29pm

Goals:

- To answer the question: Why study finite fields?
- To review the concepts of groups, rings, integral domains, and fields

CONTENTS

4.1: WHY STUDY FINITE FIELDS?

- It is almost impossible to fully understand practically any facet of modern cryptography and several important aspects of general computer security if you do not know what is meant by a finite field.

- For example, without understanding the notion of a finite field, you will not be able to understand AES (Advanced Encryption Standard) that we will take up in Lecture 8. As you will recall from Lecture 3, AES is supposed to be a modern replacement for DES. The substitution step in AES is based on the concept of a multiplicative inverse in a finite field.

- For another example, without understanding finite fields, you will NOT be able to understand the derivation of the RSA algorithm for public-key cryptography that we will take up in Lecture 12.

- And if you do not understand the basics of public-key cryptography, you will not be able to understand the workings of several modern protocols (like the SSH protocol you use everyday for

logging into other computers) for secure communications over networks. You will also not be able to understand what has become so important in computer security — *user and document authentication with certificates*.

- Another modern concept that will befuddle you if you do not understand public key cryptography is that of *digital rights management*. And, as I mentioned earlier, you cannot understand public key cryptography without coming to terms with finite fields.

- For yet another example, without understanding finite fields, you will never understand the up and coming ECC algorithm (ECC stands for Elliptic Curve Cryptography) that is already in much use and that many consider to be a replacement for RSA for public key cryptography. We will take up ECC in Lecture 14.

- As you yourself can see, if you do not understand the concepts in this and the next three lectures, you might as well give up on learning computer and network security.

- To put it very simply, a finite field is a finite set of numbers in which you can carry out the operations of addition, subtraction, multiplication, and division without error. In ordinary computing, division particularly is error prone and what you see is

a high-precision approximation to the true result. Such high-precision approximations do not suffice for cryptography work. All arithmetic operations must work without error for cryptography.

- The stepping stones to understanding the concept of a finite field are:

  1. *set*
  2. *group*
  3. *abelian group*
  4. *ring*
  5. *commutative ring*
  6. *integral domain*
  7. *field*

- In the next section, we start with the notions of *set* and *group*.

4.2: WHAT DOES IT TAKE FOR A SET OF OBJECTS TO FORM A GROUP?

A set of objects, along with a binary operation (meaning an operation that is applied to two objects at a time) on the elements of the set, must satisfy the following four properties if the set wants to be called a group:

- **Closure** with respect to the operation. Closure means that if a and b are in the set, then the element $a \circ b \;=\; c$ is also in the set. The symbol $\circ$ denotes the operator for the desired operation.

- **Associativity** with respect to the operation. Associativity means that $(a \circ b) \circ c \;=\; a \circ (b \circ c)$.

- Guaranteed existence of a unique **identity element** with regard to the operation. An element i would be called an identity element if for every a in the set, we have $a \circ i \;=\; a$.

- The existence of an **inverse element** for each element with regard to the operation. That is, for every a in the set, the set

must also contain an element b such that $a \circ b = i$ assuming that i is the identity element.

- In general, a group is denoted by $\{G, \circ\}$ where G is the set of objects and $\circ$ the operator.

- For reasons that will become clear later, even more frequently, we use the notation $\{G, +\}$ for a group. That is, instead of denoting the group operator as '$\circ$', we may denote it by '$+$' even when the operator has nothing whatsoever to do with arithmetic addition.

4.2.1: Infinite Groups vs. Finite Groups (Permutation Groups)

- Infinite groups, meaning groups based on sets of infinite size, are rather easy to imagine. For example:

  – The set of all integers — positive, negative, and zero — along with the operation of arithmetic addition constitutes a group.

  – For a given value of N, the set of all $N \times N$ matrices over real numbers under the operation of matrix addition constitutes a group.

  – The set of all **even** integers — positive, negative, and zero — under the operation of arithmetic addition is a group. [Interesting, isn't it, that zero belongs to the set of even integers. How would you justify it to yourself?]

