Number Theory

3

Key Topics

Square, rectangular and triangular Numbers
Prime numbers
Pythagorean triples
Mersenne primes
Division algorithm
Perfect and amicable numbers
Greatest common divisor
Least common multiples
Euclid's algorithm
Modular arithmetic
Binary numbers
Computer representation of numbers

3.1 Introduction

Number theory is the branch of mathematics that is concerned with the mathematical properties of the natural numbers and integers. These include properties such as the parity of a number; divisibility; additive, and multiplicative properties; whether a number is prime or composite; the prime factors of a number; the greatest common divisor and least common multiple of two numbers; and so on.

G. O'Regan, *Guide to Discrete Mathematics*, Texts in Computer Science,
DOI 10.1007/978-3-319-44561-8_3

Fig. 3.1 Pierre de Fermat

Number theory has many applications in computing including cryptography and coding theory. For example, the RSA public key cryptographic system relies on its security due to the infeasibility of the integer factorization problem for large numbers.

There are several unsolved problems in number theory and especially in prime number theory. For example, Goldbach's[1] Conjecture states that every even integer greater than two is the sum of two primes, and this result has not been proved to date. Fermat's[2] last Theorem (Fig. 3.1) states that there is no integer solution to $x^n + y^n = z^n$ for $n > 2$, and this result remained unproved for over three hundred years until Andrew Wiles finally proved it in the mid-1990s.

The natural numbers $\mathbb{N}$ consist of the numbers $\{1, 2, 3, \ldots\}$. The integer numbers $\mathbb{Z}$ consist of $\{\ldots -2, -1, 0, 1, 2, \ldots\}$. The rational numbers $\mathbb{Q}$ consist of all numbers of the form $\{p/q$ where p and q are integers and $q \neq 0\}$. The real numbers $\mathbb{R}$ is defined to be the set of converging sequences of rational numbers and they are a superset of the rational numbers. They contain the rational and irrational numbers. The complex numbers $\mathbb{C}$ consist of all numbers of the form $\{a + bi$ where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}\}$.

Pythagorean triples (Fig. 3.2) are combinations of three whole numbers that satisfy Pythagoras's equation $x^2 + y^2 = z^2$. There are an infinite number of such triples, and an example of such a triple is 3, 4, 5 since $3^2 + 4^2 = 5^2$.

[1]Goldbach was an eighteenth century German mathematician and Goldbach's conjecture has been verified to be true for all integers $n < 12 \times 10^{17}$.

[2]Pierre de Fermat was a 17th French civil servant and amateur mathematician. He occasionally wrote to contemporary mathematicians announcing his latest theorem without providing the accompanying proof and inviting them to find the proof. The fact that he never revealed his proofs caused a lot of frustration among his contemporaries, and in his announcement of his famous last theorem he stated that he had a wonderful proof that was too large to include in the margin. He corresponded with Pascal and they did some early work on the mathematical rules of games of chance and early probability theory. He also did some early work on the Calculus.

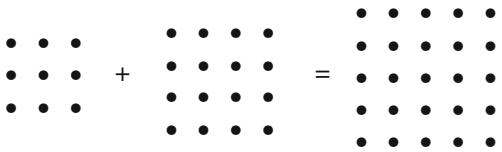

Fig. 3.2 Pythagorean triples

The Pythagoreans discovered the mathematical relationship between the harmony of music and numbers, and their philosophy was that numbers are hidden in everything from music to science and nature. This led to their philosophy that 'everything is number'.

3.2 Elementary Number Theory

A square number (Fig. 3.3) is an integer that is the square of another integer. For example, the number 4 is a square number since $4 = 2^2$. Similarly, the number 9 and the number 16 are square numbers. A number n is a square number if and only if one can arrange the n points in a square. For example, the square numbers 4, 9, 16 are represented in squares as follows:

The square of an odd number is odd, whereas the square of an even number is even. This is clear since an even number is of the form $n = 2k$ for some k, and so $n^2 = 4k^2$ which is even. Similarly, an odd number is of the form $n = 2k + 1$ and so $n^2 = 4k^2 + 4k + 1$ which is odd.

A rectangular number (Fig. 3.4) n may be represented by a vertical and horizontal rectangle of n points. For example, the number 6 may be represented by a rectangle with length 3 and breadth 2, or a rectangle with length 2 and breadth 3. Similarly, the number 12 can be represented by a 4×3 or a 3×4 rectangle.

A triangular number (Fig. 3.5) n may be represented by an equilateral triangle of n points. It is the sum of k natural numbers from 1 to k. = That is,

$$n = 1 + 2 + \cdots + k$$

Fig. 3.3 Square numbers

Fig. 3.4 Rectangular numbers

Fig. 3.5 Triangular numbers

Parity of Integers

The parity of an integer refers to whether the integer is odd or even. An integer n is odd if there is a remainder of one when it is divided by two, and it is of the form $n = 2k + 1$. Otherwise, the number is even and of the form $n = 2k$.

The sum of two numbers is even if both are even or both are odd. The product of two numbers is even if at least one of the numbers is even. These properties are expressed as

$$\begin{aligned}
&\text{even} \pm \text{even} = \text{even}\\
&\text{even} \pm \text{odd} = \text{odd}\\
&\text{odd} \pm \text{odd} = \text{even}\\
&\text{even} \times \text{even} = \text{even}\\
&\text{even} \times \text{odd} = \text{even}\\
&\text{odd} \times \text{odd} = \text{odd}
\end{aligned}$$

Divisors

Let a and b be integers with $a \neq 0$ then a is said to be a divisor of b (denoted by $a|b$) if there exists an integer k such that $b = ka$.

