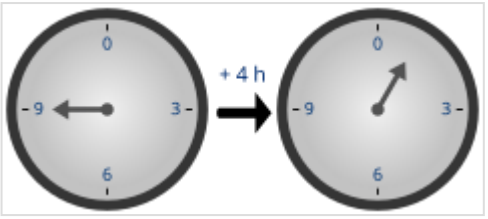
Modular arithmetic

In mathematics, **modular arithmetic** is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the **modulus**. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae*, published in 1801.



Time-keeping on this clock uses arithmetic modulo 12. Adding 4 hours to 9 o'clock gives 1 o'clock, since 13 is congruent to 1 modulo 12.

A familiar use of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. If the time is 7:00 now, then 8 hours later it will be 3:00. Simple addition would result in 7 + 8 = 15, but 15:00 reads as 3:00 on the clock face because clocks "wrap around" every 12 hours and the hour number starts over at zero when it reaches 12. We say that 15 is *congruent* to 3 modulo 12, written 15 ≡ 3 (mod 12), so that 7 + 8 ≡ 3 (mod 12). Similarly, 8:00 represents a period of 8 hours, and twice this would give 16:00, which reads as 4:00 on the clock face, written as 2 × 8 ≡ 4 (mod 12).

Congruence

Given an integer $m \geq 1$, called a **modulus**, two integers a and b are said to be **congruent** modulo m, if m is a divisor of their difference; that is, if there is an integer k such that

$$a - b = k\,m.$$

Congruence modulo m is a congruence relation, meaning that it is an equivalence relation that is compatible with the operations of addition, subtraction, and multiplication. Congruence modulo m is denoted

$$a \equiv b \pmod{m}.$$

The parentheses mean that $\pmod{m}$ applies to the entire equation, not just to the right-hand side (here, b).

This notation is not to be confused with the notation $b \bmod m$ (without parentheses), which refers to the modulo operation, the remainder of b when divided by m: that is, $b \bmod m$ denotes the unique integer r such that $0 \leq r < m$ and $r \equiv b \pmod{m}$.

The congruence relation may be rewritten as

$$a = k\,m + b,$$

explicitly showing its relationship with Euclidean division. However, the b here need not be the remainder in the division of a by m. Rather, $a \equiv b \pmod{m}$ asserts that a and b have the same remainder when divided by m. That is,

$$a = p\,m + r,$$
$$b = q\,m + r,$$

where $0 \le r < m$ is the common remainder. We recover the previous relation ($a - b = k\,m$) by subtracting these two expressions and setting $k = p - q$.

Because the congruence modulo m is defined by the divisibility by m and because -1 is a unit in the ring of integers, a number is divisible by $-m$ exactly if it is divisible by m. This means that every non-zero integer m may be taken as modulus.

Examples

In modulus 12, one can assert that:

$$38 \equiv 14 \pmod{12}$$

because the difference is $38 - 14 = 24 = 2 \times 12$, a multiple of 12. Equivalently, 38 and 14 have the same remainder 2 when divided by 12.

The definition of congruence also applies to negative values. For example:

$$\begin{aligned} 2 &\equiv -3 \pmod{5} \\ -8 &\equiv 7 \pmod{5} \\ -3 &\equiv -8 \pmod{5}. \end{aligned}$$

Basic properties

The congruence relation satisfies all the conditions of an equivalence relation:

- Reflexivity: $a \equiv a \pmod{m}$
- Symmetry: $a \equiv b \pmod{m}$ if $b \equiv a \pmod{m}$.
- Transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, or if $a \equiv b \pmod{m}$, then:[1]

- $a + k \equiv b + k \pmod{m}$ for any integer k (compatibility with translation)
- $k\,a \equiv k\,b \pmod{m}$ for any integer k (compatibility with scaling)
- $k\,a \equiv k\,b \pmod{k\,m}$ for any integer k
- $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ (compatibility with addition)
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$ (compatibility with subtraction)
- $a_1\,a_2 \equiv b_1\,b_2 \pmod{m}$ (compatibility with multiplication)
- $a^k \equiv b^k \pmod{m}$ for any non-negative integer k (compatibility with exponentiation)
- $p(a) \equiv p(b) \pmod{m}$, for any polynomial $p(x)$ with integer coefficients (compatibility with polynomial evaluation)

If $a \equiv b \pmod{m}$, then it is generally false that $k^a \equiv k^b \pmod{m}$. However, the following is true:

- If $c \equiv d \pmod{\varphi(m)}$, where φ is Euler's totient function, then $a^c \equiv a^d \pmod{m}$—provided that a is coprime with m.

For cancellation of common terms, we have the following rules:

- If $a + k \equiv b + k \pmod{m}$, where k is any integer, then $a \equiv b \pmod{m}$.
- If $k\,a \equiv k\,b \pmod{m}$ and k is coprime with m, then $a \equiv b \pmod{m}$.
- If $k\,a \equiv k\,b \pmod{k\,m}$ and $k \neq 0$, then $a \equiv b \pmod{m}$.

The last rule can be used to move modular arithmetic into division. If b divides a, then $(a/b) \bmod m = (a \bmod b\,m) / b$.

The modular multiplicative inverse is defined by the following rules:

- Existence: There exists an integer denoted a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$ if and only if a is coprime with m. This integer a^{-1} is called a *modular multiplicative inverse* of a modulo m.
- If $a \equiv b \pmod{m}$ and a^{-1} exists, then $a^{-1} \equiv b^{-1} \pmod{m}$ (compatibility with multiplicative inverse, and, if $a = b$, uniqueness modulo m).
- If $ax \equiv b \pmod{m}$ and a is coprime to m, then the solution to this linear congruence is given by $x \equiv a^{-1}b \pmod{m}$.

