Mercredi 2 août 2023 — 4. Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which plays an important role in mathematics and which is used throughout computer science, including
→ generating pseudorandom numbers
→ assigning computer memory locations to files
→ constructing check digits
→ encrypting messages

$a = d \cdot q + r$

$q = a \text{ div } d$ $\quad r = a \bmod d$

Definition 1. If a and b are integers with $a \neq 0$, we say a divides b if there is an integer c such that $c = \frac{b}{a} \Leftrightarrow b = a \cdot c$ (or equivalently, if $\frac{b}{a}$ is an integer).
When a divides b we say that a is a factor or divisor of b and that b is a multiple of a. (15 is a multiple of 5)
The notation $a|b$ denotes that a divides b.
We write $a \nmid b$ when a does not divide b.

Remark: We can express $a|b$ using quantifiers as $\exists c (ac = b)$, where the universe of discourse is the set of integers.

Theorem 1. Let a, b and c be integers, where $a \neq 0$.
Then (I.) if $a|b$ and $a|c$, then $a|(b+c)$ (additivity)
(II.) if $a|b$ then $a|bc$ $\forall c \in \mathbb{Z}$ (constant)
(III.) if $a|b$ and $b|c$, then $a|c$ (transitivity)

Direct proof.
Suppose that $a|b$ and $a|c$.
Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$.
Hence, $b + c = as + at = a(s+t)$
Therefore, a divides $(b+c)$

Corollary 1. If a, b and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb+nc)$ whenever m and n are integers.

Direct proof.
By (II.) of Th.1 we see that $a|mb$ and $a|nc$ whenever m and n are integers.
By (I.) of Th.1 it follows that $a|(mb+nc)$ ∎

Theorem 2. The division algorithm (Not really an algorithm, nevertheless, we use its traditional name)
Let a be an integer and d a positive integer.
Then there are unique integers q and r, with $0 \leq r < d$ such that $a = dq + r$ (dividend, divisor, quotient, remainder)

Definition 2. In the equality given in the division algorithm,
→ d is called the divisor
→ a is called the dividend
→ q is called the quotient
→ r is called the remainder

This notation is used to express the
(I.) quotient: $q = a \text{ div } d$
and (II.) remainder: $r = a \bmod d$

Remark: both $a \text{ div } d$ and $a \bmod d$ for a fixed d are functions on the set of integers.
Furthermore, when a is an integer and d is a positive integer, we have $a \text{ div } d = \underbrace{\left\lfloor \frac{a}{d} \right\rfloor}_{=q}$ and $a \bmod d = \underbrace{a - d}_{=r}$

Note that the integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

Modular Arithmetic

In some situation we care only about the remainder of an integer when it is divided by some positive integer.
For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have a special notations for them.

Definition 3. If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a-b$. ($m|(a-b)$)
We use the notation $a \equiv b \pmod m$ to indicate
We say that $a \equiv b \pmod m$ is a congruence and that m is its modulus (plural moduli)
If a and b are not congruent modulo m, we write $a \not\equiv b \pmod m$
$m|(a-b) \Leftrightarrow a \equiv b \pmod m$

Although both notations include "mod", they represent fundamentally different concepts.
- $a \equiv b \pmod m$ ← Represents a relation on the set of integers
- $a \bmod m = b$ ← Represents a function

However, they are closely related.

Theorem 3. Let a and b be integers, and let m be a positive integer.
Then $a \equiv b \pmod m$ if and only if $a \bmod m = b \bmod m$
if and only if a and b have the same remainder when divided by m.
$a \equiv b \pmod m \Leftrightarrow aRb$ (same remainder)

Example 1 | Determine whether $3|7$ and whether $3|12$
We see that $3 \nmid 7$ because $\frac{7}{3}$ is not an integer.
On the other hand, $3|12$ because $\frac{12}{3} = 4$.

Example 2 | Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?
The positive integers divisible by d are all the integers of the form dk, where k is a positive integer.
Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk < n$, or with $0 < k \leq \frac{n}{d}$
Therefore, there are $\left\lfloor \frac{n}{d} \right\rfloor$ positive integers not exceeding n that are divisible by d ∎

Example 3 | What are the quotient and remainder when 101 is divided by 11?
We have $\underbrace{101}_{a} = \underbrace{11}_{d} \cdot \underbrace{9}_{q} + \underbrace{2}_{r}$
Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$
and the remainder is $2 = 101 \bmod 11$.

Example 4 | What are the quotient and remainder when -11 is divided by 3?
We have $-11 = 3(-4) + 1$
Hence, the quotient is -4 and the remainder is 1
Note that the remainder cannot be negative. Consequently, the remainder is not -2, even though $-11 = 3(-3) - 2$, because $r = -2$ does not satisfy $0 \leq r < 3$

Example 5 | Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.
Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod 6$
However, because $24 - 12 = 10$ is not divisible by 6, we see that $24 \not\equiv 12 \pmod 6$

Theorem 4. *Let m be a positive integer.*
The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$

$$a \equiv b \pmod m \iff a = b + km$$

Proof:
If $a \equiv b \pmod m$, by def 3, we know that $m \mid (a-b)$.
This means that there is an integer k such that $a - b = km$, so that $a = b + km$
Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$.
Hence, m divides $a - b$, so that $a \equiv b \pmod m$.

The set of all integers congruent to an integer a modulo m is called the **congruence class** of a modulo m

there are m pairwise disjoint equivalence classes modulo m and that the union of the equivalence classes is the set of integers (Chap. 9)

Theorem 5. *Let m be a positive integer.*
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$
then (I.) $a + c \equiv b + d \pmod m$ (Sous-additive)
and (II.) $ac \equiv bd \pmod m$ (multiplication)

Direct Proof.
$a \equiv b \pmod m$ and $c \equiv d \pmod m$; by Th. 4 there are integers s and t with $\begin{cases} b = a + sm \\ d = c + tm \end{cases}$

Hence, $b + d = (a + sm) + (c + tm)$
$= (a + c) + (s + t)m$ (I.)

and $bd = (a + sm)(c + tm)$
$= ac + atm + csm + stm^2$
$= ac + (at + cs + stm)m$ (II.)