A divisor of n is called a *trivial divisor* if it is either 1 or n itself; otherwise it is called a *nontrivial divisor*. A *proper divisor* of n is a divisor of n other than n itself.

Definition (Prime Number)

A *prime number* is a number whose only divisors are trivial. There are an infinite number of prime numbers.

The *fundamental theorem of arithmetic* states that every integer number can be factored as the product of prime numbers.

Mesenne Primes

Mersenne primes are prime numbers of the form $2^p - 1$, where p is a prime. They are named after Marin Mersenne (Fig. 3.6) who was a 17th French monk, philosopher and mathematician. Mersenne did some early work in identifying primes of this format, and there are 47 known Mersenne primes. It remains an open question as to whether there are an infinite number of Mersenne primes.

Properties of Divisors

(i) $a|b$ and $a|c$ then a$|b + c$
(ii) $a|b$ then $a|bc$
(iii) $a|b$ and $b|$c then $a|c$

Proof (of i) Suppose $a|b$ and $a|$c then $b = k_1a$ and $c = k_2a$.
Then, $b + c = k_1a + k_2a = (k_1 + k_2)a$ and so $a|b + c$.

Proof (of iii) Suppose $a|b$ and $b|$c then $b = k_1a$ and $c = k_2b$.
Then, $c = k_2b = (k_2\ k_1)\ a$ and thus $a|c$.

Perfect and Amicable Numbers

Perfect and amicable numbers have been studied for millennia. A positive integer m is said to be *perfect* if it is the sum of its proper divisors. Two positive integers m and n are said to be an *amicable pair* if m is equal to the sum of the proper divisors of n and vice versa.

A *perfect number* is a number whose divisors add up to the number itself. For example, the number 6 is perfect since it has divisors 1, 2, 3 and $1 + 2 + 3 = 6$.

Perfect numbers are quite rare and Euclid showed that $2^{p-1}\ (2^p - 1)$ is an even perfect number whenever $(2^p - 1)$ is prime. Euler later showed that all even perfect numbers are of this form. It is an open question as to whether there are any odd perfect numbers, and if such an odd perfect number N was to exist then $N > 10^{1500}$.

A prime number of the form $(2^p - 1)$, where p is prime called as *Mersenne prime*. Mersenne primes are quite rare and each Mersenne prime generates an even perfect number and vice versa. That is, there is a one to one correspondence between the number of Mersenne primes and the number of even perfect numbers.

Fig. 3.6 Marin Mersenne

It remains an open question as to whether there are an infinite number of Mersenne primes and perfect numbers.

An *amicable pair* of numbers is a pair of numbers such that each number is the sum of divisors of the other number. For example, the numbers 220 and 284 are an amicable pair since the divisors of 220 are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, which have sum 284, and the divisors of 284 are 1, 2, 4, 71, 142, which have sum 220.

Theorem 3.1 (Division Algorithm) *For any integer a and any positive integer b there exist unique integers q and r such that*

$$a = bq + r \quad 0 \leq r < b$$

Proof The first part of the proof is to show the existence of integers q and r such that the equality holds, and the second part of the proof is to prove uniqueness of q and r.

Consider … $-3b$, $-2b$, $-b$, 0, b, $2b$, $3b$, … then there must be an integer q such that

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

Then $a - qb = r$ with $0 \leq r < b$ and so $a = bq + r$ and the existence of q and r is proved.

The second part of the proof is to show the uniqueness of q and r. Suppose q_1 and r_1 also satisfy $a = bq_1 + r_1$ with $0 \leq r_1 < b$ and suppose $r < r_1$. Then $bq + r = bq_1 + r_1$ and so $b(q - q_1) = r_1 - r$ and clearly $0 < (r_1 - r) < b$. Therefore, $b|(r_1 - r)$ which is impossible unless $r_1 - r = 0$. Hence, $r = r_1$ and $q = q_1$.

Theorem 3.2 (Irrationality of Square Root of Two) *The square root of two is an irrational number (i.e., it cannot be expressed as the quotient of two integer numbers).*

Proof The Pythagoreans[3] discovered this result and it led to a crisis in their community as number was considered to be the essence of everything in their

[3]Pythagoras of Samos (a Greek island in the Aegean sea) was an influential ancient mathematician and philosopher of the sixth century B.C. He gained his mathematical knowledge from his travels throughout the ancient world (especially in Egypt and Babylon). He became convinced that everything is number and he and his followers discovered the relationship between mathematics and the physical world as well as relationships between numbers and music. On his return to Samos he founded a school and he later moved to Croton in southern Italy to set up a school. This school and the Pythagorean brotherhood became a secret society with religious beliefs such as reincarnation and they were focused on the study of mathematics. They maintained secrecy of the mathematical results that they discovered. Pythagoras is remembered today for Pythagoras's Theorem, which states that for a right-angled triangle that the square of the hypotenuse is equal to the sum of the square of the other two sides. The Pythagorean's discovered the irrationality of the square root of two and as this result conflicted in a fundamental way with their philosophy that number is everything, and they suppressed the truth of this mathematical result.

world. The proof is indirect: i.e., the opposite of the desired result is assumed to be correct and it is showed that this assumption leads to a contradiction. Therefore, the assumption must be incorrect and so the result is proved.

