

CYB650

Introduction to Cryptography

Foundations and principles of Cryptography



Prepared by Dr. Esraa Saleh Alomari
Lecture #2



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

The Part 2 of the module 1 which is (Lecture 2) covers the basics of Foundations and principles of Cryptography (Number Theory) are as follows:

- *Divisibility and The Division Algorithm*
- *The Euclidean Algorithm*
- *Modular Arithmetic*
- *Groups, Rings, and Fields*
- *Finite Fields of the Form $GF(p)$*
- *Polynomial Arithmetic*
- *Finite Fields of the Form $GF(2^n)$*

Divisibility

- We say that a nonzero b **divides** a if $a = mb$ for some m , where a, b , and m are integers
- That is, b divides a if there is no remainder on division.
- The notation $b \mid a$ is commonly used to mean b divides a . Also, if $b \mid a$, we say that b is a **divisor** of a .

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
 $13 \mid 182$; $-5 \mid 30$; $17 \mid 289$; $-3 \mid 33$; $17 \mid 0$

➤ Subsequently, we will need some simple properties of divisibility for integers,

which are as follows:

- If $a \mid 1$, then $a = \pm 1$.
- If $a \mid b$ and $b \mid a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a \mid b$ and $b \mid c$, then $a \mid c$:

$$11 \mid 66 \text{ and } 66 \mid 198 = 11 \mid 198$$

- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n .

To see this last point, note that

- If $b|g$, then g is of the form $g = b \times g_1$ for some integer g_1 .
- If $b|h$, then h is of the form $h = b \times h_1$ for some integer h_1 .

So

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$$

and therefore b divides $mg + nh$.

$7 \mid 14$ and $7 \mid 63$.

To show $7 \mid (3 \times 14 + 2 \times 63)$,

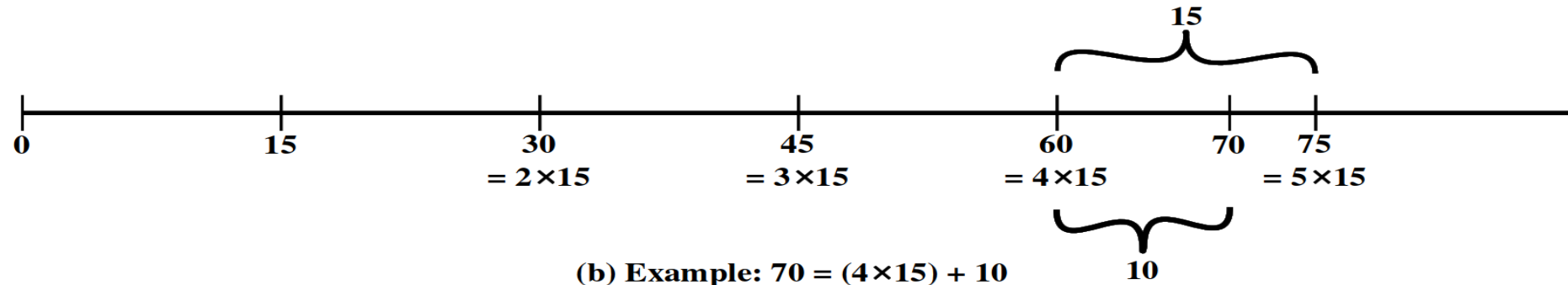
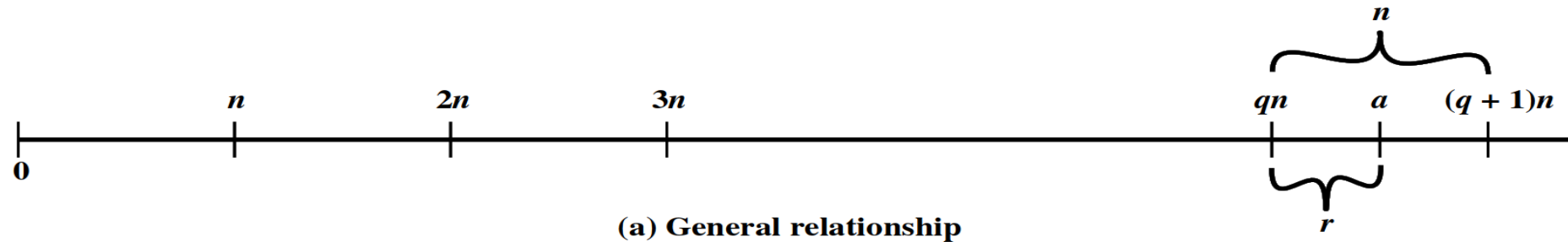
we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$,