Hence, $\begin{cases} a + c \equiv b + d \pmod m \\ ac \equiv bd \pmod m \end{cases}$

Example 6

Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, it follow from Th. 5 that

$$\begin{cases} 18 = 7 + 11 \equiv 2 + 1 \equiv 3 \pmod 5 \\ \text{and that } 77 = 7 \cdot 11 \equiv 2 \cdot 1 \equiv 2 \pmod 5 \end{cases}$$

We must be careful working with congruences. Some properties we may expect to be true are not valid.
For example, if $ac \equiv bc \pmod m$, the congruence $a \equiv b \pmod m$ may be false.
Similarly, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, the congruence $a^c \equiv b^d \pmod m$ may be false.

Example 7 Find the value $(19^3 \bmod 31)^4 \bmod 23$

To compute $(19^3 \bmod 31)^4 \bmod 23$, we will first evaluate $19^3 \bmod 31$.
Because $19^3 = 6859$ and $6859 = 221 \cdot 31 + 8$, we have $19^3 \bmod 31 = 6859 \bmod 31 = 8$
So, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 31$
Next, note that $8^4 = 4096$. Because $4096 = 178 \cdot 23 + 2$, we have $4096 \bmod 23 = 2$.
Hence $(19^3 \bmod 31)^4 \bmod 23 = 2$.

Corollary 2. *Let m be a positive integer a let a and b be integers.*
Then $(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$
and $(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m$

Proof:
By the definitions of mod m and congruence modulo m, we know that $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$
Hence, Th. 5 tells us that $a + b \equiv [(a \bmod m) + (b \bmod m)] \pmod m$
and $ab \equiv [(a \bmod m)(b \bmod m)] \pmod m$

Arithmetic Modulo m

We can define arithmetic operations on $\mathbb{Z}_m$, the set of nonnegative integers less than m, that is, the set $\{0, 1, \dots, m-1\}$
In particular, we define addition of these integers, denoted by $+_m$ by $a +_m b = (a + b) \bmod m$
and we define multiplication of these integers, denoted by $\cdot_m$ by $a \cdot_m b = (a \cdot b) \bmod m$
The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing arithmetic modulo m.
The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers.
In particular, they satisfy these properties: (I.) Closure: If a and b belong to $\mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbb{Z}_m$

modular addition is said to be a commutative group, both $+_m$ and $\cdot_m$ is said to be a commutative ring. (abstract algebra)

(II.) Associativity: If a, b and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(III.) Commutativity: If a and b belong to $\mathbb{Z}_m$ then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

(IV.) Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. That is, if a belongs to $\mathbb{Z}_m$, then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$

* (V.) Additive inverses: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

No analogous property for multiplicative inverses has been included.
This is because multiplicative inverses do not always exist modulo m.
For instance, there is no multiplicative inverse of 2 modulo 6. $2 \cdot_6 \frac{6}{2} = 2 \cdot 3 = 2 \cdot 3 \bmod 6 = 0$??

(VI.) Distributivity: If a, b and c belong to $\mathbb{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Example 8 Use the definition of addition and multiplication in $\mathbb{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$

Using the definition of addition modulo 11,
we find that $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$ and $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8 \bmod 11$ Hence, $\begin{cases} 7 +_{11} 9 = 5 \\ 7 \cdot_{11} 9 = 8 \end{cases}$

4.3 Primes and Greatest Common Divisors (GCD)

Primes have become essential in modern cryptographic systems, and we will develop some of their properties important in cryptography.
For example, finding large primes is essential in modern cryptography. The length of time required to factor large integers into their prime factors (The fundamental theorem of arithmetic) is the basis for the strength of some important modern cryptographic systems.
In this section we will also study the greatest common divisor of two integers, as well as the least common multiple of two integers
We will develop an important algorithm for computing greatest common divisor, called the Euclidean algorithm.

Definition 1. *An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.*
A positive integer that is greater than 1 and is not prime is called composite.

Remark: The integer 1 is not prime, because it has only one positive factor.
Note also that an integer n is composite if and only if there exist an integer a such that $a \mid n$ and $1 < a < n$.

Theorem 1. The Fundamental Theorem of Arithmetic
Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

Example 1

The integer 7 is prime because its only positive factors are 1 and 7,
whereas the integer 9 is composite because it is divisible by 3.

Example 2

The prime factorizations of 100, 641, 999, and 1024 are given by

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
$641 = 641$
$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdots 2 = 2^{10}$

Trial Division

It is often important to show that a given integer is prime. For instance, in cryptology, large primes are used in some methods for making messages secret.

One procedure for showing that an integer is prime is based on Th. 2.

Theorem 2. If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < a < n$.
Hence, by the definition of a factor, of a positive integer, we have $n = ab$, where b is a positive integer greater than 1.
We will show that $a \le \sqrt{n}$, or $b \le \sqrt{n}$.
If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n}\sqrt{n}$
$> n$, which is a contradiction.
Consequently, $a \le \sqrt{n}$ or $b \le \sqrt{n}$.
Because both a and b are divisors of n, we see than n has a positive divisor not exceeding $\sqrt{n}$.
This divisor is either prime or, by the Fundamental Theorem of Arithmetic, has a prime divisor less than itself.
In either case, n has a prime divisor less than or equal to $\sqrt{n}$. ∎

From Th. 2, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root.

