University of Salahaddin - Erbil

College of Engineering

Department of Software Engineering

Data Security

Academic year 2021-2022

4th Year Material

Chapter Six

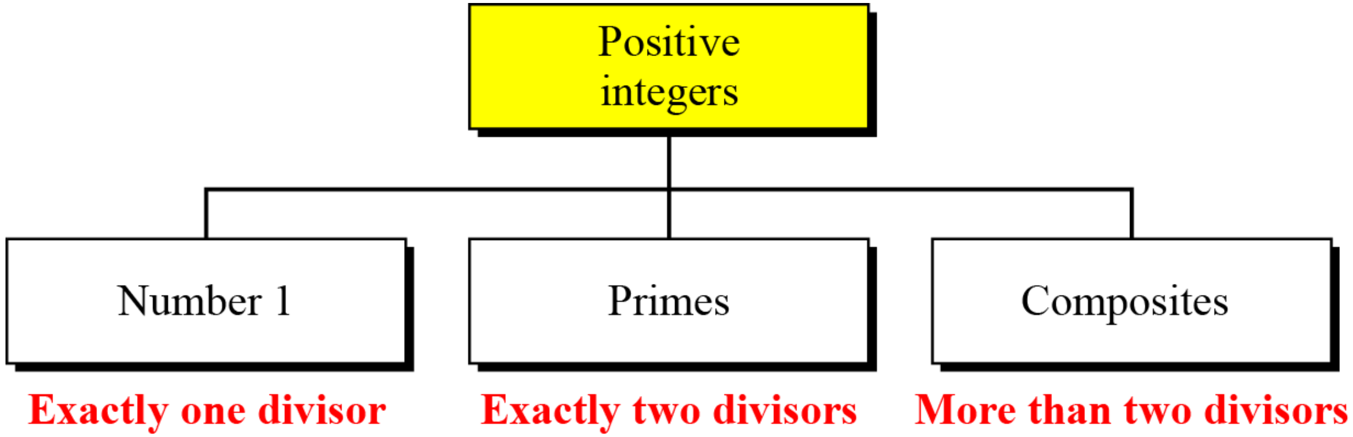
Mathematics of Cryptography

Prepared By: Mr. **Zana Farhad Doghramachi, M.Tech(CSE)**

Zana.softeng@gmail.com

Prime Numbers

- The **Positive integers** can be divided into three groups: the ***number 1***, ***primes*** and ***composites***.
- A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself, it plays a critical role in number theory. A composite is a positive integer with more than two divisors.



Checking for Primeness

- The next question that comes to mind is this; 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.

Homework

Q1 Is 97 a prime?

Q2 Is 45 a prime?

Greatest Common Divisor

- One integer often needed in cryptography is the **greatest common divisor** of two positive integers. Two positive integers may have many common divisors, but only one greatest common divisor.

- For example, the common divisors of 18 and 60 are 1, 2, 3, and 6. However, the greatest common divisor is 6.

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

- The greatest common divisor of two positive integers is the largest integer that can divide both integers.

The Euclidean Algorithm

- 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.

- Finding the ***greatest common divisor*** (**gcd**) of two positive integers by listing all common divisors is not practical when the two integers are large. Fortunately, more than 2000 years ago a mathematician named Euclid developed an algorithm that can find the greatest common divisor of two positive integers.

- The Euclidean algorithm is based on the following two facts:

1. gcd(a,0) = a
2. gcd(a,b) = gcd (b,a mod b)

The Euclidean Algorithm

- The Euclidean algorithm makes repeated use of two facts to determine the greatest common divisor. We use a variable, r to hold the changing values during the process of reduction. The steps are continued until r becomes 0. At this moment, we stop.

- The gcd (a, b) is r.

EUCLID (*a*, *b*)

1. **A $\longleftarrow$ *a*; *B* $\longleftarrow$ *b***
2. **if B = 0 return A = gcd(*a*, *b*)**
3. **r = A mod B**
4. **A $\longleftarrow$ B**
5. **B $\longleftarrow$ r**
6. **goto 2**

Homework

Q1 Find the greatest common divisor of 25 and 60?

Q2 By Using Euclid's Algorithm, find greatest common divisor of 12 and 33?

Extended Euclidean Algorithm

- If gcd(a,b) = 1, then b has a multiplicative inverse modulo a. That is, for positive integer b < a, there exists a $b^{-1} < m$ such that $bb^{-1} = 1 \bmod m$. The Euclidean algorithm can be extended so that, in addition to finding gcd(a,b), if the gcd is 1, the algorithm returns the multiplicative inverse of b.

- EXTENDED EUCLID(a,b)

1. (A1, A2, A3) ⟵ (1, 0, a); (B1, B2, B3) ⟵ (0, 1, b)
2. if B3 = 0 return A3 = gcd(m, b); no inverse
3. if B3 = 1 return B3 = gcd(m, b); B2 = b^{-1} mod m
4. Q = $\lfloor A3/B3 \rfloor$
5. (T1, T2, T3) ⟵ (A1 - QB1, A2 - QB2, A3 - QB3)
6. (A1, A2, A3) ⟵ (B1, B2, B3)
7. (B1, B2, B3) ⟵ (T1, T2, T3)goto 2

Homework

Q1 By Using Extended Euclid's Algorithm, find

1. $28^{-1} \bmod 161$?
2. $4^{-1} \bmod 9$?

