# Chapter Five
# Introduction to Number Theory

## 5.1. Prime Numbers

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

A central concern of number theory is the study of prime numbers. Indeed, whole books have been written on the subject (e.g., [CRAN01], [RIBE96]). In this section we provide an overview relevant to the concerns of this book.

An integer p > 1 is a prime number if and only if its only divisors are ± 1 and ±p. Prime numbers play a critical role in number theory and in the techniques discussed in this chapter. Table 5.1 shows the primes less than 2000. Note the way the primes are distributed. In particular, note the number of primes in each range of 100 numbers.

Recall from Chapter 4 that integer a is said to be a divisor of integer b if there is no remainder on division. Equivalently, we say that a divides b.

**Table 5.1. Primes under 2000**

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 101 | 211 | 307 | 401 | 503 | 601 | 701 | 809 | 0 | 1009 | 1103 | 1201 | 1301 | 1409 | 1511 | 1601 | 1709 | 1801 | 1901 |
| 3 | 103 | 223 | 311 | 409 | 509 | 607 | 709 | 811 | 911 | 1013 | 1109 | 1213 | 1303 | 1423 | 1523 | 1607 | 1721 | 1811 | 1907 |
| 5 | 107 | 227 | 313 | 419 | 521 | 613 | 719 | 821 | 919 | 1019 | 1117 | 1217 | 1307 | 1427 | 1531 | 1609 | 1723 | 1823 | 1913 |
| 7 | 109 | 229 | 317 | 421 | 523 | 617 | 727 | 823 | 929 | 1021 | 1123 | 1223 | 1319 | 1429 | 1543 | 1613 | 1733 | 1831 | 1931 |
| 11 | 113 | 233 | 331 | 431 | 541 | 619 | 733 | 827 | 937 | 1031 | 1129 | 1229 | 1321 | 1433 | 1549 | 1619 | 1741 | 1847 | 1933 |
| 13 | 127 | 239 | 337 | 433 | 547 | 631 | 739 | 829 | 941 | 1033 | 1151 | 1231 | 1327 | 1439 | 1553 | 1621 | 1747 | 1861 | 1949 |
| 17 | 131 | 241 | 347 | 439 | 557 | 641 | 743 | 839 | 947 | 1039 | 1153 | 1237 | 1361 | 1447 | 1559 | 1627 | 1753 | 1867 | 1951 |
| 19 | 137 | 251 | 349 | 443 | 563 | 643 | 751 | 853 | 953 | 1049 | 1163 | 1249 | 1367 | 1451 | 1567 | 1637 | 1759 | 1871 | 1973 |
| 23 | 139 | 257 | 353 | 449 | 569 | 647 | 757 | 857 | 967 | 1051 | 1171 | 1259 | 1373 | 1453 | 1571 | 1657 | 1777 | 1873 | 1979 |
| 29 | 149 | 263 | 359 | 457 | 571 | 653 | 761 | 859 | 971 | 1061 | 1181 | 1277 | 1381 | 1459 | 1579 | 1663 | 1783 | 1877 | 1987 |
| 31 | 151 | 269 | 367 | 461 | 577 | 659 | 769 | 863 | 977 | 1063 | 1187 | 1279 | 1399 | 1471 | 1583 | 1667 | 1787 | 1879 | 1999 |
| 37 | 157 | 271 | 373 | 463 | 587 | 661 | 773 | 877 | 983 | 1069 | 1193 | 1283 | | 1481 | 1597 | 1669 | 1789 | 1889 | 1997 |
| 41 | 163 | 277 | 379 | 467 | 593 | 673 | 787 | 881 | 991 | 1087 | | 1289 | | 1483 | | 1693 | | | 1999 |
| 43 | 167 | 281 | 383 | 479 | 599 | 677 | 797 | 883 | 997 | 1091 | | 1291 | | 1487 | | 1697 | | | |
| 47 | 173 | 283 | 389 | 487 | | 683 | | 887 | | 1093 | | 1297 | | 1489 | | 1699 | | | |
| 53 | 179 | 293 | 397 | 491 | | 691 | | | | 1097 | | | | 1493 | | | | | |
| 59 | 181 | | | 499 | | | | | | | | | | 1499 | | | | | |
| 61 | 191 | | | | | | | | | | | | | | | | | | |
| 67 | 193 | | | | | | | | | | | | | | | | | | |
| 71 | 197 | | | | | | | | | | | | | | | | | | |
| 73 | 199 | | | | | | | | | | | | | | | | | | |
| 79 | | | | | | | | | | | | | | | | | | | |
| 83 | | | | | | | | | | | | | | | | | | | |
| 89 | | | | | | | | | | | | | | | | | | | |
| 97 | | | | | | | | | | | | | | | | | | | |

