NUMBERS

BY PANKAJ KAMTHAN

1. INTRODUCTION

A good decision is based on knowledge and not on numbers.
— Plato

Operator! Give me the number for 911!
— Homer Simpson

A number is an abstract entity used to describe quantity [Wikipedia]. The study of the integers and their properties is known as **number theory**. This document provides an introduction to numbers, in general, and number theory, in particular.

2. SIGNIFICANCE OF NUMBERS IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING

If there were any uninteresting numbers, there would of necessity be a smallest uninteresting number and it, for that reason alone, would be very interesting.
— Constance Reid

The notion of a number has its origins in mathematics, has a history that spans millennia [Havil, 2012], and has been used for **identifying, counting, quantifying, comparing quantities, and measuring** [Driver, 1984; Posamentier, Thaller, 2015], but is also **essential** to many areas of computer science and software engineering [Gerstein, 2012, Chapter 4, Chapter 6; Lehman, Leighton, Meyer, 2012; Rosen, 2012, Chapter 4; Wallis, 2012, Chapter 1; Khare, Lachowska, 2015; Niederreiter, Winterhof, 2015; Barnes, 2016; Haigh, 2016, Section 4.5; Neto, 2018; Sundstrom, 2018, Chapter 8].

The **On-Line Encyclopedia of Integer Sequences (OEIS)**[1] provides extensive information on notable sequences.

2.1. USES OF NUMBERS

The numbers are **ubiquitous** in computer science and software engineering.

CALCULATIONS

For example, every non-trivial computer program requires/manipulates some data, and this data could be characters or **numbers** (and, in fact, **numerical programs** deal with numbers almost exclusively [Kneusel, 2015]).

COMPARISONS

The **negative numbers** represent **opposites** [Wikipedia]. If positive represents a movement to the right, negative represents a movement to the left. If positive represents above sea level, then negative represents below sea level. If positive represents a deposit, negative represents a withdrawal. In each of the above cases, there is an implicit **reference point**.

There is a need for reference points in variety of places in computer science and software engineering, including a **quantitative improvement in quality**.

CRYPTOGRAPHY

There are applications of **large prime numbers** towards **public key cryptography** [Crandall, Pomerance, 2005, Chapter 9; Wallis, 2012, Chapter 9; Kraft, Washington, 2014; Reba, Shier, 2015, Chapter 24; O'Regan, 2016, Chapter 10], which in turn is used in **computer security, network security, and document security**.

For example, the RSA public key cryptosystem, proposed in the late **1970s**, is based on based on primality testing and integer factorization.

[1] URL: http://oeis.org/ .

TIME-KEEPING

There are applications of **modular arithmetic** to modern **time-keeping systems** [Grieser, 2018, Chapter 5 and Chapter 8].

RECREATION

There is interest in certain **large numbers** [Schwartz, 2014], **nice numbers** [Barnes, 2016], **modest numbers** [Kenney, Bezuszka, 2015], **happy numbers** [Kenney, Bezuszka, 2015], **honest numbers** [Kenney, Bezuszka, 2015], **defective numbers** [Kenney, Bezuszka, 2015], and the **numbers one cannot count on** [Havil, 2012].

There is also interest in **interesting** [Wells, 1986; Reid, 2006] **as well as uninteresting numbers**[2].

Figure 1 shows a number that could be interesting. The number is a prime number, and each number obtained after removing the rightmost digit from the number is also a prime number.

Figure 1. An unusual prime number. (Source: [Maor, Jost, 2014, Chapter 15].)

Figure 2 shows one number that is interesting and does not show another number that could be interesting.

[2] URL: http://math.crg4.com/uninteresting.html .

Pi Magic Square

Figure 2. A pair of interesting numbers. (Source: Google Images.)

GOOGOL*

$$\text{Googol} = 10^{100}.$$

$$\text{Googolplex} = 10^{(10^{100})}.$$

There is a 10^{94}-volume set of books called collectively as **Googolplex Written Out**[3].

OTHER

There are possibly some numbers 'more important' than the others, as far as the **universe** is concerned [Stein, 2011].

THE WEIRD WORLD OF NUMBERS

There is no pattern to **naming** numbers. It is not uncommon in mathematics to give somewhat amusing names, perhaps unintentionally, to certain numbers.

For example, **complex number, illegal number, imaginary number, irrational number, normal number, perfect number**, and so on.

[3] URL: http://www.googolplexwrittenout.com/ .

Board Time!

Give an example of a number that you do not find amusing.

∞ IS NOT A NUMBER

The infinity (usually denoted by ∞) has been a subject of interest for centuries [Reid, 2006]. ∞ is a limit, not a number [Houston, 2009, Chapter 21].

A TALE OF TWO ZEROS

In the **IEEE Standard 754-1985** and, its successor, the **IEEE Standard 754-2008**, there are two types of 0s, −0 and +0. In an 8-bit one's complement representation, negative zero is represented by the bit string 11111111, and the positive zero is represented by 00000000.

2.2. THE RELATIONSHIP OF NUMBERS TO COMPUTER SCIENCE

In [Baldwin, Walker, Henderson, 2013], the role of mathematics in computer science is explored. The relationship of numbers to computer science is shown in Figure 3.

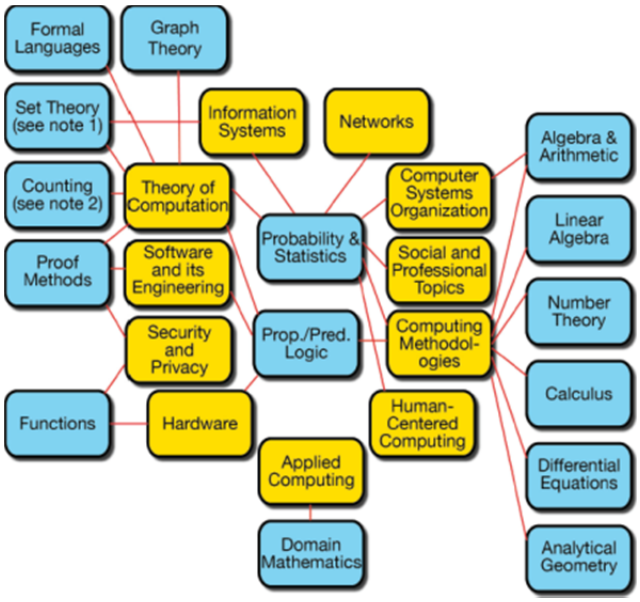

Figure 3. The areas in mathematics associated with areas in computer science. (Source: [Baldwin, Walker, Henderson, 2013].)

2.3. THE RELATIONSHIP OF NUMBERS TO SOFTWARE ENGINEERING

SWEBOK®

The **Guide to the Software Engineering Body of Knowledge (SWEBOK)** "describes the sum of knowledge within the profession of software engineering" [IEEE, 2014]. In SWEBOK, there are a number of Knowledge Areas (KAs). The study of number theory is part of **Mathematical Foundations KA** of the SWEBOK3, as shown in Figure 4.

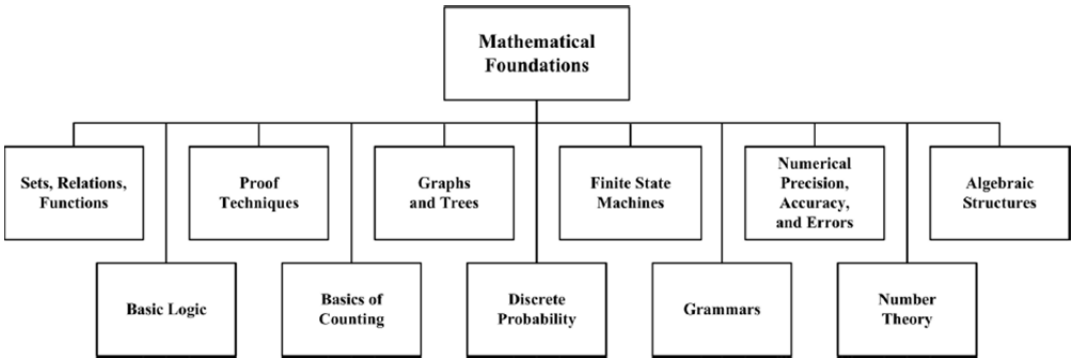

Figure 4. Mathematical Foundations is a Knowledge Area in the Guide to the Software Engineering Body of Knowledge (SWEBOK). (Source: SWEBOK [IEEE, 2014].)

