Course of Study	CM1015
Extract Title	pp. xvii-xxii (Notation); pp.111-114 1.6.1; pp.118-122 1.6.2; pp.125-127 1.6.3; pp.21-27 1.2.1
Extract Author	Yan, S. Y.
Publication Year, Volume, Issue	2002
Page extent	xvii-xxii; 21-27; 111-114; 118-122; 125-127
Source Title	Number theory for computing
ISBN-ISSN	9783540430728

Notation

All notation should be as simple as the nature of the operations to which it is applied.

CHARLES BABBAGE (1791–1871)

Notation	Explanation
$\mathbb{N}$	set of natural numbers: $\mathbb{N} = \{1, 2, 3, \cdots\}$
$\mathbb{Z}$	set of integers (whole numbers): $\mathbb{Z} = \{0, \pm n : n \in \mathbb{N}\}$
$\mathbb{Z}^+$	set of positive integers: $\mathbb{Z}^+ = \mathbb{N}$
$\mathbb{Z}_{>1}$	set of positive integers greater than 1: $\mathbb{Z}_{>1} = \{n : n \in \mathbb{Z} \text{ and } n > 1\}$
$\mathbb{Q}$	set of rational numbers: $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$
$\mathbb{R}$	set of real numbers: $\mathbb{R} = \{n + 0.d_1d_2d_3\cdots : n \in \mathbb{Z},\ d_i \in \{0, 1, \cdots, 9\}$ and no infinite sequence of 9's appears$\}$
$\mathbb{C}$	set of complex numbers: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\}$
$\mathbb{Z}/n\mathbb{Z}$	also denoted by $\mathbb{Z}_n$, residue classes modulo n; a ring of integers; a field if n is prime
$(\mathbb{Z}/n\mathbb{Z})^*$	multiplicative group; the elements of this group are the elements in $\mathbb{Z}/n\mathbb{Z}$ that are relatively prime to n: $(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} :\ \gcd(a, n) = 1\}$.
$\mathbb{F}_p$	finite field with p elements, where p is a prime number
$\mathbb{F}_q$	finite field with $q = p^k$ a prime power
$\mathcal{K}$	(arbitrary) field
$\mathcal{R}$	ring

$\mathcal{G}$	group
$\lvert\mathcal{G}\rvert$	order of group $\mathcal{G}$
B_n	Bernoulli numbers: $\binom{n+1}{1} B_n + \cdots + \binom{n+1}{n} B_1 + B_0 = 0$
F_n	Fermat numbers: $F_n = 2^{2^n} + 1,\ n \geq 0$
M_p	Mersenne primes: $M_p = 2^p - 1$ is prime whenever p is prime
$\sqrt{x}$	square root of x
$\sqrt[k]{x}$	kth root of x
$\sim$	asymptotic equality
$\approx$	approximate equality
∞	infinity
$\Longrightarrow$	implication
$\Longleftrightarrow$	equivalence
$\square$	blank symbol; end of proof
$\sqcup$	space
Prob	probability measure
$\lvert S\rvert$	cardinality of set S
$\in$	member of
$\subset$	proper subset
$\subseteq$	subset
$\star, *$	binary operations
$\oplus$	binary operation (addition); exclusive or (XOR)
$\odot$	binary operation (multiplication)
$f(x) \sim g(x)$	$f(x)$ and $g(x)$ are asymptotically equal
$(\mathcal{G}, *) \cong (\mathcal{H}, \star)$	$(\mathcal{G}, *)$ and $(\mathcal{H}, \star)$ are isomorphic
$\perp$	undefined
e_k	encryption key
d_k	decryption key
$E_{e_k}(M)$	encryption process $C = E_{e_k}(M)$, where M is the plaintext
$D_{d_k}(C)$	decryption process $M = D_{d_k}(C)$, where C is the ciphertext

$f(x)$	function of x
f^{-1}	inverse of f
$\binom{n}{i}$	binomial coefficient
$\int$	integration
$\mathrm{Li}(x)$	logarithmic integral: $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$
$\sum_{i=1}^{n} x_i$	sum: $x_1 + x_2 + \cdots + x_n$
$\prod_{i=1}^{n} x_i$	product: $x_1 x_2 \cdots x_n$
$n!$	factorial: $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$
x^k	x to the power k
kP	$kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ summands}}$, where P is a point (x, y) on an elliptic curve $E: \; y^2 = x^3 + ax + b$
$\mathcal{O}_E$	the point at infinity on an elliptic curve E over a field
e	the transcendental number $e = \sum_{n \geq 0} \frac{1}{n!} \approx 2.7182818$
$\log_b x$	logarithm of x to the base b ($b \neq 1$): $x = b^{\log_b x}$
$\log x$	binary logarithm: $\log_2 x$
$\ln x$	natural logarithm: $\log_e x$
$\exp(x)$	exponential of x: $e^x = \sum_{n \geq 0} \frac{x^n}{n!}$
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$p^\alpha \mid\mid n$	$p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$
$\gcd(a, b)$	greatest common divisor of (a, b)
$\mathrm{lcm}(a, b)$	least common multiple of (a, b)
$\lfloor x \rfloor$	the greatest integer less than or equal to x
$\lceil x \rceil$	the least integer greater than or equal to x
x mod n	remainder: $x - n \left\lfloor \frac{x}{n} \right\rfloor$
$x = y \bmod n$	x is equal to y reduced to modulo n
$x \equiv y \pmod{n}$	x is congruent to y modulo n
$x \not\equiv y \pmod{n}$	x is not congruent to y modulo n

$[a]_n$	residue class of a modulo n
$+_n$	addition modulo n
$-_n$	subtraction modulo n
$\cdot_n$	multiplication modulo n
$x^k \bmod n$	x to the power k modulo n
$kP \bmod n$	kP modulo n
$\mathrm{ord}_n(a)$	order of an integer a modulo n; also denoted by $\mathrm{ord}(a,n)$
$\mathrm{ind}_{g,n}a$	index of a to the base g modulo n; also denoted by $\mathrm{ind}_g a$ whenever n is fixed
$\pi(x)$	number of primes less than or equal to x: $\pi(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} 1$
$\tau(n)$	number of positive divisors of n: $\tau(n) = \sum_{d\mid n} 1$
$\sigma(n)$	sum of positive divisors of n: $\sigma(n) = \sum_{d\mid n} d$
$s(n)$	sum of proper divisors of n: $s(n) = \sigma(n) - n$
$\phi(n)$	Euler's totient function: $\phi(n) = \sum_{\substack{0 \le k < n \\ \gcd(k,n)=1}} 1$
$\lambda(n)$	Carmichael's function: $\lambda(n) = \mathrm{lcm}\,(\lambda(p_1^{\alpha_1})\lambda(p_2^{\alpha_2})\cdots\lambda(p_k^{\alpha_k}))$ if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$
$\mu(n)$	Möbius function
$\zeta(s)$	Riemann zeta-function: $\zeta(s) = \prod_{n=1}^{\infty} \frac{1}{n^s}$, where s is a complex variable
$\left(\frac{a}{p}\right)$	Legendre symbol, where p is prime
$\left(\frac{a}{n}\right)$	Jacobi symbol, where n is composite
Q_n	set of all quadratic residues of n
$\overline{Q}_n$	set of all quadratic nonresidues of n
J_n	$J_n = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) = 1\right\}$
$\tilde{Q}_n$	set of all pseudosquares of n: $\tilde{Q}_n = J_n - Q_n$
$K(k)_n$	set of all kth power residues of n, where $k \ge 2$
$\overline{K(k)}_n$	set of all kth power nonresidues of n, where $k \ge 2$