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

Equation 5-1

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

where $p1 < p_2 < \ldots < p_t$ are prime numbers and where each is a positive integer. This is known as the fundamental theorem of arithmetic; a proof can be found in any text on number theory.

| | |
|---|---|
| 91 | $= 7 \times 13$ |
| 3600 | $= 2^4 \times 3^2 \times 5^2$ |

| | |
|---|---|
| 11011 | = 7 x $11^2$ x 13 |

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

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

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.

| |
|---|
| The integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$. |
| The integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$. |
| The integer 91 is represented by $\{a_7 = 2, a_{13} = 1\}$. |

Multiplication of two numbers is equivalent to adding the corresponding exponents. Given a $a = \prod_{p \in P} p^{a_p} b = \prod_{p \in P} p^{b_p}$. Define k = ab We know that the integer k can be expressed as the product of powers of primes: $k = \prod_{p \in P} p^{k_p}$. It follows that $k_p = a_p + b_p$ for all $p \in P$.

| |
|---|
| k = 12 x 18 = ($2^2$ x 3) x (2 x $3^2$) = 216 |
| $k_2 = 2 + 1 = 3$; $k_3 = 1 + 2 = 3$ |
| 216 = $2^3$ x $3^3$ = 8 x 27 |

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

Given $a = \prod_{p \in P} p^{a_p}$, $b = \prod_{p \in P} p^{b_p}$ If a|b, then $a_p \leq b_p$ then for all p.

| | |
|---|---|
| a | = 12;b = 36; 12\|36 |
| 12 | = $2^2$ x 3; 36 = $2^2$ x $3^2$ |
| $a_2$ | = 2 = $b_2$ |
| $a_3$ | = 1 ≤ 2 = $b_3$ |
| Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers. | |

It is easy to determine the greatest common divisor of two positive integers if we express each integer as the product of primes. Recall from Chapter 4 that the greatest common divisor of integers a and b, expressed gcd(a, b), is an integer c that divides both a and b without remainder and that any divisor of a and b is a divisor of c.

| | |
|---|---|
| 300 | $= 2^2 \times 3^1 \times 5^2$ |
| 18 | $= 2^1 \times 3^2$ |
| gcd(18,300) | $= 2^1 \times 3^1 \times 5^0 = 6$ |

The following relationship always holds:
If k = gcd(a,b) then $k_p = \min(a_p, b_p)$ 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 practical method of calculating the greatest common divisor.

## 5.2. Fermat's and Euler's Theorems

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

### 5.2.1. Fermat's Theorem

This is sometimes referred to as Fermat's little theorem.
Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then
Equation 5-2

$$a^{p-1} \equiv 1 (\text{mod } p)$$

Proof: Consider the set of positive integers less than p:{1,2,..., p 1} and multiply each element by a, modulo p, to get the set X = {a mod p, 2a mod p, . . . (p 1)a mod 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 ≡ ka(mod p) where 1 ≤ j < k ≤ p 1. Because a is relatively prime to p, we can eliminate a from both sides of the equation [see Equation (4.3)] resulting in: j ≡ k(mode 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,..., p 1} in some order. Multiplying the numbers in both sets and taking the result mod p yields
Recall from Chapter 4 that two numbers are relatively prime if they have no prime factors in common; that is, their only common divisor is 1. This is equivalent to saying that two numbers are relatively prime if their greatest common divisor is 1.

$$a \times 2a \times \ldots \times (p\ 1) \equiv [(1 \times 2 \times \ldots \times (p\ 1)](\text{mode } p)$$

$$a^{p1(p\ 1)!} \equiv (p\ 1)!(\text{mod } p)$$

We can cancel the (p 1)! term because it is relatively prime to p [see Equation (4.3)]. This yields Equation (5.2).

| |
|---|
| a = 7, p = 19 |
| $7^2 = 49 \equiv 11(\text{mod } 19)$ |
| $7^4 \equiv 121 \equiv 7(\text{mod } 19)$ |

| |
|---|
| $7^8 \equiv 49 \equiv 7 (\text{mod } 19)$ |
| $7^{16} \equiv 121 \equiv 7 (\text{mod } 19)$ |
| $a^{p1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 (\text{mod } 19)$ |

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

Equation 5-3

$$a^p \equiv a (\text{mod } p)$$

Note that the first form of the theorem [Equation (5.2)] requires that a be relatively prime to p, but this form does not.

| | |
|---|---|
| p = 5,a = 3 | $a^p = 3^5 = 243 \equiv 3 (\text{mod } 5) = a (\text{mod } p)$ |
| p = 5, a = 10 | $a^p = 10^5 = 100000 \equiv 10 (\text{mod } 5) = 0 (\text{mod } 5) = a (\text{mod } p)$ |

## 5.2.2. 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 ∅ (n), defined as the number of positive integers less than n and relatively prime to n. By convention,

$$\varnothing(1) = 1.$$

Determine ∅ (37) and ∅ (35).

