Chapter 9

Mathematics of Cryptography

Part III: Primes and Related Congruence Equations

9-1 PRIMES

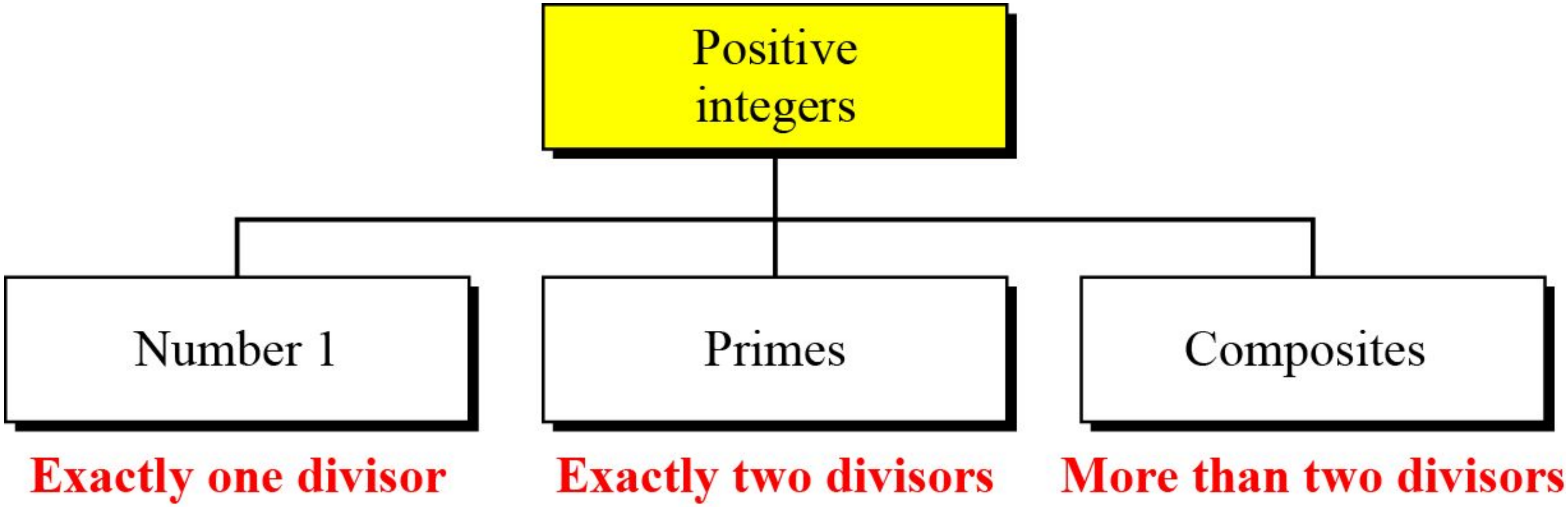
Asymmetric-key cryptography uses primes extensively. The topic of primes is a large part of any book on number theory. This section discusses only a few concepts and facts to pave the way .

Topics discussed in this section:

9.1.1 Definition
9.1.2 Cardinality of Primes
9.1.3 Checking for Primeness
9.1.4 Euler's Phi-Function
9.1.5 Fermat's Little Theorem
9.1.6 Euler's Theorem
9.1.7 Generating Primes

9.1.1 Definition

Figure 9.1 *Three groups of positive integers*



Note

A prime is divisible only by itself and 1.

9.1.1 Continued

Example 9.1

What is the smallest prime?

Solution

The smallest prime is 2, which is divisible by 2 (itself) and 1.

Example 9.2

List the primes smaller than 10.

Solution

There are four primes less than 10: 2, 3, 5, and 7. It is interesting to note that the percentage of primes in the range 1 to 10 is 40%. The percentage decreases as the range increases.

9.1.2 Cardinality of Primes

Infinite Number of Primes

Note

There is an infinite number of primes.

Number of Primes

$$[n / (\ln n)] < \pi(n) < [n/(\ln n - 1.08366)]$$

9.1.3 Checking for Primeness

Given a number n, how can we determine if n is a prime? The answer is that we need to see if the number is divisible by all primes less than

$$\sqrt{n}$$

We know that this method is inefficient, but it is a good start.

Theorem

If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof.

- Let $n = ab,\ 1 < a < n, 1 < b < n$.
- We can't have both $a > \sqrt{n}$ and $b > \sqrt{n}$ since this would lead to $ab > n$.
- Therefore, n must have a prime divisor less than or equal to $\sqrt{n}$.

$\square$

Example 9.5

Is 97 a prime?