This leads to the brute-force algorithm know as **trial division**. To use trial division we divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

Example 3 | Show that 101 is prime.

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer) it follows that 101 is prime.

Example 4 | Find the prime factorization of 7007

To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3 and 5 divides 7007.
However, 7 divides 7007, with $\frac{7007}{7} = 1001$. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $\frac{1001}{7} = 143$.

Continue by dividing 143 by successive primes, beginning with 7.
Although 7 does not divide 143, 11 does divide 143, and $\frac{143}{11} = 13$. Because 13 is prime, the procedure is completed.
It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$.
Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$

The Sieve of Eratosthenes

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Theorem 3. There are infinitely many primes.

Proof: by contradiction.
We assume that there are only finitely many primes, $p_1, p_2, \dots, p_n$.
Let $Q = p_1 p_2 \cdots p_n + 1$
By the Fundamental Theorem of Arithmetic, Q is prime or else it can be written as the product of two or more primes.
However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$
Hence, there is a prime not in the list $p_1, p_2, \dots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q.
This is a contradiction because we assumed that we have listed all the primes.
Consequently, there are infinitely many primes. ∎

Mersenne primes

The largest prime known has been an integer of the special form $2^p - 1$, where p is also prime.

Extremely efficient test, known as the Lucas-Lehmer test, for determining whether $2^p - 1$ is prime.

Example 5

The numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ are Mersenne primes

while $2^{11} - 1 = 2047$ is not a Mersenne prime because $2047 = 23 \cdot 89$.

Theorem 4. The Prime Number Theorem

The ratio of $\pi(x)$, the number of primes not exceeding x, and $\frac{x}{\ln x}$ approaches 1 as x grows without bound.

Proof using complex variables...

We can use the prime number theorem to estimate the probability that a randomly chosen number is prime.

Greatest Common Divisors & Least Common Multiples

The largest integer that divides both of two integers is called the greatest common divisor of these integers.

Definition 2. Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b.
The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Definition 3. The integers a and b are relatively prime if their gcd is 1

Definition 4. The integers $a_1, a_2, \dots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Another way to find the gcd of two positive integers is to use the prime factorizations of these integers.

Suppose that the prime factorization of the positive integers a and b are
$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$
where each exponent is a nonnegative integer.
Then $\gcd(a, b)$ is given by $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$

Definition 5. The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$

Suppose that the prime factorizations of a and b are as before.
The the lcm of a and b is given by $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$

Example 10 | What is the greatest common divisor of 24 and 36?

The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12
Hence, $\gcd(24, 36) = 12$

Example 11 | What is the greatest common divisor of 17 and 22?

The integers 17 and 22 have no positive common divisors other than 1, so $\gcd(17, 22) = 1$

Example 12

By example 11 it follows that the integers 17 and 22 are relatively prime, because $\gcd(17, 22) = 1$.

Example 13 | Determine whether the integers 10, 17 and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$
We conclude that 10, 17, and 21 are pairwise relatively prime.

Because $\gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime.

Example 14

Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$, $500 = 2^2 \cdot 5^3$
The greatest common divisor is $\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)}$
$= 2^2 \cdot 3^0 \cdot 5^1$
$= 20$

Example 15 | What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

We have $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$
$= 2^4 3^5 7^2$

Theorem 5 Let a and b be positive integers.

Then $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b) \iff \operatorname{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}$

Relationship between gcd and lcm

The Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient.

We will give a more efficient method of finding the greatest common divisor, called the Euclidean algorithm.

Lemma 1. Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$

Division algorithm.

Gcd as Linear Combinations

Theorem 6 Bézout's Theorem

If a and b a positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$

Definition 6. If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called Bézout's coefficients of a and b.

Also, the equation $\gcd(a,b) = sa + tb$ is called Bézout's identity

Use the extended Euclidean algorithm to find Bézout's coefficients of a and b (a linear combination of two integers equal to their g.c.d.)

$sa + tb = \gcd(a,b)$

Lemma 2. If a, b, and c are positive integers such $\gcd(a,b) = 1$ and $a \mid bc$, then $a \mid c$

Proof. Because $\gcd(a,b) = 1$, by Bézout's th. there are integers s and t such that $sa + tb = 1$.

Multiplying both sides of this equation by c, we obtain $sac + tbc = c$.

By (II) of Th.1 of 4.1, $a \mid bc \to a \mid tbc$

Because $a \mid sac$ and $a \mid tbc$, by (I), we conclude that a divides $sac + tbc$.

$a \mid sc \cdot a$

Because $sac + tbc = c$, we conclude that $a \mid c$ ■

Lemma 3. If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Use to prove the uniqueness of prime factorization

Theorem 7. Let m be a positive integer and let a, b, c be integers.

If $ac \equiv bc \pmod m$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod m$

Proof. Because $ac \equiv bc \pmod m$, $m \mid ac - bc \iff m \mid c(a-b)$

By lemma 2, because $\gcd(c,m) = 1$, it follows that $m \mid a - b$

We conclude that $a \equiv b \pmod m$

4.4 Solving Congruence

Solving linear congruences, which have the form $ax \equiv b \pmod m$, is an essential task in the study of number theory and its applications.

A congruence of the form $ax \equiv b \pmod m$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

How can we solve the linear congruence $ax \equiv b \pmod m$, that is, how can we find all integers x that satisfy this congruence?

One method that we will describe uses an integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod m$, if such an integer exist. Such an integer $\bar{a}$ is said to be an inverse of a modulo m.

Theorem 1. If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Proof: Because $\gcd(a,m) = 1$, there are integers s and t such that $sa + tm = 1$.