3. DIVISIBILITY

If a number a **divides** b (denoted by $a \mid b$), it is said that a is a **factor** of b, and b is a **multiple** of a.

If a number a **does not divide** b, then this is denoted by $a \nmid b$.

REMARKS

$a \mid b$ is a statement; $\frac{b}{a}$ is a number.

EXAMPLE

1 | n, where n is any number.

$2 \mid 10^{100}$.

641 | 4294967297.

3.1. DIVISIBILITY RULE

Table 1 presents a subset of the so-called Divisibility Rule. It could be useful if a calculator is not available (or not allowed).

Divisor	Sufficient Condition
2	The given number is an even number.
3	The sum of the digits of the given number is divisible by 3.
4	The last two digits of the given number form a number that is divisible by 4.
5	The last digit of the given number is 0 or 5.
6	The given number is divisible by 2 and by 3.
7	The addition of the last digit to 3 times the rest gives a multiple of 7.
8	The last three digits of the given number form a number that is divisible by 8.
9	The sum of the digits of the given number is divisible by 9.

Table 1. For some, it is back to school, again.

3.2. PROPERTIES

| is **transitive**, but **not commutative**. For example, 3 | 6, but 6 ∤ 3.

Board Time!
Give an example of an operator that is commutative, but not transitive.

4. PRIME NUMBERS

A000040

Definition [Prime Number]. Let n be a positive integer. Then, n is said to be a prime number if the only divisors of n are 1 and n.

EXAMPLE

2 is the smallest prime number. (The primality of 2 is like an **axiom**.) The other prime numbers are 3, 5, 7, 11, 13, 17, and so on.

EXAMPLE

0 is not a prime number.

EXAMPLE

1 is not a prime number.

This is done to preserve the **Fundamental Theorem of Arithmetic** which asserts the **uniqueness of the product of prime numbers** [Vince, 2015, Section 2.8.2].

If 1 were a prime number, then the Fundamental Theorem of Arithmetic would be **violated**:

$$40 = 2^3 \times 5.$$
$$40 = 1 \times 2^3 \times 5.$$

REMARKS

The notion of a prime number spans millennia. For example, the **Euclidean Algorithm** for finding the **greatest common divisor (GCD)** of two nonnegative integers is at least 300 B.C. old. Finding larger and larger prime numbers is a problem of active pursuit.

4.1. PROPERTIES

It is evident that all prime numbers, except 2, are **odd**.

The **sum** of two prime numbers **may or may not** be a prime number. For example, 2 + 3 = 5, which is a prime number, but 3 + 5 = 8, which is not a prime number.

OEIS A077800

There is interest in the **distribution** of prime numbers within the set of natural numbers[4]. A **twin prime** is a pair of prime numbers that differ by two. For example, {17, 19} is a twin prime. However, 23 is not part of a twin prime, and is therefore called **isolated prime**. It has been **conjectured** but not proven that there are infinitely many twin primes.

Goldbach Conjecture. Every even integer greater than 2 can be expressed as the sum of two prime numbers.

REMARKS

The Goldbach Conjecture is one of the oldest and most renowned **unsolved problems** in number theory.

In some cases, it is possible to express an even integer greater than 2 as the sum of two prime numbers in **more than one way**.

The even integers correspond to horizontal lines. For each odd prime number, there are two oblique lines, one red and one blue. The sums of two prime numbers are the intersections of one red and one blue line, marked by a circle. Thus, the circles on a given horizontal line give all partitions of the corresponding even integer into the sum of two prime numbers.

This is shown in Figure 5.

[4] This is related to the **Prime Number Theorem**, which explains why the prime numbers become increasingly uncommon as they become larger.

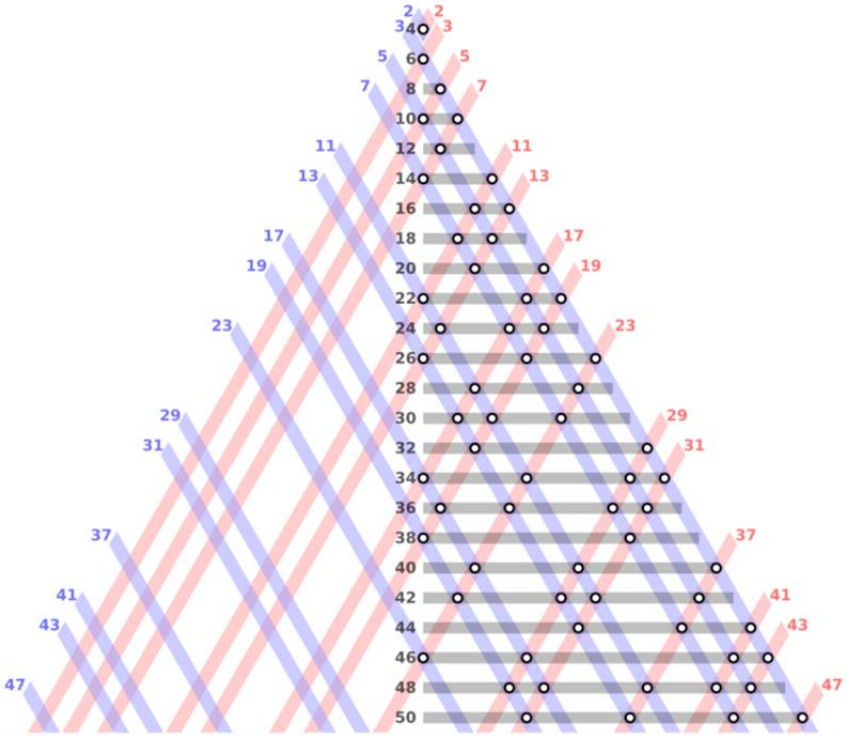

Figure 5. The even integers from 4 to 50 as sums of two prime numbers. (Source: Wikipedia.)

Proposition. If a prime number is the sum of two prime numbers, then one of these equals 2.

Proof. This can be shown by a **proof by contradiction.**

Let p_1, p_2, and p be prime numbers, with $p_1 + p_2 = p$.

Suppose that neither p_1 nor p_2 is equal to 2. Then, both p_1 and p_2 must be odd (and greater than 2). Hence, $p = p_1 + p_2$ is even, and greater than 2.

This contradicts that p is a prime number.

■

EXAMPLE

Prove that if n is a positive integer such that the sum of the divisors of n is n + 1, then n is a prime number.

Solution.

This can be shown by a **proof by contraposition**: if n is not a prime number, then the sum of its divisors is not n + 1.

There are two **exhaustive** cases.

Case 1: n = 1.

If so, the sum of the divisors is $1 \neq 1 + 1$.

Case 2: n is composite.

If so, n can be expressed as $n = ab$, where both a and b are divisors of n different from 1 and from n (although it might happen that $a = b$).

Then, n has at least three distinct divisors, namely 1, a, and n, and their sum is clearly not equal to n + 1.

REMARKS

The converse of the previous statement is also true: if n is a prime number, then the sum of its divisors is n + 1 (because its only divisors are 1 and itself).

EXAMPLE

Let n be an integer, $n \geq 2$. If the sum of the divisors of n is equal to n + 1, then n is a prime number.

Solution.

This can be shown by a **proof by contraposition**: if n is not a prime number, then the sum of the divisors of n is not equal to n + 1.

If n is not a prime number, then, n has divisors 1, n, and m, for some positive integer m, $m \neq 1$, $m \neq n$, and possibly more.

Therefore, the sum of the divisors is greater than n + 1.

EXAMPLE

Prove or disprove that for every prime number n, n + 2 is a prime number.

Solution. Improvise.

4.2. SPECIAL PRIME NUMBERS

The prime numbers are not all the same. Indeed, some prime numbers have certain characteristics that make them special.

4.2.1. FACTORIAL PRIME NUMBERS

OEIS A088054

Definition [Factorial Prime Number]. A prime number that is one less or one more than a factorial.

For example,

2 (0! + 1 or 1! + 1),
3 (2! + 1),
5 (3! – 1),
7 (3! + 1),
23 (4! – 1),
...,

are Factorial Prime Numbers.