$[q_0, q_1, q_2, \cdots, q_n]$	finite simple continued fraction
$C_k = \frac{P_k}{Q_k}$	k-th convergent of a continued fraction
$[q_0, q_1, q_2, \cdots]$	infinite simple continued fraction
$[q_0, q_1, \cdots, q_k, \overline{q_{k+1}, q_{k+2}, \cdots, q_{k+m}}]$	periodic simple continued fraction
$\mathcal{P}$	class of problems solvable in deterministic polynomial time
$\mathcal{NP}$	class of problems solvable in nondeterministic polynomial time
$\mathcal{RP}$	class of problems solvable in random polynomial time with one-sided errors
$\mathcal{BPP}$	class of problems solvable in random polynomial time with two-sided errors
$\mathcal{ZPP}$	class of problems solvable in random polynomial time with zero errors
$\mathcal{O}(\cdot)$	upper bound: $f(n) = \mathcal{O}(g(n))$ if there exists *some* constant $c > 0$ such that $f(n) \leq c \cdot g(n)$
$o(\cdot)$	upper bound that is not asymptotically tight: $f(n) = \mathcal{O}(g(n))$, $\forall c > 0$ such that $f(n) < c \cdot g(n)$
$\Omega(\cdot)$	low bound: $f(n) = \Omega(g(n))$ if there exists a constant c such that $f(n) \geq \frac{1}{c} \cdot g(n)$
$\Theta(\cdot)$	tight bound: $f(n) = \Theta(n)$ if $f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n))$
$\mathcal{O}(N^k)$	polynomial-time complexity measured in terms of arithmetic operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^k\right)$	polynomial-time complexity measured in terms of bit operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^{c \log N}\right)$	superpolynomial complexity, where $c > 0$ is a constant
$\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right)$	subexponential complexity, $\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right) = \mathcal{O}\left(N^{c\sqrt{\log\log N / \log N}}\right)$
$\mathcal{O}\left(\exp(x)\right)$	exponential complexity, sometimes denoted by $\mathcal{O}\left(e^x\right)$
$\mathcal{O}\left(N^\epsilon\right)$	exponential complexity measured in terms of bit operations; $\mathcal{O}\left(N^\epsilon\right) = \mathcal{O}\left(2^{\epsilon \log N}\right)$, where $\epsilon > 0$ is a constant
CFRAC	Continued FRACtion method (for factoring)
ECM	Elliptic Curve Method (for factoring)

NFS	Number Field Sieve (for factoring)
QS/MPQS	Quadratic Sieve/Multiple Polynomial Quadratic Sieve (for factoring)
ECPP	Elliptic Curve Primality Proving
DES	Data Encryption Standard
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
RSA	Rivest-Shamir-Adleman
WWW	World Wide Web

Example 1.1.10. The finite field $\mathbb{F}_5$ has elements $\{0, 1, 2, 3, 4\}$ and is described by the following addition and multiplication table (see Table 1.1):

Table 1.1. The addition and multiplication for $\mathbb{F}_5$

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The theory of groups, rings, and particularly finite fields plays a very important role in elementary, algorithmic and applied number theory, including cryptography and information security.

1.2 Theory of Divisibility

The primary source of all mathematics is the integers.

H. Minkowski (1864–1909)

Divisibility has been studied for at least three thousand years. From before the time of Pythagoras, the Greeks considered questions about even and odd numbers, perfect and amicable numbers, and the primes, among many others; even today a few of these questions are still unanswered.

1.2.1 Basic Concepts and Properties of Divisibility

Definition 1.2.1. Let a and b be integers with $a \neq 0$. We say a divides b, denoted by $a \mid b$, if there exists an integer c such that $b = ac$. When a divides b, we say that a is a *divisor* (or *factor*) of b, and b is a *multiple* of a. If a does not divide b, we write $a \nmid b$. If $a \mid b$ and $0 < a < b$, then a is called a *proper divisor* of b.

Remark 1.2.1. We never use 0 as the left member of the pair of integers in $a \mid b$, however, 0 may occur as the right member of the pair, thus $a \mid 0$ for every integer a not zero. Under this restriction, for $a \mid b$, we may say that b is divisible by a, which is equivalent to say that a is a divisor of b. The notation $a^\alpha \,||\, b$ is sometimes used to indicate that $a^\alpha \mid b$ but $a^{\alpha+1} \nmid b$.

Example 1.2.1. The integer 200 has the following positive divisors (note that, as usual, we shall be only concerned with positive divisors, not negative divisors, of an integer):

$$1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200.$$

Thus, for example, we can write

$$8 \mid 200,\ 50 \mid 200,\ 7 \nmid 200,\ 35 \nmid 200.$$

Definition 1.2.2. A divisor of n is called a *trivial divisor* of n if it is either 1 or n itself. A divisor of n is called a *nontrivial divisor* if it is a divisor of n, but is neither 1, nor n.

Example 1.2.2. For the integer 18, 1 and 18 are the trivial divisors, whereas 2, 3, 6 and 9 are the nontrivial divisors. The integer 191 has only two trivial divisors and does not have any nontrivial divisors.

Some basic properties of divisibility are given in the following theorem:

Theorem 1.2.1. Let a, b and c be integers. Then

(1) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
(2) if $a \mid b$, then $a \mid bc$, for any integer c.
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof.

(1) Since $a \mid b$ and $a \mid c$, we have

$$b = ma,\ c = na, \quad m, n \in \mathbb{Z}.$$

Thus $b + c = (m + n)a$. Hence, $a \mid (m + n)a$ since $m + n$ is an integer. The result follows.

(2) Since $a \mid b$ we have

$$b = ma, \quad m \in \mathbb{Z}.$$

Multiplying both sides of this equality by c gives

$$bc = (mc)a$$

which gives $a \mid bc$, for all integers c (whether or not $c = 0$).