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus ∅ (37) = 36.

To determine ∅ (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 ∅ (35) = 24.

Table 5.2 lists the first 30 values of f(n). The value f(1) is without meaning but is defined to have the value 1.

It should be clear that for a prime number p,

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

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

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

To see that f(n) = f(p) x f(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,2 p,..., (q - 1)p} and the set {q,2q,..., (p - 1)q} Accordingly,

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

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

**Table 5.2. Some Values of Euler's Totient Function f(n)**

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

### 5.2.3. Euler's Theorem

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

Equation 5-4

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

| | |
|---|---|
| a = 3; n = 10; f(10) = 4 | $a^{f(n)} = 3^4 = 81 \equiv 1 (\text{mod } 10) = 1 (\text{mod } n)$ |
| a = 2; n = 11; f(11) = 10 | $a^{f(n)} = 2^{10} = 1024 \equiv 1 (\text{mod } 11) = 1 (\text{mod } n)$ |

Proof: Equation (5.4) is true if n is prime, because in that case ∅ (n) = (n 1) and Fermat's theorem holds. However, it also holds for any integer n. Recall that ∅ (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 $\{x_1, x_2, ..., x_{f(n)}\}$

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

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 (4.3). 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:

Equation 5-5

$$a^{\phi(n)+1} \equiv a (\text{mod } n)$$

Again, similar to the case with Fermat's theorem, the first form of Euler's theorem [Equation (5.4)] requires that a be relatively prime to n, but this form does not.

## 5.3. Discrete Logarithms

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA). This section

provides a brief overview of discrete logarithms. For the interested reader, more detailed developments of this topic can be found in [ORE67] and [LEVE90].

### 5.3.1. The Powers of an Integer, Modulo n

Recall from Euler's theorem [Equation (5.4)] that, for every a and n that are relatively prime:

$af(n) \equiv 1 (\text{mod } n)$

where f(n), Euler's totient function, is the number of positive integers less than n and relatively prime to n. Now consider the more general expression:

Equation 5-6

$$a^m \equiv 1 (\text{mod } n)$$

If a and n are relatively prime, then there is at least one integer m that satisfies Equation (5.6), namely, m = f(n). The least positive exponent m for which Equation (5.6) holds is referred to in several ways:

- the order of a (mod n)
- the exponent to which a belongs (mod n)
- the length of the period generated by a

To see this last point, consider the powers of 7, modulo 19:

| | | | |
|---|---|---|---|
| $7^1$ | | $\equiv$ 7 | (mod 19) |
| $7^2$ | = 49 = 2 x 19 + 11 | $\equiv$ 11 | (mod 19) |
| $7^3$ | = 343 = 18 x 19 + 1 | $\equiv$ 1 | (mod 19) |
| $7^4$ | = 2401 = 126 x 19 + 7 | $\equiv$ 7 | (mod 19) |
| $7^5$ | = 16807 = 884 x 19 + 11 | $\equiv$ 11 | (mod 19) |

There is no point in continuing because the sequence is repeating. This can be proven by noting that $7^3 \equiv 1 (\text{mod } 19)$ and therefore $7^{3+j} \equiv 7^3 7^j \equiv 7^j (\text{mod } 19)$, and hence any two powers of 7 whose exponents differ by 3 (or a multiple of 3) are congruent to each other (mod 19). In other words, the sequence is periodic, and the length of the period is the smallest positive exponent m such that $7^m \equiv 1 (\text{mod } 19)$.

Table 5.3 shows all the powers of a, modulo 19 for all positive a < 19. The length of the sequence for each base value is indicated by shading. Note the following:

1. All sequences end in 1. This is consistent with the reasoning of the preceding few paragraphs.
2. The length of a sequence divides f(19) = 18. That is, an integral number of sequences occur in each row of the table.
3. Some of the sequences are of length 18. In this case, it is said that the base integer a generates (via powers) the set of nonzero integers modulo 19. Each such integer is called a primitive root of the modulus 19.

More generally, we can say that the highest possible exponent to which a number can belong (mod n) is ∅(n).

