MCA : MCA23203

CRYPTOGRAPHY
&
NETWORK SECURITY

UNIT - 2

Unit-2: Modular Arithmetic

Random Number Generation – Introduction to Groups-ring and field – prime and relative prime numbers – modular arithmetic – Fermat's and Euler's theorem – primality testing – Euclid's Algorithm – Chinese Remainder theorem –discrete algorithms

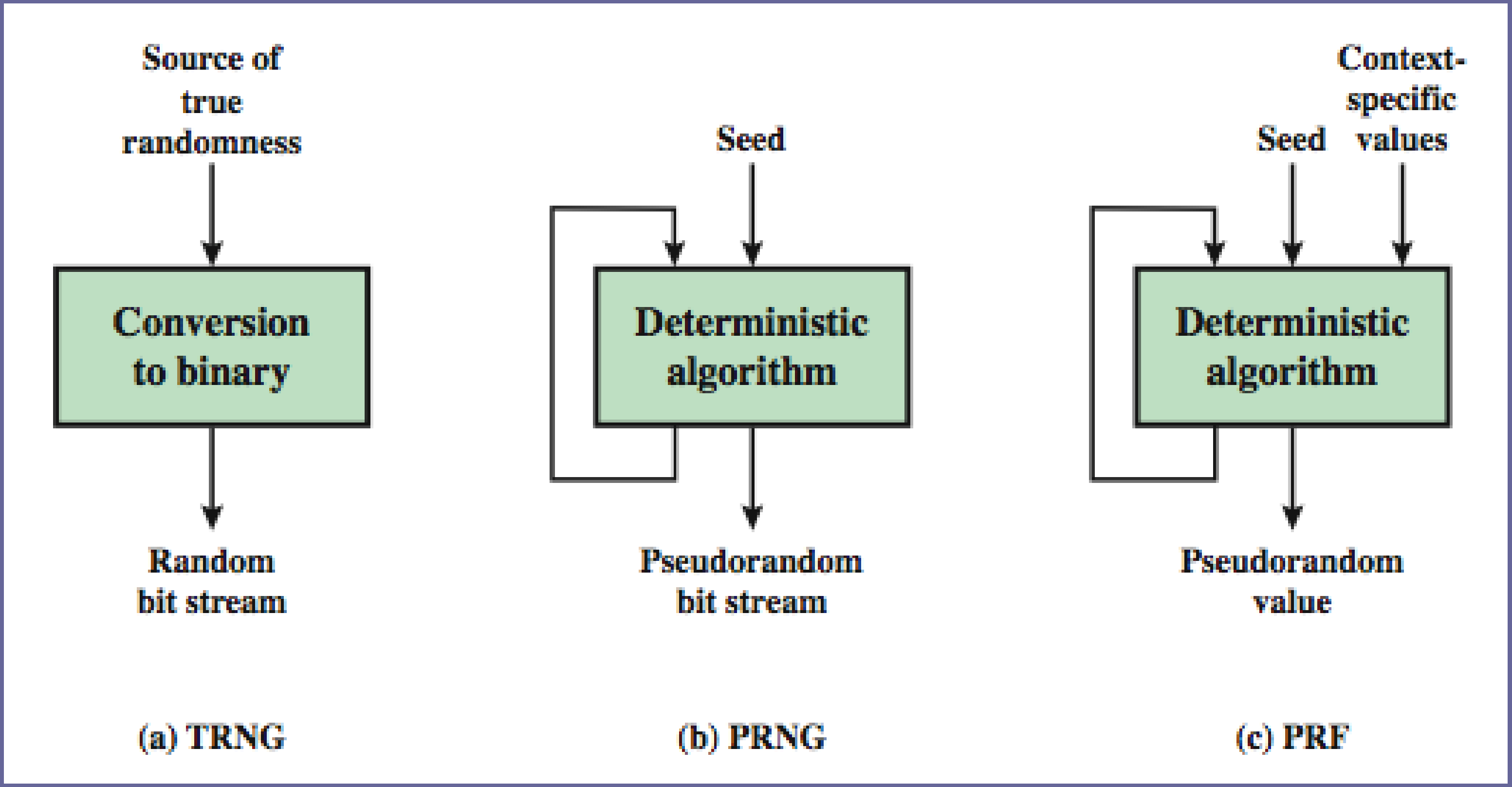
Random Numbers

- many uses of **random numbers** in cryptography
  - nonces in authentication protocols to prevent replay
  - session keys
  - public key generation
  - keystream for a one-time pad
- in all cases its critical that these values be
  - statistically random, uniform distribution, independent
  - unpredictability of future values from previous values
- true random numbers provide this
- care needed with generated random numbers

Pseudorandom Number Generators (PRNGs)

- often use deterministic algorithmic techniques to create “random numbers”
  - although are not truly random
  - can pass many tests of “randomness”
- known as “pseudorandom numbers”
- created by “Pseudorandom Number Generators (PRNGs)”

Random & Pseudorandom Number Generators



PRNG Requirements

- randomness
  - uniformity, scalability, consistency
- unpredictability
  - forward & backward unpredictability
  - use same tests to check
- characteristics of the seed
  - secure
  - if known adversary can determine output
  - so must be random or pseudorandom number

PRNG Requirements

- Randomness