and it is obvious that $7 \mid (7(3 \times 2 + 2 \times 9))$.

Given any positive integer n and any nonnegative integer a , if we divide a by n , we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \quad 0 \leq r < n; q = \lfloor a/n \rfloor$$

The Division Algorithm



Fig

Relationship $a = qn + r; 0 \leq r < n$

The Division Algorithm

where $|x|$ is the largest integer less than or equal to x . Equation is referred to as the division algorithm.

Figure demonstrates that, given a and positive n , it is always possible to find q and r that satisfy the preceding relationship. Represent the integers on the number line; a will fall somewhere on that line (positive a is shown, a similar demonstration can be made for negative a). Starting at 0, proceed to n , $2n$, up to qn , such that $qn \leq a$ and $(q + 1)n > a$. The distance from qn to a is r , and we have found the unique values of q and r . The remainder r is often referred to as a **residue**.

$$\begin{aligned} a = 11; \quad n = 7; \quad 11 &= 1 \times 7 + 4; & r = 4 \quad q = 1 \\ a = -11; \quad n = 7; \quad -11 &= (-2) \times 7 + 3; & r = 3 \quad q = -2 \end{aligned}$$

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. First, we need a simple definition: Two integers are **relatively prime** if their only common positive integer factor is 1.

Greatest Common Divisor

Recall that nonzero b is defined to be a divisor of a if $a = mb$ for some m , where a , b , and m are integers. We will use the notation $\gcd(a, b)$ to mean the greatest common divisor of a and b . The greatest common divisor of a and b is the largest integer that divides both a and b . We also define $\gcd(0,$

$0) = 0$.

More formally, the positive integer c is said to be the greatest common divisor of a and b if:

1. c is a divisor of a and of b .
2. Any divisor of a and b is a divisor of c . An equivalent definition is the following:

The Euclidean Algorithm

$$\gcd(a, b) = \max[k, \text{such that } k \mid a \text{ and } k \mid b]$$

Because we require that the greatest common divisor be positive, $\gcd(a, b)$

$$= \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b).$$

In general, $\gcd(a, b) = \gcd(|a|, |b|)$.

$$\gcd(60, 24) = \gcd(60, -24) = 12$$

Also, because all nonzero integers divide 0, we have $\gcd(a, 0) = |a|$.

We stated that two integers a and b are relatively prime if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if $\gcd(a, b) = 1$.

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Finding the Greatest Common Divisor

We now describe an algorithm credited to Euclid for easily finding the greatest common divisor of two integers. This algorithm has significance subsequently in this chapter. Suppose we have integers a, b such that $d = \gcd(a, b)$. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming $a \geq b > 0$. Now dividing a by b and applying the division algorithm, we can state:

The Euclidean Algorithm

$$a = q_1b + r_1 \quad 0 \leq r_1 < b$$

If it happens that $r_1 = 0$, then $b \mid a$ and $d = \gcd(a, b) = b$. But if $r_1 \neq 0$, we can state that $d \mid r_1$. This is due to the basic properties of divisibility: the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - q_1b)$, which is the same as $d \mid r_1$. Before proceeding with the Euclidian algorithm, **We Need to answer this question** What is the $\gcd(b, r_1)$? We know that $d \mid b$ and $d \mid r_1$. Now take any arbitrary integer c that divides both b and r_1 . Therefore, $c \mid (q_1b + r_1) = a$. Because c divides both a and b , we must have $c \leq d$, which is the greatest common divisor of a and b . Therefore $d = \gcd(b, r_1)$.