4.2.2. PALINDROME PRIME NUMBERS

OEIS A002385

Definition [Palindrome Prime Number]. A prime number that is a palindrome.

For example, 11, 101, 353, … are Palindrome Prime Numbers.

11 is the only palindrome prime number with an even number of digits; other palindrome prime numbers have an odd number of digits [O'Regan, 2016, Chapter 3].

4.2.3. PRIMORIAL NUMBERS

A002110

Definition [Primorial Number]. A number that is either the prime number 2 or a product of successive prime numbers starting at 2.

The notion of Primorial Number is inspired by the notion of factorial.

2, 6, 30, 210, 2310, and so on, are Primorial Numbers.

For example, 30 is a Primorial Number because it is a product of successive prime numbers starting at 2, that is, $30 = 2 \cdot 3 \cdot 5$. In other words, 30 can be 'factored' into a product of successive prime numbers starting at 2.

4.2.4. PYTHAGOREAN PRIME NUMBERS

A002144

Definition [Pythagorean Prime Number]. A prime number of the form 4n + 1.

Figure 6 shows a right triangle. The Pythagorean Prime Numbers are the odd prime numbers p for which $\sqrt{p}$ is the length of the hypotenuse of a right triangle with integer sides. (They are also the prime numbers p for which there exists a right triangle with integer sides whose hypotenuse has length p.)

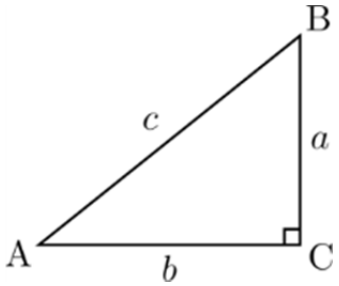

Figure 6. A right triangle.

For example, 5, 13, 17, … are Pythagorean Prime Numbers.

It should be noted that **not** every number of the form 4n + 1 is a prime number. For example, $4 \cdot 5 + 1 = 21$, which is **not** a prime number.

4.2.5. MERSENNE PRIME NUMBERS

A000668

Definition [Mersenne Prime Number]. A prime number of the form $M_n = 2^n - 1$.

In other words, a Mersenne Prime Number is a positive integer that is one less than a power of two.

For example, the first four Mersenne Prime Numbers are $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, and $M_7 = 127$.

If $M_n = 2^n - 1$ is a prime number, then n is also a prime number. For example[5], $2^{13} - 1 = 8191$ is a prime number, and so is 13. For example, $2^6 - 1 = 63$, which is **not** a prime number.

However, the converse is **not** true. For example, 11 is a prime number, but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a prime number.

The **largest known prime number**[6] as of **2017** is a Mersenne Prime Number $2^{77,232,917} - 1$, and it has 23,249,425 decimal digits.

REMARKS

It is **not known** whether there are infinitely many Mersenne primes (and therefore infinitely many perfect numbers). The Web spawned a new era in distributed computing. The **Great Internet Mersenne Prime Search (GIMPS)**[7] is a **collaborative project** of volunteers around the world to search for new **Mersenne Prime Numbers**.

[5] The asteroid with minor planet number 8191 is named 8191 Mersenne. Source: NASA JPL Small-Body Database Browser (http://ssd.jpl.nasa.gov/sbdb.cgi?sstr=8191+Mersenne).
[6] URL: http://primes.utm.edu/largest.html .
[7] URL: http://www.mersenne.org/ .

5. PRIME FACTORIZATION

The Fundamental Theorem of Arithmetic. Every integer greater than 1 has a prime factorization, that is, it can be written **uniquely** as (1) a **prime** number, or (2) **the product of two or more prime numbers**, where the prime factors are written in order of **nondecreasing size**.

This has a **proof by mathematical induction** [Grieser, 2018, Chapter 8].

EXAMPLE

The prime factorizations of 99, 100, and 101 are:

$99 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11.$
$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2.$
$101 = 101.$

EXAMPLE

Euclid's Theorem. The set of all prime numbers is infinite.

There are several possible proofs [Hardy, Woodgold, 2009].

Proof 1. This is a **proof by contradiction**.

Let the set of all prime numbers be finite. Then, there must exist a positive integer, say n, such that there are n prime numbers.

Let the prime numbers be enumerated, in an increasing order, as p_1, p_2, p_3, …, p_n. Now, consider

$$x = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1.$$

Then, by the **Fundamental Theorem of Arithmetic**, either (1) x is a prime number, or (2) x (is a composite number that) can be written as a product of two or more prime numbers.

Case (1): p_n is the largest prime number, and $x > p_n$. Therefore, x cannot be a prime number.

Case (2): If x is divided by p_i, for any i = 1, 2, 3, …, n, then that leaves a remainder of 1. Therefore, x is not divisible by any of the n prime numbers. This means that x's prime divisors are not among the n prime numbers. However, this contradicts the assumption.

■

Proof 2. This is a **proof by contradiction**.

Let the set of all prime numbers be finite. Then, there is an integer, p, which is the largest prime number.

Now, $p! = 1 \cdot 2 \cdot 3 \cdots p$ is divisible by every integer from 2 to p, as it is the product of all of them.

Hence, p! + 1 is not divisible by every integer from 2 to p (as it gives a remainder of 1 when divided by each).

Therefore, either p! + 1 is a prime number, or p! + 1 is divisible by a prime number larger than p.

This contradicts the assumption that p is the largest prime number.

■

REMARKS

The Proof 2 is a **non-constructive existence proof**. The existence of infinitely many prime numbers is shown **implicitly** (that is, without actually showing them).

The **infiniteness of prime numbers** has been voted to be among the **most beautiful theorems in mathematics**:

Rank	Theorem	Average
(1)	$e^{i\pi} = -1$	7.7
(2)	Euler's formula for a polyhedron: $V + F = E + 2$	7.5
(3)	The number of primes is infinite.	7.5
(4)	There are 5 regular polyhedra.	7.0
(5)	$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \pi^2/6.$	7.0
(6)	A continuous mapping of the closed unit disk into itself has a fixed point.	6.8
(7)	There is no rational number whose square is 2.	6.7
(8)	π is transcendental.	6.5
(9)	Every plane map can be coloured with 4 colours.	6.2
(10)	Every prime number of the form $4n + 1$ is the sum of two integral squares in exactly one way.	6.0

EXAMPLE

Show that $\log_2(3)$ is an irrational number.

Solution. This is a **proof by contradiction**.

Let $\log_2(3)$ be a rational number.

Then, it is possible to write $\log_2(3) = p/q$, such that p and q are positive integers with $q \neq 0$. From the definition of the logarithm function,

$$2^{p/q} = 3,$$

or

$$2^p = 3^q.$$

Let $n = 2^p$. Then, n is a positive integer and $n > 1$. Therefore, the **Fundamental Theorem of Arithmetic** applies.

Indeed, n has two different prime factorizations 2^p and 3^q. (It can be noted that $2^p \neq 3^q$ as LHS is an even integer and the RHS is an odd integer.)

However, this contradicts the **Fundamental Theorem of Arithmetic**.

EXAMPLE

Show that $\sqrt{6}$ is an irrational number.

Solution. Improvise. (Use the **Fundamental Theorem of Arithmetic**, and compare even powers of prime factors.)

5.1. IMPLICATIONS OF THE FUNDAMENTAL THEOREM OF ARITHMETIC

There are a number of results **based** on the **Fundamental Theorem of Arithmetic**, including the following:

Corollary 1. If n is a composite integer, then n has a prime divisor less than or equal to square root of n.

Corollary 2. If an integer n is **not** divisible by any prime number less than or equal to square root of n, then n is a prime number.

Corollary 2 is used commonly in **primality testing**.

EXAMPLE

Test whether 31 is a prime number.

Solution.

The prime numbers less than or equal to $\sqrt{31}$ are 2, 3, and 5, and 31 is not divisible by any of them. Therefore, 31 is a prime number.

6. CO-PRIME NUMBERS

Definition [Co-Prime Number]. Let m and n be two positive integers. Then m and n are said to be co-prime if they are prime with respect to each other. In other words, the only **common divisor** between m and n is 1.

(The numbers that are co-prime are also known as **relatively prime**.)

EXAMPLE

2 and 3 are co-prime. (In fact, 2 and 3 are also prime numbers.)