(3) Since $a \mid b$ and $b \mid c$, there exists integers m and n such that

$$b = ma, \quad c = nb.$$

Thus, $c = (mn)a$. Since mn is an integer the result follows.

Exercise 1.2.1. Let a, b and c be integers. Show that

(1) $1 \mid a$, $a \mid a$, $a \mid 0$.
(2) if $a \mid b$ and $b \mid a$, then $a = \pm b$.
(3) if $a \mid b$ and $a \mid c$, then for all integers m and n we have $a \mid (mb + nc)$.
(4) if $a \mid b$ and a and b are positive integers, then $a < b$.

The next result is a general statement of the outcome when any integer a is divided by any positive integer b.

Theorem 1.2.2 (Division algorithm). For any integer a and any positive integer b, there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b, \tag{1.41}$$

where a is called the *dividend*, q the *quotient*, and r the *remainder*. If $b \nmid a$, then r satisfies the stronger inequalities $0 < r < a$.

Proof. Consider the arithmetic progression

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

then there must be an integer q such that

$$qb \leq a \leq (q+1)b.$$

Let $a - qb = r$, then $a = bq + r$ with $0 \leq r < b$. To prove the uniqueness of q and r, suppose there is another pair q_1 and r_1 satisfying the same condition in (1.41), then

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

We first show that $r_1 = r$. For if not, we may presume that $r < r_1$, so that $0 < r_1 - r < b$, and then we see that $b(q - q_1) = r_1 - r$, and so $b \mid (r_1 - r)$, which is impossible. Hence, $r = r_1$, and also $q = q_1$. □

Remark 1.2.2. Theorem 1.2.2 is called the division algorithm. An *algorithm* is a mathematical procedure or method to obtain a result (we will discuss algorithms and their complexity in detail in Chapter 2). We have stated in Theorem 1.2.2 that "there exist unique integer q and r" and this wording suggests that we have an *existence theorem* rather than an *algorithm*. However, it may be observed that the proof does provide a method for obtaining the integer q and r, since q and r can be obtained by the arithmetic division a/b.

Example 1.2.3. Let $b = 15$. Then

(1) when $a = 255$, $a = b \cdot 17 + 0$, so $q = 17$ and $r = 0 < 15$.
(2) when $a = 177$, $a = b \cdot 11 + 12$, so $q = 11$ and $r = 12 < 15$.

(3) when $a = -783$, $a = b \cdot (-52) + 3$, so $q = -52$ and $r = 3 < 15$.

Definition 1.2.3. Consider the following equation

$$a = 2q + r, \quad a, q, r \in \mathbb{Z},\ 0 \leq r < q. \tag{1.42}$$

Then if $r = 0$, then a is *even*, whereas if $r = 1$, then a is *odd*.

Definition 1.2.4. A positive integer n greater than 1 is called *prime* if its only divisors are n and 1. A positive integer n that is greater than 1 and is not prime is called *composite*.

Example 1.2.4. The integer 23 is prime since its only divisors are 1 and 23, whereas 22 is composite since it is divisible by 2 and 11.

Prime numbers have many special and nice properties, and play a central role in the development of number theory. Mathematicians throughout history have been fascinated by primes. The first result on prime numbers is due to Euclid:

Theorem 1.2.3 (Euclid). There are infinitely many primes.

Proof. Suppose that $p_1, p_2, \cdots, p_k$ are all the primes. Consider the number $N = p_1 p_2 \cdots p_k + 1$. If it is a prime, then it is a new prime. Otherwise, it has a prime factor q. If q were one of the primes p_i, $i = 1, 2, \cdots, k$, then $q \mid (p_1 p_2 \cdots p_k)$, and since $q \mid (p_1 p_2 \cdots p_k + 1)$, q would divide the difference of these numbers, namely 1, which is impossible. So q cannot be one of the p_i for $i = 1, 2, \cdots, k$, and must therefore be a new prime. This completes the proof. □

Remark 1.2.3. The above proof of Euclid's theorem is based on the modern algebraic language. For Euclid's original proof, translated in English, see Figure 1.3.

Two other related elementary results about the infinitude of primes are as follows.

Theorem 1.2.4. If n is an integer ≥ 1, then there is a prime p such that $n < p \leq n! + 1$.

Proof. Consider the integer $N = n! + 1$. If N is prime, we may take $p = N$. If N is not prime, it has some prime factor p. Suppose $p \leq n$, then $p \mid n!$; hence, $p \mid (N - n!)$, which is ridiculous since $N - n! = 1$. Therefore, $p > n$. □

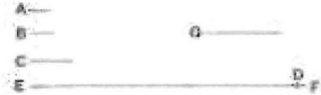
Theorem 1.2.5. Given any real number $x \geq 1$, there exists a prime between x and $2x$.

PROPOSITION 20.

Prime numbers are more than any assigned multitude of prime numbers.

Let A, B, C be the assigned prime numbers;

I say that there are more prime numbers than A, B, C.



For let the least number measured by A, B, C be taken,

and let it be DE;

let the unit DF be added to DE.

Then EF is either prime or not.

First, let it be prime;

then the prime numbers A, B, C, EF have been found which are more than A, B, C.

Next, let EF not be prime;

therefore it is measured by some prime number [VII. 31]

Let it be measured by the prime number G.

I say that G is not the same with any of the numbers A, B, C.

For, if possible, let it be so.

Now A, B, C measure DE;

therefore G also will measure DE.

But it also measures EF.

Therefore G, being a number, will measure the remainder, the unit DF;

which is absurd.

Therefore G is not the same with any one of the numbers A, B, C.

And by hypothesis it is prime.

Therefore the prime numbers A, B, C, G have been found which are more than the assigned multitude of A, B, C.

Q. E. D.

Figure 1.3. Proposition 20 of the *Elements* Book IX (by courtesy of Thomas L. Heath [73])

This is the famous Bertrand's postulate, conjectured by Joseph Bertrand (1822–1900) in 1845, and proved by Chebyshev in 1850. The proof of this result is rather lengthy; interested readers are advised to consult Hardy and Wright's book [100]. However, there do exist long sequences of consecutive integers which are barren of primes, as the next result shows.

Proposition 1.2.1. If n is an integer ≥ 2, then there are no primes between $n! + 2$ and $n! + n$.

Proof. Since if $n!$ is a product of all integers between 1 and n, then $2 \mid n!+2$, $3 \mid n! + 3, \cdots, n \mid n! + n$. □

Theorem 1.2.6. If n is a composite, then n has a prime divisor p such that $p \leq \sqrt{n}$.