That implies that $sa + tm \equiv 1 \pmod m$. Because $tm \equiv 0 \pmod m$ it follows that $sa \equiv 1 \pmod m$

Consequently, s is an inverse of a modulo m. ■

Example 16 Find the gcd of 414 and 662 using the Euclidean algorithm.

Successive uses of the division algorithm gives:

$662 = 414 \cdot 1 + 248$
$414 = 248 \cdot 1 + 166$
$248 = 166 \cdot 1 + 82$
$166 = 82 \cdot 2 + 2$
$82 = 2 \cdot 41$

$\gcd(662,414) = \gcd(248,414)$
$= \gcd(248,166)$
$= \gcd(82,166)$
$= \gcd(82,2)$

Hence, $\gcd(414,662) = 2$

because 2 is the last non zero remainder

The Euclidean algorithm is expressed in pseudocode in Algorithm 1.

ALGORITHM 1 The Euclidean Algorithm.

procedure *gcd*(a, b: positive integers)
$x := a$
$y := b$
while $y \neq 0$
  $r := x$ **mod** y
  $x := y$
  $y := r$
return x {gcd(a, b) is x}

$a \geq b$, $O(\log b)$

Example 19

The congruence $14 \equiv 8 \pmod 6$ holds, but both sides of this congruence cannot be divided by 2 to produce a valid congruence because $\frac{14}{2} = 7$ and $\frac{8}{2} = 4$, but $7 \not\equiv 4 \pmod 6$

We have shown previously that we can multiply both sides of a congruence by the same integer

However, dividing by an integer does not always produce a valid congruence (Example 19)

we can if this integer is relatively prime to the modulus (Th. 7)

$(\gcd(m,c) = 1)$

Example 1 Find an inverse of 3 modulo 7 by first finding Bézout's coeff. of 3 and 7.

Because $\gcd(3,7) = 1$, Th.1 tells us that an inverse of 3 modulo 7 exists. Euclidean algorithm ends quickly when used to find the gcd of 3 and 7: $7 = 2 \cdot 3 + 1$

From this equation we see that $7 = 2 \cdot 3 + 1 \iff -2 \cdot 3 + 7 \cdot 1 = 1$

This shows that -2 and 1 are Bézout's coeff of 3 and 7.

We see that -2 is an inverse of 3 modulo 7. Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as 5, -9, 12, and so on.

$3x \equiv 1 \pmod 7$
$\iff 3x + 7y = 1$
$[3,1,0][7,0,1]$
$[3,1,0][1,-2,1]$
$[1,5,-2][1,-2,1]$

Example 2 Find an inverse of 101 modulo 4620

First, we use the Euclidean algorithm to show that $\gcd(101, 4620) = 1$.

Then we will reverse the steps to find Bézout coeff a and b such that $101a + 4620b = 1$.

It will then follow that a is an inverse of 101 modulo 4620. The steps to find $\gcd(101, 4620)$ are

$4620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 3$
$26 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

That is $-35 \cdot 4620 + 1601 \cdot 101 = 1$

tells us that -35 and 1601 are Bézout's coeff of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

$[4620,1,0][101,0,1]$
$[75,1,-45][101,0,1]$
$[75,1,-45][26,-1,46]$
$[23,3,-137][26,-1,46]$
$[23,3,-137][3,-4,183]$
$[2,31,-1418][3,-4,183]$
$[2,31,-1418][1,-35,1601]$
$[1,66,-30019][1,-35,1601]$

Example 3 What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?

By Example 1 we know that -2 is an inverse of 3 modulo 7. Multiplying both sides of the congruence by -2 shows that $-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$.

Because $-6 \equiv 1 \pmod 7$ and $-8 \equiv 6 \pmod 7$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod 7$

We need to determine whether every x with $x \equiv 6 \pmod 7$ is a solution.

Assume that $x \equiv 6 \pmod 7$, by Th.5 of 4.1, it follows that $3x \equiv 3 \cdot 6 \equiv 18 \equiv 4 \pmod 7$

which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, namely, 6, 13, 20, ... and $-1, -8, -15, \ldots$

$3x \equiv 4 \pmod 7 \iff 3x + 7y = 4$
$\iff 3x' + 7y' = 1$

Via l'algo. d'Euclide étendu

$[3,1,0][7,0,1]$ $(x';y') = (-2,1)$
$[3,1,0][1,-2,1]$ $\Rightarrow (x,y) = (-8,4)$
$[1,5,-2][1,-2,1]$

donc $x = 7k - 8$, $k \in \mathbb{Z}$

Theorem 2. The Chinese Remainder Theorem

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers.
Then the system $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$ has a unique solution modulo $m = m_1 m_2 \cdots m_n$.
That is, there is a solution x with $0 \le x < m$,
and all other solutions are congruent modulo m to this solution.

Example 4 In the first century, the Chinese mathematician Sun-Tsu asked: There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question:
What are the solutions of the systems of congruences ?: $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$

Example 5

To solve the system of congruences in Example 4, first let $m = 3 \cdot 5 \cdot 7 = 105$,
$M_1 = \frac{m}{3} = 35$,
$M_2 = \frac{m}{5} = 21$,
$M_3 = \frac{m}{7} = 15$

We see that 2 is an inverse of $M_1 = 35$ modulo 2, because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$

1 is an inverse of $M_2 = 21$ modulo 5, because $21 \cdot 1 \equiv 1 \cdot 1 \equiv 1 \pmod 5$

1 is an inverse of $M_3 = 15$ modulo 7, because $15 \cdot 1 \equiv 1 \cdot 1 \equiv 1 \pmod 7$

The solutions to this system are those x such that $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod m$
$\equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$
$\equiv 233 \pmod{105}$
$\equiv 23 \pmod{105}$

It follows that 23 is the smallest positive integer that is a simultaneous solution.
We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

