Information Security: Principles and Practice, Second Edition
by Mark Stamp

A-2 Math Essentials

7/5ths of all people don't understand fractions.
— Anonymous

A-2.1 Introduction

This section contains a brief overview of the math topics that are relevant to understanding the material presented in this book. First, we cover some modular arithmetic basics. Modular arithmetic figures prominently in the field of public key cryptography. We then discuss a few very basic facts about permutations. Permutations are a fundamental building block of ciphers—from classic ciphers to modern block ciphers. Next, we consider a few concepts from discrete probability and, finally, we provide a quick introduction to linear algebra. Chapter 6 contains the details of the lattice-reduction attack on the knapsack cryptosystem, and that's the only place where linear algebra is used in this book.

A-2.2 Modular Arithmetic

For integers x and n, the value of x modulo n, which is abbreviated $x \bmod n$, is defined to be the remainder when x is divided by n. Note that the remainder when a number is divided by n must be one of the values $0, 1, 2 \ldots, n-1$, so these are the only possible results when you are asked to compute $x \bmod n$.

In non-modular arithmetic, the number line is used to represent the relative positions of the numbers. For modular arithmetic, a mod n "clock" labeled with the integers $0, 1, 2 \ldots, n-1$ serves a similar purpose, and for this reason modular arithmetic can be viewed as clock arithmetic. For example, the mod 6 clock appears in Figure A-7.

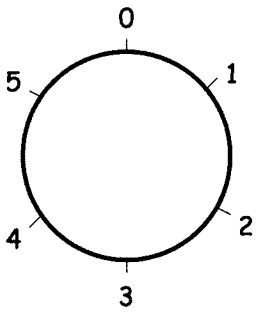

Figure A-7: Number "Line" Mod 6

The notation for modular arithmetic is flexible—we can write $x \bmod n = y$ or $x = y \bmod n$ or $x \pmod n = y$ or $x = y \pmod n$. The point here is that if a "mod n" appears anywhere in an equation, the entire equation is taken modulo n. It is common to say that we "reduce" $x \bmod n$, and if you really want to impress your friends, you can say modulo n instead of mod n.

A basic property of modular addition is

$$((a \bmod n) + (b \bmod n)) \bmod n = (a + b) \bmod n,$$

so that, for example,

$$(7 + 12) \bmod 6 = 19 \bmod 6 = 1 \bmod 6$$

and

$$(7 + 12) \bmod 6 = (1 + 0) \bmod 6 = 1 \bmod 6.$$

That is, we can apply the mod operations any place (or places) we please and the result will not change. Often, for computational efficiency (or convenience) we do the modular reductions in some not-so-obvious order.

The same property holds true for modular multiplication, that is,

$$((a \bmod n)(b \bmod n)) \bmod n = ab \bmod n.$$

For example,

$$(7 \cdot 4) \bmod 6 = 28 \bmod 6 = 4 \bmod 6$$

and

$$(7 \cdot 4) \bmod 6 = (1 \cdot 4) \bmod 6 = 4 \bmod 6.$$

This simple property is critical for effective modular exponentiation, and modular exponentiation is the fundamental computation used in the RSA public key cryptosystem.

Modular inverses play an important role in public key cryptography. In ordinary (non-modular) addition, the additive inverse of x is the number that we add to x to get 0. Of course, in non-modular arithmetic, that's just a fancy way of saying that the additive inverse of x is $-x$. The additive inverse of x mod n is denoted $-x \bmod n$, but we have to use the definition to make sense of the " $-$ ". Recall that when working modulo n, the only numbers that exist are $0, 1, 2, \ldots, n-1$. Then, from the definition, $-x \bmod n$ is the number in this range that we add to x to obtain $0 \bmod n$. For example, $-2 \bmod 6 = 4$, since $2 + 4 = 0 \bmod 6$. That is, $-2 = 4 \bmod 6$, which can also be seen by starting at 0 on the mod 6 clock and going counterclockwise by 2.

In ordinary arithmetic, the multiplicative inverse of x, denoted as x^{-1}, is the number that we multiply by x to obtain 1. In the non-modular world, this is easy, since $x^{-1} = 1/x$, provided that $x \neq 0$. But in the modular case there are no fractions, so things are not as straightforward. From the definition, the multiplicative inverse of x mod n, which is denoted $x^{-1} \bmod n$, is the number that we multiply by x to obtain 1 mod n. For example, $3^{-1} \bmod 7 = 5$, since $3 \cdot 5 = 1 \bmod 7$. That is, $3^{-1} = 5 \bmod 7$.