Proof. Let p be the smallest prime divisor of n. If $n = rs$, then $p \leq r$ and $p \leq s$. Hence, $p^2 \leq rs = n$. That is, $p \leq \sqrt{n}$. □

Theorem 1.2.6 can be used to find all the prime numbers up to a given positive integer x; this procedure is called the Sieve of Eratosthenes, attributed to the ancient Greek astronomer and mathematician Eratosthenes of Cyrene[12], assuming that x is relatively small. To apply the sieve, list all the integers from 2 up to x in order:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \cdots, x.$$

Starting from 2, delete all the multiples $2m$ of 2 such that $2 < 2m \leq x$:

$$2, 3, 5, 7, 9, 11, 13, 15, \cdots, x.$$

Starting from 3, delete all the multiples $3m$ of 3 such that $3 < 3m \leq x$:

$$2, 3, 5, 7, 11, 13, \cdots, x.$$

In general, if the resulting sequence at the kth stage is

$$2, 3, 5, 7, 11, 13, \cdots, p, \cdots, x.$$

then delete all the multiples pm of p such that $p < pm \leq x$. Continue this exhaustive computation, until $p \leq \lfloor \sqrt{x} \rfloor$. The remaining integers are all the primes between $\lfloor \sqrt{x} \rfloor$ and x and if we take care not to delete $2, 3, 5, \cdots, p \leq \lfloor \sqrt{x} \rfloor$, the sieve then gives all the primes less than or equal to x. For example, let $x = 36$, then $\sqrt{x} = 6$, there are only three primes 2, 3 and 5 below 6, and all the positive integers from 2 to 36 are as follows.

	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

First of all, we delete (marked with the symbol "_") all the multiples of 2 with $2 < 2m \leq 36$, for $m = 1, 2, \cdots, 18$, and get:

12

Eratosthenes of Cyrene (274–194 B.C.) was born in Cyrene which is now in Libya in North Africa, was one of the great men in the ancient world. He was the first to calculate the size of the Earth by making measurements of the angle of the Sun at two different places a known distance apart. His other achievements include measuring the tilt of the Earth's axis. Eratosthenes also worked on prime numbers. He is best remembered by generations of number theorists for his prime number sieve, the "Sieve of Eratosthenes" which, in modified form, is still an important tool in number theory research.

	2	3	-	5	-	7	-	9	-	11	-
13	-	15	-	17	-	19	-	21	-	23	-
25	-	27	-	29	-	31	-	33	-	35	-

Then we delete (marked with the symbol "$*$") all the multiples of 3 with $3 < 3m \leq 36$, for $m = 1, 2, \cdots, 11$, and get:

	2	3	-	5	-	7	-	$*$	-	11	-
13	-	$*$	-	17	-	19	-	$*$	-	23	-
25	-	$*$	-	29	-	31	-	$*$	-	35	-

Finally, we delete (marked with the symbol "$\times$") all the multiples of 5 with $5 < 5m \leq 35$, for $m = 1, 2, \cdots, 7$, and get:

	2	3	-	5	-	7	-	$*$	-	11	-
13	-	$*$	-	17	-	19	-	$*$	-	23	-
$\times$	-	$*$	-	29	-	31	-	$*$	-	$\times$	-

The remaining numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ are then the primes up to 36.

According to the above analysis, we can get the following algorithm for the Sieve of Eratosthenes:

Algorithm 1.2.1 (The Sieve of Eratosthenes). Given a positive integer $n > 1$, this algorithm will find all prime numbers up to n.

[1] Create a list of integers from 2 to n;

[2] For prime numbers p_i $(i = 1, 2, \cdots)$ from $2, 3, 5$ up to $\lfloor \sqrt{n} \rfloor$, delete all the multiples $p_i < p_i m \leq n$ from the list;

[3] Print the integers remaining in the list.

1.2.2 Fundamental Theorem of Arithmetic

First, let us investigate a simple but important property of composite numbers.

Theorem 1.2.7. Every composite number has a prime factor.

Proof. Let n be a composite number. Then

$$n = n_1 n_2$$

where n_1 and n_2 are positive integers with $n_1, n_2 < n$. If either n_1 or n_2 is a prime, then the theorem is proved. If n_1 and n_2 are not prime, then

$$n_1 = n_3 n_4$$

Erdös conjectured that if $\{a_i\}$ is any infinite sequence of integers for which $\sum \frac{1}{a_i}$ is divergent, then the sequence contains arbitrarily long arithmetic progressions; he offered \$3000 for a proof or disproof of this conjecture (before his death, Erdös signed some blank cheques and left them in the care of Ronald L. Graham to present to future problem solvers). A related but even more difficult problem is the following:

Conjecture 1.5.5. There are arbitrarily long arithmetic progressions of consecutive primes.

1.6 Theory of Congruences

As with everything else, so with a mathematical theory: beauty can be perceived, but not explained.

ARTHUR CAYLEY (1821–1895)

1.6.1 Basic Concepts and Properties of Congruences

The notion of congruences was first introduced by Gauss, who gave their definition in his celebrated *Disquisitiones Arithmeticae* in 1801, though the ancient Greeks and Chinese had already had the idea.

Definition 1.6.1. Let a be an integer and n a positive integer greater than 1. We define "$a \bmod n$" to be the remainder r when a is divided by n, that is

$$r = a \bmod n = a - \lfloor a/n \rfloor n. \tag{1.219}$$

We may also say that "r is equal to a reduced modulo n".

Remark 1.6.1. It follows from the above definition that $a \bmod n$ is the integer r such that $a = \lfloor a/n \rfloor n + r$ and $0 \leq r < n$, which was known to the ancient Greeks and Chinese some 2000 years ago.

Example 1.6.1. The following are some examples of $a \bmod n$:

$$35 \bmod 12 = 11,$$
$$-129 \bmod 7 = 4,$$
$$3210 \bmod 101 = 79,$$
$$1412^{13115} \bmod 12349 = 1275.$$

Given the well-defined notion of the remainder of one integer when divided by another, it is convenient to provide a special notion to indicate equality of remainders.

Definition 1.6.2. Let a and b be integers and n a positive integer. We say that "a is *congruent* to b modulo n", denoted by

$$a \equiv b \pmod{n} \tag{1.220}$$

if n is a divisor of $a - b$, or equivalently, if $n \mid (a - b)$. Similarly, we write

$$a \not\equiv b \pmod{n} \tag{1.221}$$

if a is not congruent (or incongruent) to b modulo n, or equivalently, if $n \nmid (a - b)$. Clearly, for $a \equiv b \pmod{n}$ (resp. $a \not\equiv b \pmod{n}$), we can write $a = kn - b$ (resp. $a \neq kn - b$) for some integer k. The integer n is called the *modulus*.