9 and 10 are co-prime. (However, 9 and 10 are not prime numbers.)

9 and 12 are **not** co-prime.

7. COMPOSITE NUMBERS

OEIS A002808

Definition [Composite Number]. Let n be a positive integer. Then n is said to be a composite number if it is not a prime number.

EXAMPLE

Every even number (except, of course, 2) is a composite number.

EXAMPLE

0 is not a composite number. 1 is not a composite number.

EXAMPLE

The sum of two composite numbers is not necessarily a composite number.

Solution. Improvise. (Find the smallest even composite number and add it to the smallest odd composite number.)

PROPERTIES

Every composite number has **at least three divisors**. For example, 4 is a composite number and its divisors are 1, 2, and 4. For another example, 15 is a composite number and its divisors are 1, 3, 5, and 15.

EXAMPLE

Prove or disprove that whenever n is a positive integer > 1, $n^2 - 1$ is a composite number.

Solution. Improvise.

8. MODULAR ARITHMETIC

An integer may or may not divide another integer completely. This leads to a special type of arithmetic.

Definition [Modular Arithmetic]. A system of arithmetic in which integer values lie on a **circular number line** rather than on the infinite number line.

Let n be an integer and d be a positive integer. The **remainder** of dividing n by d is denoted by n **mod** d.

8.1. THE DIVISION ALGORITHM

If n **mod** d, then for some integers q and r, $n = dq + r$.

The number n is called the **dividend**.
The number d is called the **divisor**. (It is conventional to have d to be an integer > 1.)
The number q is called the **quotient** and q = n **div** d.
The number r is called the **remainder**. (It is conventional to have $0 \leq r < d$.)

REMARKS

The Division Algorithm is also called as **The Division Theorem**.

EXAMPLE

n = 14, $d = 5$:

$14 = (2 \cdot 5) + 4$, so

14 **div** 5 = 2 and 14 **mod** 5 = 4.

EXAMPLE

n = –14, $d = 5$:

$-14 = ((-3) \cdot 5) + 1$, so

–14 **div** 5 = –3 and –14 **mod** 5 = 1.

EXAMPLE

7 **mod** 2 = 1.	2 **mod** 7 = 2.
8 **mod** 2 = 0.	–7 **mod** 7 = 0.
100 **mod** 101 = 100.	–5 **mod** 7 = 2.

EXAMPLE

Find a **div** d and a **mod** d in each of the following cases:

(a) $a = -111$, $d = 99$.
(b) $a = -9999$, $d = 101$.
(c) $a = 123456$, $d = 1001$.

Solution.

The problem requires one to do the division and report the quotient, namely a **div** d, and the remainder, namely a **mod** d.

The quotient is rounded down. This means that if the dividend is negative, the **quotient is a number with a larger absolute value**.

(a) 111/99 is between 1 and 2, so the quotient is –2 and the remainder is $-111 - (-2)\cdot 99 = -111 + 198 = 87$.

(b) –9999/101 = –99, so that is the quotient and the remainder is 0.

(c) 123456 **div** 1001 = 123 and 123456 **mod** 1001 = 333.

8.2. THE MEANING OF MOD: MOD AS A FUNCTION

It is possible to view 'mod' as function

$$\text{mod}: \mathbf{Z} \times \mathbf{Z}^{+} \longrightarrow \mathbf{N},$$

where the **dividend** belongs to the set of integers, the **divisor** belongs to the set of positive integers, and the **remainder** belongs to the set of natural numbers.

EXAMPLE

Let a be an integer and d be an integer greater than 1. Then, show the following:

(a) The **quotient** obtained when a is divided by d is $\lfloor a/d \rfloor$.
(b) The **remainder** obtained when a is divided by d is $a - d\lfloor a/d \rfloor$.

Solution.

It is possible to express a as

$$a = d\text{q} + \text{r}, \text{ where } 0 \leq \text{r} < d.$$

(a)

It follows that

$$a/d = \text{q} + (\text{r}/d), \text{ where } 0 \leq (\text{r}/d) < 1.$$

Therefore, by one of the properties of the floor function,

$$\text{q} = \lfloor a/d \rfloor.$$

(b)

It follows that

$$\text{r} = a - d\text{q}, \text{ where } 0 \leq \text{r} < d.$$

Therefore, by (a),

$$\text{r} = a - d\lfloor a/d \rfloor.$$

REMARKS

It follows from the previous example that **mod can be calculated using the floor function**.

In fact, mod is one of the commonly-found functions on **scientific calculators**, such as the one shown in Figure 7.

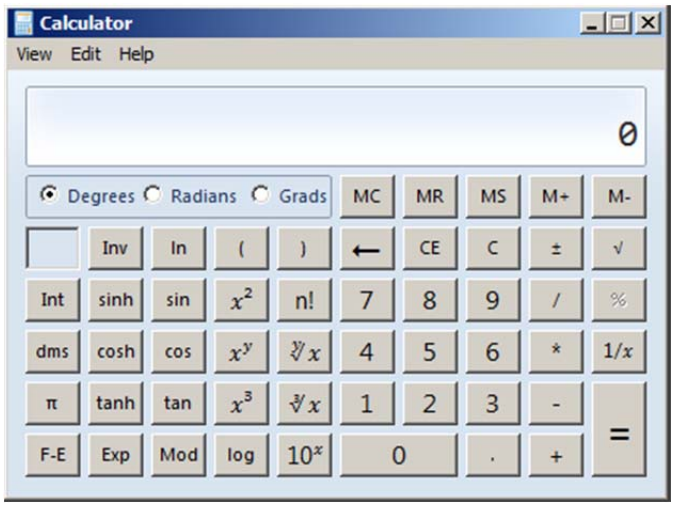

Figure 7. A snapshot of the user interface of a calculator showing several functions, including the mod function.

EXAMPLE

Find 0 **div** 19 and 0 **mod** 19.

Solution.

It follows from the previous example that

0 **div** 19 = $\lfloor$ 0/19 $\rfloor$ = 0.
0 **mod** 19 = 0 − 19 $\lfloor$ 0/19 $\rfloor$ = 0 – 0 = 0.

PROPERTIES

The properties given below are more interesting if viewed **qualitatively** rather than quantitatively and if the **underlying reasons** for their existence are understood. Their proofs are straightforward, and the proofs of some properties use other properties.

PROPERTY 1

For an integer a and a positive integer d,

$$ad \textbf{ mod } d = 0.$$

For example,

$$23 \cdot 7 \textbf{ mod } 7 = 0.$$

Board Time!
Calculate 138 **mod** 6.

PROPERTY 2

For an integer n and a positive integer *d*,

$$0 \leq \text{n } \textbf{mod } d < d.$$

PROPERTY 3

$$\text{n} = (\text{n } \textbf{div } d) \cdot d + \text{n } \textbf{mod } d.$$

For example,

$$23 = (23 \textbf{ div } 7) \cdot 7 + 23 \textbf{ mod } 7 = 21 + 2 = 23.$$

PROPERTY 4

$$\text{If } 0 \leq \text{r} < d, \text{ then } (\text{q}d + \text{r}) \textbf{ mod } d = \text{r}.$$

For example,

$$(5 \cdot 7 + 3) \textbf{ mod } 7 = 3.$$

PROPERTY 5

$$(\text{q}d + \text{n } \textbf{mod } d) \textbf{ mod } d = \text{n } \textbf{mod } d.$$

For example,

$$(5 \cdot 7 + 23 \textbf{ mod } 7) \textbf{ mod } 7 = 23 \textbf{ mod } 7.$$

PROPERTY 6

For integers a and b, and positive integer d,

$$(ad + b) \textbf{ mod } d = b \textbf{ mod } d.$$

For example,

$$(57 \cdot 7 + 13) \textbf{ mod } 7 = 13 \textbf{ mod } 7.$$

EXAMPLE

Give a proof of Property 6.

Solution.

If b **mod** d, then for some integers q and r,

$$b = dq + r, \text{ where } r = b \textbf{ mod } d \text{ and } 0 \leq r < d.$$

Then,

$(ad + b)$ **mod** d
$= ((a + q)d + r)$ **mod** d
$= r$, by Property 4
$= b$ **mod** d.