What is $2^{-1} \bmod 6$? Since we are working mod 6, the only possible choices are $0, 1, 2, 3, 4, 5$, and it's easy to verify by an exhaustive search that none of these satisfy the definition. Consequently, 2 does not have a multiplicative inverse, modulo 6, which shows that for modular arithmetic, there are numbers other than 0 that do not have multiplicative inverses.

When does a (modular) multiplicative inverse exist? To answer that, we must delve slightly deeper. A number p is said to be *prime* if it has no factors other than 1 and p. We say that two numbers x and y are *relatively prime* if they have no common factor other than 1. For example, 8 and 9 are relatively prime, although neither 8 nor 9 is prime. It can be shown that $x^{-1} \bmod y$ exists if and only if x and y are relatively prime. When the modular inverse exists, it's easy to find—in a computational sense—using the Euclidean algorithm [43]. It's also easy (computationally) to tell when a modular inverse doesn't exist, that is, it's easy to test whether x and y are relatively prime.

For our discussion of public key cryptography, we require one additional result from number theory. The *totient function* (or Euler's totient function), which is denoted as $\phi(n)$, is the number of positive integers less than n that

are relatively prime to n. For example, $\phi(4) = 2$ since 4 is relatively prime to 3 and 1, but not 2. Also, $\phi(5) = 4$ since 5 is relatively prime to 1,2,3 and 4, while $\phi(12) = 4$, since the only positive integers less than 12 that are relatively prime to 12 are 1, 5, 7, and 11.

For any prime number p, it's easy to see that $\phi(p) = p - 1$. Furthermore, it is fairly easy to show that if p and q are prime, then $\phi(pq) = (p-1)(q-1)$; see Burton's fine book [43] for the details. These elementary properties of $\phi(n)$ are used in Section 4.3 of Chapter 4, which covers the RSA public key cryptosystem.

A-2.3 Permutations

Let S be a given set. Then a *permutation* of S is an ordered list of the elements of S, where each element appears exactly once. For example, $(3,1,4,0,5,2)$ is a permutation of $\{0,1,2,3,4,5\}$, but $(3,1,4,0,5)$ is not and neither is the list $(3,1,4,2,5,2)$.

It's easy to count the number of permutations of a set of n elements: there are n ways to choose the first element of the permutation, $n-1$ selections remain for the next element, and so on. Consequently, there are $n!$ permutations of any set of n elements. For example, there are 24 permutations of the set $\{0,1,2,3\}$.

Permutations play a prominent role in cryptography. Classic ciphers are often based on permutations, while many modern block ciphers also make heavy use of permutations.

A-2.4 Probability

In this book, we only require a few elementary facts from the field of discrete probability. Let $S = \{0,1,2,\ldots,N-1\}$ represent the set of all possible outcomes of some experiment. If each outcome is *equally likely*, then the probability of the *event* X, where $X \subset S$, is

$$P(X) = \text{number of elements in } X/\text{number of elements in } S.$$

For example, if we roll two dice, the set S can be taken to be the 36 equally likely ordered pairs

$$S = \{(1,1),(1,2),\ldots,(1,6),(2,1),(2,2),\ldots,(6,6)\}.$$

Then when we roll two dice we find, for example,

$$P(\text{sum equal } 7) = 6/36 = 1/6,$$

since 6 of the elements in S sum to 7.

Often, it's easier to compute the probability of X using the fact

$$P(X) = 1 - P(\text{complement of } X),$$

where the complement of X is the set of elements in S that are not in X. For example, when rolling two dice,

$$P(\text{sum } > 3) = 1 - P(\text{number } \leq 3) = 1 - 3/36 = 11/12.$$

Although there are many good sources of information on discrete probability, probably your author's favorite is the ancient—but excellent—book by Feller [109]. Feller covers all of the basics and many interesting and useful advanced topics, all in a very readable and engaging style.

A-2.5 Linear Algebra

In Chapter 6, the discussion of the attack on the knapsack cryptosystem requires a small amount of linear algebra. Here, we present only the minimum amount of linear algebra required to understand the material in that particular section.

We write $v \in \mathbf{R}^n$ to denote a vector containing n components, where each element is a real number. For example,

$$v = [v_1, v_2, v_3, v_4] = [4, 7/3, 13, -3/2] \in \mathbf{R}^4.$$

The *dot product* of two vectors $u, v \in \mathbf{R}^n$, is

$$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

Note that the dot product only applies to vectors of the same length and the result of the dot product is a number, not a vector.