Clearly,

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (a - b) \\ &\iff a = kn + b, \quad k \in \mathbb{Z} \end{aligned}$$

and

$$\begin{aligned} a \not\equiv b \pmod{n} &\iff n \nmid (a - b) \\ &\iff a \neq kn + b, \quad k \in \mathbb{Z} \end{aligned}$$

So, the above definition of congruences, introduced by Gauss in his *Disquisitiones Arithmeticae*, does not offer any new idea than the divisibility relation, since "$a \equiv b \pmod{n}$" and "$n \mid (a - b)$" (resp. "$a \not\equiv b \pmod{n}$" and "$n \nmid (a - b)$") have the same meaning, although each of them has its own advantages. However, Gauss did present a *new* way (i.e., congruences) of looking at the old things (i.e., divisibility); this is exactly what we are interested in. It is interesting to note that the ancient Chinese mathematician Ch'in Chiu-Shao[30] already had the idea and theory of congruences in his famous book *Mathematical Treatise in Nine Chapters* appeared in 1247.

Definition 1.6.3. If $a \equiv b \pmod{n}$, then b is called a *residue* of a modulo n. If $0 \leq b \leq m - 1$, b is called the *least nonnegative residue* of a modulo n.

Remark 1.6.2. It is common, particularly in computer programs, to denote the least nonnegative residue of a modulo n by $a \bmod n$. Thus, $a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$, and, of course, $a \not\equiv b \pmod{n}$ if and only if $a \bmod n \neq b \bmod n$.

[30] Ch'in Chiu-Shao (1202–1261) was born in the southwest Chinese province of Sichuan, but studied astronomy in Hangzhou, the capital of the Song dynasty, now the capital of the Chinese southeast province Zhejiang. Ch'in was a genius in mathematics and was also accomplished in poetry, fencing, archery, riding, music and architecture. He wrote *Mathematical Treatise in Nine Chapters* which appeared in 1247. It contains simultaneous integer congruences, the Chinese Remainder Theorem, and considers algebraic equations, areas of geometrical figures and linear simultaneous equations. This work on *congruences* was rediscovered by Gauss, Lebesgue and Stieltjes.

Example 1.6.2. The following are some examples of congruences or incongruences.

$$\begin{aligned} 35 &\equiv 11 \pmod{12} && \text{since} && 12 \mid (35-11) \\ &\not\equiv 12 \pmod{11} && \text{since} && 11 \nmid (35-12) \\ &\equiv 2 \pmod{11} && \text{since} && 11 \mid (35-2) \end{aligned}$$

The congruence relation has many properties in common with the equality relation. For example, we know from high-school mathematics that equality is

(1) reflexive: $a = a$, $\forall a \in \mathbb{Z}$;
(2) symmetric: if $a = b$, then $b = a$, $\forall a, b \in \mathbb{Z}$;
(3) transitive: if $a = b$ and $b = c$, then $a = c$, $\forall a, b, c \in \mathbb{Z}$.

We shall see that congruence modulo n has the same properties:

Theorem 1.6.1. Let n be a positive integer. Then the congruence modulo n is

(1) reflexive: $a \equiv a \pmod{n}$, $\forall a \in \mathbb{Z}$;
(2) symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, $\forall a, b \in \mathbb{Z}$;
(3) transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$, $\forall a, b, c \in \mathbb{Z}$.

Proof.

(1) For any integer a, we have $a = 0 \cdot n + a$, hence $a \equiv a \pmod{n}$.
(2) For any integers a and b, if $a \equiv b \pmod{n}$, then $a = kn + b$ for some integer k. Hence $b = a - kn = (-k)n + a$, which implies $b \equiv a \pmod{n}$, since $-k$ is an integer.
(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a = k_1 n + b$ and $b = k_2 n + c$. Thus, we can get

$$a = k_1 n + k_2 n + c = (k_1 + k_2)n + c = k'n + c$$

which implies $a \equiv c \pmod{n}$, since k' is an integer. □

Theorem 1.6.1 shows that the congruence modulo n is an equivalence relation on the set of integers $\mathbb{Z}$. But note that the divisibility relation $a \mid b$ is reflexive, and transitive but not symmetric; in fact if $a \mid b$ and $b \mid a$ then $a = b$, so it is not an equivalence relation. The congruence relation modulo n partitions $\mathbb{Z}$ into n *equivalence classes*. In number theory, we call these classes *congruence classes*, or *residue classes*. More formally, we have:

Definition 1.6.4. If $x \equiv a \pmod{n}$, then a is called a *residue* of x modulo n. The *residue class* of a modulo n, denoted by $[a]_n$ (or just $[a]$ if no confusion will be caused), is the set of all those integers that are congruent to a modulo n. That is,

$$\begin{aligned}[a]_n &= \{x : x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n}\} \\ &= \{a + kn : k \in \mathbb{Z}\}. \end{aligned} \tag{1.222}$$

Note that writing $a \in [b]_n$ is the same as writing $a \equiv b \pmod{n}$.

Example 1.6.3. Let $n = 5$. Then there are five residue classes, modulo 5, namely the sets:

$$\begin{aligned}
[0]_5 &= \{\cdots, -15, -10, -5, 0, 5, 10, 15, 20, \cdots\}, \\
[1]_5 &= \{\cdots, -14, -9, -4, 1, 6, 11, 16, 21, \cdots\}, \\
[2]_5 &= \{\cdots, -13, -8, -3, 2, 7, 12, 17, 22, \cdots\}, \\
[3]_5 &= \{\cdots, -12, -7, -2, 3, 8, 13, 18, 23, \cdots\}, \\
[4]_5 &= \{\cdots, -11, -6, -1, 4, 9, 14, 19, 24, \cdots\}.
\end{aligned}$$

The first set contains all those integers congruent to 0 modulo 5, the second set contains all those congruent to 1 modulo 5, $\cdots$, and the fifth (i.e., the last) set contains all those congruent to 4 modulo 5. So, for example, the residue class $[2]_5$ can be represented by any one of the elements in the set

$$\{\cdots, -13, -8, -3, 2, 7, 12, 17, 22, \cdots\}.$$

Clearly, there are infinitely many elements in the set $[2]_5$.

Example 1.6.4. In residue classes modulo 2, $[0]_2$ is the set of all even integers, and $[1]_2$ is the set of all odd integers:

$$\begin{aligned}
[0]_2 &= \{\cdots, -6, -4, -2, 0, 2, 4, 6, 8, \cdots\}, \\
[1]_2 &= \{\cdots, -5, -3, -1, 1, 3, 5, 7, 9, \cdots\}.
\end{aligned}$$

Example 1.6.5. In congruence modulo 5, we have

$$\begin{aligned}[9]_5 &= \{9 + 5k : k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \cdots\} \\ &= \{\cdots, -11, -6, -1, 4, 9, 14, 19, 24, \cdots\}.\end{aligned}$$

We also have

$$\begin{aligned}[4]_5 &= \{4 + 5k : k \in \mathbb{Z}\} = \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \cdots\} \\ &= \{\cdots, -11, -6, -1, 4, 9, 14, 19, 24, \cdots\}.\end{aligned}$$

So, clearly, $[4]_5 = [9]_5$.