Let us now return to Equation (4.2) and assume that $r_1 \neq 0$. Because $b > r_1$, we can divide b by r_1 and apply the division algorithm to obtain:

$$b = q_2r_1 + r_2 \quad 0 \leq r_2 < r_1$$

The Euclidean Algorithm

stage where r_{n-1} is divided by r_n . The result is the following system of equations:

$$\left. \begin{array}{ll} a = q_1b + r_1 & 0 < r_1 < b \\ b = q_2r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3r_2 + r_3 & 0 < r_3 < r_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ r_{n-2} = q_nr_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1}r_n + 0 & \\ d = \gcd(a, b) = r_n & \end{array} \right\}$$

At each iteration, we have $d = \gcd(r_i, r_{i+1})$ until finally $d = \gcd(r_n, 0) = r_n$. Thus, we can find the greatest common divisor of two integers by repetitive application of the division algorithm. This scheme is known as the Euclidean algorithm.

We have essentially argued from the top down that the final result is the $\gcd(a, b)$. We can also argue from the bottom up. The first step is to show that r_n divides a and b . It follows from the last division in Equation (4.3) that r_n divides r_{n-1} . The next to last division shows that r_n divides r_{n-2} because it divides both terms on the right. Successively, one sees that r_n divides all r_i 's and finally a and b .

If we take any arbitrary integer that divides a and b , it must also divide r_1 , as explained previously. We can follow the sequence of equations in Equation down and show that c must divide all r_i 's. Therefore c must divide r_n , so that $r_n = \gcd(a, b)$.

The Euclidean Algorithm

Let us now look at an example with relatively large numbers to see the power of this algorithm:

To find $d = \gcd(a,b) = \gcd(1160718174, 316258250)$		
$a = q_1b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	211943424)
$b = q_2r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	104314826)
$r_1 = q_3r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	3313772)
$r_2 = q_4r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	1587894)
$r_3 = q_5r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	137984)
$r_4 = q_6r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9r_8 + r_9$	$67914 = 31 \times 2156 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10}r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

The Euclidean Algorithm

Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

The Modulus

If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n . The integer n is called the modulus.

Thus, for any integer a , we can rewrite Equation as follows:

$$a = qn + r \quad 0 \leq r < n; \quad q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor * n + (a \bmod n)$$

$$11 \bmod 7 = 4; \quad -11 \bmod 7 = 3$$

$$a = qn + r \quad 0 \leq r < n; \quad q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor * n + (a \bmod n)$$

$$11 \bmod 7 = 4; \quad -11 \bmod 7 = 3$$

Two integers a and b are said to be congruent modulo n , if $(a \bmod n) = (b \bmod n)$. This is written as $a \equiv b \pmod{n}$.

$$73 \equiv 4 \pmod{23}; \quad 21 \equiv -9 \pmod{10}$$

Note that if $a \equiv 0 \pmod{n}$, then $n \mid a$.



Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

To demonstrate the first point, if $n \mid (a - b)$, then $(a - b) = kn$ for some k . So we can write $a = b + kn$. Therefore,
divided by n = (remainder when b is divided by n) = $(b \pmod{n})$.

$23 \equiv 8 \pmod{5}$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod{8}$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

The remaining points are as easily proved.

Modular Arithmetic Operations

Note that, by definition the $(\text{mod } n)$ operator maps all integers into the set of integers $\{0, 1, \dots, (n - 1)\}$. This suggests the question: Can we perform arithmetic operations within the confines of this set? It turns out that we can; this technique is known as modular arithmetic.

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$



We demonstrate the first property. Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$.

Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer

k . Then

$$(a + b) \bmod n = (r_a + jn + r_b + kn) \bmod n$$

$$= (r_a + r_b + (k + j)n) \bmod n$$

$$= (r_a + r_b) \bmod n$$

$$= [(a \bmod n) + (b \bmod n)] \bmod n$$



The remaining properties are proven as easily. Here are examples of the three properties:

$$11 \bmod 8 = 3; 15 \bmod 8 = 7$$

$$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$$

$$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$$

$$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$$

$$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$$

$$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$$

$$(11 * 15) \bmod 8 = 165 \bmod 8 = 5$$



Exponentiation is performed by repeated multiplication, as in ordinary arithmetic

To find $117 \bmod 13$, we can proceed as follows:

$$112 = 121 \text{ K } 4 \pmod{13}$$

$$114 = (112)^2 \text{ K } 42 \text{ K } 3 \pmod{13}$$

$$117 \text{ K } 11 * 4 * 3 \text{ K } 132 \text{ K } 2 \pmod{13}$$



Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

Table 4.2 provides an illustration of modular addition and multiplication modulo 8. Looking at addition, the results are straightforward, and there is a regular pattern to the matrix. Both matrices are symmetric about the main diagonal in conformance to the commutative property of addition and multiplication.



As in ordinary addition, there is an additive inverse, or negative, to each integer in modular arithmetic. In this case, the negative of an integer x is the integer y . Such that $(x + y) \bmod 8 = 0$. To find the additive inverse of an integer in the left-hand column, scan across the corresponding row of the matrix to find the value 0; the integer at the top of that column is the additive inverse; thus, $(2 + 6) \bmod 8 = 0$. Similarly, the entries in the multiplication table are straightforward.



As in ordinary addition, there is an additive inverse, or negative, to each integer in modular arithmetic. In this case, the negative of an integer x is the integer y . Such that $(x + y) \bmod 8 = 0$. To find the additive inverse of an integer in the left-hand column, scan across the corresponding row of the matrix to find the value 0; the integer at the top of that column is the additive inverse; thus, $(2 + 6) \bmod 8 = 0$. Similarly, the entries in the multiplication table are straightforward.



In ordinary arithmetic, there is a multiplicative inverse, or reciprocal, to each integer. In modular arithmetic mod 8, the multiplicative inverse of x is the integer y such that $(x * y) \bmod 8 = 1 \bmod 8$. Now, to find the multiplicative inverse of an integer from the multiplication table, scan across the matrix in the row for that integer to find the value 1; the integer at the top of that column is the multiplicative inverse; thus, $(3 * 3) \bmod 8 = 1$. Note that not all integers mod 8 have a multiplicative inverse; more about that later.