  - Uniformity – at any point in the generation of the PRN sequence, the occurrence of a zero or a one is equally likely (i.e., p = 0.5)
  - Scalability – any test for randomness applicable to a sequence can also be applied to any random subsequence (it should pass)
  - Consistency – the characteristics of the PRN sequence of the PRNG must not depend on the seed used

Linear Congruential Generator

- common iterative technique using:

$$X_{n+1} = (aX_n + c) \bmod m$$

- given suitable values of parameters can produce a long random-like sequence
- suitable criteria to have are:
  - function generates a full-period
  - generated sequence should appear random
  - efficient implementation with 32-bit arithmetic
- note that an attacker can reconstruct sequence given a small number of values
- have possibilities for making this harder

Blum Blum Shub Generator

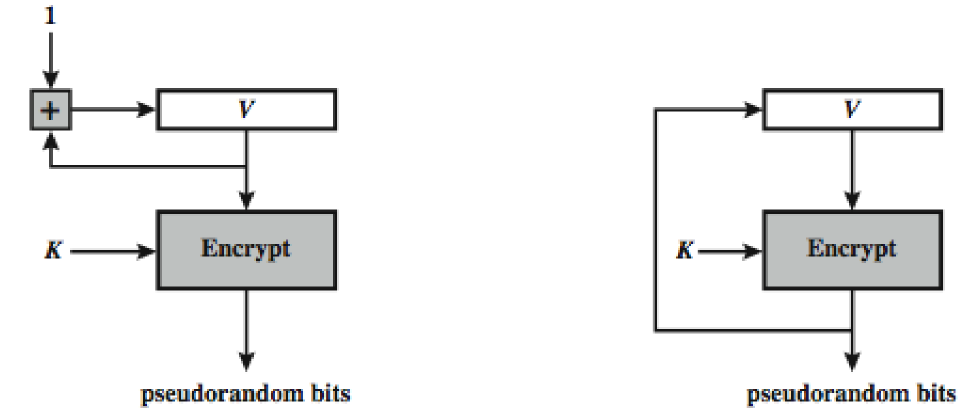
- based on public key algorithms
- use least significant bit from iterative equation:
  - $x_i = x_{i-1}^2 \bmod n$
  - where $n=p.q$, and primes $p,q=3 \bmod 4$
- unpredictable, passes **next-bit** test
- security rests on difficulty of factoring N
- is unpredictable given any run of bits
- slow, since very large numbers must be used
- too slow for cipher use, good for key generation

Using Block Ciphers as PRNGs

- for cryptographic applications, can use a block cipher to generate random numbers
- often for creating session keys from master key
- CTR