Suppose $\sqrt{2}$ is rational then it can be put in the form p/q, where p and q are integers and $q \neq 0$. Therefore, we can choose p, q to be co-prime (i.e., without any common factors) and so

$$\begin{aligned}
&(p/q)^2 = 2 \\
\Rightarrow\ & p^2/q^2 = 2 \\
\Rightarrow\ & p^2 = 2q^2 \\
\Rightarrow\ & 2|p^2 \\
\Rightarrow\ & 2|p \\
\Rightarrow\ & p = 2k \\
\Rightarrow\ & p^2 = 4k^2 \\
\Rightarrow\ & 4k^2 = 2q^2 \\
\Rightarrow\ & 2k^2 = q^2 \\
\Rightarrow\ & 2|q^2 \\
\Rightarrow\ & 2|q
\end{aligned}$$

This is a contradiction as we have chosen p and q to be co-prime, and our assumption that there is a rational number that is the square root of two results in a contradiction. Therefore, this assumption must be false and we conclude that there is no rational number whose square is two.

3.3 Prime Number Theory

A positive integer $n > 1$ is called prime if its only divisors are n and 1. A number that is not a prime is called composite.

Properties of Prime Numbers

(i) There are an infinite number if primes.
(ii) There is a prime number p between n and $n! + 1$ such that $n < p \leq n! + 1$
(iii) If n is composite then n has a prime divisor p such that $p \leq \sqrt{n}$
(iv) There are arbitrary large gaps in the series of primes (given any $k > 0$ there exist k consecutive composite integers).

Proof (i) Suppose there are a finite number of primes and they are listed as p_1, p_2, p_3, …, p_k. Then consider the number N obtained by multiplying all known primes and adding one. That is,

$$N = p_1 p_2 p_3 \ldots p_k + 1.$$

Clearly, N is not divisible by any of p_1, p_2, p_3, …, p_k since they all leave a remainder of 1. Therefore, N is either a new prime or divisible by a prime q (that is not in the list of p_1, p_2, p_3, …, p_k.).

This is a contradiction since this was the list of all the prime numbers, and so the assumption that there are a finite number of primes is false, and we deduce that there are an infinite number of primes.

Proof (ii) Consider the integer $N = n! + 1$. If N is prime then we take $p = N$. Otherwise, N is composite and has a prime factor p. We will show that $p > n$.

Suppose, $p \leq n$ then $p|n!$ and since $p|N$ we have $p|n!$ +1 and therefore $p|1$, which is impossible. Therefore, $p > n$ and the result is proved.

Proof (iii) Let p be the smallest prime divisor of n. Since n is composite $n = uv$ and clearly $p \leq u$ and $p \leq v$. Then $p^2 \leq uv = n$ and so $p \leq \sqrt{n}$.

Proof (iv) Consider the k consecutive integers $(k + 1)! + 2$, $(k + 1)! + 3$, …, $(k + 1)! + k$, $(k + 1)! + k + 1$. Then each of these is composite since $j|(k + 1)! + j$ where $2 \leq j \leq k + 1$.

Algorithm for Determining Primes

The *Sieve of Eratosthenes algorithm* (Fig. 3.7) is a famous algorithm for determining the prime numbers up to a given number n. It was developed by the Hellenistic mathematician, Eratosthenes.

The algorithm involves first listing all of the numbers from 2 to n. The first step is to remove all multiples of two up to n; the second step is to remove all multiples of three up to n; and so on.

The kth step involves removing multiples of the kth prime p_k up to n and the steps in the algorithm continue while $p \leq \sqrt{n}$. The numbers remaining in the list are the prime numbers from 2 to n.

1. List the integers from 2 to n.
2. For each prime p_k up to $\sqrt{n}$ remove all multiples of p_k.
3. The numbers remaining are the prime numbers between 2 and n.

	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

Fig. 3.7 Primes between 1 and 50

The list of primes between 1 and 50 are given in Fig. 3.7. They are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47.

Theorem 3.3 (Fundamental Theorem of Arithmetic) *Every natural number* n > *1 may be written uniquely as the product of primes*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}$$

Proof There are two parts to the proof. The first part shows that there is a factorization and the second part shows that the factorization is unique.

Part(a)

If n is prime then it is a product with a single prime factor. Otherwise, n can be factored into the product of two numbers ab, where $a > 1$ and $b > 1$. The argument can then be applied to each of a and b each of which is either prime or can be factored as the product of two numbers both of which are greater than one. Continue in this way with the numbers involved decreasing with every step in the process until eventually all of the numbers must be prime. (This argument can be made more rigorous using strong induction).

Part(b)

Suppose the factorization is not unique and let $n > 1$ be the smallest number that has more than one factorization of primes. Then n may be expressed as follows:

$$n = p_1 p_2 p_3 \ldots p_k = q_1 q_2 q_3 \ldots q_r$$

Clearly, $k > 1$ and $r > 1$ and $p_i \neq q_j$ for ($i = 1,\ldots k$) and ($j = 1,\ldots, r$) as otherwise we could construct a number smaller than n (e.g., n/p_i where $p_i = q_j$) that has two distinct factorizations. Next, without loss of generality take $p_1 < q_1$ and define the number N by

$$\begin{aligned} N =& (q_1 - p_1) q_2 q_3 \ldots q_r \\ =& p_1 p_2 p_3 \ldots p_k - p_1 q_2 q_3 \ldots q_r \\ =& p_1 (p_2 p_3 \ldots p_k - q_2 q_3 \ldots q_r) \end{aligned}$$

Clearly $1 < N < n$ and so N is uniquely factorizable into primes. However, clearly p_1 is not a divisor of $(q_1 - p_1)$, and so N has two distinct factorizations, which is a contradiction of the choice of n.