  – The set of all 3×3 nonsingular matrices, along with the matrix multiplication as the operator, forms a group. [**This group, denoted $GL(3)$, plays a very important role in computer graphics and computer vision. GL stands for 'General Linear'.**]

- But what about finite groups?

- As you will see, it takes a bit of mental effort to conjure up finite groups. The goal of this and the next two subsections is to illustrate a finite group — just to point out that such things do exist. [As you'll see in the lectures that follow, the concept of a "finite group" is particularly importat to us since finte fields are based on finte groups.]

- Let $s_n = <1, 2, ..., n>$ denote a *sequence* of integers 1 through n. [Note that the order in which the items appear in a sequence is important. A sequence is typically shown delimited by angle brackets, as in the definition of s_n.]

- Let's now consider the *set of all permutations* of the sequence s_n. **Denote this set by P_n.** Each element of the set P_n stands for a permutation $<p_1, p_2, p_3, ..., p_n>$ of the sequence s_n. [What is the size of the set P_n? Answer: $n!$ In general, given a set of n distinct labels, the total number of permutations of the n labels is $n!$. Can you justify this answer?]

- Consider, for example, the case when $s_3 = <1, 2, 3>$. In this case, the set of permutations of the sequence s_3 is given by $P_3 = \{<1, 2, 3>, <1, 3, 2>, <2, 1, 3>, <2, 3, 1>, <3, 1, 2>, <3, 2, 1>\}$. The set P_3 is of size 6. A highbrow way of saying the same thing is that the **cardinality** of P_3 is 6.

- Now let the binary operation on the elements of P_n be that of *composition of permutations*. We will denote a composition of two permutations by the symbol $\circ$. For any two elements ρ and π of the set P_n, the composition $\pi \circ \rho$ **means that we**

want to re-permute the elements of ρ according to the elements of π. The next page explains this operation with the help of an example.

4.2.2: An Example That Illustrates the Binary Operation of Composition of Two Permutations

- Let's go back to the example in which the starting sequence is given by $s_3 = <1, 2, 3>$.

- As already shown, each element of P_3 is a distinct permutation of the three integers in s_3. That is,

$$P_3 \;=\; \{\; <p_1, p_2, p_3> \;\mid\; p_1, p_2, p_3 \in s_3 \;\; with \;\; p_1 \neq p_2 \neq p_3 \;\}$$

- Consider the following two elements π and ρ in the set P_3 of permutations:

$$\begin{aligned} \pi &= < 3, 2, 1 > \\ \rho &= < 1, 3, 2 > \end{aligned}$$

- Let's now consider the following composition of the two permutations π and ρ:

$$\pi \circ \rho \;=\; <3, 2, 1> \;\circ\; <1, 3, 2>$$

What that means is to permute ρ according to the elements of π. For our example, that is accomplished by first choosing the

third element of ρ, followed by the second element of ρ, followed finally by the first element of ρ. The result is the permutation $<2, 3, 1>$. So we say

$$\pi \circ \rho \;\; = \;\; <3, 2, 1> \;\circ\; <1, 3, 2> \;\; = \;\; <2, 3, 1>$$

Therefore, the composition of the two permutations $<3, 2, 1>$ and $<1, 3, 2>$ is the permutation $<2, 3, 1>$.

- Clearly, $\pi \circ \rho \;\in\; P_3$.

- This shows that P_3 **closed** with respect to the operation of composition of two permutations.

4.2.3: What About the Other Three Conditions that P_3 Must Satisfy If It is a Group?