PROPERTY 7

For an integer a and a positive integer d,

$$(a \textbf{ mod } d) \textbf{ mod } d = a \textbf{ mod } d.$$

For example,

$$(59 \textbf{ mod } 7) \textbf{ mod } 7 = 3 = 59 \textbf{ mod } 7.$$

Board Time!
Give a proof of Property 7. (Hint: Use Property 8.)

PROPERTY 8

For integers a and b, and positive integer d,

$$(a \textbf{ mod } d \pm b \textbf{ mod } d) \textbf{ mod } d = (a \pm b) \textbf{ mod } d.$$

For example,

$$(5 + 8) \textbf{ mod } 3 = 1 = (5 \textbf{ mod } 3 + 8 \textbf{ mod } 3) \textbf{ mod } 3.$$
$$(5 - 8) \textbf{ mod } 3 = 0 = (5 \textbf{ mod } 3 - 8 \textbf{ mod } 3) \textbf{ mod } 3.$$

EXAMPLE

(This example illustrates the **significance** of Property 8.)

(a) Give integers a and b, and positive integer d such that a **mod** $d + b$ **mod** $d = (a + b)$ **mod** d.
(b) Give integers a and b, and positive integer d such that a **mod** $d + b$ **mod** $d \neq (a + b)$ **mod** d.

Solution.

(a) 3 **mod** $2 + 4$ **mod** $2 = 1 + 0 = 1 = 7$ **mod** 2.
(b) 3 **mod** $2 + 5$ **mod** $2 = 1 + 1 = 2 \neq 0 = 8$ **mod** 2.

EXAMPLE

Give a proof of the positive incarnation of Property 8.

Solution.

Let $r = a$ **mod** d and $s = b$ **mod** d. Then, $a = pd + r$ and $b = qd + s$, where $0 \leq r < d$ and $0 \leq s < d$.

Now,

$(a + b)$ **mod** d
$= (pd + r + qd + s)$ **mod** d
$= ((p + q)d + r + s)$ **mod** d
$= (r + s)$ **mod** d, by Property 6
$= (a$ **mod** $d + b$ **mod** $d)$ **mod** d.

EXAMPLE

Let $S_n = \{0, 1, 2, \ldots, n - 1\}$, where $n \geq 2$, and let $f : S_n \longrightarrow S_n$ be defined by

$$f(pk + s) = (pk + s) \textbf{ mod } n,$$

where p is a prime number, $p > n$, and $s \in S_n$. Prove that f is one-to-one.

Solution.

Let $f(k_1) = f(k_2)$, where $0 \leq k_1 \leq n - 1$ and $0 \leq k_2 \leq n - 1$.

Thus,

$$(pk_1 + s) \textbf{ mod } n = (pk_2 + s) \textbf{ mod } n,$$

which implies that

$$n \mid [(pk_1 + s) - (pk_2 + s)].$$

Therefore,

$$n \mid [\, p(k_1 - k_2) \,] ,$$

where $-(n - 1) \leq k_1 - k_2 \leq n - 1$.

Now, no factor of n divides p, because p is prime, with $p > n$.

Also, between $-(n - 1)$ and $(n - 1)$ only 0 is divisible by n.

Hence $k_1 - k_2 = 0$, that is, $k_1 = k_2$.

Thus, f is one-to-one.

■

EXAMPLE

Let $S = \{0, 1, 2, \ldots, 9\}$, and let $f : S \longrightarrow S$ be defined by $f(k) = (5k + 3)$ **mod** 10. Determine whether f is invertible.

Solution. Improvise. (To be invertible, f must be one-to-one and onto. Check whether f is one-to-one.)

9. LINEAR CONGRUENCE

Let a and b be integers, and d be a positive integer. It is said that a is **congruent** to b modulo d if d divides $a - b$.

The phrase ***a* is congruent to *b* modulo *d*** is denoted by $a \equiv b \pmod{d}$. The congruence is **"linear"** as the variables involved have power one.

REMARKS

$a \equiv b \pmod{d}$ is a **statement**; a **mod** d is a **number**.

EXAMPLE

$17 \equiv 7 \pmod{2}$ because $17 - 7 = 10$ is divisible by 2.

EXAMPLE

$-7 \equiv 70 \pmod{11}$ because $-7 - 70 = -77$ is divisible by 11.

EXAMPLE

Find all integer solutions of

$$2x \equiv 7 \pmod{17}.$$

Solution.

If $17 \mid (2x - 7)$, then $2x = 17q + 7$, for some integer q.

This means that 17q + 7 must be even, and so q must be odd, that is, q = 2k + 1, for some integer k.

$$2x = 17(2k + 1) + 7 = 34k + 24,$$

or

$$x = 17k + 12,$$

or

$$x = 12 \pmod{17}.$$

EXAMPLE

Find all integer solutions of

$$4x \equiv 5 \pmod{9}.$$

Solution.

If $9 \mid (4x - 5)$, then $4x = 9q + 5$, for some integer q.

This means that 9q + 5 must be even, and so q must be odd, that is, q = 2k + 1, for some integer k.

$$4x = 9(2k + 1) + 5 = 18k + 14,$$

or

$$2x = 9k + 7.$$

This means that 9k + 7 must be even, and so k must be odd, that is, k = 2m + 1, for some integer m.

$$2x = 9(2m + 1) + 7 = 18s + 16,$$

or

$$x = 9s + 8,$$

or

$$x = 8 \pmod 9.$$

EXAMPLE

Using **direct proof**, show that if k is any integer such that $k \equiv 1 \pmod 3$, then $k^3 \equiv 1 \pmod 9$.

Solution.

(The following is **one** possible approach: use the definition of modulo in the hypotheses, do some algebraic manipulation to bring it to a form of the conclusion, and then use the definition of modulo in the conclusion.)

$k \equiv 1 \pmod 3$
$\Longrightarrow \exists n$ such that $k - 1 = 3n$
$\Longrightarrow \exists n$ such that $k = 3n + 1$
$\Longrightarrow \exists n$ such that $k^3 = (3n + 1)^3$
$\Longrightarrow \exists n$ such that $k^3 = 27n^3 + 27n^2 + 9n + 1$
$\Longrightarrow \exists n$ such that $k^3 - 1 = 27n^3 + 27n^2 + 9n$
$\Longrightarrow \exists n$ such that $k^3 - 1 = 9(3n^3 + 3n^2 + n)$
$\Longrightarrow \exists m$ such that $k^3 - 1 = 9m$
$\Longrightarrow k^3 \equiv 1 \pmod 9$.

EXAMPLE

Prove that if n is an integer not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

Solution.

Step 1. Reformulate the Problem.

If n is an integer not divisible by 3, then either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$.

Step 2. Prove Each Case.

Let p_1: $n \equiv 1 \pmod 3$, p_2: $n \equiv 2 \pmod 3$, and q: $n^2 \equiv 1 \pmod 3$. Prove $(p_1 \longrightarrow q)$ is true and $(p_2 \longrightarrow q)$ is true.

EXAMPLE

Let a and b be integers, such that $a \equiv 11 \pmod{19}$ and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

(a) $c \equiv 13a \pmod{19}$.
(b) $c \equiv a - b \pmod{19}$.
(c) $c \equiv 2a^2 + 3b^2 \pmod{19}$.

Solution.

The aspect **common** to all the parts is that the RHS has **some expression mod 19**. Therefore, all that is needed is to do the arithmetic and compute the remainder upon division by 19.

(a) Scratch Work: $13 \cdot 11 = 143 = 19 \cdot 7 + 10 = 10 \pmod{19}$. Therefore, $c = 10$.

(b) Scratch Work: $11 - 3 \pmod{19} = 11 - 3 = 8 = 8 \pmod{19}$. Therefore, $c = 8$.

(c) Scratch Work: $2 \cdot 11^2 + 3 \cdot 3^2 = 269 = 19 \cdot 14 + 3 = 3 \pmod{19}$. Therefore, $c = 3$.

EXAMPLE

Find the integer a such that

(a) $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$.
(b) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$.
(c) $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$.

Solution.

(a) It is possible to get into the desired range and stay within the same modular equivalence class by subtracting $2 \cdot 23$, and so $a = 43 - 46 = -3$.

(b) $17 - 29 = -12$, and so $a = -12$.

(c) $a = -11 + 5 \cdot 21 = 94$.