3.3.1 Greatest Common Divisors (GCD)

Let a and b be integers not both zero. The *greatest common divisor* d of a and b is a divisor of a and b (i.e., $d|a$ and $d|b$), and it is the largest such divisor (i.e., if $k|a$ and $k|b$ then $k|d$). It is denoted by gcd (a, b).

Properties of greatest common divisors

(i) Let a and b be integers not both zero then exists integers x and y such that:

$$d = \gcd(a, b) = ax + by$$

(ii) Let a and b be integers not both zero then the set S = {ax + by where $x, y \in \mathbb{Z}$} is the set of all multiples of d = gcd (a, b).

Proof (of i) Consider the set of all linear combinations of a and b forming the set {ka + nb: k, $n \in \mathbb{Z}$}. Clearly, this set includes positive and negative numbers. Choose x and y such that $m = ax + by$ is the smallest positive integer in the set. Then we shall show that m is the greatest common divisor.

We know from the division algorithm that $a = mq + r$ where $0 \leq r < m$. Thus

$$r = a - mq = a - (ax + by)q = (1 - qx)a + (-yq)b$$

r is a linear combination of a and b and so r must be 0 from the definition of m. Therefore, $m|a$ and similarly $m|b$ and so m is a common divisor of a and b. Since, the greatest common divisor d is such that $d|a$ and $d|b$ and $d \leq m$ we must have $d = m$.

Proof (of ii) This follows since $d|a$ and $d|b$ => $d|ax + by$ for all integers x and y and so every element in the set S = {ax + by where $x, y \in \mathbb{Z}$} is a multiple of d.

Relatively Prime
Two integers a, b are relatively prime if gcd(a, b) = 1

Properties
If p is a prime and $p|ab$ then $p|a$ or $p|b$.

Proof Suppose $p \nmid a$ then from the results on the greatest common divisor we have gcd (a, p) = 1. That is,

$$\begin{aligned} & ra + sp = 1 \\ \Rightarrow\ & rab + spb = b \\ \Rightarrow\ & p \mid b (\text{since } p \mid rab \text{ and } p \mid spb \text{ and so } p \mid rab + spb) \end{aligned}$$

3.3.2 Least Common Multiple (LCM)

If m is a multiple of a and m is a multiple of b then it is said to be a *common multiple* of a and b. The least common multiple is the smallest of the common multiples of a and b and it is denoted by lcm (a, b).

Fig. 3.8 Euclid of Alexandria

Properties

If x is a common multiple of a and b then $m|x$. That is, every common multiple of a and b is a multiple of the least common multiple m.

Proof We assume that both a and b are nonzero as otherwise the result is trivial (since all common multiples are 0). Clearly, by the division algorithm we have

$$x = mq + r \qquad \text{where } 0 \leq r < m$$

Since x is a common multiple of a and b we have $a|x$ and $b|x$ and also that $a|m$ and $b|m$. Therefore, $a|r$ and $b|r$. and so r is a common multiple of a and b and since m is the least common multiple we have r is 0. Therefore, x is a multiple of the least common multiple m as required,

3.3.3 Euclid's Algorithm

Euclid's[4] algorithm is one of the oldest known algorithms and it provides a procedure for finding the greatest common divisor of two numbers. It appears in Book VII of Euclid's Elements, and the algorithm was known prior to Euclid (Fig. 3.8).

Lemma *Let a, b, q, and r be integers with $b > 0$ and $0 \leq r < b$ such that $a = bq + r$. Then $gcd(a, b) = gcd(b, r)$.*

Proof Let $K = \gcd(a, b)$ and let $L = \gcd(b, r)$ and we therefore need to show that $K = L$. Suppose m is a divisor of a and b then as $a = bq + r$ we have m which is a divisor of r and so any common divisor of a and b is a divisor of r.

Similarly, any common divisor n of b and r is a divisor of a. Therefore, the greatest common divisor of a and b is equal to the greatest common divisor of b and r.

[4]Euclid was a third century B.C. Hellenistic mathematician and is considered the father of geometry.

Theorem 3.4 (Euclid's Algorithm) *Euclid's algorithm for finding the greatest common divisor of two positive integers a and b involves applying the division algorithm repeatedly as follows:*

$$\begin{aligned}
&a = bq_0 + r_1 && 0 < r_1 < b\\
&b = r_1 q_1 + r_2 && 0 < r_2 < r_1\\
&r_1 = r_2 q_2 + r_3 && 0 < r_3 < r_2\\
&\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1}\\
&r_{n-1} = r_n q_n
\end{aligned}$$

Then r_n (i.e., the last nonzero remainder) is the greatest common divisor of a and b: i.e., gcd(a, b) = r_n.

