DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA

UNIVERSITY'S MOHAMED BOUDIAF OF M'SILA

Faculty of Mathematics and computer sciences

Department of Mathematics

END OF STUDY MEMORANDUM

Presented to obtain the MASTER Diploma in Mathematics and Computer Science Option Mathematics

Field: Mathematics and Computer Science

Speciality: Mathematics

Option : Algebre and Discrete Mathematics

By

BOUKHALET Fouzia

Title

Congruences and application on cryptography

Date of Graduation Ceremony **: 01/07/2019**

Master's committee :

Mr HABOUB Lakhdar	M.A.A. Univ OF M'sila	President
Mr.MIHOUBI Douadi	Prof. Univ of M'sila	Advisor
Mr.GHADBANE Nacer	M.A.A. Univ of M'sila	Examiner

Promotion : 2018 / 2019

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the God, the Almighty, which made it easier for me to accomplish this work and gave me the strength of patience to complete it.

Iwould like to express my deep and sincere gratitude to my framer Mr.MIHOUBI Douadi, professor of mathematics at the university Mohamed BOUDHIAF-M'sila-to help him value and good guidance. It was great privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me.

I would also like to thank the members of the jury, Mr. Lakhdar HABOUB as president and Mr. Nacer GHADBANE as examiner.

In the finely, i would like to thank my parents, my brothers and sisters, all my friends and all those who helped me a lot in finalizing this work within the limited time frame.

Thanks.

Contents

Notations

- $\mathbb{Z}$ set of integers
- $a \backslash b$ $a \in \mathbb{Z}$ divides $b \in \mathbb{Z}$
- G Represent the group
- $o(G)$ or $|G|$ The number of elements in G
- H Represent the subgroup
- $\mathbb{Z}_n$ Residue class modulo n
- $\mathbb{Z}_n^*$ The invertible group
- φ Euler phi-function
- $log_g(h)$ Logarithm in base b of n

Introduction

Number theory plays a key role in cryptography, the subject of transforming information that it cannot be easily recovered without special knowledge. It is also the basis of many classical cipher, first used thousands of years ago. Accordingly, the purpose of this memo is to study congruences in $\mathbb{Z}$ and application on cryptography.

In the introductory chapter (Fundamentals Algebra), we set up notions on divisibility the first section, and the theory of groups in the second and last section.

The second chapter, devoted to the study of the congruences and their properties, without exception the most famous theories, the chinese remainder theorem, wilson's theorem, fermat's theorem, euler's theorem, who have great role in cryptography.

In the third chapter, we explain the concept of cryptography and the role of congruences in the encryption and decryption methods of cryptography.

Chapter 1

Fundamentals Algebra

The aim of this chapter is to recall some notions about the divisibility over the ring $\mathbb{Z}$ and the elementary results of arithmetic.

1.1 Notions on divisibility

1.1.1 Divisibility

Definition 1.1.1 *Let a and b be integers with $b \neq 0$. We say that b divides a, or that a is divisible by b, if there is an integer c such that*

$$a = bc.$$

We write $b|a$ to indicate that b divides a. If b does not divide a, then we write $b \nmid a$.

Proposition 1.1.1 *Let a, b, $c \in \mathbb{Z}$ be integers.*

1. If $a|b$ and $b|c$, then $a|c$.
2. If $a|b$ and $b|a$, then $a = \pm b$.
3. If $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.

1.1.2 Prime numbers and unique factorization

Definition 1.1.2 *An integer p is called a prime if $p \geq 2$ and if the only positive integers dividing p are 1 and p.*

Proposition 1.1.2 *Let p be a prime number, and suppose that p divides the product ab of two integers a and b. Then p divides at least one of a and b. More generally, if p divides a product of integers, say*

$$p|a_1a_2\cdots a_n,$$

then p divides at least one of the individual a_i.

Theorem 1.1.1 *(The Fundamental Theorem of Arithmetic). Let $a \geq 2$ be an integer. Then a can be factored as a product of prime numbers*

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_r^{e_r}.$$

Further, other than rearranging the order of the primes, this factorization into prime powers is unique.

Proof. It is not hard to prove that every $a \geq 2$ can be factored into a product of primes. It is tempting to assume that the uniqueness of the factorization also obvious. However, this is not the case; unique factorization is a somewhat subtle property of the integers. We will prove it using the general form of Proposition 1.1.2. Suppose that a has two factorizations into products of primes,

$$a = p_1p_2\cdots\ p_s = q_1q_2\cdots q_t, \qquad (*)$$

where the p_i and q_j are all primes, not necessarily distinct, and s does not necessarily equal t. Since $p_1|a$, we see that p_1 divides the product $q_1q_2\cdots q_t$. Thus by the general form of Proposition 1.1.2, we find that p_1 divides one of the q_i. Rearranging the order of the q_i

if necessary, we may assume that $p_1|q_1$. But p_1 and q_1 are both primes, so we must have $p_1 = q_1$. This allows us to cancel them from both sides of $(*)$, which yields

$$p_2 p_3 \cdots \ p_s = q_2 q_3 \cdots q_t.$$

Repeating this process s times, we ultimately reach an equation of the form

$$1 = q_{t-s} q_{t-s+1} \cdots q_t.$$

It follows immediately that $t = s$ and that the original factorizations of a were identical up to rearranging the order of the factors. ■

1.1.3 The Division Algorithm

Theorem 1.1.2 *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r \qquad 0 \leq r < b$$

The integers q and r are called, respectively, the quotient and remainder in the division of a by b.

1.1.4 The Greatest Commun Divisors

Let a and b be integers. An integer d is called a common divisor of a and b if $d|a$ and $d|b$.

Definition 1.1.3 *Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $gcd(a, b)$, is the positive integer d sitisfying the following:*

- $d|a$ and $d|b$.
- If $c|a$ and $c|b$, then $c \leq d$.

Definition 1.1.4 *If $gcd(a, b) = 1$, the number a and b are said to be relatively prime (or coprime).*

Example 1.1.1 *Let $a = 24$ and $b = 17$. the $gcd(a, b) = gcd(24, 17) = 1$, so a and b are relatively prime.*

Theorem 1.1.3 ***Euclids lemma**. If $a|bc$, with $gcd(a, b) = 1$, then $a|c$.*

Lemma 1.1.1 *Given integers a, b, c, $gcd(a, bc) = 1$ if and only if $gcd(a, b) = 1$ and*

$gcd(a, c) = 1$.

1.1.5 The Euclidean Algorithme

Proposition 1.1.3 *Let a, b, q, r be any integers such that $a = qb + r$. Then $gcd(a, b) = gcd(b, r)$.*

Proof. Indeed, if d is a common divisor of a and b, we have $a = a'd$ and $b = b'd$. Then $r = a - qb = a'd - qb'd = (a' - qb')d$ and d is also a common divisor of b and r. Also, if d is a common divisor of b and r, then $b = b'd$, $r = r'd$ and $a = qb + r = qb'd + r'd = (qb' + r')d$, whence d is a common divisor of a and b. ■

Theorem 1.1.4 *(The Euclidean Algorithm) Let a and b be positive integers. We use the division algorithm several times to find:*

$$\begin{aligned}
a &= q_1 b + r_1,\ 0 < r_1 < b,\\
b &= q_2 r_1 + r_2,\ 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3,\ 0 < r_3 < r_2,\\
&\ \ \vdots\\
r_{s-2} &= q_s r_{s-1} + r_S,\ 0 < r_S < r_{s-1},\\
r_{s-1} &= q_{s+1} r_s.
\end{aligned}$$

Then $r_s = gcd(a, b)$.

Proof. By Proposition 1.1.3. $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) =\cdot\cdot\cdot = gcd(r_{s-1}, r_s) = r_s$. ■

We are now going to analyse an example to understand how to use Euclidean algorithm to find a greatest commun divisor

Example 1.1.2 *Let $a = 321$, $b = 843$. Find the greatest common divisor $gcd(a, b)$.*

The Euclidean algorithm yields

$$\begin{aligned} 321 &= 0 \cdot\ 843 + 321 \\ 843 &= 2 \cdot\ 321 + 201 \\ 321 &= 1 \cdot\ 201 + 120 \\ 201 &= 1 \cdot 120 + 81 \\ 120 &= 1 \cdot\ 81 + 39 \\ 81 &= 2 \cdot\ 39 + 3 \\ 39 &= 13 \cdot\ 3 + 0, \end{aligned}$$

and therefore $gcd(321, 843) = 3$.

1.1.6 Bezout's identity

The Euclidean algorithm also provides a way of proving that a relation of the form

$$GCD(a, b) = \alpha a + \beta b \qquad (**)$$

holds, with α and β suitable integers. Equation $(**)$ is called **Bezout's identity** and turns out to be very useful. For instance, it is the starting point for the resolution of linear

Diophantine equations, which we shall shortly deal with, and linear congruences, which will be covered in the next chapter.[**4**]

Proposition 1.1.4 *Let a and b be two positive integers. They are coprime if and only if there exist two integers α, β such that*

$$\alpha a + \beta b \quad = 1.$$

Proof. If a and b are coprime, we have $GCD(a, b) = 1$ and the claim follows from Bezout's identity.

On the other hand, suppose equation $(**)$ holds. Let d be a common divisor of a and b. Then clearly d divides $\alpha a + \beta b$ too, and so divides 1. Thus either $d = 1$ or $d = -1$, and consequently a and b are relatively prime. ■

We are now going to analyse an example to understand how to use Euclidean algorithm to find a Bezout relation.

Example 1.1.3 *We intend to find a Bezout's identity for $GCD(1245, 56)$. Following the Euclidean algorithm, we proceed as follows:*

$$\begin{aligned} 1245 &= 56 \cdot 22 + 13, \\ 56 &= 13 \cdot 4 + 4, \\ 13 &= 4 \cdot 3 + 1, \\ 4 &= 1 \cdot 4 + 0. \end{aligned}$$

So we find $GCD(1245, 56) = 1$. Now we want to express 1 in the form $\alpha a + \beta b$, with $a = 1245, b = 56$.