**Table 5.3. Powers of Integers, Modulo 19**

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 16 | 13 | 7 | 14 | 9 | 18 | 17 | 15 | 11 | 3 | 6 | 12 | 5 | 10 | 1 |
| 3 | 9 | 8 | 5 | 15 | 7 | 2 | 6 | 18 | 16 | 10 | 11 | 14 | 4 | 12 | 17 | 13 | 1 |
| 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 | 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 |
| 5 | 6 | 11 | 17 | 9 | 7 | 16 | 4 | 1 | 5 | 6 | 11 | 17 | 9 | 7 | 16 | 4 | 1 |
| 6 | 17 | 7 | 4 | 5 | 11 | 9 | 16 | 1 | 6 | 17 | 7 | 4 | 5 | 11 | 9 | 16 | 1 |
| 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 |
| 8 | 7 | 18 | 11 | 12 | 1 | 8 | 7 | 18 | 11 | 12 | 1 | 8 | 7 | 18 | 11 | 12 | 1 |
| 9 | 5 | 7 | 6 | 16 | 11 | 4 | 17 | 1 | 9 | 5 | 7 | 6 | 16 | 11 | 4 | 17 | 1 |
| 10 | 5 | 12 | 6 | 3 | 11 | 15 | 17 | 18 | 9 | 14 | 7 | 13 | 16 | 8 | 4 | 2 | 1 |
| 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 |
| 12 | 11 | 18 | 7 | 8 | 1 | 12 | 11 | 18 | 7 | 8 | 1 | 12 | 11 | 18 | 7 | 8 | 1 |
| 13 | 17 | 12 | 4 | 14 | 11 | 10 | 16 | 18 | 6 | 2 | 7 | 15 | 5 | 8 | 9 | 3 | 1 |
| 14 | 6 | 8 | 17 | 10 | 7 | 3 | 4 | 18 | 5 | 13 | 11 | 2 | 9 | 12 | 16 | 15 | 1 |
| 15 | 16 | 12 | 9 | 2 | 11 | 13 | 5 | 18 | 4 | 3 | 7 | 10 | 17 | 8 | 6 | 14 | 1 |
| 16 | 9 | 11 | 5 | 4 | 7 | 17 | 6 | 1 | 16 | 9 | 11 | 5 | 4 | 7 | 17 | 6 | 1 |
| 17 | 4 | 11 | 16 | 6 | 7 | 5 | 9 | 1 | 17 | 4 | 11 | 16 | 6 | 7 | 5 | 9 | 1 |
| 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 | 18 | 1 |

If a number is of this order, it is referred to as a **primitive root** of n. The importance of this notion is that if a is a primitive root of n, then its powers

$$a, a^2, \ldots, a^{f(n)}$$

are distinct (mod n) and are all relatively prime to n. In particular, for a prime number p, if a is a primitive root of p, then

$$a, a^2, \ldots, a^{p1}$$

are distinct (mod p). For the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15. Not all integers have primitive roots. In fact, the only integers with primitive roots are those of the form 2, 4, $p^a$, and $2p^a$, where p is any odd prime and a is a positive integer. The proof is not simple but can be found in many number theory books, including [ORE76].

## 5.3.2. Logarithms for Modular Arithmetic

With ordinary positive real numbers, the logarithm function is the inverse of exponentiation. An analogous function exists for modular arithmetic.

Let us briefly review the properties of ordinary logarithms. The logarithm of a number is defined to be the power to which some positive base (except 1) must be raised in order to equal the number. That is, for base x and for a value y:

$$y = x^{\log x(y)}$$

The properties of logarithms include the following:

$$\log_x(1) = 0$$
$$\log_x(x) = 1$$

Equation 5-7

$$\log_x(yz) = \log_x(y) + \log_x(z)$$

Equation 5-8

$$\log_x(y^r) = r \times \log_x(y)$$

Consider a primitive root a for some prime number p (the argument can be developed for nonprimes as well). Then we know that the powers of a from 1 through (p - 1)

produce each integer from 1 through (p 1) exactly once. We also know that any integer b satisfies

$$b \equiv r \pmod{p} \text{ for some r, where } 0 \le r \le (p - 1)$$

by the definition of modular arithmetic. It follows that for any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$$b \equiv a^i \pmod{p} \text{ where } 0 \le i \le (p - 1)$$

This exponent i is referred to as the **discrete logarithm** of the number b for the base a (mod p). We denote this value as $\text{dlog}_{a,p}(b)$.

Many texts refer to the discrete logarithm as the *index*. There is no generally agreed notation for this concept, much less an agreed name.

