Appendix B
Some Aspects of Number Theory

William Stallings

Copyright 2014
Supplement to
Computer Security, Third Edition
Pearson 2014
http://williamstallings.com/ComputerSecurity

This appendix provides some background on number theory concepts referenced in this book.

B.1 PRIME AND RELATIVELY PRIME NUMBERS

In this section, unless otherwise noted, we deal only with nonnegative integers. The use of negative integers would introduce no essential differences.

Divisors

We say that $b \neq 0$ 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 $b|a$ is commonly used to mean b divides a. Also, if $b|a$, we say that b is a **divisor** of a. For example, the positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

The following relations hold:

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- 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 $mg + nh$.

Prime Numbers

An integer $p > 1$ is a prime number if its only divisors are ±1 and $\pm p$. Prime numbers play a critical role in number theory and in the algorithms discussed in Chapter 23.

Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$$

where $p_1 < p_2 < . . . < p_t$ are prime numbers and where each a_i is a positive integer. For example, $91 = 7 \times 13$; and $11011 = 7 \times 11^2 \times 13$.

It is useful to cast this another way. If P is the set of all prime numbers, then any positive integer can be written uniquely in the following form:

$$a = \prod_{p \in \mathrm{P}} p^{a_p} \quad \text{where each } a_p \geq 0$$

The right-hand side is the product over all possible prime numbers p; for any particular value of a, most of the exponents a_p will be 0.

The value of any given positive integer can be specified by simply listing all the nonzero exponents in the foregoing formulation. Thus, the integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$, and the integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$. Multiplication of two numbers is equivalent to adding the corresponding exponents:

$$k = mn \rightarrow \quad k_p = m_p + n_p \text{ for all } p$$

What does it mean, in terms of these prime factors, to say that $a|b$? Any integer of the form p^k can be divided only by an integer that is of a lesser or equal power of the same prime number, p^j with $j \leq k$. Thus, we can say

$$a|b \rightarrow \quad a_p \leq b_p \qquad \text{for all } p$$

Relatively Prime Numbers

We will use the notation gcd(a, b) to mean the **greatest common divisor** of a and b. 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:

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

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 |). For example, gcd(60, 24) = gcd(60, −24) = 12. Also, because all nonzero integers divide 0, we have gcd(a, 0) = | a |.

It is easy to determine the greatest common divisor of two positive integers if we express each integer as the product of primes. For example, $300 = 2^2 \times 3^1 \times 5^2$; $18 = 2^1 \times 3^2$; $\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$.

In general,

$$k = \gcd(a, b) \quad \rightarrow \quad k_p = \min(a_p, b_p) \quad \text{for all } p$$

Determining the prime factors of a large number is no easy task, so the preceding relationship does not directly lead to a way of calculating the greatest common divisor.

The integers *a* and *b* are relatively prime if they have no prime factors in common; that is, if their only common factor is 1. This is equivalent to saying that *a* and *b* are relatively prime if gcd(*a*, *b*) = 1. For example, 8 and 15 are relatively prime because the divisors of 8 are 1, 2, 4, and 8, and the divisors of 15 are 1, 3, 5, and 15, so 1 is the only number on both lists.