Firstly, we rewrite the steps of Euclidean algorithm as follows:

$$\begin{aligned} 13 &= 1245 - 56 \cdot 22 \\ 4 &= 56 - 13 \cdot 4 \\ 1 &= 13 - 4 \cdot 3 \end{aligned}$$

hence

$1 = 13-4\cdot 3 = 13-(56-13\cdot 4)\cdot 3 = (-3)\cdot 56+(13)\cdot 13 = (-3)\cdot 56+(13)\cdot(1245-56\cdot 22) = (-289)\cdot 56 + (13)1245.$

so a Bezout's identity for $GCD(1245, 56)$ is

$$1 = (-289) \cdot 56 + 13 \cdot 1245$$

Corollary 1.1.1 *If $gcd(a, b) = d$, then $gcd(a/d, b/d) = 1$.*

1.1.7 Linear Diophantine equation

We now want to study the so-called linear Diophantine equations. These are equations of the form

$$ax + by = c,$$

where a, b, c are in $\mathbb{Z}$. The case when a or b is equal to zero is trivial, so we omit it. We want to ascertain whether the equation admits integer solutions, that is solutions (x, y) with $x, y \in \mathbb{Z}$.

The following theorem gives a necessary and sufficient condition for the equation $ax + by = c$ to admit integer solutions.[**4**]

Theorem 1.1.5 *The Linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + (b/d)t \qquad\qquad y = y_0 - (a/d)t$$

Where t is an arbitrary integer.

Proof. To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by'$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y')$$

By the corollary1.1.1. There exist relatively prime integers r and s such that $a = dr, b = ds$. Substituting the values into the last-written equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y')$$

The situation is now this: $r|s(y_0 - y')$, with $gcd(r, s) = 1$. Using Euclids's lemma, it must be the case that $r|(y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st$$

This leads us to the formulas

$$\begin{aligned} x' &= x_0 + st = x_0 + (b/d)t \\ y' &= y_0 - rt = y_0 - (a/d)t \end{aligned}$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for

$$\begin{aligned} ax' + by' &= a\left[x_0 + (b/d)t\right] + b\left[y_0 - (a/d)t\right] \\ &= (ax_0 + by_0) + (ab/d - ab/d)t \\ &= c + 0 \cdot t \\ &= c \end{aligned}$$

Thus, there are an infinite number of solutions of the given equation, one for each value of t. ■

Example 1.1.4 *Consider the Linear Diophantine equation*

$$172x + 20y = 1000$$

Applying the Euclidean's Algorithm to the evaluation of $gcd(172, 20)$, we find that

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

Whence $gcd(172, 20) = 4$. Because $4|1000$, a solution to this equation exists. To obtaine the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ 4 &= 12 - (20 - 12) \\ 4 &= 2 \cdot 12 - 20 \\ 4 &= 2(172 - 8 \cdot 20) - 20 \\ 4 &= 2 \cdot 172 + (-17)20 \end{aligned}$$

Upon multiplying this relation by 250, we arrive at

$$\begin{aligned} 1000 &= 250 \cdot 4 \\ &= 250\,[2 \cdot 172 + (-17)20] \\ &= 500 \cdot 172 + (-4250)20 \end{aligned}$$

So that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question. All other solutions are expressed by

$$\begin{aligned} x &= 500 + (\frac{20}{4})t = 500 + 5t \\ y &= -4250 - (\frac{172}{4})t = -4250 - 43t \end{aligned}$$

1.2 The theory of Groups

1.2.1 Binary operation

Definition 1.2.1 *A **binary operation** on a nonempty set $\boldsymbol{A}$ is a mapping f from $\boldsymbol{A}\times\boldsymbol{A}$ to $\boldsymbol{A}$.*

Definition 1.2.2 ***Commutativity, Associativity.*** *If $*$ is a binary operation on the nonempty set $\boldsymbol{A}$, then $*$ is called **commutative** if $x * y = y * x$ for all x and y in $\boldsymbol{A}$. If $x * (y * z) = (x * y) * z$ for all x, y, z in $\boldsymbol{A}$, then we say that the binary operation is **associative**.*

Definition 1.2.3 ***Closure.*** *Suppose that $*$ is a binary operation on a nonempty set $\boldsymbol{A}$, and let $\boldsymbol{B} \subseteq \boldsymbol{A}$. If $x * y$ is an element of $\boldsymbol{B}$ for all $x \in \boldsymbol{B}$ and $y \in \boldsymbol{B}$, then $\boldsymbol{B}$ is closed with respect to $*$.*

Definition 1.2.4 ***Identity Element.*** *Let $*$ be a binary operation on the nonempty set $\boldsymbol{A}$. An element e in $\boldsymbol{A}$ is called an **identity element** with respect to the binary operation $*$ if e has the property that*

$$e * x = x * e = x$$

for all $x \in \boldsymbol{A}$.

Definition 1.2.5 ***Right Inverse, Left Inverse, Inverse.*** *Suppose that e is an identity element for the binary operation $*$ on the set $\boldsymbol{A}$, and let $a \in \boldsymbol{A}$. If there exists an element $b \in \boldsymbol{A}$ such that $a * b = e$, then b is called a **right inverse** of a with respect to this operation. Similarly, if $b * a = e$, then b is called a **left inverse** of a. If both of $a * b = e$ and $b * a = e$ hold, then b is called an **inverse** of a, and a is called an **invertible** element of $\boldsymbol{A}$.*

1.2.2 Group

Definition 1.2.6 *Suppose the binary operation $*$ is defined for elements of the set G. Then G is a group with*

respect to $*$ provided the following four conditions hold:

1. G is closed under $*$. That is, $x \in G$ and $y \in G$ imply that $x * y$ is in G.
2. $*$ is associative. For all x,y,z in G, $x * (y * z) = (x * y) * z$.
3. G has an identity element e. There is an e in G such that $x * e = e * x = x$ for all $x \in G$.
4. G contains inverses. For each $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$.

Example 1.2.1 *:*

1. $(\mathbb{Z}, +)$ the set $\mathbb{Z}$ of all integers is a group with respect to addition, so the identity element is 0.
2. $(\mathbb{R}^*, \times)$ the set $\mathbb{R}^*$ of all the real numbers except zero is a group with respect to multiplication, so the identity element is 1.

Abelian Group

Definition 1.2.7 *Let G be a group with respect to $*$. Then G is called a commutative group, or an abelian group, if $*$ is commutative. That is, $x * y = y * x$ for all x, y in G.*

1. $(\mathbb{Z}, +)$ and $(\mathbb{R}^*, \times)$ are abelian groups.
2. $(\mathbb{C}, +)$ The set $\mathbb{C}$ of all complex numbers is an abelian group with respect to addition.

Finite Group, Infinite Group, Order of a Group

Definition 1.2.8 *If a group G has a finite number of elements, G is called a finite group, or a group of finite order.*

The number of elements in G is called the order of G and is denoted by either $o(G)$ or $|G|$.

If G does not have a finite number of elements, G is called an infinite group.

Properties of Group Elements

Let G be a group with respect to a binary operation that is written as multiplication.

- The identity element e in G is unique.
- For each $x \in G$, the inverse x^{-1} in G is unique.
- For each $x \in G$, $(x^{-1})^{-1} = x$
- Reverse order law. For any x and y in G, $(xy)^{-1} = y^{-1}x^{-1}$.
- Cancellation laws. If a, x, and y are in G, then either of the equations $ax = ay$ or $xa = ya$ implies that $x = y$.

1.2.3 Subgroup

Definition 1.2.9 *Let G be a group with respect to the binary operation $*$. A subset H of G is called a subgroup of G if H forms a group with respect to the binary operation $*$ that is defined in G.*

The following two theories gives the equivalent set of condition for a subgroup.

Theorem 1.2.1 *A subset H of the group G is a subgroup of G if and only if these conditions are satisfied:*

1. H is nonempty;
2. $x \in H$ and $y \in H$ imply $xy \in H$; and
3. $x \in H$ implies $x^{-1} \in H$.

Theorem 1.2.2 *A subset H of the group G is a subgroup of G if and only if*

1. H is nonempty; and

2. $x \in H$ and $y \in H$ imply $xy^{-1} \in H$.

1.2.4 Cyclic Groups

a group G was defined to be cyclic if there exists an element $a \in G$ such that $G = \langle a \rangle$. It may happen that there is more than one element $a \in G$ such that $G = \langle a \rangle$. For the additive group $\mathbb{Z}$, we have $\mathbb{Z} = \langle 1 \rangle$ and also $\mathbb{Z} = \langle -1 \rangle$.

Definition 1.2.10 *Any element a of the group G such that $G = \langle a \rangle$ is a **generator** of G.*

Theorem 1.2.3 *Let a be an element in the group G. If $a^n \neq e$ for every positive integer n, then $a^p \neq a^q$ whenever $p \neq q$ in $\mathbb{Z}$, and $\langle a \rangle$is an **infinite cyclic group**.*

Corollary 1.2.1 *If G is a finite group and $a \in G$, then $a^n = e$ for some positive integer n.*

Theorem 1.2.4 *Let a be an element in a group G, and suppose $a^n = e$ for some positive integer n. If m is the least positive integer such that $a^m = e$, then*

1. $\langle a \rangle$ has order m, and $\langle a \rangle = \{a^0 = e = a^m, a^1, a^2, ..., a^{m-1}\}$

2. $a^s = a^t$ if and only $s \equiv t \pmod{m}$.

1.2.5 Ring

Definition 1.2.11 *Suppose R is a set in which a relation of equality, denoted by $=$, and operations of addition and multiplication, denoted by $+$ and $\cdot$, respectively, are defined. Then R is a ring (with respect to these operations) if the following conditions are satisfied:*

1. R is closed under addition: $x \in R$ and $y \in R$ imply $x + y \in R$.

2. Addition in R is associative: $x + (y + z) = (x + y) + z$ for all x, y, z in R.

3. R contains an additive identity 0: $x + 0 = 0 + x = x$ for all $x \in R$.

4. R contains additive inverses: For x in R, there exists $-x$ in R such that $x + (-x) = (-x) + x = 0$.

5. Addition in R is commutative: $x + y = y + x$ for all x, y in R.

6. R is closed under multiplication: $x \in R$ and $y \in R$ imply $x \cdot y \in R$.

7. Multiplication in R is associative: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all x, y, z in R.

8. Two distributive laws hold in R: $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$ for all x, y, z in R.

Example 1.2.2 *$(\mathbb{Z}_n, +, \times)$ forms a ring.(see congruence classes).*

Ring with Unity, Commutative Ring

Definition 1.2.12 *Let R be a ring. If there exists an element e in R such that $x \cdot e = e \cdot x = x$ for all x in R, then e is called a unity, and R is a ring with unity. If multiplication in R is commutative, then R is called a commutative ring.*

Theorem 1.2.5 *If R is a ring that has a unity, the unity is unique*

Multiplicative Inverse

Definition 1.2.13 *Let R be a ring with unity e, and let $a \in R$. If there is an element x in R such that $ax = xa = e$, then x is a multiplicative inverse of a and a is called a unit (or an invertible element) in R.*

Theorem 1.2.6 *Suppose R is a ring with unity e. If an element $a \in R$ has a multiplicative inverse, the multiplicative inverse of a is unique.*

1.2.6 Subring

Definition 1.2.14 *Whenever a ring R_1 is a subset of a ring R_2 and has addition and multiplication as defined in R_2, we say that R_1 is a subring of R_2.*

The following theorem gives the equivalent set of condition for a Subring.