EXAMPLE

List five integers that are congruent to 4 (mod 12).

Solution.

The set of possibilities is infinite, five of which are 4, 16, –8, 1204, and –7016360.

EXAMPLE

Decide whether each of these integers is congruent to 3 (mod 7):

(a) 37.
(b) 66.
(c) –17.
(d) –67.

Solution.

In each case, subtract 3 from the given number. If the difference is divisible by 7, then the integer is congruent to 3 (mod 7).

(a) $37 - 3 \pmod 7 = 34 \pmod 7 = 6 \neq 0$, so $37 \not\equiv 3 \pmod 7$.

(b) $66 - 3 \pmod 7 = 63 \pmod 7 = 0$, so $66 \equiv 3 \pmod 7$.

(c) $-17 - 3 \pmod 7 = -20 \pmod 7 = 1 \neq 0$, so $-17 \not\equiv 3 \pmod 7$.

(d) $-67 - 3 \pmod 7 = -70 \pmod 7 = 0$, so $-67 \equiv 3 \pmod 7$.

PROPERTIES

Theorem. Let a and b be integers, and d be a positive integer. Then,

$$a \equiv b \pmod d \text{ if and only if } a \textbf{ mod } d = b \textbf{ mod } d.$$

REMARKS

- This property is saying that $a \equiv b \pmod{d}$ if and only if a and b have the **same remainder** when divided by d.

- This property '**connects'** the **mod function** and **linear congruence**.

- This property is so important that it is sometimes used as the **definition of linear congruence**.

9.1. THE MEANING OF CONGRUENCE

The term **"congruence"** means **"state of agreement"**. There are multiple notions of 'congruence' in mathematics.

In **geometry**, the **"state of agreement"** between two objects is **"having the same shape and size"** (or "having the same shape and size as the mirror image of the other"). (In general, two sets of points are called congruent if and only if, one can be transformed into the other by an **isometry**, that is, a combination of **translation, rotation, and/or reflection**.)

Figure 8 shows an example of congruent triangles.

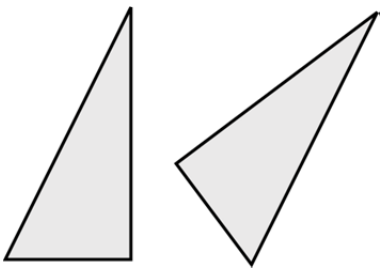

Figure 8. A pair of congruent triangles. (Source: Wikipedia.)

In **modular arithmetic**, the **"state of agreement"** between two integers is **"having the same remainder"** when divided by a specified integer.

REMARKS

There are other terms related to congruence, as illustrated by Figure 9.

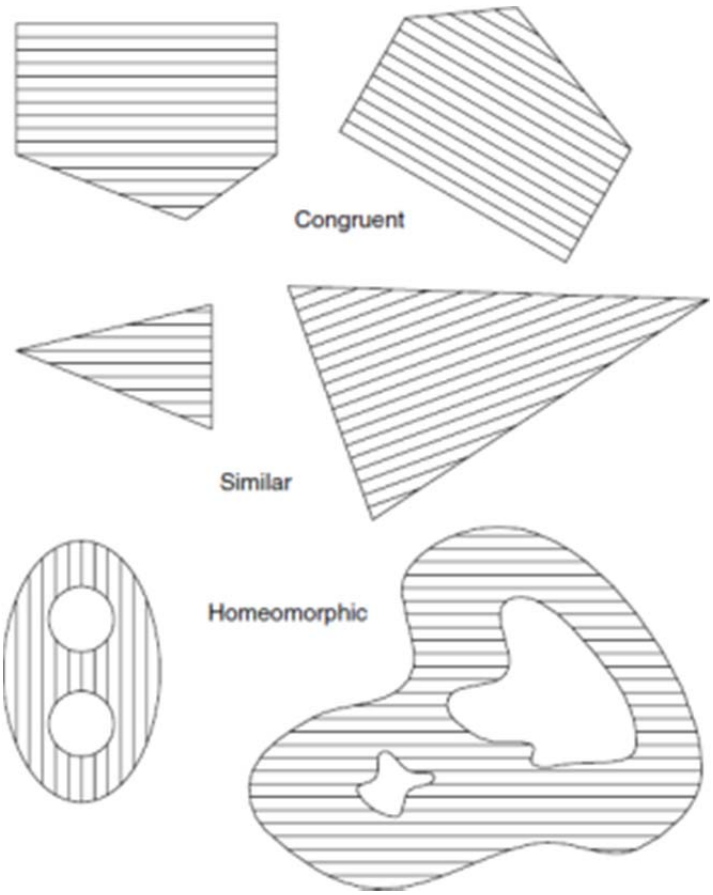

Figure 9. An illustrated collection of terms related to congruence (Source: [Huggett, Jordan, 2009].

9.2. THE MEANING OF ≡

The purpose of '≡' in modular arithmetic with integers on a **circular number line** is similar to the purpose of '=' in conventional arithmetic with integers on an **infinite number line**. In each case, the purpose is **a comparison of two numbers**.

In some sense, the symbol '≡' in modular arithmetic is a **generalization** of '=' in conventional arithmetic. Hence, the reason for the choice of the symbol '≡' in modular arithmetic.

EXAMPLE

A **pair of even (or odd) numbers** a and b can be compared because $a \equiv b \pmod 2$ is always 0.

An **even number** a and **an odd number** b can be compared because $a \equiv b \pmod 2$ is always 1.

EXAMPLE

Let a and b be integers, and d be a positive integer. Show that a **mod** $d = b$ **mod** d if $a \equiv b \pmod d$.

Solution.

Let $a \equiv b \pmod d$. This means that $d \mid a - b$, say $a - b = dc$, for some integer c, so that

$$a = b + dc.$$

Now, $r = b$ **mod** d means that $b = qd + r$, for some q and nonnegative r less than d.

Therefore,

$$a = qd + r + dc = (q + c)d + r,$$

which means that $r = a$ **mod** d.

Theorem.

Let a, b be integers, and c and d be positive integers. Then,

$$\text{if } a \equiv b \pmod d, \text{ then } ac \equiv bc \pmod{dc}.$$

Proof.

$a \equiv b \pmod d$ if and only if $d \mid a - b$.

$a - b = qd$, for some integer q. Then, $ac - bc = qdc$, and so $dc \mid (ac - bc)$.

Therefore, $ac \equiv bc \pmod{dc}$.

■

Theorem.

Let d be a positive integer. Then, $a \equiv b \pmod{d}$ if and only if there is an integer k such that $a = b + kd$.

Proof. There are two parts.

(1)

If $a \equiv b \pmod{d}$, then, by the **definition of linear congruence**, $d \mid a - b$. This means that there is an integer k such that $a - b = kd$. Thus, so that $a = b + kd$.

(2)

If there is an integer k such that $a = b + kd$, then $kd = a - b$. This means that d divides $a - b$, and so $a \equiv b \pmod{d}$.

■

EXAMPLE

Let a, b, and c be integers such that $a \neq 0$. Show that if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ for all integers c.

Solution.

If $a \mid b$ and $a \mid c$, then $b = as$, for some integer s, and $c = at$, for some integer t. Then,

$$b + c = (as + at) = a(s + t),$$

which means that $a \mid (b + c)$.

EXAMPLE

Let a, b, and c be integers such that $a \neq 0$. Show that if $a \mid b$, then $a \mid bc$ for all integers c.

Solution. There are two parts.

(1) $c = 0$.

This is a trivial case, as then $bc = 0$, and therefore $a \mid bc$.

(2) $c \neq 0$.

Improvise.

EXAMPLE

Let a, b, and c be integers such that $a \neq 0$. Show that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Solution.

If $a \mid b$ and $b \mid c$, then $b = as$, for some integer s, and $c = bt$, for some integer t. Then,

$$c = (as)t = a(st),$$

which means that $a \mid c$.

EXAMPLE

Let a, b, and c be integers such that $a \neq 0$. Show that if $a \mid b$ and $a \mid c$, then $a \mid mb + nc$, whenever m and n are integers.

Solution.

If $a \mid b$ and $a \mid c$, then $b = as$, for some integer s, and $c = at$, for some integer t. Then,

$$mb + nc = mas + nat = a(ms + nt),$$

which means that $a \mid mb + nc$.