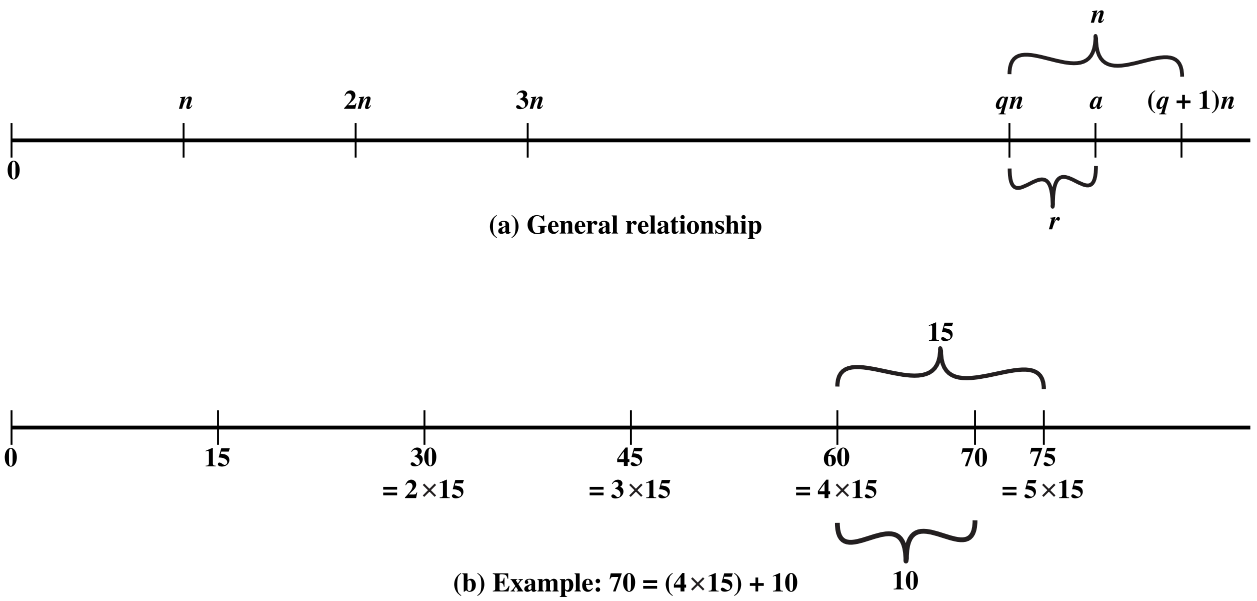
B.2 MODULAR ARITHMETIC

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:

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to *x*.

Figure B.1 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,



(a) General relationship

(b) Example: 70 = (4×15) + 10

Figure B.1 The Relationship $a = qn + r;\ 0 \leq r < n$

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**.

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. Thus, for any integer a, we can always write

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

Two integers a and b are said to be **congruent modulo *n***, if (a mod n) = (b mod n). This is written $a \equiv b$ mod n. For example, $73 \equiv 4$ mod 23; and $21 \equiv -9$ mod 10. Note that if $a \equiv 0$ mod n, then $n|a$.

The modulo operator has the following properties:

1. $a \equiv b$ mod n if $n|(a - b)$

2. (a mod n) = (b mod n) implies $a \equiv b$ mod n

3. $a \equiv b \bmod n$ implies $b \equiv a \bmod n$

4. $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply $a \equiv c \bmod n$

To demonstrate the first point, if $n|(a - b)$, then $(a - b) = kn$ for some k. So we can write $a = b + kn$. Therefore, (a mod n) = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = (b mod n). The remaining points are as easily proved.

Modular Arithmetic Operations

The (mod n) operator maps all integers into the set of integers $\{0, 1, . . . (n - 1)\}$. This suggests the question, Can we perform arithmetic operations within the confines of this set? It turns out that we can; the 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. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

We demonstrate the first property. Define (a mod n) = r_a and (b mod 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

$$\begin{aligned}(a + b) \bmod n &= (r_a + jn + r_b + kn) \bmod n \\ &= (r_a + r_b + (\mathrm{k} + \mathrm{j})\mathrm{n}) \bmod n \\ &= (r_a + r_b) \bmod n \\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$

The remaining properties are as easily proved.

Inverses

As in ordinary arithmetic, we can write the following:

$$\textbf{if } (a + b) \equiv (a + c) \pmod{n} \quad \textbf{then} \quad b \equiv c \pmod{n} \qquad \textbf{(B.1)}$$

(5 + 23) ≡ (5 + 7) (mod 8);   23 ≡ 7 (mod 8)

For example, (5 + 23) ≡ (5 + 7) (mod 8) implies that 23 ≡ 7 (mod 8). Equation (B.1) is consistent with the existence of an **additive inverse**. Adding the additive inverse of *a* to both sides of Equation (B.1), we have

$$((-a) + a + b) \equiv ((-a) + a + c) \pmod{n}$$
$$b \equiv c \pmod{n}$$

However, the following statement is true only with the attached condition:

$$\begin{aligned} &\textbf{if } (a \times b) \equiv (a \times c) \pmod{n} \\ &\quad \textbf{then } b \equiv c \pmod{n} \;\; \textbf{if } a \text{ is relatively prime to } n \qquad \textbf{(B.2)} \end{aligned}$$

Similar to the case of Equation (B,1), we can say that Equation (B.2) is consistent with the existence of a **multiplicative inverse**. Applying the multiplicative inverse of *a* to both sides of Equation (B.2), we have

$$((a^{-1})ab) \equiv ((a^{-1})ac) \pmod{n}$$
$$b \equiv c \pmod{n}$$

The proof that we must add the condition in Equation (B.2) is beyond the scope of this book but is explored in [STAL11b].