Theorem 1.2.7 *A subset S of the ring R is a subring of R if and only if these conditions are satisfied:*

1. S is nonempty.
2. $x \in S$ and $y \in S$ imply that $x + y$ and $x \cdot y$ are in S.
3. $x \in S$ implies $-x \in S$.

Characterization of a Subring

Theorem 1.2.8 *A subset S of the ring R is a subring of R if and only if these conditions are satisfied:*

1. S is nonempty.
2. $x \in S$ and $y \in S$ imply that $x - y$ and $x \cdot y$ are in S.

1.2.7 Field

Definition 1.2.15 *Let F be a ring. Then F is a field provided these conditions hold:*

1. F is a commutative ring.
2. F has a unity e, and $e \neq 0$.
3. Every nonzero element of F has a multiplicative inverse.

Let $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$. (See congruence classes)

Corollary 1.2.2 *$\mathbb{Z}_n$ is a field if and only if n is a prime.*

Chapter 2

Congruences

2.1 Introduction to Congruences

Another approach to divisibility questions is through the arithmetic of remainders, or the theory of congruences as it now commonly know. The concept, and the notation that makes it such a powerful tool, was first introduced by the German mathematician Carl Friedrich Gauss (he explains that he was induced to adopt the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If the number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent." putting this into the form of the following definition.[**2**]

2.1.1 Definition of congruences

Definition 2.1.1 *Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by*

$$a \equiv b \ (mod \ n)$$

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k. On the other hand, if $n \nmid (a - b)$, we say that a is incongruent to b modulo n, and in this case we write

$$a \not\equiv b \ (mod \ n)$$

Let's rewrite the definition in terms of our earlier notion of divisibility. For n to divide $a - b$, we must have an integer k so that $a - b = kn$.

Written another way, for a and b to be congruent modulo n requires an integer k that makes the equation $a = b + kn$ true.

Proposition 2.1.1 *If a and b are integers, then $a \equiv b \ (mod\ n)$, if and only if there is an integer k such that $a = b + kn$.*

Proof. If $a \equiv b \ (mod\ n)$, then $n|(a - b)$. This means that there is an integer k with $a - b = kn$, so that $a = b + kn$ ■

Let a be an integer. Given the positive integer n, $n > 1$, by the division algorithm, we have $a = bn + r$ where $0 \leq r \leq n - 1$. From the equation $a = bn + r$, we see that $a \equiv r(\mathrm{mod}\, n)$. So any integer a is congruent to its remainder when divided by n. This means that any a is congruent to one of

$$0, 1, 2, ..., n - 1$$

Theorem 2.1.1 *For arbitrary integers a and b, $a \equiv b \ (mod\ n)$ if and only if a and b leave the same nonnegative remainder when divided by n.*

Proof. First take $a \equiv b \ (mod\ n)$, so that $a = b + kn$ for some $k \in \mathbb{Z}$. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$, where $0 \leq r < n$.Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n|(a - b)$, In the language of congruences, we have $a \equiv b \ (mod\ n)$. ■

2.1.2 some properties of congruences

Congruence modulo n is an equivalence relation on $\mathbb{Z}$, and this fact is important enough to be stated as a theorem.

Theorem 2.1.2 ***Equivalence Relation.*** *The relation of congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Proof. We shall show that congruence modulo n is (1) reflexive, (2) symmetric, and (3) transitive. Let $n > 1$, and let a, b, and c be arbitrary in $\mathbb{Z}$.

1. Reflexive: $a \equiv a \ (mod\ n)$ since $a - a = (n)(0)$.

2. Symmetric: $a \equiv b \ (mod\ n) \Rightarrow a - b = nq$ for some $q \in \mathbb{Z}$

$$\Rightarrow \quad b - a = nq = n(-q) \text{ and } -q \in \mathbb{Z}$$
$$\Rightarrow \quad b \equiv a(modn).$$

3. Transitive: $a \equiv b \ (mod\ n)$ and $b \equiv c \ (mod\ n)$

$\Rightarrow a - b = nq$ and $b - c = nk$ and $q, k \in \mathbb{Z}$
$\Rightarrow a - c = a - b + b - c$
$= n(q + k), \quad$ and $\quad q + k \in \mathbb{Z}$
$\Rightarrow a \equiv c \ (mod\ n)$. ■

As with any equivalence relation, the equivalence classes for congruence modulo n form a partition of $\mathbb{Z}$; that is, they separate $\mathbb{Z}$ into mutually disjoint subsets. These subsets are called **congruence classes** or **residue classes** knowledge as follows.

Definition 2.1.2 *The set of numbers that correspond to the same remainder r when divided by n forms a* ***residue class*** *modulo n. We assume that $m \geq 2$.*

Referring to our discussion concerning remainders, we see that there are n distinct congruence classes modulo n, given by

$$\begin{aligned}
[0] &= \{..., -2n, -n, 0, n, 2n, ...\} \\
[1] &= \{..., -2n+1, -n+1, 1, n+1, 2n+1, ...\} \\
[2] &= \{..., -2n+2, -n+2, 2, n+2, 2n+2, ...\} \\
&\vdots \\
[n-1] &= \{..., -n-1, -1, n-1, 2n-1, 3n-1, ...\}.
\end{aligned}$$

When $n = 4$, these classes appear as

$$\begin{aligned}
[0] &= \{..., -8, -4, 0, 4, 8, ...\} \\
[1] &= \{..., -7, -3, 1, 5, 9, ...\} \\
[2] &= \{..., -6, -2, 2, 6, 10, ...\} \\
[3] &= \{..., -5, -1, 3, 7, 11, ...\}.
\end{aligned}$$

Congruence classes are useful in connection with numerous examples, and we shall see more of them later.

Now let us recall the following theorem for **Addition, Subtraction** and **Multiplication** Properties.

Theorem 2.1.3 *Start with a positive integer $m \geq 2$ and two integers a and b satisfying $a \equiv b \ (mod\ m)$. If c is any integer, then*

1. $a + c \equiv b + c \ (mod\ m)$.
2. $a - c \equiv b - c \ (mod\ m)$.
3. $ac \equiv bc \ (mod\ m)$.

Proof.

1. We need to show $(a + c) - (b + c)$ is divisible by m. But $(a + c) - (b + c) = a - b$, which is divisible by m since we assumed that $a \equiv b \ (mod\ m)$.

2. The proof is similar to 1. The reader should be able to supply the details.

3. Here, we need $ac - bc$ to be divisible by m. But $ac - bc = (a - b)c$. Since $a - b$ is divisible by m, it follows that $(a - b)c$ is divisible by m.

■

Theorem 2.1.4 *If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then*

1. $a + c \equiv b + d \ (mod\ m)$.

2. $ac \equiv bd \ (mod\ m)$.

Proof. We know that $a + c \equiv b + c \ (mod\ m)$ and $b + c \equiv b + d \ (mod\ m)$ by Theorem 2.1(2). Therefore, by Theorem 2.1(3), $a + c \equiv b + d \ (mod\ m)$. The proof of the second statement is similar. ■

Theorem 2.1.5 *If a, b, k, and m are integers such that $k > 0$, $m > 0$, and $a \equiv b \ (mod\ m)$, then $a^k \equiv b^k \ (mod\ m)$.*

Proof. Because $a \equiv b \ (mod\ m)$, we have $m|(a - b)$. Since

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

we see that $(a-b)|(\ a^k - b^k)$. Therefore, from proposition 1.1.1(1) it follows that $m|(a^k - b^k)$. Hence, $a^k \equiv b^k \ (mod\ m)$. ■

Theorem 2.1.6 *If a, b, c, and m are integers such that $m > 0$, $d = (c, m)$, and $ac \equiv bc \ (mod\ m)$, then $a \equiv b \ (mod\ m/d)$.*

Proof. *By hypothesis, we can write*

$$c(a - b) = ca - cb = km$$

for some integer k. Knowing that $gcd(c, m) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $m = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks$$

Hense, $s|r(a - b)$ and $gcd(r, s) = 1$. Euclid's lemma yields $s|(a - b)$, which may be recast as $a \equiv b (mod\ s)$; in other words, $a \equiv b\ (mod\ m/d)$. ■

Corollary 2.1.1 *If $ca \equiv cb\ (mod\ m)$ and $gcd(c, m) = 1$, then $a \equiv b\ (mod\ m)$.*

Corollary 2.1.2 *If $ca \equiv cb\ (mod\ p)$ and $p \nmid c$, where p is a prime number, then*

$a \equiv b\ (mod\ p)$.

Proof. The conditions $p \nmid c$ and p a prime imply that $gcd(c, p) = 1$. ■

Proposition 2.1.2 *Let $a, b, c \in \mathbb{Z}, m, n \in \mathbb{N}$, and $a \equiv b\ (mod\ n)$. Then each of the following holds.*

1. $am \equiv bm\ (mod\ mn)$.
2. $a^m \equiv b^m\ (mod\ n)$.
3. If m divides n, then $a \equiv b\ (mod\ m)$.

Proof.

1. Given that $a \equiv b\ (mod\ n)$, $a - b = kn$ for some integer k. Multiplying by m, we get $(a - b)m = knm$, so $am - bm = (km)n$, namely $am \equiv bm\ (mod\ n)$.
2. Since $n|(a - b)$, then

$$n|(a - b)(a^{m-1} + a^{m-2}b + \cdots + b^m) = a^m - b^m.$$

   In other words, $a^m \equiv b^m (mod\ n)$.