Example 6 Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$

By Th 4. in section 4.1, the first congruence can be rewritten as an equality, $x = 5t + 1$, where t is an integer.
Substituting this expression for x into the second congruence tells us that $x \equiv 5t + 1 \equiv 2 \pmod 6$ which can be solved to show that $t \equiv 5 \pmod 6$

$5t+1 \equiv 2 \pmod 6$
$\Leftrightarrow 5t \equiv 1 \pmod 6$
$\Leftrightarrow 5t + 6s = 1$
Via l'algo d'Euclide étendu, on a
$[5,1,0][6,0,1]$
$[5,1,0][1,-1,1]$
$[1,5,-4][1,-1,1]$
On retrouve $(t,u) = (5,-4)$
d'où $t = 6u + 5$

Using Th. 4 again, we see that $t = 6u + 5$, where u is an integer.
Substituting this expression for t back into the equation $x = 5t + 1$ tells us that $x = 5(6u+5) + 1$
$= 30u + 26$

We insert this into the third equation to obtain $x \equiv 30u + 26 \equiv 3 \pmod 7$. Solving this congruence tells us that $u \equiv 6 \pmod 7$

$30u + 26 \equiv 3 \pmod 7$
$\Leftrightarrow 30u \equiv -23 \pmod 7$
$\equiv -2 \pmod 7$.
$\Leftrightarrow 30u + 7v = -2$
$\Leftrightarrow 30u' + 7v' = 1$
Via E.-é, $[30,1,0][7,0,1]$
$[2,1,-4][7,0,1]$
$[2,1,-4][1,-3,13]$
$[1,4,-17][1,-3,13]$
On a donc, $(u',v') = (-3,13)$
$\Rightarrow (u,v) = (6,-26)$
Donc $u = 7v + 6$, $v \in \mathbb{Z}$

Hence, $x = 30(7v+6) + 26$
$= 210v + 206$
Translating this back into congruence, we find the solution to the simultaneous congruences,
$\Leftrightarrow x \equiv 206 \pmod{210}$
or $x = 210k + 206$ où $k \in \mathbb{Z}$ ☐

Theorem 3. Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, (where p is prime and $p \nmid a$ ($\gcd(a,p) = 1$))
then $a^{p-1} \equiv 1 \pmod p$

Furthermore, for every integer a we have
$a^p \equiv a \pmod p$ $\quad a \in \{1, 2, \dots, p-1\}$

Remark: Fermat's little theorem tells us that if $a \in \mathbb{Z}_p$, then $a^{p-1} = 1$ in $\mathbb{Z}_p$

Fermat's little theorem is extremely useful in computing the remainders modulo p of large powers of integers

Pseudoprimes

Definition 1. Let b be a positive integer.
If n (not prime) is a composite, and $b^{n-1} \equiv 1 \pmod n$, then n is called a pseudoprime to the base b.

Useful test that provides some evidence concerning whether n is prime, by determining if $2^{n-1} \equiv 1 \pmod n$ (Mersenne prime)
In particular, if n satisfies this congruence, then it is either prime or a pseudoprime to the base 2; if n does not satisfy this congruence, it is composite.

Definition 2. A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod n$ for all positive integers b with $\gcd(b,n) = 1$ is called a Carmichael number (Carmichael number)

Definition 3. A primitive root modulo a prime p is an integer r in $\mathbb{Z}_p$ such that every nonzero element of $\mathbb{Z}_p$ is a power of r.

Definition 4. Suppose that p is a prime, r is a primitive root modulo p, and a is an integer between 1 and $p-1$ inclusive ($\mathbb{Z}_p$)
If $r^e \bmod p = a$ and $0 \le e \le p-1$, we say that e is the discrete logarithm of a modulo p to the base r and we write $\log_r a = e$ (The discrete logarithm problem is hard. The difficulty plays an important role in cryptography.)

Example 9 Find $7^{222} \bmod 11$.

We can use Fermat's little theorem to evaluate $7^{222} \bmod 11$ rather than using the fast modular exponentiation algorithm.
By Fermat's little theorem we know that $7^{10} \equiv 1 \pmod{11}$, so $(7^{10})^k \equiv 1 \pmod{11}$ for every integer k.
To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$.
We know see that $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv (1)^{22} \cdot 7^2 \equiv 49 \equiv 5 \pmod{11}$.
It follows that $7^{222} \bmod 11 = 5$

First, we use the division algorithm to find the quotient q and remainder r when n is divided by $p-1$,
so that $n = q(p-1) + r$, where $0 \le r < p-1$
It follows that $a^n = a^{q(p-1)+r}$
$= (a^{p-1})^q a^r$
$\equiv 1^q a^r \pmod p$
$\equiv a^r \pmod p$

Hence, to find $a^n \bmod p$, we only need to compute $a^r \bmod p$.
We will take advantage of this simplification many times in our study of number theory.

Example 11 The integer 561 is a Carmichael number.

To see this, first note that 561 is composite because $561 = 3 \cdot 11 \cdot 17$
Next, note that if $\gcd(b, 561) = 1$, then $\gcd(b,3) = \gcd(b,11) = \gcd(b,17) = 1$.
Using Fermat's little theorem we find that $\begin{cases} b^2 \equiv 1 \pmod 3 \\ b^{10} \equiv 1 \pmod{11} \\ b^{11} \equiv 1 \pmod{17} \end{cases}$

It follows that $\begin{cases} b^{560} = (b^2)^{280} \equiv 1 \pmod 3 \\ b^{560} = (b^{10})^{56} \equiv 1 \pmod 3 \\ b^{560} = (b^{11})^{35} \equiv 1 \pmod{17} \end{cases}$

It follows that $b^{560} \equiv 1 \pmod{561}$ for all positive integers b with $\gcd(b, 561) = 1$
Hence, 561 is a Carmichael number ☐

4.5 Applications of Congruences

We will introduce three applications in this section: the use of congruences (I.) to assign memory locations to computer files (hashing function with modular arithmetic)

(II.) the generation of pseudorandom numbers (with pseudoprime numbers)

(III.) and check digits.