Definition 1.6.5. If $x \equiv a \pmod{n}$ and $0 \leq a \leq n - 1$, then a is called the *least (nonnegative) residue* of x modulo n.

Example 1.6.6. Let $n = 7$. There are seven residue classes, modulo 7. In each of these seven residue classes, there is exactly one least residue of x modulo 7. So, the complete set of all least residues x modulo 7 is $\{0, 1, 2, 3, 4, 5, 6\}$.

1.6.2 Modular Arithmetic

The finite set $\mathbb{Z}/n\mathbb{Z}$ is closely related to the infinite set $\mathbb{Z}$. So, it is natural to ask if it is possible to define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ and do some reasonable kind of arithmetic there. Surprisingly, addition, subtraction and multiplication in $\mathbb{Z}/n\mathbb{Z}$ will be much the same as that in $\mathbb{Z}$. Let us first investigate some elementary arithmetic properties of congruences.

Theorem 1.6.5. For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. then

(1) $a \pm b \equiv c \pm d \pmod{n}$,
(2) $a \cdot b \equiv c \cdot d \pmod{n}$,
(3) $a^m \equiv b^m \pmod{n}$, $\forall m \in \mathbb{N}$.

Proof.

(1) Write $a = kn + b$ and $c = ln + d$ for some $k, l \in \mathbb{Z}$. Then $a + c = (k+l)n + b + d$. Therefore, $a + c = b + d + tn$, $t = k + l \in \mathbb{Z}$. Consequently, $a + c \equiv b + d \pmod{n}$, which is what we wished to show. The case of subtraction is left as an exercise.

(2) Similarly,
$$\begin{aligned} ac &= bd + bln + knd + kln^2 \\ &= bd + n(bl + k(d + ln)) \\ &= bd + n(bl + kc) \\ &= bd + sn \end{aligned}$$
where $s = bl + kc \in \mathbb{Z}$. Thus, $a \cdot b \equiv c \cdot d \pmod{n}$.

(3) We prove Part (3) by induction. We have $a \equiv b \pmod{n}$ (base step) and $a^m \equiv b^m \pmod{n}$ (inductive hypothesis). Then by Part (2) we have $a^{m+1} \equiv aa^m \equiv bb^m \equiv b^{m+1} \pmod{n}$. □

Theorem 1.6.5 is equivalent to the following theorem, since

$$\begin{aligned} a \equiv b \pmod{n} &\iff a \bmod n = b \bmod n, \\ a \bmod n &\iff [a]_n, \\ b \bmod n &\iff [b]_n. \end{aligned}$$

Theorem 1.6.6. For all $a, b, c, d \in \mathbb{Z}$, if $[a]_n = [b]_n$, $[c]_n = [d]_n$, then

(1) $[a \pm b]_n = [c \pm d]_n$,
(2) $[a \cdot b]_n = [c \cdot d]_n$,
(3) $[a^m]_n = [b^m]_n$, $\forall m \in \mathbb{N}$.

The fact that the congruence relation modulo n is stable for addition (subtraction) and multiplication means that we can define binary operations, again called addition (subtraction) and multiplication on the set of $\mathbb{Z}/n\mathbb{Z}$ of equivalence classes modulo n as follows (in case only one n is being discussed, we can simply write $[x]$ for the class $[x]_n$):

$$[a]_n + [b]_n = [a+b]_n \tag{1.225}$$
$$[a]_n - [b]_n = [a-b]_n \tag{1.226}$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n \tag{1.227}$$

Example 1.6.11. Let $n = 12$, then

$$[7]_{12} +_{12} [8]_{12} = [7+8]_{12} = [15]_{12} = [3]_{12},$$
$$[7]_{12} -_{12} [8]_{12} = [7-8]_{12} = [-1]_{12} = [11]_{12},$$
$$[7]_{12} \cdot_{12} [8]_{12} = [7 \cdot 8]_{12} = [56]_{12} = [8]_{12}.$$

In many cases, we may still prefer to write the above operations as follows:

$$7+8 = 15 \equiv 3 \pmod{12},$$
$$7-8 = -1 \equiv 11 \pmod{12},$$
$$7 \cdot 8 = 56 \equiv 8 \pmod{12}$$

We summarise the properties of addition and multiplication modulo n in the following two theorems.

Theorem 1.6.7. The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to addition:

(1) Closure: $[x] + [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
(2) Associative: $([x] + [y]) + [z] = [x] + ([y] + [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
(3) Commutative: $[x] + [y] = [y] + [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
(4) Identity, namely, $[0]$.
(5) Additive inverse: $-[x] = [-x]$, for all $[x] \in \mathbb{Z}/n\mathbb{Z}$.

Proof. These properties follow directly from the stability and the definition of the operation in $\mathbb{Z}/n\mathbb{Z}$. □

Theorem 1.6.8. The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to multiplication:

(1) Closure: $[x] \cdot [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
(2) Associative: $([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
(3) Commutative: $[x] \cdot [y] = [y] \cdot [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
(4) Identity, namely, $[1]$.
(5) Distributivity of multiplication over addition: $[x] \cdot ([y]) + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.

Proof. These properties follow directly from the stability of the operation in $\mathbb{Z}/n\mathbb{Z}$ and and the corresponding properties of $\mathbb{Z}$. □

The division a/b (we assume a/b is in lowest terms and $b \not\equiv 0 \pmod{n}$) in $\mathbb{Z}/n\mathbb{Z}$, however, will be more of a problem; sometimes you can divide, sometimes you cannot. For example, let $n = 12$ again, then

$$3/7 \equiv 9 \pmod{12} \qquad \text{(no problem)},$$
$$3/4 \equiv \perp \pmod{12} \qquad \text{(impossible)}.$$

Why is division sometimes possible (e.g., $3/7 \equiv 9 \pmod{12}$) and sometimes impossible (e.g., $3/4 \equiv \perp \pmod{12}$)? The problem is with the modulus n; if n is a prime number, then the division $a/b \pmod{n}$ is always possible and unique, whilst if n is a composite then the division $a/b \pmod{n}$ may be not possible or the result may be not unique. Let us observe two more examples, one with $n = 13$ and the other with $n = 14$. First note that $a/b \equiv a \cdot 1/b \pmod{n}$ if and only if $1/b \pmod{n}$ is possible, since multiplication modulo n is always possible. We call $1/b \pmod{n}$ the *multiplicative inverse* (or *modular inverse*) of b modulo n. More generally, we have:

Definition 1.6.10. Two integers x and y are said to be multiplicative inverses if

$$xy \equiv 1 \pmod{n}, \tag{1.228}$$

where n is a positive integer greater than 1.