EXAMPLE

Let a, b, c, and d be integers such that $a \neq 0$. Show that if $a \mid c$ and $b \mid d$, then $ab \mid cd$.

Solution. Improvise. (Use the fact that c and d can be expressed as $c = as$ and $d = bt$, for some integers s and t.)

EXAMPLE

Prove or disprove that if $a \mid bc$, where a, b, and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

Solution.

If $a = 4$ and $b = c = 2$, then $a \mid bc$, but neither $a \mid b$ nor $a \mid c$.

EXAMPLE

Let a, b, c, d, and m are integers with $m \geq 2$. Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv (b - d) \pmod{m}$.

Solution.

From $a \equiv b \pmod{m}$, it follows that

$$b = a + sm,$$

for some integer s.

From $c \equiv d \pmod{m}$, it follows that

$$d = c + tm,$$

for some integer t.

From these equations, it follows that

$$b - d = (a - c) + (s - t)m,$$

which means that $a - c \equiv (b - d) \pmod{m}$.

EXAMPLE

Let a, b, c, and d be integers such that $c > 0$ and $d \geq 2$. Show that if $a \equiv b \pmod{d}$, then $ac \equiv bc \pmod{dc}$.

Solution.

From $a \equiv b \pmod{d}$, it follows that

$$b = a - sd,$$

for some integer s.

Now, multiplying both sides of the equation by c, the result is

$$bc = ac - s(dc),$$

which means that $ac \equiv bc \pmod{dc}$.

EXAMPLE

Show that if n is an integer, then either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Solution.

There are two cases.

Case 1: n is even.

In this case, n = 2k, for some integer k, so

$$n^2 = 4k^2,$$

which means that $n^2 \equiv 0 \pmod 4$.

Case 2: n is odd.

In this case, n = 2k + 1, for some integer k, so

$$n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1,$$

which means that $n^2 \equiv 1 \pmod 4$.

EXAMPLE

Prove that if n is an odd positive integer, then $n^2 \equiv 1 \pmod 8$.

Solution.

As n is an odd positive integer, $n = 2k + 1$, for some integer k. Then,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Now, either k or k + 1 is even, so 4k(k + 1) is a multiple of 8.

Therefore, $n^2 - 1$ is a multiple of 8, which means $n^2 \equiv 1 \pmod 8$.

EXAMPLE

Give the number of zeros at the end of 100!.

Solution.

In general, a number has a 0 at the end of it if and only if the number has 10 as a factor. Therefore, the problem is about factors of 10 in 100!.

Now, 10 is not a prime number. Indeed, the **prime factorization** of 10 is $2 \cdot 5$. Therefore, the **problem is transformed** to finding pairs of factors of 2 and factors of 5 in 100!.

The number of factors of 2 and number of factors of 5 in 100! **may not be the same**, so the problem is, once again, transformed to finding

min(number of factors of 2 in 100!, number of factors of 5 in 100!).

It can be easily seen that the number of factors of 2 in 100! is **greater** than the number of factors of 5 in 100!.

Thus, the problem is reduced to finding the number of factors of 5 in 100! as that is the same as the number of factors of 10 in 100!.

Numbers Contributing a Factor of 5	Number of Factors of 5 Contributed	Count
5, 10, 15, …, 100	1	20
25, 50, 75, 100	2	4

Therefore, there are 24 factors of 5 in 100!, and so 100! ends in exactly 24 0's.

10. GREATEST COMMON DIVISOR

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 (GCD)** of a and b. The GCD of a and b is denoted by **gcd(a, b)**.

PROPERTIES

The integers a and b are **relatively prime** if their GCD is 1.

10.1. NOTABLE RESULTS ON FINDING GCD

The common ways of finding GCD of two numbers are (1) **Prime Factorization**, and (2) the **Euclidean Algorithm**. In theory, they are the same; however, in practice, they are not, as, for large numbers, (1) can be considerably slower than (2).

EXAMPLE

Find the GCDs of the following pairs of integers:

$$22 \cdot 33 \cdot 55 \text{ and } 25 \cdot 33 \cdot 52.$$

Solution.

The GCD is formed by finding **common prime factors** across the given numbers, and then multiplying the **minimum exponent** of those common prime factors to produce the GCD.

The prime factorization of $22 \cdot 33 \cdot 55$ is

$$2 \cdot 3 \cdot 5 \cdot 11^3.$$

The prime factorization of $25 \cdot 33 \cdot 52$ is

$$2^2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13.$$

Therefore, the GCD is $2 \cdot 3 \cdot 5 \cdot 11 = 330$.

Bézout's Lemma. Let a and b be positive integers. Then, there exist integers s and t such that gcd(a, b) = sa + tb.

In other words, gcd(a, b) can be expressed as a **linear combination** with **integer coefficients** of a and b. This combination is not necessarily unique.

EXAMPLE

Let a = 12 and b = 42. Therefore, gcd (12, 42) = 6. Then,

$$\gcd(12, 42) = 6 = 4 \cdot 12 + (-1) \cdot 42.$$
$$\gcd(12, 42) = 6 = (-3) \cdot 12 + 1 \cdot 42.$$

Lemma. Let a, b, q, and r be integers such that $a = bq + r$. Then gcd(a, b) = gcd(b, r).

In other words, the lemma provides a **relationship between the GCD and the Division Algorithm**. It is also the **basis for the Euclidean Algorithm** [Hougardy, Vygen, 2016, Section 3.3].

10.1.1. THE EUCLIDEAN ALGORITHM

The following is a compact and simplified incarnation of the Euclidean Algorithm:

Input: Two positive integers, a and b
Output: gcd(a, b)
Process:
1. If $a < b$, swap a and b
2. Divide a by b and get the remainder, r
   (a) If $r = 0$, report b as the gcd(a, b)
   (b) If $r \neq 0$, go to Step 3
3. Replace a by b, and replace b by r; Return to Step 2

REMARKS

The Euclidean Algorithm is based on the **principle** that the GCD of two numbers does **not** change if the larger number is replaced by its difference with the smaller number. This replacement **reduces** the larger of the two numbers.

Thus, repeating this process gives successively smaller pairs of numbers until one of the two numbers reaches zero. In such a case, the other number (the one that is not zero) is the GCD of the original two numbers.

EXAMPLE

Use the Euclidean Algorithm to find

(a) gcd(1, 5).
(b) gcd(12, 15).
(c) gcd(356, 96).
(d) gcd(100, 101).
(e) gcd(11111, 111111).

Solution.

(a) gcd(1, 5) = gcd(1, 0) = 1.
(b) gcd(12, 15) = gcd(12, 3) = gcd(3, 0) = 3.
(c) gcd(356, 96) = gcd(96, 68) = gcd(68, 28) = gcd(28, 12) = gcd(12, 4) = gcd(4, 0) = 4.
(d) gcd(100, 101) = gcd(100, 1) = gcd(1, 0) = 1.
(e) gcd(11111, 111111) = gcd(11111, 1) = gcd(1, 0) = 1.

EXAMPLE

Let a, b, and d be integers such that $d \geq 2$ and $a \equiv b \pmod{d}$, then $\gcd(a, d) = \gcd(b, d)$.

Solution.

From $a \equiv b \pmod{d}$, it follows that

$$b = a - sd,$$

for some integer s.

Now, if d is a **common divisor** of a and d, then it divides the RHS of this equation, and so it also divides the LHS of this equation, namely b.

The previous equation can be rewritten as

$$a = b + sd.$$

Then, by similar reasoning, it follows that every common divisor of b and d is also a divisor of a.

This shows that the set of common divisors of a and d is **equal to** the set of common divisors of b and d, and so $\gcd(a, d) = \gcd(b, d)$.

EXAMPLE

Find positive integers that are less than 12 and are relatively prime to 12.

Solution.

The goal is to find those integer x's from 1 to 11 for which $\gcd(x, 12) = 1$. These x's are 1, 5, 7, and 11.

11. PERFECT NUMBERS

OEIS A000396

Definition [Perfect Number]. A **perfect number** is a number that is equal to the sum of all of its divisors, including 1 but **excluding** the number itself.

EXAMPLE

6 is perfect:

$$6 = 1 + 2 + 3.$$

28 is perfect:

$$28 = 1 + 2 + 4 + 7 + 14.$$

EXAMPLE

Find the next perfect number (that is, after 28).