Proof t is clear from the construction that r_n is a divisor of r_{n-1}, r_{n-2}, …, r_3, r_2, r_1 and of a and b. Clearly, any common divisor of a and b will also divide r_n. Using the results from the lemma above we have

$$\begin{aligned}
&\gcd(a, b)\\
&\quad = \gcd(b, r_1)\\
&\quad = \gcd(r_1\, r_2)\\
&\quad = \ldots\\
&\quad = \gcd(r_{n-2}\, r_{n-1})\\
&\quad = \gcd(r_{n-1},\, r_n)\\
&\quad = r_n
\end{aligned}$$

Lemma *Let n be a positive integer greater than one then the positive divisors of n are precisely those integers of the form:*

$$d = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \ldots p_k^{\beta_k} \qquad (\text{where } 0 \le \beta_i \le \alpha_i),$$

where the unique factorization of n is given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}$$

Proof Suppose d is a divisor of n then $n = dq$. By the unique factorization theorem the prime factorization of n is unique, and so the prime numbers in the factorization of d must appear in the prime factors p_1, p_2, p_3, …, p_k of n.

Clearly, the power β_i of p_i must be less than or equal to α_i: i.e., $\beta_i \le \alpha_i$. Conversely, whenever $\beta_i \le \alpha_i$ then clearly d divides n.

3.3.4 Distribution of Primes

We already have shown that there are an infinite number of primes. However, most integer numbers are composite and a reasonable question to ask is how many primes are there less than a certain number. The number of primes less than or equal to x is known as the prime distribution function (denoted by $\pi(x)$) and it is defined by

$$\pi(x) = \sum_{p \leq x} 1 \qquad (\text{where } p \text{ is prime})$$

The prime distribution function satisfies the following properties:

(i) $\lim_{x \to \infty} \frac{\pi(x)}{x} = 0$
(ii) $\lim_{x \to \infty} \pi(x) = \infty$

The first property expresses the fact that most integer numbers are composite, and the second property expresses the fact that there are an infinite number of prime numbers.

There is an approximation of the prime distribution function in terms of the logarithmic function $(x/\ln x)$ as follows:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1 \qquad (\text{Prime Number Theorem})$$

The approximation $x/\ln x$ to $\pi(x)$ gives an easy way to determine the approximate value of $\pi(x)$ for a given value of x. This result is known as the *Prime Number Theorem*, and Gauss originally conjectured this theorem.

Palindromic Primes

A palindromic prime is a prime number that is also a palindrome (i.e., it reads the same left to right as right to left). For example, 11, 101, 353 are all palindromic primes.

All palindromic primes (apart from 11) have an odd number of digits. It is an open question as to whether there are an infinite number of palindromic primes.

Let $\sigma(m)$ denote the sum of all the positive divisors of m (including m):

$$\sigma(m) = \Sigma_{d \mid m} d$$

Let $s(m)$ denote the sum of all the positive divisors of m (excluding m):

$$s(m) = \sigma(m) - m.$$

Clearly, $s(m) = m$ and $\sigma(m) = 2\ m$ when m is a perfect number.

Theorem 3.5 (Euclid–Euler Theorem) *The positive integer* n *is an even perfect number if and only if* $n = 2^{p-1}(2^p - 1)$, *where* $2^p - 1$ *is a Mersenne prime.*

Proof Suppose $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime then

$$\begin{aligned}
\sigma(n) &= \sigma\left(2^{p-1}(2^p-1)\right) \\
&= \sigma\left(2^{p-1}\right)\sigma(2^p-1) \\
&= \sigma\left(2^{p-1}\right)2^p \qquad (2^p-1 \text{ is prime with 2 divisors : 1 and itself}) \\
&= (2^p-1)\,2^p \qquad (\text{Sum of arithmetic series}) \\
&= (2^p-1)\,2.2^{p-1} \\
&= 2.2^{p-1}(2^p-1) \\
&= 2n
\end{aligned}$$

Therefore, n is a perfect number since $\sigma(n) = 2n$.

The next part of the proof is to show that any even perfect number must be of the form above. Let n be an arbitrary even perfect number ($n = 2^{p-1}q$) with q odd and so the gcd $(2^{p-1}, q) = 1$ and so

$$\begin{aligned}
&\sigma(n) \\
&\qquad = \sigma\left(2^{p-1}q\right) \\
&\qquad = \sigma\left(2^{p-1}\right)\sigma(q) \\
&\qquad = (2^p-1)\sigma(q) \\
&\sigma(n) \\
&\qquad = 2n \qquad (\text{since } n \text{ is perfect}) \\
&\qquad = 2.2^{p-1}q \\
&\qquad = 2^p q
\end{aligned}$$

Therefore,

$$\begin{aligned}
&2^p q \\
&\qquad = (2^p-1)\sigma(q) \\
&\qquad = (2^p-1)\,(s(q)+q) \\
&\qquad = (2^p-1)s(q) + (2^p-1)q \\
&\qquad = (2^p-1)s(q) + 2^p q - q
\end{aligned}$$

Therefore, $(2^p - 1)\, s(q) = q$

Therefore, $d = s(q)$ is a proper divisor of q. However, $s(q)$ is the sum of all the proper divisors of q including d, and so d is the only proper divisor of q and $d = 1$. Therefore, $q = (2^p - 1)$ is a Mersenne prime.

Fig. 3.9 Leonard Euler

Euler φ Function

The Euler[5] φ function (also known as the *totient function*) is defined for a given positive integer n to be the number of positive integers k less than n that are relatively prime to n (Fig. 3.9). Two integers a, b are relatively prime if gcd(a, b) = 1.

$$\varphi(n) = \sum_{1 \le k < n} 1 \qquad \text{where } \gcd(k, n) = 1$$

3.4 Theory of Congruences[6]

Let a be an integer and n a positive integer greater than 1 then (a mod n) is defined to be the remainder r when a is divided by n. That is,

$$a = kn + r \qquad \text{where } 0 \le r < n.$$

Definition Suppose a, b are integers and n a positive integer then a is said to be congruent to b modulo n denoted by $a \equiv b \pmod{n}$ if they both have the same remainder when divided by n.