It is now clear that given (x, n), y does not always exist. Let $n = 13$ be a prime, then the following table gives all the possible values of the multiplicative inverses $y = 1/x \pmod{13}$ for $x = 1, 2, \cdots, 12$:

x	1	2	3	4	5	6	7	8	9	10	11	12
y	1	7	9	10	8	11	2	5	3	4	6	12

This means that divisions in $\mathbb{Z}/13\mathbb{Z}$ are always possible and unique (i.e., the multiplicative inverses y of x in $\mathbb{Z}/13\mathbb{Z}$ do always exist and are unique). On the other hand, if $n = 14$ (n now is a composite), then for $x = 1, 2, \cdots, 13$, some values for $y = 1/x \pmod{14}$ exist, whereas others do not:

x	1	2	3	4	5	6	7	8	9	10	11	12	13
y	1	$\perp$	5	$\perp$	3	$\perp$	$\perp$	$\perp$	11	$\perp$	9	$\perp$	13

This means that only the numbers $1, 3, 5, 9, 11$ and 13 have multiplicative inverses modulo 14, or equivalently only those divisions by $1, 3, 5, 9, 11$ and 13 modulo 14 are possible. This observation leads to the following important results:

Theorem 1.6.9. The multiplicative inverse $1/b$ modulo n exists if and only if $\gcd(b, n) = 1$.

But how many b's are there that satisfy $\gcd(b, n) = 1$? The following result answers this question.

Corollary 1.6.2. There are $\phi(n)$ numbers b for which $1/b \pmod{n}$ exists.

Example 1.6.12. Let $n = 21$. Since $\phi(21) = 12$, there are twelve b for which $1/b \pmod{21}$ exists. In fact, the multiplicative inverse modulo 21 only exists for each of the following b:

b	1	2	4	5	8	10	11	13	16	17	19	20
$1/b \pmod{21}$	1	11	16	17	8	19	2	13	4	5	10	20

Corollary 1.6.3. The division a/b modulo n (assume that a/b is in lowest terms) is possible if and only if $1/b \pmod{n}$ exists, i.e., if and only if $\gcd(b, n) = 1$.

Example 1.6.13. Compute $6/b \pmod{21}$ whenever it is possible. By the multiplicative inverses of $1/b \pmod{21}$ in the previous table, we just need to calculate $6 \cdot 1/b \pmod{21}$:

b	1	2	4	5	8	10	11	13	16	17	19	20
$6/b \pmod{21}$	6	3	12	18	6	9	12	15	3	9	18	15

As it can be seen, addition (subtraction) and multiplication are always possible in $\mathbb{Z}/n\mathbb{Z}$, with $n > 1$, since $\mathbb{Z}/n\mathbb{Z}$ is a ring. Note also that $\mathbb{Z}/n\mathbb{Z}$ with n prime is an Abelian group with respect to addition, and all the non-zero elements in $\mathbb{Z}/n\mathbb{Z}$ form an Abelian group with respect to multiplication (i.e., a division is always possible for any two non-zero elements in $\mathbb{Z}/n\mathbb{Z}$ if n is prime); hence $\mathbb{Z}/n\mathbb{Z}$ with n prime is a field. That is,

Theorem 1.6.10. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

The above results only tell us when the multiplicative inverse $1/a$ modulo n is possible, without mentioning how to find the inverse. To actually find the multiplicative inverse, we let

$$1/a \pmod{n} = x, \tag{1.229}$$

which is equivalent to

$$ax \equiv 1 \pmod{n}. \tag{1.230}$$

Since

$$ax \equiv 1 \pmod{n} \iff ax - ny = 1. \tag{1.231}$$

So the finding of the multiplicative inverse becomes to find the solution of the linear Diophantine equation $ax - ny = 1$, which, as we know in Section 1.3, can be solved by using the continued fraction expansion of a/n, and can, of course, be solved by using Euclid's algorithm.

Example 1.6.14. Find

(1) $1/154 \pmod{801}$,

(2) $4/154 \pmod{801}$.

Solution:

(1) Since

$$1/a \pmod{n} = x \Longleftrightarrow ax \equiv 1 \pmod{n} \Longleftrightarrow ax - ny = 1, \quad (1.232)$$

we only need to find x and y in

$$154x - 801y = 1.$$

To do so, we first use the Euclid's algorithm to find $\gcd(154, 801)$ as follows.

$$\begin{aligned} 801 &= 154 \cdot 5 + 31 \\ 154 &= 31 \cdot 4 + 30 \\ 31 &= 30 \cdot 1 + 1 \\ 30 &= 10 \cdot 3 + 0. \end{aligned}$$

Since $\gcd(154, 801) = 1$, by Theorem 1.6.9, the equation $154x - 801y = 1$ is soluble. We now rewrite the above resulting equations

$$\begin{aligned} 31 &= 801 - 154 \cdot 5 \\ 30 &= 154 - 31 \cdot 4 \\ 1 &= 31 - 30 \cdot 1 \end{aligned}$$

and work backwards on the above new equations

$$\begin{aligned} 1 &= 31 - 30 \cdot 1 \\ &= 31 - (154 - 31 \cdot 4) \cdot 1 \\ &= 31 - 154 + 4 \cdot 31 \\ &= 5 \cdot 31 - 154 \\ &= 5 \cdot (801 - 154 \cdot 5) - 154 \\ &= 5 \cdot 801 - 26 \cdot 154 \\ &= 801 \cdot 5 - 154 \cdot 26 \end{aligned}$$

So, $x \equiv -26 \equiv 775 \pmod{801}$. That is, $1/154 \bmod 801 = 775$.

(2) Since $4/154 \equiv 4 \cdot 1/154 \pmod{801}$, then $4/154 \equiv 4 \cdot 775 \equiv 697 \pmod{801}$.