A *matrix* is an $n \times m$ array of numbers. For example,

$$A = \begin{bmatrix} 3 & 4 & 2 \\ 1 & 7 & 9 \end{bmatrix} \tag{A-1}$$

is a 2×3 matrix, and we sometimes write $A_{2\times 3}$ to emphasize the dimensions. We denote the element in the ith row and jth column of A as a_{ij}. For example, in the matrix A, above, $a_{1,2} = 4$.

To multiply a matrix by a number, we simply multiply each element of the matrix by the number. For example, for the matrix A in equation (A-1), we have

$$3A = \begin{bmatrix} 3\cdot 3 & 3\cdot 4 & 3\cdot 2 \\ 3\cdot 1 & 3\cdot 7 & 3\cdot 9 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 6 \\ 3 & 21 & 27 \end{bmatrix}$$

Addition of matrices is only defined if the matrices have the same dimensions. If so, the corresponding elements are simply added. For example,

$$\begin{bmatrix} 3 & 2 \\ 1 & 5 \end{bmatrix} + \begin{bmatrix} -1 & 4 \\ 6 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ 7 & 7 \end{bmatrix}.$$

Matrix multiplication, on the other hand, is less intuitive than matrix addition or multiplication by a number. Given matrices $A_{m\times n}$ and $B_{k\times \ell}$, the product $C = AB$ is only defined if $n = k$, in which case the product C is $m \times \ell$. When the product is defined, the element in row i and column j of C, that is, c_{ij}, is given by the dot product of the ith row of A with the jth column of B. For example, for the matrix A in (A-1) and

$$B = \begin{bmatrix} -1 & 2 \\ 2 & -3 \end{bmatrix}$$

the product

$$BA = C_{2\times 3} = \begin{bmatrix} [-1,2] \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix} & [-1,2] \cdot \begin{bmatrix} 4 \\ 7 \end{bmatrix} & [-1,2] \cdot \begin{bmatrix} 2 \\ 9 \end{bmatrix} \\ [2,-3] \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix} & [2,-3] \cdot \begin{bmatrix} 4 \\ 7 \end{bmatrix} & [2,-3] \cdot \begin{bmatrix} 2 \\ 9 \end{bmatrix} \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 10 & 16 \\ 3 & -13 & -23 \end{bmatrix}.$$

Note that for these two matrices, the product AB is undefined, which shows that matrix multiplication is, in general, not commutative.

The *identity matrix* $I_{n\times n}$ has 1s on the main diagonal, and 0s elsewhere. Note that the identity matrix is always a square matrix, that is, a matrix with an equal numbers of rows and columns. For example, the 3×3 identity matrix is

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

For a square matrix A, the identity matrix of the appropriate size is the multiplicative identity, that is, $AI = IA = A$.

We can also define block matrices, where the elements are themselves matrices. We can multiply block matrices provided that the dimensions meet the requirements for matrix multiplications, *and* the dimensions on all of the individual blocks that are to be multiplied also are appropriate for multiplication. For example, if

$$M = \begin{bmatrix} I_{n\times n} & C_{n\times 1} \\ A_{m\times n} & B_{m\times 1} \end{bmatrix} \text{ and } V = \begin{bmatrix} U_{n\times \ell} \\ T_{1\times \ell} \end{bmatrix},$$

then

$$MV = \begin{bmatrix} X_{n\times\ell} \\ Y_{m\times\ell} \end{bmatrix},$$

where $X = U + CT$ and $Y = AU + BT$. You should verify that all of these operations are defined.

We'll require only one more result from linear algebra. Suppose x and y are vectors in R^n. Then we say that x and y are *linearly independent* provided that the only scalars (i.e., numbers) α and β for which

$$\alpha x + \beta y = 0$$

are $\alpha = \beta = 0$. For example,

$$\begin{bmatrix} 1 \\ -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

are linearly independent. Linear independence extends to more than two vectors. The importance of linear independence derives from the fact that if a set of vectors are linearly independent, then none of the vectors can be written as a *linear combination* of the other vectors, that is, none of the vectors can be written as a sum of multiples of the other vectors in the set. This is the sense in which the vectors are independent.

A-2.6 Conclusions

That concludes our brief review of the math used in this book. Hopefully, you're still awake. In any case, the math required in this text is minimal, so fear not if some of the details discussed here appear somewhat opaque. You can simply review this material as needed if you run into any mathematical speed bumps on your way to security enlightenment.