3. Since $a = b + kn$ for some $k \in \mathbb{Z}$ and $n = lm$ for some $l \in \mathbb{N}$, then $a = b + klm$, so $a - b = (kl)m$, whence $a \equiv b\ (mod\ m)$.

■

2.1.3 Congruence Classes

In connection with the relation of congruence modulo n, we have observed that there are n distinct congruence classes. Let $\mathbb{Z}_n$ denote this set of classes:

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}.$$

When addition and multiplication are defined in a natural and appropriate manner in $\mathbb{Z}_n$, these sets provide useful examples for our work in later chapters.

Theorem 2.1.7 ***Addition in*** $\mathbb{Z}_n$. *Consider the rule given by*

$$[a] + [b] = [a + b].$$

1. This rule defines an addition that is a binary operation on $\mathbb{Z}_n$.
2. Addition is associative in $\mathbb{Z}_n$:

$$[a] + ([b] + [c]) = ([a] + [b]) + [c].$$

3. Addition is commutative in $\mathbb{Z}_n$:

$$[a] + [b] = [b] + [a].$$

4. $\mathbb{Z}_n$ has the additive identity$[0]$.
5. Each $[a]$ in $\mathbb{Z}_n$ has $[-a]$ as its additive invers in $\mathbb{Z}_n$.

Theorem 2.1.8 ***Multiplication in*** $\mathbb{Z}_n$.*Consider the rule for multiplication in* $\mathbb{Z}_n$ *given by*

$$[a][b] = [ab].$$

1. Multiplication as defined by this rule is a binary operation on $\mathbb{Z}_n$.

2. Multiplication is associative in $\mathbb{Z}_n$:

$$[a]\,([b]\,[c]) = ([a]\,[b])\,[c]\,.$$

3. Multiplication is commutative in $\mathbb{Z}_n$:

$$[a]\,[b] = [b]\,[a]\,.$$

4. $\mathbb{Z}_n$ has the multiplicative identity$[1]$.

Theorem 2.1.9 ***Multiplicative Inverses in*** $\mathbb{Z}_n$. *An element* $[a]$ *of* $\mathbb{Z}_n$ *has a multiplicative inverse in* $\mathbb{Z}_n$ *if and only if* a *and* n *are relatively prime.*

Theorem 2.1.10 ***Multiplicative Inverses in*** $\mathbb{Z}_p$. *Every nonzero element of* $\mathbb{Z}_n$ *has a multiplicative inverse if and only if* n *is a prime.*

2.1.4 Linear Congruences

A linear Congruence is an equation of the form $ax \equiv b(\mathrm{mod}\, m)$ such that x is an unknown integer. The problem of finding all integers x that will satisfy this equation is identical with that of obtaining all solulions of the Linear Diophantine equation $ax - my = b$. This allows us to bring the results of chapter 1 into play.

Theorem 2.1.11 *Let* a, b *and* m *be integers with* $m > 0$ *and* $(a, m) = d$. *If* $d \nmid b$, *then* $ax \equiv b(\mathrm{mod}\, m)$ *has no solutions. If* $d|b$, *then* $ax \equiv b(\mathrm{mod}\, m)$ *has exactly* d *incongruent solutions modulo* m.

Proof. From the Proposition 2.1.1, the linear congruence $ax \equiv b\ (\mathrm{mod}\, m)$ is equivalent to the Linear Diophantine equation $ax - my = b$. The integer x is a solution of $ax \equiv b\ (\mathrm{mod}\, m)$ if and only if there is an integer y with $ax - my = b$. From Theorem 1.1.4, we know that if $d \nmid b$, there are no solutions, given by

$$x = x_0 + (m/d)t \qquad\qquad y = y_0 + (a/d)t$$

where $x = x_0$ and $y = y_0$ is a particular solution of the equation. The values of x given above,

$$x = x_0 + (m/d)t,$$

are the solutions of the linear congruence; there are infinitely many of these.

To determine how many incongruent solutions there are, we find the condition that describes when two of the solutions $x_1 = x_0 + (m/d)t_1$ and $x_2 = x_0 + (m/d)t_2$ are congruent modulo m. If these two solutions are congruent, then

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2 (\mathrm{mod}\, m).$$

Subtracting x_0 from both sides of this Congruence, we find that

$$(m/d)t_1 \equiv (m/d)t_2 (\mathrm{mod}\, m).$$

Now $(m, m/d) = m/d$ since $(m/d)|m$, so that by Theorem 2.1.6, we see that

$$t_1 \equiv t_2 (\mathrm{mod}\, d).$$

This shows that a complete set of incongruent solutions is obtained by taking $x = x_0 + (m/d)t$, where t ranges through a complete system of residues modulo d. One such set is given by $x = x_0 + (m/d)t$ where $t = 0, 1, 2, ..., d - 1$. ■

Example 2.1.1 *To find all solutions of* $9x \equiv 12 (\mathrm{mod}\, 15)$, *we first note that since* $(9, 15) = 3$ *and* $3|12$, *there are exactly three incongruent solutions. We can find these solutions by first finding a particular solution and then adding the appropriate multiples of* $15|3 = 5$.

To find a particular solution, we consider the Linear Diophantine equation $9x - 15y = 12$. The Euclidean algorithm shows that

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2, \end{aligned}$$

Whence $gcd(15, 9) = 3$. So that $3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15$. Hence $9 \cdot 8 - 15 \cdot 4 = 12$, and a paticular solution of $9x - 15y = 12$ is given by $x_0 = 8$ and $y_0 = 4$. From the proof of theorem 2.2.1, we see that a complete set of 3 incongruent solutions is given by $x = x_0 \equiv 8(\mathrm{mod}\, 15)$, $x = x_0 + 5 \equiv 13(\mathrm{mod}\, 15)$, and $x = x_0 + 5 \cdot 2 \equiv 18(\mathrm{mod}\, 15)$ whence $x \equiv 3(\mathrm{mod}\, 15)$

Corollary 2.1.3 *If $gcd(a, m) = 1$, then the linear congruence $ax \equiv b(\mathrm{mod}\, m)$ has a unique solution modulo n.*

Having considered a single linear congruence, it is natural to turn to the problem of solving a system of simultaneous linear congruences. The theory behind the solution of these systems is provided by the following theorem.

Theorem 2.1.12 ***The Chinese Remainder Theorem.*** *Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system*

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1), \\ x &\equiv a_2 \ (mod\ m_2), \\ x &\equiv a_n \ (mod\ m_n) \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

2.2 Some Special Congruences

2.2.1 Wilson's Theorem

Theorem 2.2.1 ***Wilson.*** *If p is prime, then $(p-1)! \equiv -1(\mathrm{mod}\, p)$.*

Proof. Dismissing the cases $p = 2$ and $p = 3$ as being evident, let us take $p > 3$. Suppose that a is any one of the $p - 1$ positive integers

$$1, 2, 3, ..., p - 1$$

and concider the linear congruence $ax \equiv 1(\mathrm{mod}\, p)$. Then $gcd(a, p) = 1$. By Theorem 2.2.1, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1(\mathrm{mod}\, p)$.

Because p is prime, $a = a'$ if and only if $a = 1$or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1(\mathrm{mod}\, p)$ is equivalent to $(a-1)\cdot(a+1) \equiv 0(\mathrm{mod}\, p)$. Therefore, either $a-1 \equiv 0(\mathrm{mod}\, p)$, in which case $a = 1$, or $a + 1 \equiv 0(\mathrm{mod}\, p)$, in which case $a = p - 1$.

If we omit the numbers 1 and $p-1$, the effect is to group the remaining integers $2, 3, ..., p-2$ into pairs a, a', where $a \neq a'$, such that their product $aa' \equiv 1(\mathrm{mod}\, p)$. When these $(p-3)/2$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdots (p - 2) \equiv 1(\mathrm{mod}\, p)$$

or rather

$$(p - 2)! \equiv 1(\mathrm{mod}\, p)$$

Now multiply by $p - 1$ to obtain the congruence

$$(p - 1)! \equiv p - 1 \equiv -1(\mathrm{mod}\, p)$$

as was to be proved. ■

Example 2.2.1 *Let a prime number $p = 5$, we have $(5 - 1)! = 4! = 1 \cdot 2 \cdot 3 \cdot 4$, and we have $2 \cdot 3 \equiv 1(mod\ 5)$. Hence,*

$$\begin{aligned} 4! &\equiv 1 \cdot (2 \cdot 3) \cdot 4(mod\ 5) \\ &\equiv 1 \cdot 4(mod\ 5) \\ &\equiv -1(mod\ 5) \end{aligned}$$

2.2.2 Fermat's theorem

Theorem 2.2.2 ***Fermat's Theorem.*** *Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.*

Proof. We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, ..., (p-1)a$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa (\mathrm{mod}\, p) \qquad\qquad 1 \leq r < s \leq p-1$$

then a could be canceled to give $r \equiv s (\mathrm{mod}\, p)$, which is impossible. Therefore, the previous set of integers must be congruent modulo p to $1, 2, 3, ..., p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\mathrm{mod}\, p)$$

whence

$$a^{p-1}(p-1)! \equiv (p-1)! (\mathrm{mod}\, p)$$

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p-1)!$, our line of reasoning culminaties in the statement that $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, which is Fermat's Theorem. ■

This result can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

Corollary 2.2.1 *If p is a prime, then $a^p \equiv a (\mathrm{mod}\, p)$ for any integer a.*

Proof. When $p|a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a (\mathrm{mod}\, p)$. If $p \nmid a$, then according to Fermat's theorem, we have $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. When this congruence is multiplied by a, the conclution $a^p \equiv a (\mathrm{mod}\, p)$ follows. ■

2.2.3 Euler's Generalization of Fermat's Theorem

Euler's Phi-Function

Definition 2.2.1 *For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.*

The function ϕ is usually called the Euler Phi-function (sometimes, the indicator or totient) after its originator; the functional notation $\phi(n)$, however, is credited to **Gauss**.

Example 2.2.2 *By the definition, we find that $\phi(30) = 8$; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically,*

$$1, 7, 11, 13, 17, 19, 23, 29$$

Let us denote by $\mathbb{Z}_n$ the set $\{0, 1, 2, ..., n-1\}$ and by $\mathbb{Z}_n^*$ the set of those positive numbers from $\mathbb{Z}_n$ that are relatively prime to n. Then $\phi(n)$ is the number of elements of $\mathbb{Z}_n^*$, i.e., $\phi(n) = |\mathbb{Z}_n^*|$.