(I.) Hashing Functions

The central computer at an insurance company maintains records for each of its customers.
How can memory locations be assigned so that customer records can be retreived quickly?
The solution to this problem is to use a suitable chosen **hashing function**.
Records are identified using a **key** in the form of the Social Security number, which uniquely identifies each customer's records.
In practice, many different hashing functions are used. One of the most common is the function $h(k) = k \bmod n$, where n is the number of available memory locations.

Linear probing function

$h(k,i) = h(k) + i \bmod m$, where i runs from 0 to $m-1$

$= k \bmod n + i \bmod m$

(II.) Pseudorandom Numbers

Randomly chosen numbers are often needed for computer simulations. Because numbers generated by systematic method are not truly random, they are called **pseudorandom numbers**.

The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**.

We choose four integers: (I.) the **modulus** m with $2 \le a < m$,
(II.) **multiplier** a $0 \le c < m$,
(III.) **increment** c and $0 \le x_0 < m$
(IV.) and **seed** x_0

We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n < m \ \forall n$ by successively using the recursively defined function $x_{n+1} = (a \cdot x_n + c) \bmod n$

Many computer experiments require the generation of pseudorandom numbers between 0 and 1.
To generate such numbers, we divide numbers generated with a linear congruential generator by the modulus: that is, we use the numbers $\frac{x_n}{m}$

Often, a linear congruential generator with increment $c = 0$ is used. Such a generator is called a **pure multiplicative generator**.

(III.) Check Digits

Congruences are used to check for errors in digit strings. A common technique for detecting errors in such strings is to add an extra digit at the end of the string.
This final digit, or **check digit**, is calculated using a particular function.

Parity Check Bits

Digital information is represented by bit string, split into blocks of specified size. Before each block is stored or transmitted, an extra bit, called a **parity check bit**, can append to each block.
The parity check bit x_{n+1} for the bit string $x_1, x_2, \dots, x_n$ is defined by $x_{n+1} = (x_1 + x_2 + \dots + x_n) \bmod 2$. It follows that x_{n+1} is 0 if there are an even number of 1 bits in the block of n bits and it is 1 if there are an odd number of 1 bits in the block of n bits. When we examine a string that includes a parity check bit, we know that there is an error in it if the parity check bits is wrong.
However, when the parity check bit is correct, there still may be an error. A parity check can detect an odd number of errors in the previous bits, but not an even numbers of errors.
Check bits computing using congruences are used extensively to verify the correctness of various kinds of identification numbers, including:
- → identify products (UPC)
- → identify books (ISBN)
- → money order numbers
- → airline ticket numbers
- → bank account numbers
- → drivers license numbers
- → credit card numbers
- → etc... many other types of id numbers.

Universal Product Codes (UPCs)

Retail products are identified by their UPCs. The most common form of a UPC has 12 decimal digits, where the last digit is a check digit.
The check digit is determined by the congruence $3x_1 + x_2 + 3x_3 + x_4 + \dots + 3x_{11} + x_{12} \equiv 0 \pmod{10}$

$\sum_{i=1}^{12} 3^{i \bmod 2} x_i$

International Standard Book Number (ISBN-10)

This check digit is selected so that $x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}$

or equivalently, so that

$$\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$$

Several kinds of errors often arise identification numbers. A **single error**, an error in one digit of an identification number, is perhaps the most common type of error.
Another common kind of error is a **transposition error**, which occurs when two digits are accidentally interchanged.

Example 1 Find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to the records of customers with Social Security numbers 064212848 and 037149212

The record of the customer with Social Security number 064212848 is assigned to memory location 14 because $h(064212848) = 064212848 \bmod 111 = 14$

Similarly, because $h(037149212) = 037149212 \bmod 111 = 65$

Because a hashing function is not one-to-one (because there are more possible keys than memory locations), more than one file may be assigned to a memory location. When this happens, we say that a **collision** occurs. One way to resolve a collision is to assign the first free location following the occupied memory location assigned by the hashing function.

Example 2 Assign a memory location to the record of the customer with SS number 107405723

First note that hashing function $h(k) = k \bmod 111$ maps the SS number 107405723 to location 14 because $h(107405723) = 10740523 \bmod 111 = 14$.

However, this location is already occupied. But, because memory location 15, the first location following memory location 14, is free, we assign to this location.

Example 3 Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$

We compute the terms of this sequence by successively using the recursively defined function $x_{n+1} = (7x_n + 4) \bmod 9$, begining by inserting the seed $x_0 = 3$ to find x_1.

We find that $x_1 = (7x_0 + 4) \bmod 9 = 25 \bmod 9 = 7$

$x_2 = (7x_1 + 4) \bmod 9 = 53 \bmod 9 = 8$

$\vdots$

$x_9 = (7x_8 + 4) \bmod 9 = 39 \bmod 9 = 3$

Because $x_9 = x_0$ and because each term depends only on the previous term, we see that the sequence 3, 7, 8, 6, 1, 2, 0, 5, 3.... is generated.
This sequence contains nine different numbers before repeating.

Example 4 Suppose we receive in a transmission the bit strings 01100101 and 11010110, each ending with a parity check bit. Should we accept these bit strings as correct?