- Since it is a small enough set, we can also easily demonstrate that P_3 obeys the associativity property with respect to the composition-of-permutations operator. This we can do by showing that for any three elements ρ_1, ρ_2, and ρ_3 of the set P_3, the following will always be true

$$\rho_1 \circ (\rho_2 \circ \rho_3) \;\; = \;\; (\rho_1 \circ \rho_2) \circ \rho_3$$

- The set P_3 obviously contains a special element $<1,2,3>$ that can serve as the identity element with respect to the composition-of-permutations operator. It is definitely the case that for any $\rho \in P_3$ we have

$$<1,2,3> \;\circ\; \rho \;\; = \;\; \rho \;\circ\; <1,2,3> \;\; = \;\; \rho$$

- Again, because P_3 is a small sized set, we can easily demonstrate that for every $\rho \in P_3$ there exists another unique element $\pi \in P_3$ such that

$$\rho \circ \pi \;\; = \;\; \pi \circ \rho \;\; = \;\; \textit{the identity element}$$

For each ρ, we may refer to such a π as ρ's inverse. For the sake of convenience, we may use the notation $-\rho$ for such a π.

- Obviously, then, P_3 along with the *composition-of-permutations* operator is a group.

- Note that the set P_n of all permutations of the starting sequence s_n can only be finite. As a result, P_n along with the operation of composition as denoted by '$\circ$' forms a **finite group**.

- The set P_n of permutations along with the composition-of-permutations operator is referred to as a **permutation group**.

4.3: ABELIAN GROUPS AND THE GROUP NOTATION

- If the operation on the set elements is **commutative**, the group is called an **abelian group**. An operation $\circ$ is commutative if $a \circ b \;=\; b \circ a$.

- Is $\{S_n, \circ\}$ as defined in Section 4.2.2 an abelian group? If not for n in general, is $\{S_n, \circ\}$ an abelian group for any particular value of n? [S_n is abelian for only $n = 2$.]

- Is the set of all integers, positive, negative, and zero, along with the operation of arithmetic addition an abelian group? [The answer is yes.]

- Earlier I mentioned that a group is generally denoted by $\{G, \circ\}$, where G denotes the set and $\circ$ the group operator. I also mentioned earlier that, frequently, a group is also denoted by $\{G, +\}$, where '+' represents the group operator. [As to why we may want to denote the group operator by the symbol '+' will become clear when we introduce the notion of rings.]

- In keeping with the notation $\{G, +\}$ for a group, the group operator is commonly referred to as *addition*, even when the actual operation carried out on the set elements bears no resemblance to arithmetic addition as you know it.

- **IMPORTANT**: When a group is denoted $\{G, +\}$, it is common to use the symbol '0' for denoting the group identity element.

4.3.1: If the Group Operation is Referred to as Addition, then the Group Also Allows for Subtraction

- As you are well aware by now, a group is guaranteed to have a special element called the identity element. **As mentioned in the previous subsection, the identity element of a group is frequently denoted by the symbol** 0**.**

- As you now know, for every element ρ_1, the group must contain its inverse element ρ_2 such that

$$\rho_1 \;+\; \rho_2 \;\;=\;\; 0$$

  where the operator '+' is the group operator.

- So if we maintain the illusion that we want to refer to the group operation as addition, we can think of ρ_2 in the above equation as the **additive inverse** of ρ_1 and even denote it by $-\rho_1$. We can therefore write

$$\rho_1 \;+\; (-\rho_1) \;\;=\;\; 0$$

  or more compactly as $\rho_1 \;-\; \rho_1 \;\;=\;\; 0.$

- In general

$$\rho_1 \;-\; \rho_2 \;\;=\;\; \rho_1 \;+\; (-\rho_2)$$

where $-\rho_2$ is the additive inverse of ρ_2 with respect to the group operator $+$. **We may now refer to an expression of the sort $\rho_1 \;-\; \rho_2$ as representing subtraction.**

4.4: RINGS

- If we can define one more operation on an **abelian group**, we have a **ring**, provided the elements of the set satisfy some properties with respect to this new operation also.

- Just to set it apart from the operation defined for the abelian group, we will refer to the new operation as *multiplication*. **Note that the use of the name 'multiplication' for the new operation is merely a notational convenience.**

- A ring is typically denoted $\{R, +, \times\}$ where R denotes the set of objects, '+' the operator with respect to which R is an abelian group, the '$\times$' the additional operator needed for R to form a ring.

4.4.1: Rings: Properties of the Elements with Respect to the Ring Operator

- R must be **closed** with respect to the additional operator '$\times$'.