Example 2.2.3 *Let $n = 20$. Then $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $\phi(20) = 8$.*

Theorem 2.2.3 *If p is prime, then $\phi(p) = p - 1$. Conversely, if p is a positive integer with $\phi(p) = p - 1$, then p is prime.*

Theorem 2.2.4 *If p is a prime and $k > 0$, then*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

Example 2.2.4 *Let the number $n = 25$, we have*

$$\phi(n) = \phi(25) = \phi(5^2) = 5^2 - 5 = 5^2(1 - \frac{1}{5}) = 20$$

Theorem 2.2.5 *If the integer $n > 1$ has the prime factorization $n = p_1^{k_1}\ p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\ (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})\end{aligned}$$

Example 2.2.5 *Let us calculate the values $\phi(360)$, for instance. The prime-power de composition of 360 is $2^3 \cdot 3^2 \cdot 5$. So we have*

$$\begin{aligned}\phi(360) &= 360(1 - \frac{1}{2})(1 - \frac{1}{3}) \cdots (1 - \frac{1}{5}) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \\ &= 96\end{aligned}$$

Euler's Theorem

As a prelude to launching our proof of Euler's Theorem, we require a preliminary.

Lemma 2.2.1 *Let $n > 1$ and $gcd(a, n) = 1$. If $a_1, a_2, ..., a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then*

$$aa_1, aa_2, ..., aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, ..., a_{\phi(n)}$ in some order.

Theorem 2.2.6 ***Euler:*** *If $n \geq 1$ and $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$.*

Proof. There is no harm in talking $n > 1$. Let $a_1, a_2, ..., a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n. Because $gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent, not necessarily in order of appearance, to $a_1, a_2, ..., a_{\phi(n)}$.

Then

$$\begin{aligned} aa_1 &\equiv a'_1 \pmod{n} \\ aa_2 &\equiv a'_2 \pmod{n} \\ &\vdots \\ aa_{\phi(n)} &\equiv a'_{\phi(n)} \pmod{n} \end{aligned}$$

where $a'_1, a'_2, ..., a'_{\phi(n)}$ are the integers $a_1, a_2, ..., a_{\phi(n)}$ in some order. On taking the product of these $\phi(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a'_1 a'_2 \cdots a'_{\phi(n)} (\mathrm{mod}\, n) \\ &\equiv a_1 a_2 \cdots a_{\phi(n)} (\mathrm{mod}\, n) \end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} (\mathrm{mod}\, n)$$

Because $gcd(a_i, n) = 1$ for each i, the lemma preceding Theorem implies that $gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 \cdots a_{\phi(n)}$, leaving us with

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

■

Chapter 3

Cryptography

3.1 Introduction to Cryptography

Cryptography is the study of sending and receiving secret messages. The aim of cryptography is to send messages across a **channel** so only the intended recipient of the message can read it. This channel could be a telephone line or computer network, for example.

The message to be sent is called the **plaintext** message. The disguised message is called the **ciphertext**. The plaintext and the ciphertext are both written in an alphabet, consisting of letters or characters. Characters can include not only the familiar alphabetic characters $A, ..., Z$ and $a, ..., z$ but also digits, punctuation marks, and blanks.

A cryptosystem, or **cipher**, has two parts: **encryption**, the process of transforming a plaintext message to a ciphertext message, and **decryption**, the reverse transformation of changing a ciphertext message into a plaintext message.

There are many different families of cryptosystems, each distinguished by a particular encryption algorithm. Cryptosystems in a specifed cryptographic family are distinguished from one another by a parameter to the encryption function called a **key**.[**10**] [**11**]

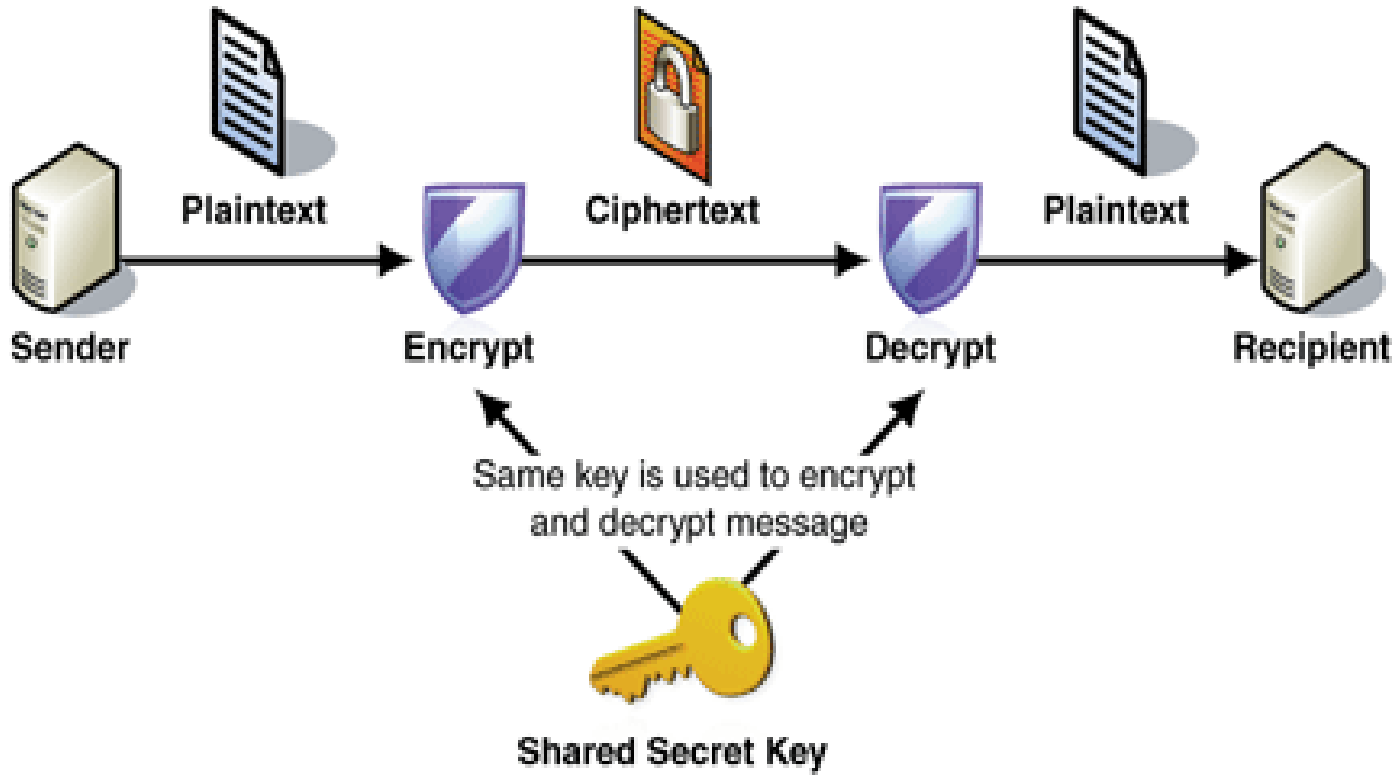
Definition 3.1.1 *A cryptosystem is a five-tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, where the following condition are satisfied:*

1. $\mathcal{P}$ is a finite set of possible plaintexts;
2. $\mathcal{C}$ is a finite set of possible ciphertexts;
3. $\mathcal{K}$ the keyspace, is a finite set of possible keys;
4. For each $k \in \mathcal{K}$, there is an encryption rule $e_k \in \mathcal{E}$ and a corresponding decryption rule $d_k \in \mathcal{D}$. Each $e_k : \mathcal{P} \to \mathcal{C}$ and $d_k : \mathcal{C} \to \mathcal{P}$ are functions such that $d_k(e_k(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

3.2 Classical Cryptography

A symmetric encryption scheme has five ingredients (Figure 1):

- **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.



(**Figure** 1)

Some Simple Cryptosystems

3.2.1 Shift Cipher

One of the earliest cryptosystems is often attributed to **Julius Caesar**. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. So a became D, b became E, c became F, etc. The end of the alphabet wrapped around to the beginning, so x became A, y became B, and z became C.

$$a \longmapsto D \quad b \longmapsto E \quad c \longmapsto F \quad \ldots \quad w \longmapsto Z \quad x \longmapsto A \quad y \longmapsto B \quad z \longmapsto C$$

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter $\mathcal{P}$, substitute the ciphertext letter $\mathcal{C}$:

$$\mathcal{C} = (\mathcal{P}+3) mod\ 26$$

For the encryption algorithm, and

$$\mathcal{P} = (\mathcal{C}-3) mod\ 26$$

For the decryption algorithm.

A shift may be of any amount, so that the general Caesar algorithm is defined in the following cryptosystem.

Cryptosystem 1.1: Shift Cipher
Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \leq K \leq 25$, define

$$e_k(x) = (x + k)\ mod\ 26$$

and

$$d_k(y) = (y - k)\ mod\ 26$$

$(x, y \in \mathbb{Z}_{26})$.

Example 3.2.1 *For to encrypt the plaintext:*

Suppose the key for a Shift Cipher is $k = 7$, and the plaintext is

cryptography

We first convert the plaintext to a sequence of itegers using the specified correspondence, obtaining the following:

$$2 \quad 17 \quad 24 \quad 15 \quad 19 \quad 14 \quad 6 \quad 17 \quad 0 \quad 15 \quad 7 \quad 24$$

Next, we add 7 to each value, reducing each sum modulo 26:

$$9 \quad 24 \quad 5 \quad 22 \quad 0 \quad 21 \quad 13 \quad 24 \quad 7 \quad 22 \quad 14 \quad 5$$

Finally, we convert the sequence of integers to alphabetic characters, obtaining the ciphertext:

$$JYFWAVNYHWOF$$

Example 3.2.2 *For to decrypt the ciphertext:*

Suppose the key for a Shift Cipher is $k = 3$, and the ciphertext is

$$DOJHEUD$$

We first convert the ciphertext to a sequence of itegers using the specified correspondence, obtaining the following:

$$3 \quad 14 \quad 9 \quad 7 \quad 4 \quad 20 \quad 3$$

Next, we subtract 3 from each value, reducing modulo 26:

$$0 \quad 11 \quad 6 \quad 4 \quad 1 \quad 17 \quad 0$$

Finally, we convert the sequence of integers to alphabetic characters, obtaining the plaintext:

$$algebra$$

3.2.2 Substitution Cipher

Another well-known cryptosystem is the Substitution Cipher, which we define as following.