  $X_i = E_K[V_i]$
- OFB

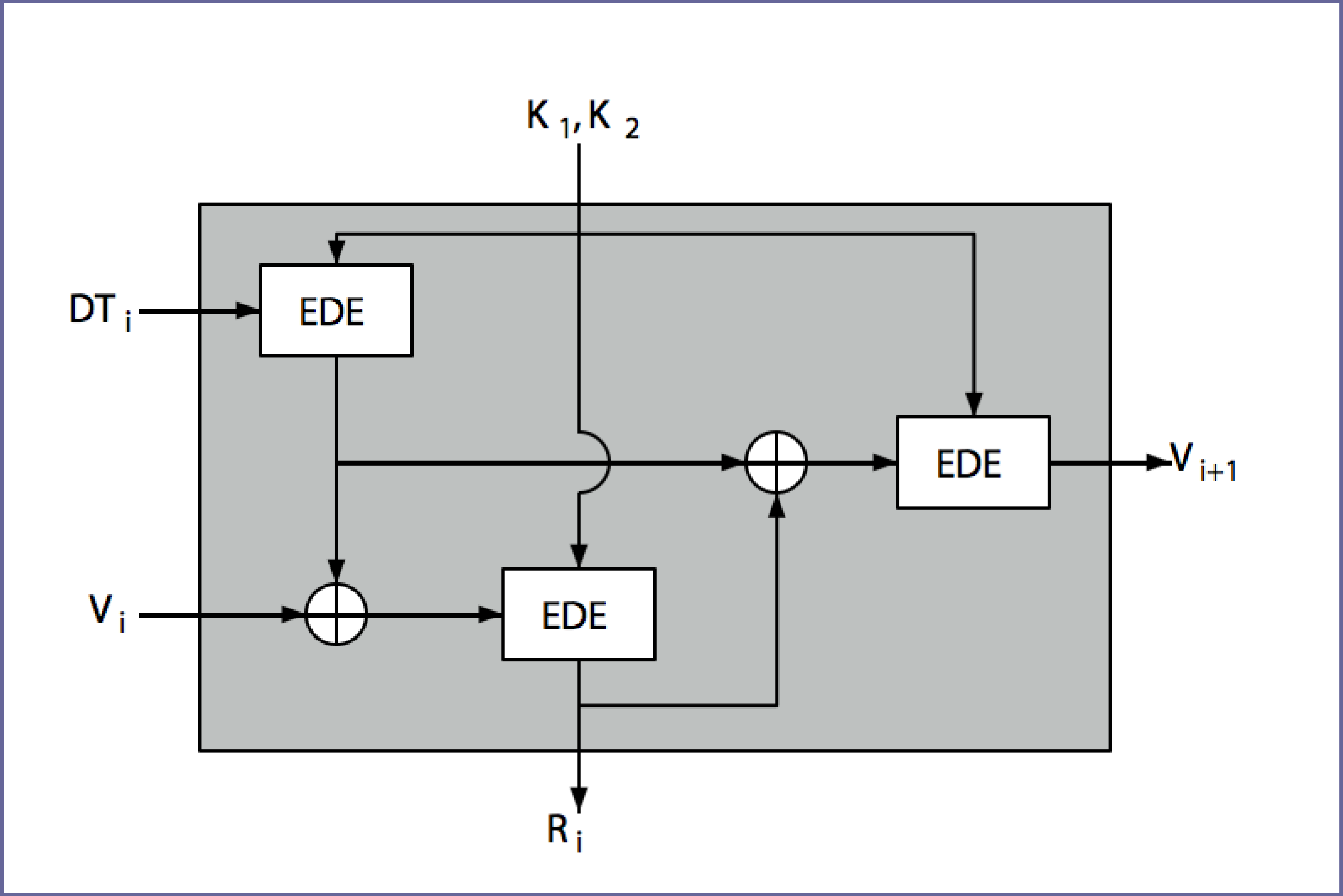
  $X_i = E_K[X_{i-1}]$



(a) CTR Mode

(b) OFB Mode

ANSI X9.17 PRG



Dti = date and time

Groups, Rings, Fields

- *Group*
  - *A set of numbers with some addition operation whose result is also in the set (closure)*
  - *Obeys associative law, has an identity, has inverses*
  - *If also is commutative its an Abelian group*
- *Ring*
  - *An Abelian group with a multiplication operation also*
  - *Multiplication is associative and distributive over addition*
  - *If multiplication is commutative, its a commutative ring*
  - *e.g., integers mod N for any N*
- *Field*
  - *An Abelian group for addition*
  - *A ring*
  - *An Abelian group for multiplication (ignoring 0)*
  - *e.g., integers mod P where P is prime*

Groups

- A ***group***, *G*, is a *set of elements with an associated binary operation*, $\bullet$. It is sometimes denoted $\{G, \bullet\}$
  - For each ordered pair (*a*, *b*) of elements in G, there is an associated element ($a \bullet b$), such that the following axioms hold:

1) ***Closure*** : If a and $b \in G$, then $a \bullet b \in G$

2) ***Associative*** : $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in G$

3) ***Identity element*** : There is an element $e \in G$ such that

$$a \bullet e = e \bullet a = a \text{ for all } a \in G$$

4) ***Inverse element*** : For each $a \in G$ there is an element $a' \in G$ such that

$$a \bullet a' = a' \bullet a = e$$

Groups

- A ***finite group*** is a group with a finite number of elements, otherwise, a group is an ***infinite group***.
- A group is said to be an ***abelian group*** if it satisfies the following condition:

$$5)\ \textbf{\textit{Commutative}}: \qquad a \bullet b = b \bullet a \text{ for all } a, b \in G$$

- Examples of abelian groups:
  - The set of integers (negative, zero, and positive), ***Z***, under addition.
    The identity element of ***Z*** under addition is 0;
    the inverse of *a* is -*a*, for all *a* in ***Z***.
  - The set of non-zero real numbers, ***R****, under multiplication.
    The identity element of ***R**** under multiplication is 1;