B.3 FERMAT'S AND EULER'S THEOREMS

Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.

Fermat's Theorem[1]

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p} \tag{B.3}$$

Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p - 1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka \pmod{p}$, where $1 \leq j < k \leq p - 1$. Because a is relatively prime to p, we can eliminate a from both sides of the equation [see Equation (B.2)] resulting in $j \equiv k \pmod{p}$. This last equality is impossible because j and k are both positive integers less than p. Therefore, we know that the $(p - 1)$ elements of X are all positive integers, with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p - 1\}$ in some order. Multiplying the numbers in both sets and taking the result mod p yields

[1] This is sometimes referred to as Fermat's little theorem.

$$a \times 2a \times . . . \times (p - 1)a \equiv [(1\times 2 \times \ldots\times (p - 1)] \pmod{p}$$

$$a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}$$

We can cancel the $(p - 1)!$ term because it is relatively prime to p [see Equation (B.2)]. This yields Equation (B.3).

$a = 7, p = 19$
$7^2 = 49 \equiv 11 \pmod{19}$
$7^4 \equiv 121 \equiv 7 \pmod{19}$
$7^8 \equiv 49 \equiv 11 \pmod{19}$
$7^{16} \equiv 121 \equiv 7 \pmod{19}$
$a^{p-1} = 7^{18} = 7^{16}\times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$

An alternative form of Fermat's theorem is also useful: If p is prime and a is a positive integer, then

$$a^p \equiv a \pmod{p} \qquad \textbf{(B.4)}$$

Note that the first form of the theorem [Equation (B.3)] requires that a be relatively prime to p, but this form does not.

$p = 5, a = 3$	$a^p = 3^5 = 243 \equiv 3 \pmod{5} = a \pmod{p}$
$p = 5, a = 10$	$a^p = 10^5 = 100000 \equiv 10 \pmod{5} \equiv 0 \pmod{5} = a \pmod{p}$

Euler's Totient Function

Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as Euler's totient function and written $\phi(n)$, defined as the number of positive integers less than n and relatively prime to n.

Determine $\phi(37)$ and $\phi(35)$.
Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.
To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

$$1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,$$
$$19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.$$

There are 24 numbers on the list, so $\phi(35) = 24$.

Table B.1 lists the first 30 values of $\phi(n)$. The value $\phi(1)$ is without meaning but is defined to have the value 1.

Table B.1 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

It should be clear that for a prime number p,

$$\phi(p) = p - 1$$

Now suppose that we have two prime numbers p and q, with $p \neq q$. Then we can show that for $n = pq$,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less that n is the set $\{1, . . . , (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, . . . , (q - 1)p\}$ and the set $\{q, 2q, . . . , (p - 1)q\}$. Accordingly,

$$\begin{aligned} \phi(n) &= (pq - 1) - [(q - 1) + (p - 1)] \\ &= pq - (p + q) +1 \\ &= (p - 1) \times (q - 1) \\ &= \phi(p) \times \phi(q) \end{aligned}$$

$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

Euler's Theorem

Euler's theorem states that for every a and n that are relatively prime,

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{B.5}$$

$a = 3;\ n = 10;\ \phi(10) = 4 \qquad a^{\phi(n)} = 3^4 = 81 \equiv 1 \pmod{10} = 1 \pmod{n}$
$a = 2;\ n = 11;\ \phi(11) = 10 \qquad a^{\phi(n)} = 2^{10} = 1024 \equiv 1 \pmod{11} = 1 \pmod{n}$

Proof: Equation (B.5) is true if n is prime, because in that case $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as follows:

$$R = \{x_1, x_2, . . ., x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), . . ., (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.
2. There are no duplicates in S. Refer to Equation (B.2). If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \equiv 1 \pmod n$$

This is the same line of reasoning applied to the proof of Fermat's theorem.

As is the case for Fermat's theorem, an alternative form of the theorem is also useful:

$$a^{\phi(n)+1} \equiv a \pmod n \qquad \textbf{(B.6)}$$

Again, similar to the case with Fermat's theorem, the first form of Euler's theorem [Equation (B.6)] requires that *a* be relatively prime to *n*, but this form does not.