Before accepting these strings as correct, we examine their parity check bits.
The parity check bit of the first string is 1. Because $0+1+1+0+0+1+0 \equiv 1 \pmod 2$, the parity check bit is correct.
The parity check bit of the second string is 0. We find that $1+1+0+1+0+1+1 \equiv 1 \pmod 2$, so the parity check is incorrect.
We conclude that the first string may have been transmitted correctly and we know for certain that the second string was transmitted incorrectly.
We accept the first string as correct (even though it still may contain an even number of errors), but we reject the second string.

Example 5 Answer these questions:
(a) Suppose that the first 11 digits of UPC are 79357343104. What is the check digit?
(b) Is 041331021641 a valid UPC?

(a) We insert the digits of 79357343104 into the congruence for UPC check digits. This gives $3 \cdot 7 + 9 + 3 \cdot 3 + \dots + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$
Simplifying, we have $98 + x_{12} \equiv 0 \pmod{10}$. It follows that $x_{12} \equiv 2 \pmod{10}$, so the check digit is 2.

(b) To check whether 041331021641 is valid, we insert the digits into the congruence these digits must satisfy. This gives $3 \cdot 0 + 4 + \dots + 3 \cdot 4 + 1 \equiv 4 \not\equiv 0 \pmod{10}$. Hence, not valid.

4.6 Cryptography

Number theory plays a key role in cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge.
Number theory is the basis of many classical ciphers, these ciphers encrypt messages by changing each letter to a different letter, or each block of letters to a different bloc of letters (shift ciphers)

private key ciphers: two parties who wish to communicate in secret must share a secret key.
Knowing how to encrypt allows someone to also decrypt messages (Vulnerable to cryptanalysis).

Number theory is also important in public key cryptography.
In public key cryptography, knowing how to encrypt does not also tell someone how to decrypt. The most widely used public key system, called RSA cryptosystem, encrypts messages using modulow exponentiation,
where the modulus is the product of two large peimes. Knowing how to encrypt requires that someone know the modulus and an exponent (It does not required that the two peime factors of the modulus be known).
As for it is known, knowing how to decrypt requires someone to know how to invert the encryption function, which can only be done in a practical ammount of time when someone know the two large peime factors.
Data can become vulnerable if they must be decrypted for use as input to programs. Homomorphic encryption eliminates this vulnerability by allowing programs to be run on encrypted data. The
The output of these programs is then the encryption of the desired output.

Plays an important role in cloud computing.

Classical Cryptography

Julius Caesar made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three).
To express Caesar's encryption process mathematically, first replace each letter by an element of $\mathbb{Z}_{26}$, replace A by 0, K by 10, and Z by 25.
Caesars encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer $f(p)$ is the set $\{0,1,\dots,25\}$ with $f(p) = (p+3) \bmod 26$
To recover the original message from a secret message encrypted by the Caesar cipher, the function $f^{-1}(p) = (p-3) \bmod 26$ is used.

The process of determing the original message from the encrypted message is called decryption.

We can generalize the Caesar cipher, $\begin{cases} f(p) = (p+k) \bmod 26 \\ f^{-1}(p) = (p-k) \bmod 26 \end{cases} \Rightarrow \begin{cases} c = (p+k) \bmod 26 \\ p = (c-k) \bmod 26 \end{cases}$

We can generalize shift ciphers further to slightly enhance security by using a function of the form $f(p) = (ap+b) \bmod 26$, where a and b are integers, chosen so that f is a bijection
(f is a bijection if and only if $\gcd(a,26) = 1$)
Such a mapping is called an affine transformation
and the resulting cipher is called an affine cipher.

How to decrypt messages encrypted using an affine cipher.
Suppose that $c = (ap+b) \bmod 26$ with $\gcd(a,26) = 1$. To decrypt we need to show how to express p in terms of c. To do this, we apply the encrypting congruence $c \equiv ap+b \pmod{26}$ and solve it for p.
We first substract 6 from both sides, to obtain $c - b \equiv ap \pmod{26}$.
Because $\gcd(a,26) = 1$, we know that there is an inverse $\bar{a}$ of a modulo 26.
Multiplying both sides of the last equation by $\bar{a}$ gives us $\bar{a}(b-c) \equiv \bar{a}ap \pmod{26}$
Because $\bar{a}a \equiv 1 \pmod{26}$, this tells that $p \equiv \bar{a}(c-b) \pmod{26}$.
This determines p because p belongs to $\mathbb{Z}_{26}$.

Example 1 What is the secret message produced from the message "MEET YOU IN THE PARK" using Caesar cipher?
First replace the letters in the message with numbers. This produces 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10
Now replace each of these numbers p by $f(p) = (p+3) \bmod 26$: 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13
Translating this back to letters produces the encrypted message. "PHHW BRX LQ WKH SDUN"

Example 3 Decrypt the ciphertext message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted with the shift cipher with shift $k = 7$.
We first translate the letters back to elements of $\mathbb{Z}_{26}$. We obtain 11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0...
Nex we shift each of these numbers by $-k = -7$ modulo 26 to obtain 4 23 15 4 17 8 4 13 2 4....
Finally, we translate these numbers back to letters to obtain the plaintext.
We obtain "EXPERIENCE IS A GREAT TEACHER".

Example 4 What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?
First, note that 10 represents K. Then, using the encryption function specified, it follows that $f(10) = (7 \cdot 10 + 3) \bmod 21 = 21$
Because 21 represents V, K is replaced by V in the encrypted message.

Public Key Cryptography.

In such a system, every can have a publicly known encryption key. Only the decryption key are kept secret, and only the intended recipient of a message can decrypt it.
Although public key cryptography has the advantage that two parties who wish to communicate securely do not need to exchange keys, it has the disadvantage that encryption and decryption can be extremely time-consuming.
For many applications, this makes public key cryptography impractical. In such situation, private key cryptography is used instead. However, public key cryptography may still be used in the key exchange process.
In the RSA cryptosystem, each individual has an encryption key (n,e), where $n = p \cdot q$, the modulus is the product of two large prime p and q, say with 300 digit each, and an exponent e that is relatively prime to $(p-1)(q-1)$.