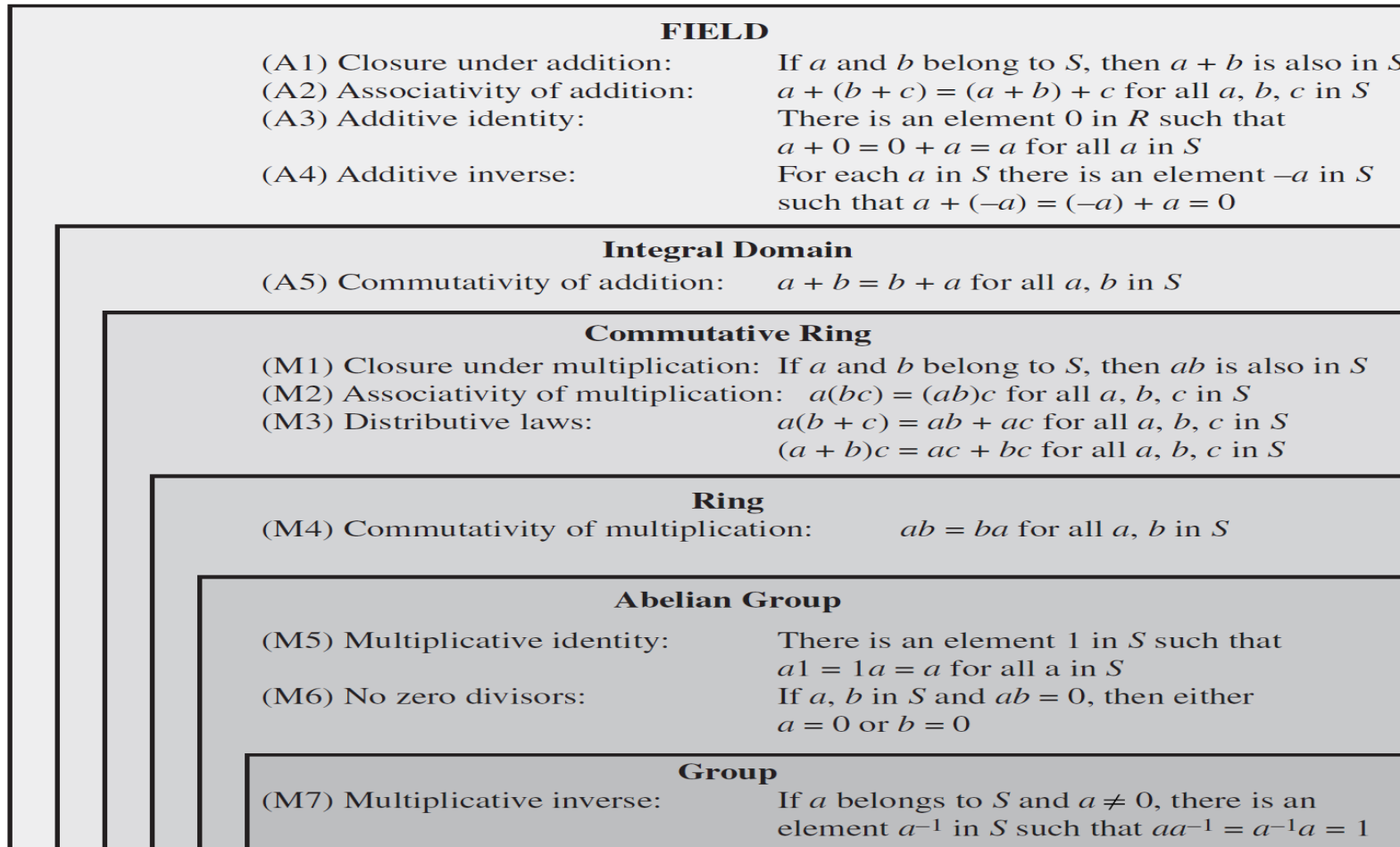


Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra. In abstract algebra, we are concerned with sets on whose elements we can operate algebraically; that is, we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set. These operations are subject to specific rules, which define the nature of the set.



By convention, the notation for the two principal classes of operations on set elements is usually the same as the notation for addition and multiplication on ordinary numbers. However, it is important to note that, in abstract algebra, we are not limited to ordinary arithmetical operations. All this should become clear as we proceed.

GROUPS, RINGS, AND FIELDS



We are concerned with polynomials in a single variable x , and we can distinguish three classes of polynomial arithmetic.

- Ordinary polynomial arithmetic, using the basic rules of algebra.
- Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo p ; that is, the coefficients are in $GF(p)$.
- Polynomial arithmetic in which the coefficients are in $GF(p)$, and the polynomials are defined modulo a polynomial $m(x)$ whose highest power is some integer n .



Virtually all encryption algorithms, both symmetric and public key, involve arithmetic operations on integers. If one of the operations that is used in the algorithm is division, then we need to work in arithmetic defined over a field. For convenience and for implementation efficiency, we would also like to work with integers that fit exactly into a given number of bits with no wasted bit patterns. That is, we wish to work with integers in the range 0 through $2^n - 1$, which fit into an n -bit word.



Thank You

ANY
QUESTIONS?