    the inverse of *a* is 1/*a* for all *a* in ***R****.

Exponentiation and Cyclic Groups

- ***Exponentiation*** within a group is repeated application of the group operator, such that:

$$a^0 = e, \quad \text{the identity element}$$

$$a^n = a \bullet a \bullet \cdots \bullet a \quad (\text{i.e.} \bullet \text{applied } n\text{-1 times})$$

$$a^{-n} = (a')^n, \text{ where } a' \text{ is the inverse of } a$$

- A group G is ***cyclic*** if every element of G is a power g^k (k is an integer) of a fixed element $g \in G$. The element g is said to ***generate the group***, or to be ***a generator of the group***.
- A cyclic group is always abelian, and may be finite or infinite
  - Example of a cyclic group:
    - The group of positive integers, {***N***, +}, (***N*** = {1, 2, 3, ...}) under addition is an infinite cyclic group generated by the element 1. (i.e. 1 + 1 = 2, 1 + 1 + 1 = 3, etc.)

Rings

- A ***ring***, *R*, denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called ***addition*** (+) ***and multiplication*** ($\times$), such that, for *a*, *b*, *c* in *R*:

addition and ***multiplication*** are abstract operations here

1)-5) ***R is an abelian group with respect to addition***; for this case of an additive group, we denote the identity element as 0, and the inverse of *a* as -*a*.

6) ***Closure under multiplication:***

If *a* and *b* belong to *R*, then $a \times b$ is also in *R*

7) ***Associativity of multiplication:***

$a \times (b \times c) = (a \times b) \times c$ for all *a*, *b*, *c*, in *R*

8) ***Distributive Laws:***

$a \times (b + c) = a \times b + a \times c$ for all *a*, *b*, *c*, in *R*

$(a + b) \times c = a \times c + b \times c$ for all *a*, *b*, *c*, in *R*

Note that we often write $a \times b$ as simply *ab*

Commutative Rings

- A ring is ***commutative*** if it satisfies the following additional condition:

9) ***Commutativity of multiplication:***

a b = b × a for all *a*, *b*, *c*, in *R*

Example of a commutative ring:

The set of even integers, {..., -4, -2, 0, 2, 4, ...}) under the normally defined integer operations of addition and multiplication.