Solution

The floor of $\sqrt{97} = 9$. The primes less than 9 are 2, 3, 5, and 7. We need to see if 97 is divisible by any of these numbers. It is not, so 97 is a prime.

Example 9.6

Is 301 a prime?

Solution

The floor of $\sqrt{301} = 17$. We need to check 2, 3, 5, 7, 11, 13, and 17. The numbers 2, 3, and 5 do not divide 301, but 7 does. Therefore 301 is not a prime.

9.1.4 Euler's Phi-Function

Euler's phi-function, φ (n), which is sometimes called the Euler's totient function plays a very important role in cryptography.

1. $\phi(1) = 0.$
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

9.1.4 Continued

We can combine the above four rules to find the value of φ(n). For example, if n can be factored as

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

then we combine the third and the fourth rule to find

$$\boxed{\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) \times (p_2^{e_2} - p_2^{e_2 - 1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k - 1})}$$

Note

The difficulty of finding φ(n) depends on the difficulty of finding the factorization of *n*.

9.1.4 Continued

Example 9.7

What is the value of $\varphi(13)$?

Solution

Because 13 is a prime, $\varphi(13) = (13 - 1) = 12$.

Example 9.8

What is the value of $\varphi(10)$?

Solution

We can use the third rule: $\varphi(10) = \varphi(2) \times \varphi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Example 9.9

What is the value of $\varphi(240)$?

Solution

We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

$$\varphi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$

Example 9.10

Can we say that $\varphi(49) = \varphi(7) \times \varphi(7) = 6 \times 6 = 36$?

Solution

No. The third rule applies when *m* and *n* are relatively prime. Here $49 = 7^2$. We need to use the fourth rule: $\varphi(49) = 7^2 - 7^1 = 42$.

Example 9.11

What is the number of elements in Z_{14}*?

Solution

The answer is $\varphi(14) = \varphi(7) \times \varphi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\varphi(n)$ is even.

9.1.5 Fermat's Little Theorem

First Version

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

Second Version

$$\boxed{a^{p} \equiv a \bmod p}$$

Example 9.12

Find the result of 6^{10} mod 11.

Solution

We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where p = 11.

Example 9.13

Find the result of 3^{12} mod 11.

Solution

Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using Fermat's little theorem.

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\,(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Multiplicative Inverses

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

Example 9.14

The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

9.1.6 Euler's Theorem

First Version

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

Second Version

$$\boxed{a^{k \times \varphi(n) + 1} \equiv a \pmod{n}}$$

Note

The second version of Euler's theorem is used in the RSA cryptosystem

Example 9.15

Find the result of 6^{24} mod 35.

Solution

We have 6^{24} mod 35 = $6^{\varphi(35)}$ mod 35 = 1.

Example 9.16

Find the result of 20^{62} mod 77.

Solution

If we let k = 1 on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\ (20^{\varphi(77)+1} \bmod 77) \bmod 77$$
$$= (20)(20) \bmod 77 = 15.$$

9.1.6 Continued

Multiplicative Inverses

Euler's theorem can be used to find multiplicative inverses modulo a composite.

$$\boxed{a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n}$$

9.1.5 Continued

Example 9.17

The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

9-2 CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

9-2 Continued

Example 9.18

The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is $x = 23$. This value satisfies all equations: $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, and $23 \equiv 2 \pmod{7}$.

9-2 Continued

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

9-2 Continued

Example 9.19

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

9-2 Continued

Example 9.20

Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

Solution

This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

If we follow the four steps, we find x = 276. We can check that 276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

9-2 Continued

Example 9.21

Assume we need to calculate $z = x + y$ where $x = 123$ and $y = 334$, but our system accepts only numbers less than 100.

$$\begin{array}{ll} x \equiv 24 \pmod{99} & \qquad y \equiv 37 \pmod{99} \\ x \equiv 25 \pmod{98} & \qquad y \equiv 40 \pmod{98} \\ x \equiv 26 \pmod{97} & \qquad y \equiv 43 \pmod{97} \end{array}$$

Adding each congruence in x with the corresponding congruence in y gives

$$\begin{array}{lcl} x + y \equiv 61 \pmod{99} & \rightarrow & z \equiv 61 \pmod{99} \\ x + y \equiv 65 \pmod{98} & \rightarrow & z \equiv 65 \pmod{98} \\ x + y \equiv 69 \pmod{97} & \rightarrow & z \equiv 69 \pmod{97} \end{array}$$

Now three equations can be solved using the Chinese remainder theorem to find z. One of the acceptable answers is $z = 457$.