- R must exhibit **associativity** with respect to the additional operator '$\times$'.

- The additional operator (that is, the "multiplication operator") must **distribute** over the group addition operator. That is

$$\begin{aligned} a \times (b + c) &= a \times b + a \times c \\ (a + b) \times c &= a \times c + b \times c \end{aligned}$$

- The "multiplication" operation is frequently shown by just concatenation in such equations:

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}$$

4.4.2: Examples of Rings

- For a given value of N, the set of all $N \times N$ square matrices over the real numbers under the operations of **matrix addition** and **matrix multiplication** constitutes a **ring**.

- The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication is a **ring**.

- The set of **all integers** under the operations of arithmetic addition and multiplication is a **ring**.

- The set of **all real numbers** under the operations of arithmetic addition and multiplication is a **ring**.

4.4.3: Commutative Rings

- A **ring** is **commutative** if the **multiplication operation** is commutative for all elements in the ring. That is, if all a and b in R satisfy the property

$$ab \;=\; ba$$

- Examples of a **commutative ring**:

  - The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication.

  - The set of **all integers** under the operations of arithmetic addition and multiplication.

  - The set of **all real numbers** under the operations of arithmetic addition and multiplication.

4.5: INTEGRAL DOMAIN

An **integral domain** $\{R, +, \times\}$ is a **commutative ring** that obeys the following two additional properties:

- **ADDITIONAL PROPERTY 1:** The set R must include an **identity element** for the **multiplicative operation**. That is, it should be possible to symbolically designate an element of the set R as '1' so that for every element a of the set we can say

$$a1 \;=\; 1a \;=\; a$$

- **ADDITIONAL PROPERTY 2:** Let 0 denote the identity element for the **addition operation**. If a multiplication of any two elements a and b of R results in 0, that is if

$$ab \;=\; 0$$

  then either a or b **must be** 0.

- Examples of an **integral domain**:

  – The set of **all integers** under the operations of arithmetic addition and multiplication.

– The set of **all real numbers** under the operations of arithmetic addition and multiplication.

4.6: FIELDS

A **field**, denoted $\{F, +, \times\}$, is an **integral domain** whose elements satisfy the following additional property:

- For **every element** a in F, except the element designated 0 (which is the identity element for the '+' operator), there must also exist in F its **multiplicative inverse**. That is, if $a \in F$ and $a \neq 0$, then there must exist an element $b \in F$ such that

$$ab \;=\; ba \;=\; 1$$

  where '1' symbolically denotes the element which serves as the identity element for the multiplication operation. For a given a, such a b is often designated a^{-1}.

- Note again that a field has a multiplicative inverse for every element except the element that serves as the identity element for the group operator.

4.6.1: Positive and Negative Examples of Fields

- The set of **all real numbers** under the operations of arithmetic addition and multiplication **is** a **field**.

- The set of **all rational numbers** under the operations of arithmetic addition and multiplication **is** a **field**.

- The set of **all complex numbers** under the operations of complex arithmetic addition and multiplication **is** a **field**.

- The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication is **NOT** a **field**.

- The set of **all integers** under the operations of arithmetic addition and multiplication is **NOT** a **field**.

4.7: HOMEWORK PROBLEMS

1. When does a set become a group?

2. What is the 0 element for the permutation group defined over N objects? Note that the 0 element is the identity element for the group operator, usually denoted '+'.

3. What is an example of an infinite group?

4. If the group operator is referred to as "addition", then the group also allows for "subtraction." What do we mean by that?

5. When does a group become a ring?

6. What is the most elementary reason for the fact that the set of all possible permutations over N objects along with the permutation operator is not a ring?

7. For a given N, the set of all square $N \times N$ matrices of real numbers is a ring, the group operator being matrix addition and the additional ring operator being matrix multiplication. Why can this ring not be an integral domain?

8. What does a field have that an integral domain does not?

9. What is a good notation for a field? Explain your notation.

10. Does a field contain a multiplicative inverse for every element of the field?