Integral Domains

- An ***integral domain*** is a commutative ring that obeys the following:

10) ***Multiplicative identity:***

There is an element 1 in R such that $a \times 1 = 1 \times a = a$ for all a in R

11)*No zero divisors:*

If a, b in R and $a \times b = 0$, then either $a = 0$ or $b = 0$

Example of an integral domain:

The set of all integers (***Z*** = {..., -3, -2, -1, 0, 1, 2, 3, ...}) under the normally defined integer operations of addition and multiplication, {***Z***, +, $\times$ }

$\times$

Fields

- A ***field***, *F*, denoted by {*F*, +, $\times$}, is a set of elements with two binary operations, called *addition* and *multiplication*, such that, for all *a*, *b*, *c* in *F*, the following apply:

Again, ***addition*** and ***multiplication*** are abstract operations

1)-11) *F is an integral domain*

11) ***Multiplicative inverse:***

For each *a* in *F*, except 0, there is an element a^{-1} in *F* such that:

$a \times a^{-1} = a^{-1} \times a = 1$

Fields

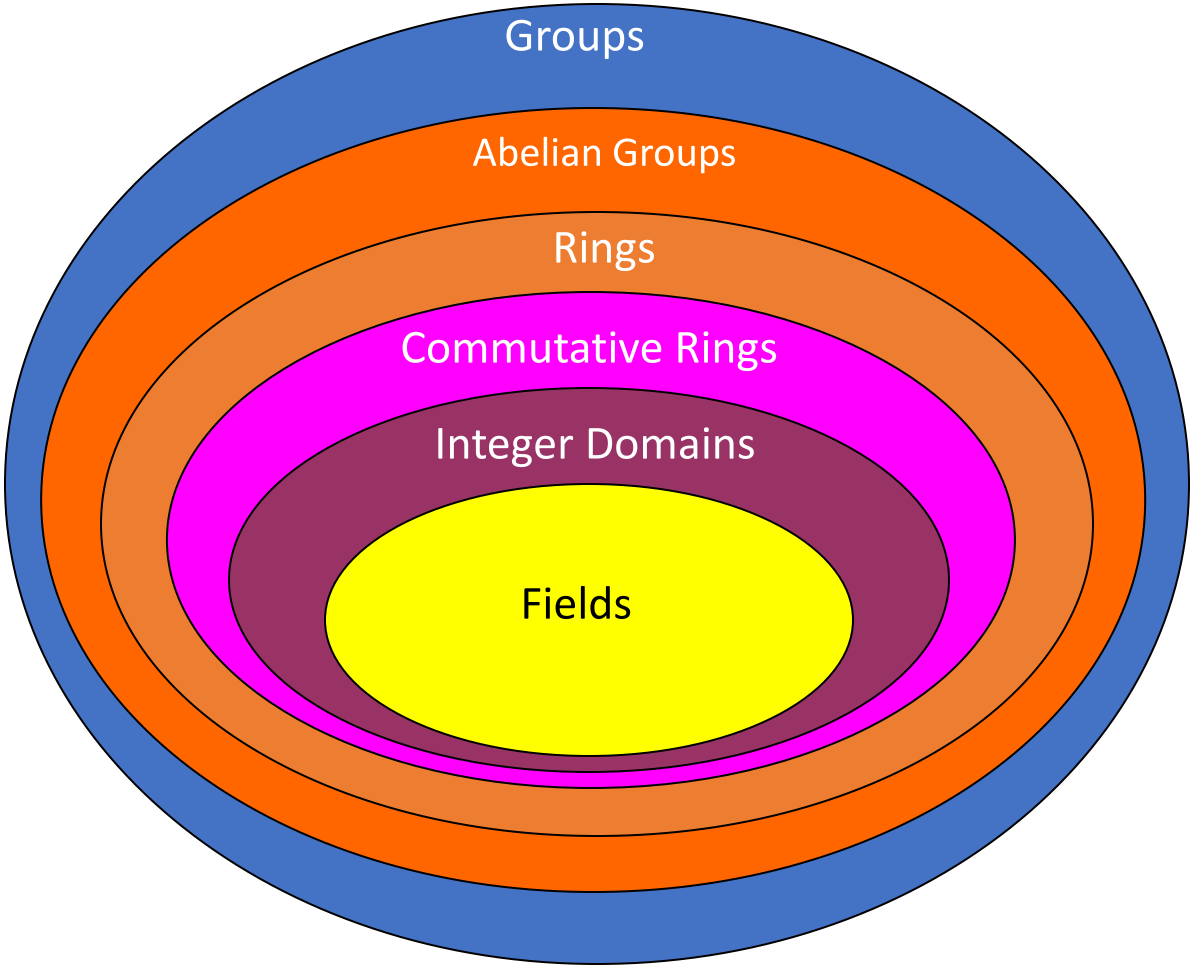
- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
- Division is defined:

$$a/b = a(b^{-1})$$

Examples:

- The set of rational numbers, ***Q***; the set of real numbers, ***R***, the set of complex numbers, ***C***.
- The set of all integers, ***Z***, is *not* a field, because only the elements 1 and -1 have multiplicative inverses in the integers.

Groups, Rings, and Fields



Prime Number

- Prime numbers only have divisors of 1 and self they cannot be written as a product of other numbers.

eg. 2,3,5,7 are prime, 4,6,8,9,10 are not

- prime numbers are central to number theory
- list of prime number less than 200 is:

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59

  61 67 71 73 79 83 89 97 101 103 107 109 113 127

  131 137 139 149 151 157 163 167 173 179 181 191

  193 197 199

- An integer p > 1 is a prime number if and only if its only divisors are ± 1 and ±p.
- 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 p1 < p_2 < … < p_t are prime numbers and where each is a positive integer. This is known as the fundamental theorem of arithmetic

91	= 7 x 13
3600	= 2^4 x 3^2 x 5^2
11011	= 7 x 11^2 x 13

- 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.

Relatively Prime Numbers

- Two numbers a,b are **relatively prime (coprime)** if they have **no common divisors** apart from 1

- eg. 8 and 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor.

Modular Arithmetic

Given two positive integer **n** and **a**, if we divide a by n, we get an integer **quotient q** and an integer **remainder r** that obey the following relationship:

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

Properties of Modular Arithmetic

- Modulo arithmetic over $Z_n = \{0, 1, \ldots, n-1\}$ (called a set of residues of modulo n)
- Integers modulo n with addition and multiplication form a commutative ring
  - *Commutative laws* $(a + b) \bmod n = (b + a) \bmod n$

    $(a \times b) \bmod n = (b \times a) \bmod n$
  - *Associative laws* $[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$

    $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
  - *Distributive laws* $[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
  - *Identities* $(a + 0) \bmod n = a \bmod n$

    $(a \times 1) \bmod n = a \bmod n$
  - *Additive inverse (-a)* $\forall a \in Z_n\ \exists b$ s.t. $a + b \equiv 0 \bmod n$
  - *Multiplicative inverse (a^{-1})* $\forall a\ (\neq 0) \in Z_n$, if a is relative prime to n,

    $\exists b$ s.t. $a \times b \equiv 1 \bmod n$
- ***If n is not prime, Z_n is a ring, but not a field***
- ***Z_p is a field***

Modular Arithmetic Operations

- *Modulo arithmetic operation over* $Z_n = \{0, 1, \ldots, n\text{-}1\}$
- *Properties*
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Table 7.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Modular 7 Arithmetic

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	-w	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

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.