RSA Encryption

To encrypt message using a particular key (n,e), we first translate a plaintext message M into sequences of integers $m_1, m_2, \dots m_k$ for some k integer, using the same translation we employed for shift ciphers, with one key difference.
This is done using the function $C = M^e \bmod n$. To perform the encryption, we use an algorith for fast modulow exponentiation.

RSA Decryption

The plaintext message can be quickly recovered from a ciphertext messages when the decryption key k, an inverse of e modulo $(p-1)(q-1)$, is known. Such an inverse exist because $\gcd(e, (p-1)(q-1)) = 1$.
Knowing d let us decrypt messages sent using our key.
Find an inverse d of e modulo $(p-1)(q-1)$ using Euclidean algorithm to find Bézout coeff t and s for d and $(p-1)(q-1)$
A public key cryptosystem, such as RSA, can be used to distribute private keys to pairs of individuals when the wish to communicate.
These people then use a private key system for the encryption and decryption of messages.

To see this, note that if $de \equiv 1 \pmod{(p-1)(q-1)}$,
there is an integer k such that $de = 1 + k(p-1)(q-1)$
It follows that $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \pmod n$
By Fermat's little theorem (assuming that $\gcd(m,p) = \gcd(m,q) = 1$),
its follows that $\begin{cases} m^{p-1} \equiv 1 \pmod p \\ m^{q-1} \equiv 1 \pmod q \end{cases}$
Consequently, $\begin{cases} C^d \equiv m \cdot \underbrace{(m^{p-1})^{k(q-1)}}_{\equiv 1} \equiv m \cdot 1 \equiv m \pmod p \\ C^d \equiv m \cdot (m^{q-1})^{k(p-1)} \equiv m \pmod q \end{cases}$
Because $\gcd(p,q) = 1$, if follows by the Chinese remainder theorem
that $C^d \equiv m \pmod{\underbrace{p \cdot q}_{=n}}$

Example 8 Encrypt the message STOP using the RSA cryptosystem with key $(2537, 13)$. Note that $2537 = 43 \cdot 59$ $\Rightarrow \begin{cases} p = 43 \\ q = 59 \end{cases}$ are primes and $\gcd(e, (p-1)(q-1)) = \gcd(13; 42 \cdot 58) = 1$
To encrypt, we first translate the letters in STOP into their numerical equivalents.
We then group these numbers into blocks of four digits (because $2525 < 2537 < 252525$)
to obtain 1819 1415
We encrypt each block using the mapping $C = M^{13} \bmod 2537$.
Computing using fast modulow multiplication show that $\begin{cases} 1819^{13} \bmod 2537 = 2081 \\ 1415^{13} \bmod 2537 = 2182 \end{cases}$
The encrypted message is 2081 2182.

Example 9 We receive the encrypted message 0981 0461. What is the decrypted message if it was encrypted using the RSA cipher from Ex8.
The message was encrypted using the RSA cryptosystem with $n = 43 \cdot 59$ and exponent 13.
$d = 937$ is an inverse of 13 modulo $42 \cdot 58$. We use 937 as our decryption exponent.
2436
Consequently, to decrypt a block c, we compute $m = c^{937} \bmod 2537$.
To decrypt the message, we use the fast modulow exponentiation algorithm to compute $\begin{cases} 0981^{937} \bmod 2537 = 0704 \\ 0461^{937} \bmod 2537 = 1115 \end{cases}$
Consequently, the numerical version of the original message is 0704 1115.
Translating this back to English letters, we see that the message is HELP.

Key Exchange (Diffie-Hellman key agreement protocol)

Suppose that Alice and Bob want to share a common key. The protocol follows these steps, where the computations are done in Z_p.
(1) Alice and Bob agree to use a prime p and a primitive root a of p.
(2) Alice chooses a secret integer k_1 and sends $a^{k_1} \bmod p$ to Bob.
(3) Bob chooses a secret integer k_2 and sends $a^{k_2} \bmod p$ to Alice.
(4) Alice computes $(a^{k_2})^{k_1} \bmod p$.
(5) Bob computes $(a^{k_1})^{k_2} \bmod p$.
At the end of this protocol, Alice and Bob have computed their shared key, namely,
$(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p$.

$p, a, a^{k_1} \bmod p$, and $a^{k_2} \bmod p$ are assumed to be public information.
The protocol ensures that k_1, k_2 and the common key $(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p$ are kept secret.

Homomorphic Encryption

A cryptosystem, such as RSA, can be used to encrypt files to keep them secret. Today, many users store encrypted files in the cloud, where they reside on remote computers.
It is often necessary to run programs using data from files stores on the cloud. These data are vulnerable to users with access to the remote computer where our data are stored if we run programs on the cloud without downloading these data.

RSA is partially homomorphic
Let (n,e) be a public key for the RSA cryptosystem and suppose that M_1 and M_2 are plaintext messages, so that $0 \leq M_1 < n$ and $0 \leq M_2 < n$

Then $E_{(n,e)}(M_1) \cdot E_{(n,e)}(M_2) \bmod m = (M_1^e \bmod n \cdot M_2^e \bmod m) \bmod m$
$= (M_1 M_2)^e \bmod m$
$= E_{(n,e)}(M_1 \cdot M_2)$ in $\mathbb{Z}_n$ (RSA is multiplicatively homomorphic).
However, we cannot add the encryption of two numbers to obtain the encryption of their sum.
We say that RSA is not additively homomorphic.