Solution. Improvise.

REMARKS

There are several **open problems** related to perfect numbers.

For example, it is **not known** whether there are any **odd perfect numbers**. It is also **not known** whether **infinitely many perfect numbers exist**.

11.1. PERFECT NUMBERS AND MERSENNE PRIME NUMBERS

There is a **one-to-one relationship** between **even perfect numbers and Mersenne Prime Numbers**: each Mersenne Prime Number generates one even perfect number, and conversely.

It can be shown that **every even perfect number** is of the form $2^{(p-1)} \cdot (2^p - 1)$, where $2p - 1$ is a prime number, and conversely.

For example, $2^1(2^2 - 1) = 6$ and $2^2(2^3 - 1) = 28$.

EXAMPLE

Let p be a positive integer > 1.

Show that if $2^p - 1$ is a prime number, then $q = 2^{(p-1)} \cdot (2^p - 1)$ is a perfect number.

Solution.

Let $2^p - 1$ be a prime number. Then, the divisors of p are

$$1, 2, 2^2, \ldots, 2^{(p-1)},$$

and

$$(2^p - 1), 2(2^p - 1), 2^2(2^p - 1), \ldots, 2^{(p-2)} \cdot (2^p - 1), 2^{(p-1)} \cdot (2^p - 1).$$

The last divisor is equal to the number, and is therefore **not** included in the sum.

Now,

$[\ 1 + 2 + 2^2 + \cdots + 2^{(p-1)}\ ] + (2^p - 1) \cdot [\ 1 + 2 + 2^2 + \cdots + 2^{(p-2)}\ ]$

$= (\ 1 - 2^p\ ) / (1 - 2\ ) + (2^p - 1) \cdot (\ 1 - 2^{(p-1)}\ ) / (1 - 2\ ).$

$= (2^p - 1) + (2^p - 1) \cdot (\ 2^{(p-1)} - 1\ ).$

$= (2^p - 1) \cdot [\ 1 + (\ 2^{(p-1)} - 1\ )\ ]$

$= 2^{(p-1)} \cdot (2^p - 1)$

$= n.$

REMARKS

- The previous example used a result from series. The **sum of numbers in a geometric series** is given by

  $$1 + x + x^2 + \cdots + x^n = (\ 1 - x^{n+1}\ ) / (\ 1 - x\ ), \text{ for } x \neq 0 \text{ or } 1.$$

- The example is a **special case** of the **Euclid-Euler Theorem**.

  (**Euclid–Euler Theorem.** Every even perfect number can be represented by the form $2^{n-1}(2n - 1)$, where $2n - 1$ is a prime number.)

  In other words, the Euclid-Euler Theorem relates **perfect numbers to Mersenne Prime Numbers**.

ACKNOWLEDGEMENT

The inclusion of images from external sources is solely for non-commercial educational purposes, and their use is hereby acknowledged.

REFERENCES

[Andreescu, Andrica, 2009] Number Theory: Structures, Examples, and Problems. By T. Andreescu, D. Andrica. Birkhäuser. 2009.

[Baldwin, Walker, Henderson, 2013] The Roles of Mathematics in Computer Science. By D. Baldwin, H. M. Walker, P. B. Henderson. ACM Inroads. Volume 4. Issue 4. 2013. Pages 74-80.

[Barnes, 2016] Nice Numbers. By J. Barnes. Birkhäuser. 2016.

[Coppel, 2009] Number Theory: An Introduction to Mathematics. By W. A. Coppel. Second Edition. Springer Science+Business Media. 2009.

[Crandall, Pomerance, 2005] Prime Numbers: A Computational Perspective. By R. Crandall, C. Pomerance. Second Edition. Springer Science+Business Media. 2005.

[Driver, 1984] Why Math? By R. D. Driver. Springer-Verlag. 1984.

[Gerstein, 2012] Introduction to Mathematical Structures and Proofs. By L. J. Gerstein. Springer Science+Business Media. 2012.

[Grieser, 2018] Exploring Mathematics: Problem-Solving and Proof. By D. Grieser. Springer International Publishing. 2018.

[Haigh, 2016] Mathematics in Everyday Life. By J. Haigh. Springer International Publishing. 2016.

[Hardy, Woodgold, 2009] Prime Simplicity. By M. Hardy, C. Woodgold. The Mathematical Intelligencer. Volume 31. Number 4. 2009. Pages 44-52.

[Havil, 2012] The Irrationals: A Story of the Numbers You Can't Count On. By J. Havil. Princeton University Press. 2012.

[Hougardy, Vygen, 2016] Algorithmic Mathematics. By S. Hougardy, J. Vygen. Springer International Publishing. 2016.

[Houston, 2009] How to Think Like a Mathematician: A Companion to Undergraduate Mathematics. By K. Houston. Cambridge University Press. 2009.

[Huggett, Jordan, 2009] A Topological Aperitif. By S. Huggett, D. Jordan. Revised Edition. Springer-Verlag. 2009.

[IEEE, 2014] Guide to the Software Engineering Body of Knowledge (SWEBOK) Version 3.0. The Institute of Electrical and Electronics Engineers (IEEE) Computer Society. 2014.

[Kenney, Bezuszka, 2015] Number Treasury 3 - Investigations, Facts And Conjectures About More Than 100 Number Families. By M. J. Kenney, S. J. Bezuszka. Third Edition. World Scientific. 2015.

[Khare, Lachowska, 2015] Beautiful, Simple, Exact, Crazy: Mathematics in the Real World. By A. Khare, A. Lachowska. Yale University Press. 2015.

[Kneusel, 2015] Numbers and Computers. By R. T. Kneusel. Springer International Publishing. 2015.

[Kraft, Washington, 2014] An Introduction to Number Theory with Cryptography. By J. S. Kraft, L. C. Washington. CRC Press. 2014.

[Lehman, Leighton, Meyer, 2012] Mathematics for Computer Science. By E. Lehman, F. T. Leighton, A. R. Meyer. January 4, 2012.

[Maor, Jost, 2014] Beautiful Geometry. By E. Maor, E. Jost. Princeton University Press. 2014.

[Neto, 2018] An Excursion through Elementary Mathematics, Volume III: Discrete Mathematics and Polynomial Algebra. By A. C. M. Neto. Springer International Publishing. 2018.

[Nickerson, 2010] Mathematical Reasoning: Patterns, Problems, Conjectures, and Proofs. By R. S. Nickerson. Psychology Press. 2010.

[Niederreiter, Winterhof, 2015] Applied Number Theory. By H. Niederreiter, A. Winterhof. Springer International Publishing. 2015.

[O'Regan, 2016] Guide to Discrete Mathematics: An Accessible Introduction to the History, Theory, Logic and Applications. By G. O'Regan. Springer International Publishing. 2016.

[Posamentier, Thaller, 2015] Numbers: Their Tales, Types, and Treasures. By A. S. Posamentier, B. Thaller. Prometheus Books. 2015.

[Reba, Shier, 2015] Puzzles, Paradoxes, and Problem Solving: An Introduction to Mathematical Thinking. By M. A. Reba, D. R. Shier. CRC Press. 2015.

[Reid, 2006] From Zero to Infinity: What Makes Numbers Interesting. By C. Reid. A K Peters. 2006.

[Rosen, 2012] Discrete Mathematics and Its Applications. By K. H. Rosen. Seventh Edition. McGraw-Hill. 2012.

[Schwartz, 2014] Really Big Numbers. By R. E. Schwartz. American Mathematical Society. 2014.

[Stein, 2011] The 13 Most Important Numbers in the Universe. By J. D. Stein. Popular Mechanics. September 15, 2011.

[Sundstrom, 2018] Mathematical Reasoning: Writing and Proof. By T. Sundstrom. Version 2.1. Grand Valley State University. Allendale, U.S.A. October 16, 2018.

[Vince, 2015] Foundation Mathematics for Computer Science: A Visual Approach. By J. Vince. Springer International Publishing. 2015.

[Wallis, 2012] A Beginner's Guide to Discrete Mathematics. By W. D. Wallis. Second Edition. Springer Science+Business Media. 2012.

[Wells, 1986] The Penguin Dictionary of Curious and Interesting Numbers. By D. Wells. Penguin Books. 1986.