Greatest Common Divisor

- **The greatest common divisor of a and b is the largest integer that** divides both a and b . We also define gcd(0, 0) = 0.
- 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:

  gcd(a, b) = max[k, such that k|a and k|b]

  gcd(60, 24) = gcd(60,-24) = 12

In general, gcd(a, b) = gcd(|a|, |b|).

Finding the Greatest Common Divisor

- The Euclidean algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

$$\gcd(a,b)=\gcd(b, a \bmod b)$$

$$\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$$

$$
\left.
\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\quad\bullet & \quad\bullet \\
\quad\bullet & \quad\bullet \\
\quad\bullet & \quad\bullet \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 & \\
d = \gcd(a, b) = r_n &
\end{array}
\right\}
$$

Example GCD(1970,1066)

```
1970 = 1 x 1066 + 904  gcd(1066, 904)
1066 = 1 x 904 + 162   gcd(904, 162)
904 = 5 x 162 + 94     gcd(162, 94)
162 = 1 x 94 + 68      gcd(94, 68)
94 = 1 x 68 + 26       gcd(68, 26)
68 = 2 x 26 + 16       gcd(26, 16)
26 = 1 x 16 + 10       gcd(16, 10)
16 = 1 x 10 + 6        gcd(10, 6)
10 = 1 x 6 + 4         gcd(6, 4)
6 = 1 x 4 + 2          gcd(4, 2)
4 = 2 x 2 + 0          gcd(2, 0)
GCD(1970,1066)=2
```

CONGRUENT MODULO

- Two integers a and b are said to be congruent modulo of n if

  a mod n= b mod n.

then this is written as **a ≡ b mod n.**

Ex: a=73 b=4 and n=23

73 mod 23 =4

4 mod 23 =4

So 73 ≡ *4 mod 23*

Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ if $n|(a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

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

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

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

- a=7 p=19

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

Euler's Totient Function

- It is defined as the number of positive integers less than 'n' and relatively prime to 'n' and is written as ø(n). By convention ø(1)=1.
- It should be clear that, for a prime number p,

$$ø(p) = p - 1$$

$$ø(37) = 36$$

- To determine ø(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 . ø(35) = 24

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

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

$$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$$

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:

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

THE 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:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

The Chinese remainder theorem states that the above equations have a unique solution if the moduli are relatively prime.

SOLUTION The solution to the set of equations follows these steps:

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 $M_1, M_2, \ldots, M_k$ using the corresponding moduli $(m_1, m_2, \ldots, m_k)$. Call the inverses

   $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$.
4. The solution to the simultaneous equations is

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

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

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

EXAMPLE 9.37 Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

$x \equiv 3 \bmod 7$

$x \equiv 3 \bmod 13$

$x \equiv 0 \bmod 12$

$x = 276$

Primality Test

Naïve Primality Test

Input: Integer $n > 2$

Output: PRIME or COMPOSITE

```
for (i from 2 to n-1){
    if (i divides n)
        return COMPOSITE;
}
return PRIME;
```

Still Naïve Primality Test

Input/Output: same as the naïve test

for (*i* from 1 to $\sqrt{n}$){

    if (*i* divides *n*)

        return COMPOSITE;

}

return PRIME;

Primality Testing

Two categories of primality tests

- Probablistic
  - Miller-Rabin Probabilistic Primality Test
  - Cyclotomic Probabilistic Primality Test
  - Elliptic Curve Probabilistic Primality Test
- Deterministic
  - Miller-Rabin Deterministic Primality Test
  - Cyclotomic Deterministic Primality Test
  - Agrawal-Kayal-Saxena (AKS) Primality Test

Running Time of Primality Tests

- Miller-Rabin Primality Test
  - Polynomial Time
- Cyclotomic Primality Test
  - Exponential Time, but *almost* poly-time
- Elliptic Curve Primality Test
  - Don’t know. Hard to Estimate, but *looks* like poly-time.
- AKS Primality Test
  - Poly-time, but only asymptotically good.