This is equivalent to n being a divisor of $(a - b)$ or $n|(a - b)$ since we have $a = k_1 n + r$ and $b = k_2 n + r$ and so $(a - b) = (k_1 - k_2)\, n$ and so $n|(a - b)$.

[5]Euler was an eighteenth century Swiss mathematician who made important contributions to mathematics and physics. His contributions include graph theory (e.g., the well-known formula V − E + F = 2), calculus, infinite series, the exponential function for complex numbers, and the totient function.

[6]The theory of congruences was introduced by the German mathematician, Carl Friedrich Gauss.

Theorem 3.6 *Congruence modulo n is an equivalence relation on the set of integers: i.e., it is a reflexive, symmetric and transitive relation.*

Proof

(i) Reflexive
For any integer a it is clear that $a \equiv a \pmod{n}$ since $a - a = 0.n$

(ii) Symmetric
Suppose $a \equiv b \pmod{n}$ then $a - b = kn$. Clearly, $b - a = -kn$ and so $b \equiv a \pmod{n}$.

(iii) Transitive.

$$\begin{aligned}
&\text{Suppose } a \equiv b \,(\text{mod} n) \text{ and } b \equiv c (\text{mod} n) \\
&\Rightarrow a - b = k_1 n \text{ and } b - c = k_2 n \\
&\Rightarrow a - c = (a - b) + (b - c) \\
&\qquad\quad = k_1 n + k_2 n \\
&\qquad\quad = (k_1 + k_2) n \\
&\Rightarrow a \equiv c (\text{mod}\, n).
\end{aligned}$$

Therefore, congruence modulo n is an equivalence relation, and an equivalence relation partitions a set S into equivalence classes (Theorem 2.2). The integers are partitioned into n equivalence classes for the congruence modulo n equivalence relation, and these are called *congruence classes* or *residue classes*. The residue class of a modulo n is denoted by $[a]_n$ or just $[a]$ when n is clear. It is the set of all those integers that are congruent to a modulo n.

$$[a]_n = \{x : x \in \mathbb{Z} \text{ and } x \equiv a (\text{mod}\, n)\} = \{a + kn : k \in \mathbb{Z}\}$$

Any two equivalence classes $[a]$ and $[b]$ are either equal or disjoint: i.e., we have $[a] = [b]$ or $[a] \cap [b] = \varnothing$. The set of all residue classes modulo n is denoted by

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \left\{[a]_n : 0 \le a \le n - 1\right\} = \left\{[0]_n, [1]_n, \ldots, [n-1]_n\right\}$$

For example, consider $\mathbb{Z}_4$ the residue classes mod 4 then

$$\begin{aligned}
[0]_4 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
[1]_4 &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
[2]_4 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
[3]_4 &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

The *reduced residue class* is a set of integers r_i such that $(r_i, n) = 1$ and r_i is not congruent to $r_j \pmod{n}$ for $i \neq j$, and such that every x relatively prime to n is

congruent modulo n to for some element r_i of the set. There are $\varphi(n)$ elements $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ in the reduced residue class set S.

Modular Arithmetic
Addition, subtraction and multiplication may be defined in $\mathbb{Z}/n\mathbb{Z}$ and are similar to these operations in $\mathbb{Z}$. Given a positive integer n and integers a, b, c, d such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then the following are properties of modular arithmetic.

(i) $a + c \equiv b + d \pmod{n}$ and $a - c \equiv b - d \pmod{n}$
(ii) $ac \equiv bd \pmod{n}$
(iii) $a^m \equiv b^m \pmod{n}\ \forall m \in \mathbb{N}$

Proof (of ii) Let $a = kn + b$ and $c = ln + d$ for some $k, l \in \mathbb{Z}$ then

$$\begin{aligned} ac &= (kn+b)(ln+d) \\ &= (kn)(ln) + (kn)d + b(ln) + bd \\ &= (knl + kd + bl)n + bd \\ &= sn + bd, \qquad (\text{where } s = knl + kd + bl) \end{aligned}$$

and $ac \equiv bd \pmod{n}$
The three properties above may be expressed in the following equivalent formulation:

(i) $[a + c]_n = [b + d]_n$ and $[a - c]_n = [b - d]_n$
(ii) $[ac]_n = [bd]_n$
(iii) $[a^m]_n = [b^m]_n\ \forall m \in \mathbb{N}$

Two integers x, y are said to be multiplicative inverses of each other modulo n if

$$xy \equiv 1 \pmod{n}$$

However, x does not always have an inverse modulo n, and this is clear since, for example, $[3]_6$ is a zero divisor modulo 6, i.e., $[3]_6$. $[2]_6 = [0]_6$ and it does not have a multiplicative inverse. However, if n and x are relatively prime then it is easy to see that x has an inverse (mod n) since we know that there are integers k,l such that $kx + ln = 1$.

Given $n > 0$ there are $\varphi(n)$ numbers b that are relatively prime to n and there are $\varphi(n)$ numbers that have an inverse modulo n. Therefore, for p prime there are $p - 1$ elements that have an inverse (mod p).