Cryptosystem 1.2: Substitution Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ consists of all possible permutations of the 26 symbols $0, 1, ..., 25$. For each permutation $\pi \in k$, define

$$e_\pi(x) = \pi(x),$$

and define

$$d_\pi(y) = \pi^{-1}(y),$$

where π^{-1} is the inverse permutation to π.

The main problem with the shift cipher is that the number of keys is too small; we only have 26 possible keys. To increase the number of keys the substitution cipher was invented. To write down a key for the substitution cipher we first write down the alphabet, and then a permutation of the alphabet directly below it. This mapping gives the substitution we make between the plaintext and the ciphertex

Plaintext alphabet	*ABCDEFGHIJKLMNOPQRSTUVWXYZ*
Ciphertext alphabet	*GOYDSIPELUAVCRJWXZNHBQFTMK*

Encryption involves replacing each letter in the top row by its value in the bottom row. **Decryption** involves first looking for the letter in the bottom row and then seeing which letter in the top row maps to it. Hence, the plaintext word HELLO would encrypt to the ciphertext ESVVJ if we used the substitution given above.

The number of possible keys is equal to the total number of permutations on 26 letters, namely the size of the group $\mathbb{Z}_{26}$, which is

$$26! \approx 4.03 \cdot 10^{26} \approx 2^{88}.$$

3.2.3 Affine Cipher

The Shift Cipher is a special case of the Substitution Cipher which includes only 26 of the 26! possible permutations of 26 elements. The shift ciphers may be generalized and slightly strengthened as follows.

Choose two integers $a, b \in \mathbb{Z}_{26}$, with $gcd(a, 26) = 1$, Suppose that the encrypyion function is given by

$$e(x) \longrightarrow (ax + b)(mod\ 26).$$

For example, let $a = 9$ and $b = 2$, so we are working with $9x + 2$. Take a plaintext letter such as $h = 7$. It is encrypted to $9 \cdot 7 + 2 = 65 \equiv 13 (\mathrm{mod}\, 26)$, which is the letter N . Using the same function, we obtain

$$affine \longmapsto CVVWPM.$$

How do we decrypt? We first need to find out when a decryption function $d(y)$ exists. Such a decoding function exists when we can solve the equation

$$y \equiv (ax + b)(mod\ 26)$$

which equivalent to

$$ax \equiv d\ (mod\ 26) \qquad \text{such that} \quad d = y - b$$

for x. Since $gcd(a, 26) = 1$, by theorem2.1.10. There is a multiplicative inverse for a and by corollary2.1.3. this equation has a unique solution modulo 26 which is as follows

$$x \equiv \alpha^{-1} b (\mathrm{mod}\, 26),$$

from where, the decryption function is $d(y) \equiv a^{-1}(y - b)(\mathrm{mod}\, 26)$.

The key for this encryption method is the pair (a, b). There are 12 possible choices for a with $gcd(a, b) = 1$ and there are 26 choices for b (since we are working mod 26, we only

need to consider a and b between 0 and 25). Therefore, there are $12 \cdot 26 = 312$ choices for the key.[**10**] [**13**]

So, finally, the complete description of the Affine Cipher is given as the following Cryptosystem.

Cryptosystem 1.3: Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. and let

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} : gcd\ (a, 26) = 1\}.$$

For $k = (a, b) \in \mathcal{K}$, define

$$e_k(x) = (ax + b)\ mod\ 26$$

and

$$d_k(y) = a^{-1}(y - b) mod 26$$

$(x, y \in \mathbb{Z}_{26})$.

3.2.4 Vigenère Cipher

The problem with the shift cipher and the substitution cipher was that each plaintext letter always encrypted to the same ciphertext letter. Hence underlying statistics of the language could be used to break the cipher. From the early 1800s onwards, cipher designers tried to break this link between the plaintext and ciphertext.

The substitution cipher we used above was a mono-alphabetic substitution cipher, in that only one alphabet substitution was used to encrypt the whole alphabet. One way to solve our problem is to take a number of substitution alphabets and then encrypt each letter with a different alphabet. Such a system is called a polyalphabetic substitution cipher.

For example we could take

Plaintext alphabet	$ABCDEFGHIJKLMNOPQRSTUVWXYZ$
Ciphertext alphabet one	$TMKGOYDSIPELUAVCRJWXZNHBQF$
Ciphertext alphabet two	$DCBAHGFEMLKJIZYXWVUTSRQPON$

Then we encrypt the plaintext letters in odd-numbered positions encrypt using the first ciphertext alphabet, whilst we encrypt the plaintext letters in even-numbered positions using the second alphabet. For example, the plaintext word **HELLO** would encrypt to **SHLJV**, using the above two alphabets. Notice that the two occurrences of L in the plaintext encrypt to two different ciphertext characters. Thus we have made it harder to use the underlying statistics of the language.

Essentially we are encrypting the message two letters at a time, hence we have a block cipher with block length two English characters. In real life one may wish to use around five rather than just two alphabets and the resulting key becomes very large indeed. With five alphabets the total the total key space is

$$(26!)^5 \approx 2^{441},$$

but the user only needs to remember the key which is a sequence of

$$26 \cdot 5 = 130$$

letters. However, just to make life hard for the attacker, the number of alphabets in use should also be hidden from his view and form part of the key.

The Vigenère cipher, invented in 1533 by Giovan Battista Bellaso, was a variant on the above theme, but the key was easy to remember.

When looked at in one way theVigenère cipher is a polyalphabetic block cipher, but when looked at in another, it is a natural generalization of the shift cipher.

The description of the Vigenère cipher as a block cipher takes the description of the polyalphabetic cipher above but restricts the possible ciphertext alphabets to one of the

26 possible cyclic shifts of the standard alphabet. Suppose five alphabets were used, this reduces the key space down to

$$26^5 \approx 2^{23}$$

and the size of the key to be remembered to a sequence of five numbers between 0 and 25.

The Vigenère cipher again identifies letters with the numbers $0, ..., 25$. The secret key is a short sequence of letters (e.g. a word) which is repeated again and again to form a keystream. Encryption involves adding the plaintext letter to a key letter. Thus if the key is $SESAME$, encryption works as follows,

Plaintext alphabet	$THISISATESTMESSAGE$
keyword	$SESAMESESAMESESAME$
Ciphertextalphabet	$LLASUWSXWSFQWWKASI$

In the finally, the cryptosystem of the Vigenère Cipher is given as follows .

Cryptosystem 1.4: Vigenère Cipher

Let m be a positive integer. Define $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$, For a key $K = (k_1, k_2, ..., k_m)$, we define

$$e_k(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m)$$

and

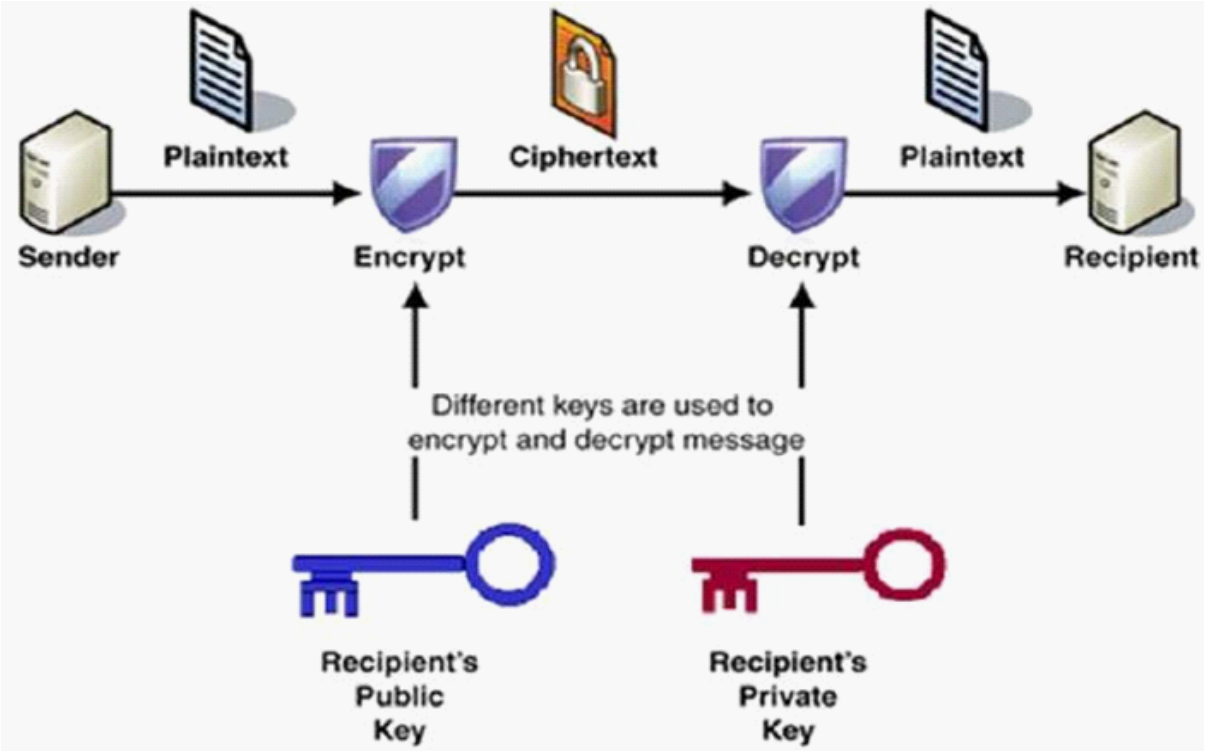
$$d_k(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m),$$

where all operations are performed in $\mathbb{Z}_{26}$.

3.3 Public-Key Cryptosystems

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.

- **Plaintext**: This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various transformations on the plaintext.
- **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm**: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.



3.3.1 RSA Cryptosystem

The **RSA** cryptosystem introduced by **R. Rivest, A. Shamir, and L. Adleman** in 1978, is based on the difficulty of factoring large numbers. Though it is not a difficult task to find two large random primes and multiply them together, factoring a 150-digit number that is the product of two large primes would take 100 million computers operating at 10 million instructions per second about 50 million years under the fastest algorithms currently known.