Note the following:

Equation 5-9

$$\text{dlog}_{a,p}(1) = 0, \text{ because } a^0 \bmod p = 1 \bmod p = 1$$

Equation 5-10

$$\text{dlog}_{a,p}(a) = 1, \text{ because } a^1 \bmod p = a$$

Here is an example using a nonprime modulus, n = 9. Here f(n) = 6 and a = 2 is a primitive root. We compute the various powers of a and find

$2^0 = 1$ $2^4 \equiv 7 \pmod{9}$

$2^1 = 2$ $2^5 \equiv 5 \pmod{9}$

$2^2 = 4$ $2^6 \equiv 1 \pmod{9}$

$2^3 = 8$

This gives us the following table of the numbers with given discrete logarithms (mod 9) for the root a = 2:

| Logarithm | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Number | 1 | 2 | 4 | 8 | 7 | 5 |

To make it easy to obtain the discrete logarithms of a given number, we rearrange the table:

| Number | 1 | 2 | 4 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| Logarithm | 0 | 1 | 2 | 5 | 4 | 3 |

Now consider

$$x = a^{\text{dloga,p(x)}} \bmod p \quad y = a^{\text{dloga,p(y)}} \bmod p$$

$$xy = a^{\text{dloga,p(xy)}} \bmod p$$

Using the rules of modular multiplication,

$$xy \bmod p = [(x \bmod p)(y \bmod p)] \bmod p$$

$$a^{\text{dlog}_{a,p}(xy)} \bmod p = \left[\left(a^{\text{dlog}_{a,p}(x)} \bmod p\right)\left(a^{\text{dlog}_{a,p}(y)} \bmod p\right)\right] \bmod p$$

$$= \left(a^{\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)}\right) \bmod p$$

But now consider Euler's theorem, which states that, for every a and n that are relatively prime:

$$a^{f(n)} \equiv 1 (\text{mod } n)$$

Any positive integer z can be expressed in the form z = q + kf(n), with $0 \leq q < f(n)$. Therefore, by Euler's theorem,

$$a^z \equiv a^q (\text{mod } n) \text{ if } z \equiv q \text{ mod } f(n)$$

Applying this to the foregoing equality, we have

$$\text{dlog}_{a,p}(xy) \equiv [\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)] \text{ (mod } f(p))$$

and generalizing,

$$\text{dlog}_{a,p}(y^r) \equiv [r \text{ x } \text{dlog}_{a.p}(y)] \text{ (mod } f(n))$$

This demonstrates the analogy between true logarithms and discrete logarithms.

Keep in mind that unique discrete logarithms mod m to some base a exist only if a is a primitive root of m.

**Table 5.4. Tables of Discrete Logarithms, Modulo 19**

(a) Discrete logarithms to the base 2, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{2,19}(a)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

(b) Discrete logarithms to the base 3, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{3,19}(a)$ | 18 | 7 | 1 | 14 | 4 | 8 | 6 | 3 | 2 | 11 | 12 | 15 | 17 | 13 | 5 | 10 | 16 | 9 |

(c) Discrete logarithms to the base 10, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{10,19}(a)$ | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |

(d) Discrete logarithms to the base 13, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{13,19}(a)$ | 18 | 11 | 17 | 4 | 14 | 10 | 12 | 15 | 16 | 7 | 6 | 3 | 1 | 5 | 13 | 8 | 2 | 9 |

(e) Discrete logarithms to the base 14, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{14,19}(a)$ | 18 | 13 | 7 | 8 | 10 | 2 | 6 | 3 | 14 | 5 | 12 | 15 | 11 | 1 | 17 | 16 | 4 | 9 |

(f) Discrete logarithms to the base 15, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{15,19}(a)$ | 18 | 5 | 11 | 10 | 8 | 16 | 12 | 15 | 4 | 13 | 6 | 3 | 7 | 17 | 1 | 2 | 14 | 9 |

Table 5.4, which is directly derived from Table 5.3, shows the sets of discrete logarithms that can be defined for modulus 19.

## 5.3.3. Calculation of Discrete Logarithms

Consider the equation

$$y = g^x \text{ mod } p$$

Given g, x, and p, it is a straightforward matter to calculate y. At the worst, we must perform x repeated multiplications, and algorithms exist for achieving greater efficiency.

However, given y, g, and p, it is, in general, very difficult to calculate x (take the discrete logarithm). The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA. At the time of this writing, the asymptotically fastest known algorithm for taking discrete logarithms modulo a prime number is on the order of [BETH91]:

$$e^{((\ln p)1/3(\ln(\ln p))2/3)}$$

which is not feasible for large primes.