Modular Arithmetic

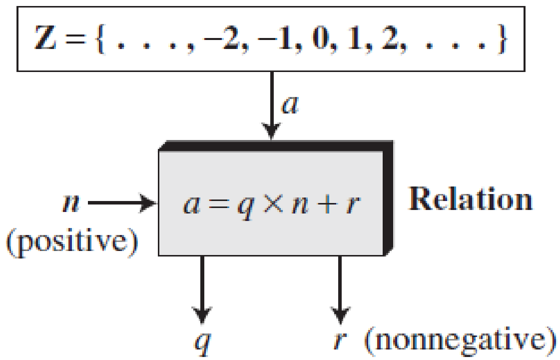
- The division relationship ($a = q \times n + r$) has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r. We don't care about the quotient q. In other words, we want to know what is the value of r when we divide a by n. This implies that we can change the above relation into a binary operator with two inputs a and n and one output r.

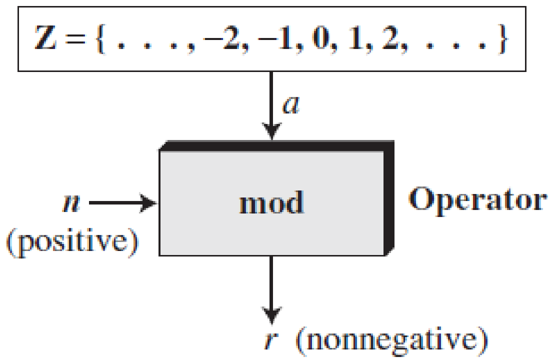
- The binary operator is called the modulo operator and is shown as mod. The second input (n) is called the modulus. The output r is called the residue. The modulo operator (mod) takes an integer (a) from the set Z and a positive modulus (n). The operator creates a nonnegative residue (r), we can say a mod n = r.

Modular Arithmetic

- The result of the modulo operation with modulus **n** is always an integer between **0** and **n-1**. In other words, the result of **a** mod **n** is always a nonnegative integer less than **n**.

- We use modular arithmetic in our daily life; for example, we use a clock to measure time. c uses modulo 12 arithmetic. However, instead of a 0 we use the number 12. So our clock system starts with 0 (or 12) and goes until 11. Because our days last 24 hours, we navigate around the circle two times and denote the first revolution as A.M and the second as P.M.





Inverse in Modular Arithm.

- When we are working in modular arithmetic, we often need to find the **inverse** of a number relative to an operation. We are normally looking for an **additive inverse (**relative to an addition operation) or a **multiplicative inverse (**relative to a multiplication operation).

- **Additive Inverse,** in **Zn,** two numbers a and b are additive inverses of each other if **a + b ≡ 0 (mod n)**, and two numbers a and b are the **multiplicative inverse** of each other if **a × b ≡ 1 (mod n)**.

- In modular arithmetic, each integer has one additive inverse, the sum of an integer and its additive inverse is congruent to 0 modulo n. And an integer may or may not have a multiplicative inverse.

Homework

Q1 Find the result of the following operations:

a. 27 mod 5
b. 36 mod 12
c. -21 mod 15
d. - 7 mod 11

Q2 Find the additive inverse and multiplicative inverse of 3 and 8 in Z_{10}.

Q3 Find all additive and multiplicative inverses in Z_{10}.

Modular Arithm. Operations

- Modular arithmetic exhibits the following properties:

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n
2. [(a mod n) - (b mod n)] mod n = (a - b) mod n
3. [(a mod n) x (b mod n)] mod n = (a x b) mod n

Properties of Modular Arithm.

1. **Commutative laws**
   - (w + x) mod n = (x + w) mod n
   - (w * x) mod n = (x * w) mod n
2. **Associative laws**
   - [(w + x) + y] mod n = [w + (x + y)] mod n
   - [(w * x) * y] mod n = [w * (x * y)] mod n
3. **Distributive laws**
   - [w * (x + y)] mod n = [(w * x) + (w * y)] mod n
   - [w + (x * y)] mod n = [(w + x) * (w + y)] mod n
4. **Identities**
   - (0 + w) mod n = w mod n
   - (1 * w) mod n = w mod n
5. **Additive inverse (-w)**
   - For each w in Zn, there exists a z such that w + z ≡ 0 mod n

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. The function finds the number of integers that are both smaller than n and relatively prime to n, rules to find the value of φ(n).

  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.

- We can combine the above four rules to find the value of φ(n).

- It is very important to notice that the value of (n) for large composites can be found only if the number n can be factored into primes. In other words, the difficulty of finding φ(n) depends on the difficulty of find the factorization of n.

Homework

Q1 Find the value of $\varphi(13)$, $\varphi(10)$ and $\varphi(49)$.