Cryptosystem 1.1: RSA Cryptosystem

Let $n = pq$, where p and q are primes. and define

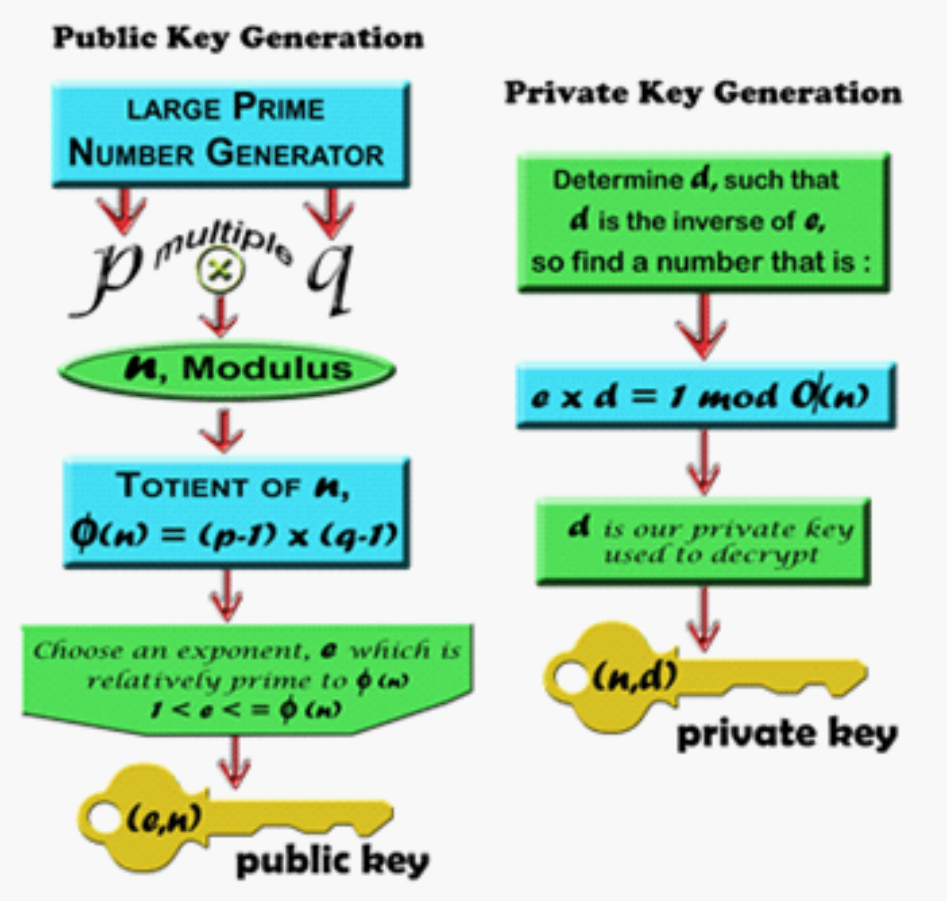
$$\mathcal{K} = \{(n, p, q, d, e) : ed \equiv 1 (mod\ \phi(n))\}.$$

For $k = (n, p, q, d, e)$, define

$$e_k(x) = x^e mod\ n$$

and

$$d_k(y) = y^d mod\ n$$



$(x, y \in \mathbb{Z}_n)$. The values n and e comprise the public key, and the values p, q and d form the private key.

The **RSA** cryptosystem works as follows. Suppose that we choose two random 150-digit prime numbers p and q. Next, we compute the product $n = pq$ and also compute $\phi(n) = m = (p-1)(q-1)$, where ϕ is the $Euler\ \phi - function$. Now we start choosing random integers E until we find one that is relatively prime to m; that is, we choose E such that $gcd(E, m) = 1$. Using the Euclidean algorithm, we can find a number D such that $DE \equiv 1\ (mod\ m)$. The numbers n and E are now made public.

Suppose now that person B (Bob) wishes to send person A (Alice) a message over a public line. Since E and n are known to everyone, anyone can encode messages. Bob first digitizes the message according to some scheme, say $A = 00, B = 02, ..., Z = 25$. If necessary, he will break the message into pieces such that each piece is a positive integer

less than n. Suppose x is one of the pieces. Bob forms the number $y = x^E \ mod \ n$ and sends y to Alice. For Alice to recover x, she need only compute $x = y^D mod \ n$. Only Alice knows D.

Example 3.3.1 *Before exploring the theory behind the RSA cryptosystem or attempting to use large integers, we will use some small integers just to see that the system does indeed work. Suppose that we wish to send some message, which when digitized is* 23. *Let* $p = 23$ *and* $q = 29$. *Then*

$$n = pq = 667$$

and

$$\phi(n) = m = (p-1)(q-1) = 616.$$

We can let $E = 487$, since $gcd(616, 487) = 1$. The encoded message is computed to be

$$23^{487} mod \ 667 = 368.$$

Using the Euclidean algorithm, we determine

that $191E = 1 + 151m$; therefore, the decrypting key is $(n, D) = (667, 191)$. We can recover the original message by calculating

$$368^{191} mod \ 667 = 23.$$

Now let us examine why the RSA cryptosystem works. We know that $DE \equiv 1 \ mod \ m$; hence, there exists a k such that

$$DE = km + 1 = k\phi(n) + 1.$$

By Theorem

$$y^D = (x^E)^D = x^{DE} = x^{km+1} = (x^{\phi(n)})^k x = x \ mod \ n.$$

We can now ask how one would go about breaking the RSA cryptosystem. To find D given n and E, we simply need to factor n and solve for D

by using the Euclidean algorithm. If we had known that $667 = 23 \cdot 29$, we could have recovered D.

3.4 Discrete Logarithm

Let p be a (large) prime. tells us that there exists a primitive element g. This means that every nonzero element of F_p is equal to some power of g. In particular, $g^{p-1} = 1$ by Fermat's theorem, and no smaller power of g is equal to 1. Equivalently, the list of elements

$$1, g, g^2, g^3, ..., g^{p-2} \in F_P^*$$

is a complete list of the elements in F_P^*.

Definition 3.4.1 *Let g be a primitive root for F_p and let h be a nonzero element of Fp. The Discrete Logarithm Problem **(DLP)** is the problem of finding an exponent x such that*

$$g^x \equiv h \ (mod\ p).$$

The number x is called the discrete logarithm of h to the base g and is denoted by $log_g(h)$.

3.4.1 One-Way Functions

A **one-to-one function** f from a set $\mathcal{M}$ to a set $\mathcal{C}$ is called one-way if $f(m)$ is "easy" to compute for all $m \in \mathcal{M}$, but for a randomly selected c in the image of f, finding an $m \in \mathcal{M}$ such that $c = f(m)$ is computationally infeasible. In other words, we can easily compute f, but it is computationally infeasible to compute f^{-1}.

Diagram.One-Way Function

$$\boxed{m \in \mathcal{M}} \xrightarrow{f: \text{ computationally easy}} \boxed{f(m) \in \mathcal{C}}$$

$$\xleftarrow{f^{-1}: \text{computationally infeasible}}$$

One-way functions have a plethora of cryptographic uses. For instance, one use of one-way functions, is password security. But, there is no rigorous mathematical proof that **one-way functions** actually exist. Yet, we have working definitions, pragmatic ones, that serve us well. Moreover, we now have "candidate" **one-way functions** such as the **DLP**, The reader may wonder at this point how it is that we could devise a cryptosystem using **one-way functions**.

That's what we'll see later.

Trapdoor One-Way Functions

A **trapdoor one-way function** or **public-key enciphering function** is a one-way function,

$$f : \mathcal{M} \to \mathcal{C},$$

satisfying the additional property that there exists information, called trapdoor information, or simply trapdoor, that makes it feasible to find $m \in \mathcal{M}$ for a given

$c \in img(f)$ such that $f(m) = c$, but without the trapdoor this task becomes infeasible.

Diagram.Trapdoor One-Way Function

$$\underrightarrow{f: \text{ computationally easy}}$$

$$\boxed{m \in \mathcal{M}} \qquad \overset{f(m) \in C}{\text{trapdoor}}$$

$$\underleftarrow{f^{-1}: \text{computationally infeasible}}$$

3.4.2 Diffie-Hellmun Key Exchange

The essential idea behind the Diffie-Hellman key exchange is the use of trapdoor one-way functions.

The Diffie–Hellman key exchange algorithm solves the following dilemma.

Alice and **Bob** want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary **Eve**. How is it possible for **Alice** and *Bob* to share a key without making it available to **Eve**? At first glance it appears that Alice and Bob face an impossible task. It was a brilliant insight of Diffie and Hellman that the difficulty of the discrete logarithm problem for F_P^* provides a possible solution.

The first step is for **Alice** and **Bob** to agree on a large prime p and a nonzero integer g modulo p. **Alice** and **Bob** make the values of p and g public knowledge; for example, they might post the values on their web sites, so **Eve** knows them.

The next step is for Alice to pick a secret integer a that she does not reveal to anyone, while at the same time **Bob** picks an integer b that he keeps secret.

Bob and Alice use their secret integers to compute

$$\underbrace{A \equiv g^a \ (mod\ p)}_{\text{Alice computes this}} \qquad \underbrace{B \equiv g^b \ (mod\ p)}_{\text{Bob computes this}}$$

They next exchange these computed values, **Alice** sends **A** to **Bob** and **Bob** sends **B** to **Alice**. Note that **Eve** gets to see the values of **A** and **B**, since they are sent over the insecure communication channel.

Finally, **Bob** and **Alice** again use their secret integers to compute

$$\underbrace{A' \equiv B^a \ (mod\ p)}_{\text{Alice computes this}} \qquad \text{and} \qquad \underbrace{B' \equiv A^b \ (mod\ p)}_{\text{Bob computes this}}$$

The values that they compute, $\mathbf{A'}$ and $\mathbf{B'}$ respectively, are actually the same, since $A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \ (mod\ p)$.

Definition 3.4.2 *Let p be a prime number and g an integer. The Diffie–Hellman Problem* ***(DHP)*** *is the problem of computing the value of $g^{ab} \ (mod\ p)$ from the known values of*

$g^a \ (mod\ p)$ and $g^b \ (mod\ p)$.