Theorem 3.7 (Euler's Theorem) *Let* a *and* n *be positive integers with gcd(*a, n*) = 1. Then*

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

Proof Let $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ be the reduced residue system (mod n). Then $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ is also a reduced residue system (mod n) since $ar_i \equiv ar_j$ (mod n) and $(a, n) = 1$ implies that $r_i \equiv r_j$ (mod n).

For each r_i there is exactly one r_j such that $ar_i \equiv r_j (\mathrm{mod}\, n)$, and different r_i will have different corresponding ar_j Therefore, $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ are just the residues module n of $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ but not necessarily in the same order. Multiplying we get

$$\prod_{j=1}^{\varphi(n)} (ar_j) \equiv \prod_{i=1}^{\varphi(n)} r_i \qquad (\mathrm{mod}\, n)$$

$$a^{\phi(n)} \prod_{j=1}^{\varphi(n)} (r_j) \equiv \prod_{i=1}^{\varphi(n)} r_i \qquad (\mathrm{mod}\, n)$$

Since $(r_j, n) = 1$ we can deduce that $a^{\phi(n)} \equiv 1$ (mod n) from the result that $ax \equiv ay$ (mod n) and $(a, n) = 1$ then $x \equiv y$ (mod n).

Theorem 3.8 (Fermat's Little Theorem) *Let a be a positive integer and p a prime. If gcd* $(a, p) = 1$ *then*

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

Proof This result is an immediate corollary to Euler's Theorem as $\varphi(p) = p - 1$.

Theorem 3.9 (Wilson's Theorem) *If p is a prime then* $(p - 1)! \equiv -1$ (mod p).

Proof Each element $a \in 1, 2, \ldots, p - 1$ has an inverse a^{-1} such that $aa^{-1} \equiv 1$ (mod p). Exactly two of these elements 1 and $p - 1$ are their own inverse (i.e., $x^2 \equiv 1$ (mod p) has two solutions 1 and $p - 1$). Therefore, the product 1, 2, …, $p - 1$ (mod p) = $p - 1$ (mod p) $\equiv -1$ (mod p)

Diphantine equations

The word "*Diophantine*" is derived from the name of the third century mathematician, Diophantus, who lived in the city of Alexandria in Egypt. Diophantus studied various polynomial equations of the form $f(x,y,z,\ldots) = 0$ with integer coefficients to determine which of them had integer solutions.

A Diophantine equation may have no solution, a finite number of solutions or an infinite number of solutions. The integral solutions of a Diophantine equation $f(x, y) = 0$ may be interpreted geometrically as the points on the curve with integral coordinates.

Example A linear Diophantine equation $ax + by = c$ is an algebraic equation with two variables x and y, and the problem is to find integer solutions for x and y.

Table 3.1 Binary number system

Binary	Dec.	Binary	Dec.	Binary	Dec.	Binary	Dec.
0000	0	0100	4	1000	8	1100	12
0001	1	0101	5	1001	9	1101	13
0010	2	0110	6	1010	10	1110	14
0011	3	0111	7	1011	11	1111	15

3.5 Binary System and Computer Representation of Numbers

Arithmetic has traditionally been done using the decimal notation,[7] and this positional number system involves using the digits 0, 1, 2, …, 9. Leibniz[8] was one of the earliest people to recognize the potential of the binary number system, and this base 2 system uses just two digits namely "0" and "1". Leibniz described the binary system in *Explication de l'Arithmétique Binaire* [1], which was published in 1703. His 1703 paper describes how binary numbers may be added, subtracted, multiplied and divided, and Leibniz was an advocate of their use.

The number two is represented by 10; the number four by 100; and so on. A table of values for the first fifteen binary numbers is given in Table 3.1.

The binary number system (base 2) is a positional number system, which uses two binary digits 0 and 1, and an example binary number is 1001.01_2 which represents $1 \times 2^3 + 1 + 1 \times 2^{-2} = 8 + 1 + 0.25 = 9.25$.

The binary system is ideally suited to the digital world of computers, as a binary digit may be implemented by an *on off switch*. In the digital world devices that store information or data on permanent storage media such as disks, and CDs, or temporary storage media such as random access memory (RAM) consist of a large number of memory elements that may be in one of two states (i.e., on or off).

The digit 1 represents that the switch is on, and the digit 0 represents that the switch is off. Claude Shannon showed in his Master's thesis [2] that the binary digits (i.e., 0 and 1) can be represented by electrical switches. This allows binary arithmetic and more complex mathematical operations to be performed by relay circuits, and provided the foundation of digital computing.

[7]Other bases have been employed such as the segadecimal (or base-60) system employed by the Babylonians. The decimal system was developed by Indian and Arabic mathematicians between 800–900AD, and it was introduced to Europe in the late twelfth/early thirteenth century. It is known as the *Hindu–Arabic system*.

[8]Wilhelm Gottfried Leibniz was a German philosopher, mathematician and inventor in the field of mechanical calculators. He developed the binary number system used in digital computers, and invented the Calculus independently of Sir Issac Newton. He was embroiled in a bitter dispute towards the end of his life with Newton, as to who developed the calculus first.

The decimal system (base 10) is more familiar for everyday use, and there are algorithms to convert numbers from decimal to binary and vice versa. For example, to convert the decimal number 25 to its binary representation we proceed as follows:

2	25
12	1
6	0
3	0
1	1
0	1

The base 2 is written on the left and the number to be converted to binary is placed in the first column. At each stage in the conversion the number in the first column is divided by 2 to form the quotient and remainder, which are then placed on the next row. For the first step the quotient when 25 is divided by 2 is 12 and the remainder is 1. The process continues until the quotient is 0, and the binary representation result is then obtained by reading the second column from the bottom up. Thus, we see that the binary representation of 25 is 11001_2.