The above procedure used to find the x and y in $ax + by = 1$ can be generalized to find the x and y in $ax + by = c$; this procedure usually called the *extended Euclid's algorithm.* We shall discuss the solution of the general equation $ax + by = c$ in the next subsection.

$$
\begin{aligned}
777, \quad & 154 \cdot 777 \equiv 11 \pmod{803} \\
777 + 803/11 \equiv 47, \quad & 154 \cdot 47 \equiv 11 \pmod{803} \\
777 + 2 \cdot 803/11 \equiv 120, \quad & 154 \cdot 120 \equiv 11 \pmod{803} \\
777 + 3 \cdot 803/11 \equiv 193, \quad & 154 \cdot 193 \equiv 11 \pmod{803} \\
777 + 4 \cdot 803/11 \equiv 266, \quad & 154 \cdot 266 \equiv 11 \pmod{803} \\
777 + 5 \cdot 803/11 \equiv 339, \quad & 154 \cdot 339 \equiv 11 \pmod{803} \\
777 + 6 \cdot 803/11 \equiv 412, \quad & 154 \cdot 412 \equiv 11 \pmod{803} \\
777 + 7 \cdot 803/11 \equiv 485, \quad & 154 \cdot 485 \equiv 11 \pmod{803} \\
777 + 8 \cdot 803/11 \equiv 558, \quad & 154 \cdot 558 \equiv 11 \pmod{803} \\
777 + 9 \cdot 803/11 \equiv 631, \quad & 154 \cdot 631 \equiv 11 \pmod{803} \\
777 + 10 \cdot 803/11 \equiv 704, \quad & 154 \cdot 704 \equiv 11 \pmod{803}.
\end{aligned}
$$

Remark 1.6.4. To find the solution for the linear Diophantine equation

$$ax \equiv b \pmod{n} \tag{1.238}$$

is equivalent to find the quotient of the modular division

$$x \equiv \frac{b}{a} \pmod{n} \tag{1.239}$$

which is, again, equivalent to find the multiplicative inverse

$$x \equiv \frac{1}{a} \pmod{n} \tag{1.240}$$

because, if $\frac{1}{a}$ modulo n exists, the multiplication $b \cdot \frac{1}{a}$ is always possible.

In what follows, we shall introduce some important results on linear congruences. Our first result will be Fermat's little theorem (or just Fermat's theorem, for short), due to Fermat.

Theorem 1.6.15 (Fermat's little theorem). Let a be a positive integer, and p prime. If $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.241}$$

Proof. First notice that the residues modulo p of a, $2a$, $\cdots$, $(p-1)a$ are $1, 2, \cdots, (p-1)$ in some order, because no two of them can be equal. So, if we multiply them together, we get

$$
\begin{aligned}
a \cdot 2a \cdots (p-1)a &\equiv [(a \bmod p) \cdot (2a \bmod p) \cdots (p-1)a \bmod p)] \pmod{p} \\
&\equiv (p-1)! \pmod{p}.
\end{aligned}
$$

This means that

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Now we can cancel the $(p-1)!$ since $p \nmid (p-1)!$, and the result thus follows. □

There is a more convenient and more general form of Fermat's little theorem:

$$a^p \equiv a \pmod{p}, \tag{1.242}$$

for $a \in \mathbb{N}$. The proof is easy: if $\gcd(a,p) = 1$, we simply multiply (1.241) by a. If not, then $p \mid a$. So $a^p \equiv 0 \equiv a \pmod{p}$.

Fermat's theorem has several important consequences which are very useful in compositeness; one of the these consequences is as follows:

Corollary 1.6.4 (Converse of Fermat's little theorem, 1640). Let n be an odd positive integer. If $\gcd(a,n) = 1$ and

$$a^{n-1} \not\equiv 1 \pmod{n}, \tag{1.243}$$

then n is composite.

Remark 1.6.5. As mentioned in Subsection 1.2.3, Fermat, in 1640, made a false conjecture that all the numbers of the form $F_n = 2^{2^n} + 1$ were prime. Fermat really should not have made such a "stupid" conjecture, since $F_5 = 2^{32} + 1$ can be relatively easily verified to be composite, by just using his own recently discovered theorem – Fermat's little theorem:

$$\begin{aligned}
3^{2^2} &\equiv 81 && \pmod{2^{32}+1} \\
3^{2^3} &\equiv 6561 && \pmod{2^{32}+1} \\
3^{2^4} &\equiv 43046721 && \pmod{2^{32}+1} \\
3^{2^5} &\equiv 3793201458 && \pmod{2^{32}+1} \\
&\cdots\cdots \\
&\cdots\cdots \\
3^{2^{32}} &\equiv 3029026160 && \pmod{2^{32}+1} \\
&\not\equiv 1 && \pmod{2^{32}+1}.
\end{aligned}$$

Thus, by Fermat's little theorem, $F_5 = 2^{32} + 1$ is not prime!

Based on Fermat's little theorem, Euler established a more general result in 1760:

Theorem 1.6.16 (Euler's theorem). Let a and n be positive integers with $\gcd(a,n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{1.244}$$

Proof. Let $r_1, r_2, \cdots, r_{\phi(n)}$ be a reduced residue system modulo n. Then $ar_1, ar_2, \cdots, ar_{\phi(n)}$ is also a residue system modulo n. Thus we have

$$(ar_1)(ar_2)\cdots(ar_{\phi(n)}) \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n},$$

since $ar_1, ar_2, \cdots, ar_{\phi(n)}$, being a reduced residue system, must be congruent in some order to $r_1, r_2, \cdots, r_{\phi(n)}$. Hence,

$$a^{\phi(n)} r_1 a r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n},$$

which implies that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

It can be difficult to find the order[31] of an element a modulo n but sometimes it is possible to improve (1.244) by proving that every integer a modulo n must have an order smaller than the number $\phi(n)$ – this order is actually the number $\lambda(n)$.

Theorem 1.6.17 (Carmichael's theorem). Let a and n be positive integers with $\gcd(a, n) = 1$. Then

$$a^{\lambda(n)} \equiv 1 \pmod{n}, \tag{1.245}$$

where $\lambda(n)$ is Carmichael's function.

Proof. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. We shall show that

$$a^{\lambda(n)} \equiv 1 \pmod{p_i^{\alpha_i}}$$

for $1 \leq i \leq k$, since this implies that $a^{\lambda(n)} \equiv 1 \pmod{n}$. If $p_k^{\alpha_k} = 2, 4$ or a power of an odd prime, then by Definition 1.4.7, $\lambda(\alpha_k) = \phi(\alpha_k)$, so $a^{\lambda(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Since $\lambda(p_i^{\alpha_i}) \mid \lambda(n)$, $a^{\lambda(n)} \equiv 1 \pmod{p_i^{\alpha_i}}$. The case that $p_i^{\alpha_i}$ is a power of 2 greater than 4 is left as an exercise. □

Note that $\lambda(n)$ will never exceed $\phi(n)$ and is often much smaller than $\phi(n)$; it is the value of the largest order it is possible to have.

Example 1.6.16. Let $a = 11$ and $n = 24$. Then $\phi(24) = 8$, $\lambda(24) = 2$. So,

$$11^{\phi(24)} = 11^8 \equiv 1 \pmod{24},$$

$$11^{\lambda(24)} = 11^2 \equiv 1 \pmod{24}.$$

That is, $\mathrm{ord}_{24}(11) = 2$.

[31] The order of an element a modulo n is the smallest integer r such that $a^r \equiv 1 \pmod{n}$; we shall discuss this later in Subsection 1.6.7.