Example 3.4.1 ***Alice*** *and* ***Bob*** *agree to use the prime $p = 941$ and the primitive root $g = 627$.* ***Alice*** *chooses the secret key $a = 347$ and computes $A = 390 \equiv 627^{347} \ (mod\ 941)$. Similarly,* ***Bob*** *chooses the secret key $b = 781$ and computes $B = 691 \equiv 627^{781} \ (mod\ 941)$.* ***Alice*** *sends* ***Bob*** *the number 390 and* ***Bob*** *sends* ***Alice*** *the number 691. Both of these transmissions are done over an insecure channel, so both $A = 390$ and $B = 691$ should be considered public knowledge. The numbers $a = 347$ and $b = 781$ are not transmitted and remain secret. Then Alice and Bob are both able to compute the number $470 \equiv 627^{347 \cdot 781} \equiv A^b \equiv B^a \ (mod\ 941)$, so 470 is their shared secret.*

If **Eve** can solve the **DLP**, then she can clearly solve the **DHP**. Whether the converse is true or not is unknown. In other words, it is not known if it is possible

for a cryptanalyst to solve the **DHP** without solving the **DLP**. Nevertheless, the consensus is that the two problems are equivalent. Thus, for practical purposes, one may assume that the Diffie-Hellman Key-Exchange protocol is secure as long as the **DLP** is intractable.[**1**] [**8**]

3.4.3 The ElGamal Cryptosystem

Although the Diffie–Hellman key exchange algorithm provides a method of publicly sharing a random secret key, it does not achieve the full goal of being a public key cryptosystem, since a cryptosystem permits exchange of specific information, not just a random string of bits.

The ElGamal public key encryption algorithm is based on the discrete log problem and is closely related to Diffie–Hellman key exchange.

In this section we describe the version of the ElGamal PKC that is based on the discrete logarithm problem for F_P^*, but the construction works quite generally using the DLP in any group.

The ElGamal PKC is our first example of a public key cryptosystem, so we proceed slowly and provide all of the details. **Alice** begins by publishing information consisting of a public key and an algorithm. The public key is simply a number, and the algorithm is the method by which **Bob** encrypts his messages using **Alice's** public key. **Alice** does not disclose her private key, which is another number. The private key allows **Alice**, and only **Alice**, to decrypt messages that have been encrypted using her public key.

This is all somewhat vague and applies to any public key cryptosystem. For the ElGamal PKC, **Alice** needs a large prime number p for which the discrete logarithm problem in F_P^* is difficult, and she needs an element g modulo p of large (prime) order. She may choose p and g herself, or they may have been preselected by some trusted party such as an industry panel or government agency.

Alice chooses a secret number a to act as her private key, and she computes the quantity

$$A \equiv g^a \ (mod\ p).$$

Notice the resemblance to Diffie–Hellman key exchange. **Alice** publishes her public key **A** and she keeps her private key a secret.

Now suppose that **Bob** wants to encrypt a message using **Alice's** public key **A**. We will assume that **Bob's** message m is an integer between 2 and p. In order to encrypt m, **Bob**

first randomly chooses another number k modulo p[5] **Bob** uses k to encrypt one, and only one, message, and then he discards it. The number k is called an ephemeral key, since it exists only for the purposes of encrypting a single message.

Bob takes his plaintext message m, his chosen random ephemeral key k, and **Alice's** public key **A** and uses them to compute the two quantities

$$c_1 \equiv g^k \ (mod\ p) \qquad and \qquad c_2 \equiv mA^k \ (mod\ p).$$

(Remember that g and p are public parameters, so **Bob** also knows their values.) **Bob's** ciphertext, i.e., his encryption of m, is the pair of numbers (c_1, c_2), which he sends to Alice.

How does Alice decrypt **Bob's** ciphertext (c_1, c_2)? Since Alice knows a, she can compute the quantity

$$x \equiv c_1^a \ (mod\ p),$$

and hence also $x^{-1}(mod\ p)$. Alice next multiplies c_2 by x^{-1}, and lo and behold, the resulting value is the plaintext m. To see why, we expand the value of $x^{-1} \cdot c_2$ and find that

$$\begin{aligned}
x^{-1} \cdot c_2 &\equiv (c_1^a)^{-1} \cdot c_2 \ (mod\ p), && \text{since } x \equiv c_1^a \ (mod\ p),\\
&\equiv (g^{ak})^{-1} \cdot (mA^k) \ (mod\ p), && \text{since } c_1 \equiv g^k, c_2 \equiv mA^k \ (mod\ p),\\
&\equiv (g^{ak})^{-1} \cdot (m(g^a)^k) \ (mod\ p), && \text{since } A \equiv g^a \ (mod\ p),\\
&\equiv m \ (mod\ p), && \text{since the } g^{ak} \text{ terms cancel out.}
\end{aligned}$$

What is **Eve's** task in trying to decrypt the message? **Eve** knows the public parameters p and g, and she also knows the value of $A \equiv g^a \ (mod\ p)$, since **Alice's** public key **A** is public knowledge. If Eve can solve the discrete logarithm problem, she can find a and decrypt the message. Otherwise it appears difficult for **Eve** to find the plaintext.

Alice uses the prime $p = 467$ and the primitive root $g = 2$. She chooses $a = 153$ to be her private key and computes her public key

$$A \equiv g^a \equiv 2^{153} \equiv 224 \ (mod\ 467).$$

Bob decides to send **Alice** the message $m = 331$. He chooses an ephemeral key at random, say he chooses $k = 197$, and he computes the two quantities

$$c_1 \equiv 2^{197} \equiv 87 \ (mod\ 467) \qquad \text{and} \qquad c_2 \equiv 331 \cdot 224^{197} \equiv 57 \ (mod\ 467).$$

The pair $(c_1, c_2) = (87, 57)$ is the ciphertext that **Bob** sends to **Alice**.
Alice, knowing $a = 153$, first computes

$$x \equiv c_1^a \equiv 87^{153} \equiv 367 \ (mod\ 467), \qquad \text{and then} \quad x^{-1} \equiv 14 \ (mod\ 467).$$

Finally, she computes

$$c_2 x^{-1} \equiv 57 \cdot 14 \equiv 331 \ (mod\ 467)$$

and recovers the plaintext message m.

Conclusion

In the beginning, we presented the concept of cryptography and the ingredients of symmetric and asymmetric encryption, as we explained in the classicall cryptography that one of the earliest cryptosystems is often attributed to julius caesar, wich is special case of the substitution cipher like it affine cipher vigenère cipher. In the finley our study of assymmetric encryption was clear as we provided some coding methods like R. S. A, Diffie-Hellmun and ElGamal wich were safer than the methods symmetric.

Bibliography

[1] H. Jeffrey, P. Pipher, S. Joseph, An Introduction to Mathematical Cryptography, Springer, San francisco (2008).

[2] David. M. Burton, Elementary Number Theory, (5th Ed), McGraw-Hill, 2002.

[3] Arkadii Slinko, Algebra for Applications, Springer, 2015.

[4] M. W. Baldoni, C. Ciliberto, G.M. Piacenti Cattaneo, Springer, 2009

[5] G. Linda, G. Jimmie, Elements of Modern Algebra, (7th Ed), Brooks/Cole, Cengage Learning, 2009.

[6] ROSEN, Kenneth H.; KRITHIVASAN, Kamala. Discrete mathematics and its applications: with combinatorics and graph theory. Tata McGraw-Hill Education, 2012.

[7] Diane L. Herrmann, Paul J. Sally, Jr, Number, Shape, and Symmetry, CRC Press (2013).

[8] MOLLIN, Richard A. An introduction to cryptography. Chapman and Hall/CRC, 2006.

[9] Kenneth H. Rosen, Discrete Mathematics and Its Applications, (7th Ed), New York: McGraw-Hill, 2012.

[10] L. Haboub, cours crypt 2017, Abstract Algebra, Thomas W. Judson (1997).

[11] STINSON, Douglas R. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[12] STALLINGS, William. Cryptography and network security: principles and practice. Upper Saddle River: Pearson, 2017.

[13] D. Mihoubi, Cours 2^{ime} Mastre Discréte "*la cryptographie*", Université M'sila, 2018-2019.

[14] TRAPPE, Wade. Introduction to cryptography with coding theory. Pearson Education India, 2006.

[15] SMART, Nigel Paul, et al. Cryptography: an introduction. New York: McGraw-Hill, 2003.

Abstract

In this memo, we study the congruences and application in cryptography.

First, we study the concept and some properties of congruences without forgetting mention some special theorems: Wilson, Fermat and Euler.

Also, we study some encryption methods in cryptography and the role of congruence in this type of encryption. We provided in the clasical gryptography the substitution ciphers (Shift Cipher, affine Cipher and Vigenère Cipher), and in the asymmetric encryption (RSA Cryptosystem, Diffie-Hellmun Key Exchange, The ElGamal Cryptosystem). Such that, the RSA method based on the difficulty of factorization the prime number, and the Elgamal method based on the difficulty of solving the problem of Diffie-Hellman.

Résumé

Dans ce mémoire, nous étudions les congruences et application en cryptographie. Dans un premier temps, nous étudions le concept et certaines propriétés des congruences sans oublier quelques théorèmes particuliers: Wilson, Fermat et Euler. Nous étudions certaines méthodes de cryptage en cryptographie et le role de la congruences dans ce type de cryptage. Ensuite, en étudions dans la cryptographie classique les chiffrements par substitution (chiffrement par décalege, chiffrement d'affine, chiffrement de vigenère), et dans le chiffrement asymétrique les Cryptosystèmes suivant: "RSA, Diffie-Hellmun, The ElGamal". La méthode RSA basée sur la difficulté de factorisation des nombres premiers, et la méthode Elgamal basé sur la difficulté de résoudre le problème de Diffie-Hellman.

ملخص

في هذه المذكرة ندرس الموافقات في $\mathbb{Z}$ و تطبيقاتها على التشفير. نقدم أولا مفهوم الموافقات و بعض خصائصها دون أن ننسى ذكر بعض النظريات الخاصة مثل: ويلسون, فيرما وأولر. ثم نتطرق الى دراسة بعض طرق التشفيروالدور الذي تلعبه الموافقات في هذه الطرق من التشفير, و الذي ينقسم بدوره الى التشفير المتماثل مثل : (التشفير بالازاحة وتشفيرVigenère) و التشفيرالغير متماثل مثل (RSA , The ElGamal,

RSA على صعوبة تحليل العدد الأولي، أما Diffie-Hellmun Key Exchange, ...), بحيث تعتمد طريقة
طريقة The ElGamal تعتمد على حل مشكل Diffie-Hellmun .