Similarly, there are algorithms to convert decimal fractions to binary representation (to a defined number of binary digits as the representation may not terminate), and the conversion of a number that contains an integer part and a fractional part involves converting each part separately and then combining them.

The octal (base 8) and hexadecimal (base 16) are often used in computing, as the bases 2, 8 and 16 are related bases and easy to convert between, as to convert between binary and octal involves grouping the bits into groups of three on either side of the point. Each set of 3-bits corresponds to one digit in the octal representation. Similarly, the conversion between binary and hexadecimal involves grouping into sets of 4 digits on either side of the point. The conversion the other way from octal to binary or hexadecimal to binary is equally simple, and involves replacing the octal (or hexadecimal) digit with the 3-bit (or 4-bit) binary representation.

Numbers are represented in a digital computer as sequences of bits of fixed length (e.g., 16-bits, 32-bits). There is a difference in the way in which integers and real numbers are represented, with the representation of real numbers being more complicated.

An integer number is represented by a sequence (usually 2 or 4) bytes where each byte is 8-bits. For example, a 2-byte integer has 16 bits with the first bit used as the sign bit (the sign is 1 for negative numbers and 0 for positive integers), and the remaining 15 bits represent the number. This means that two bytes may be used to represent all integer numbers between −32,768 and 32,767. A positive number is represented by the normal binary representation discussed earlier, whereas a negative number is represented using 2's complement of the original number (i.e., 0 changes to 1 and 1 changes to 0 and the sign bit is 1). All of the standard arithmetic operations may then be carried out (using modulo 2 arithmetic).

The representation of floating point real numbers is more complicated, and a real number is represented to a fixed number of significant digits (the significand) and scaled using an exponent in some base (usually 2). That is, the number is represented (approximated as):

$$\text{significand} \times \text{base}^{\text{exponent}}$$

The significand (also called mantissa) and exponent have a sign bit. For example, in simple floating point representation (4 bytes) the mantissa is generally 24-bits and the exponent 8-bits, whereas for double precision (8 bytes) the mantissa is generally 53 bits and the exponent 11 bits. There is an IEEE standard for floating point numbers (IEEE 754).

3.6 Review Questions

1. Show that
   (*i*) if $a|b$ then $a|bc$
   (*ii*) If $a|b$ and $c|d$ then $ac|bd$
2. Show that 1184 and 1210 are an amicable pair.
3. Use the Euclidean Algorithm to find $g = \gcd(b, c)$ where $b = 42{,}823$ and $c = 6409$, and find integers x and y such that $bx + cy = g$
4. List all integers x in the range $1 \leq x \leq 100$ such that $x \equiv 7 \pmod{17}$.
5. Evaluate $\phi(m)$ for $m = 1, 2, 3, \ldots. 12$.
6. Determine a complete and reduced residue system modulo 12.
7. Convert 767 to binary, octal and hexadecimal.
8. Convert (you may need to investigate) 0.32_{10} to binary (to 5 places).
9. Explain the difference between binary, octal and hexadecimal.
10. Find the 16-bit integer representation of −4961.

3.7 Summary

Number theory is concerned with the mathematical properties of the natural numbers and integers. These include properties such as, whether a number is prime or composite, the prime factors of a number, the greatest common divisor and least common multiple of two numbers and so on.

The natural numbers $\mathbb{N}$ consist of the numbers $\{1, 2, 3, \ldots\}$. The integer numbers $\mathbb{Z}$ consist of $\{\ldots -2, -1, 0, 1, 2, \ldots\}$. The rational numbers $\mathbb{Q}$ consist of all numbers of the form $\{p/q$ where p and q are integers and $q \neq 0\}$. Number theory has been applied to cryptography in the computing field.

Prime numbers have no factors apart from themselves and one, and there are an infinite number of primes. The Sieve of Eratosthene's algorithm may be employed to determine prime numbers, and the approximation to the distribution of prime numbers less than a number n is given by the prime distribution function $\pi(n) = n/\ln n$. Prime numbers are the key building blocks in number theory, and the fundamental theorem of arithmetic states that every number may be written uniquely as the product of factors of prime numbers.

Mersenne primes and perfect numbers were considered and it was shown that there is a one to one correspondence between the Mersenne primes and the even perfect numbers.

Modulo arithmetic including addition, subtraction and multiplication were defined, and the residue classes and reduced residue classes discussed. There are unsolved problems in number theory such as Goldbach's conjecture that states that every even integer is the sum of two primes. Other open questions include whether there are an infinite number of Mersenne primes and palindromic primes.

We discussed the binary number system, which is ideally suited for digital computers. We discussed the conversion between binary and decimal systems, as well as the octal and hexadecimal systems. Finally, we discussed the representation of integers and real numbers on a computer. For more detailed information on number theory see [3].

References

1. *Explication de l'Arithmétique Binaire* Wilhelm Gottfried Leibniz. *Memoires de l'Academie Royale des Sciences.* 1703.
2. A Symbolic Analysis of Relay and Switching Circuits. Claude Shannon. Masters Thesis. Massachusetts Institute of Technology. 1937.
3. Number Theory for Computing. Song Y. Yan 2nd Edition. Springer. 1998.