The multiplicative inverse $x \equiv a^{-1} \pmod{m}$ may be efficiently computed by solving Bézout's equation $a\,x + m\,y = 1$ for x, y, by using the Extended Euclidean algorithm.

In particular, if p is a prime number, then a is coprime with p for every a such that $0 < a < p$; thus a multiplicative inverse exists for all a that is not congruent to zero modulo p.

Advanced properties

Some of the more advanced properties of congruence relations are the following:

- Fermat's little theorem: If p is prime and does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.
- Euler's theorem: If a and m are coprime, then $a^{\varphi(m)} \equiv 1 \pmod{m}$, where φ is Euler's totient function.
- A simple consequence of Fermat's little theorem is that if p is prime, then $a^{-1} \equiv a^{p-2} \pmod{p}$ is the multiplicative inverse of $0 < a < p$. More generally, from Euler's theorem, if a and m are coprime, then $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$. Hence, if $ax \equiv 1 \pmod{m}$, then $x \equiv a^{\varphi(m)-1} \pmod{m}$.
- Another simple consequence is that if $a \equiv b \pmod{\varphi(m)}$, where φ is Euler's totient function, then $k^a \equiv k^b \pmod{m}$ provided k is coprime with m.
- Wilson's theorem: p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.
- Chinese remainder theorem: For any a, b and coprime m, n, there exists a unique $x \pmod{mn}$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. In fact, $x \equiv b\,{m_n}^{-1}\,m + a\,{n_m}^{-1}\,n \pmod{mn}$ where ${m_n}^{-1}$ is the inverse of m modulo n and ${n_m}^{-1}$ is the inverse of n modulo m.

- Lagrange's theorem: If p is prime and $f(x) = a_0 x^d + ... + a_d$ is a polynomial with integer coefficients such that p is not a divisor of a_0, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most d non-congruent solutions.
- Primitive root modulo m: A number g is a primitive root modulo m if, for every integer a coprime to m, there is an integer k such that $g^k \equiv a \pmod{m}$. A primitive root modulo m exists if and only if m is equal to 2, 4, p^k or $2p^k$, where p is an odd prime number and k is a positive integer. If a primitive root modulo m exists, then there are exactly $\varphi(\varphi(m))$ such primitive roots, where φ is the Euler's totient function.
- Quadratic residue: An integer a is a quadratic residue modulo m, if there exists an integer x such that $x^2 \equiv a \pmod{m}$. Euler's criterion asserts that, if p is an odd prime, and a is not a multiple of p, then a is a quadratic residue modulo p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Congruence classes

The congruence relation is an equivalence relation. The equivalence class modulo m of an integer a is the set of all integers of the form $a + k\,m$, where k is any integer. It is called the **congruence class** or **residue class** of a modulo m, and may be denoted as $(a \bmod m)$, or as $\overline{a}$ or $[a]$ when the modulus m is known from the context.

Each residue class modulo m contains exactly one integer in the range $0, \ldots, |m| - 1$. Thus, these $|m|$ integers are representatives of their respective residue classes.

It is generally easier to work with integers than sets of integers; that is, the representatives most often considered, rather than their residue classes.

Consequently, $(a \bmod m)$ denotes generally the unique integer k such that $0 \leq k < m$ and $k \equiv a \pmod{m}$; it is called the **residue** of a modulo m.

In particular, $(a \bmod m) = (b \bmod m)$ is equivalent to $a \equiv b \pmod{m}$, and this explains why "=" is often used instead of "≡" in this context.

Residue systems

Each residue class modulo m may be represented by any one of its members, although we usually represent each residue class by the smallest nonnegative integer which belongs to that class[2] (since this is the proper remainder which results from division). Any two members of different residue classes modulo m are incongruent modulo m. Furthermore, every integer belongs to one and only one residue class modulo m.[3]

The set of integers $\{0, 1, 2, ..., m - 1\}$ is called the **least residue system modulo m**. Any set of m integers, no two of which are congruent modulo m, is called a **complete residue system modulo m**.

The least residue system is a complete residue system, and a complete residue system is simply a set containing precisely one representative of each residue class modulo m.[4] For example, the least residue system modulo 4 is $\{0, 1, 2, 3\}$. Some other complete residue systems modulo 4 include:

- $\{1, 2, 3, 4\}$
- $\{13, 14, 15, 16\}$
- $\{-2, -1, 0, 1\}$
- $\{-13, 4, 17, 18\}$
- $\{-5, 0, 6, 21\}$
- $\{27, 32, 37, 42\}$

Some sets that are *not* complete residue systems modulo 4 are:

- $\{-5, 0, 6, 22\}$, since 6 is congruent to 22 modulo 4.
- $\{5, 15\}$, since a complete residue system modulo 4 must have exactly 4 incongruent residue classes.

Reduced residue systems

Given the Euler's totient function $\varphi(m)$, any set of $\varphi(m)$ integers that are relatively prime to m and mutually incongruent under modulus m is called a **reduced residue system modulo m**.[5] The set $\{5, 15\}$ from above, for example, is an instance of a reduced residue system modulo 4.

Covering systems

Covering systems represent yet another type of residue system that may contain residues with varying moduli.

Integers modulo *m*

Remark: In the context of this paragraph, the modulus m is almost always taken as positive.

The set of all congruence classes modulo m is called the **ring of integers modulo m**,[6] and is denoted $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/m$, or $\mathbb{Z}_m$.[7] The notation $\mathbb{Z}_m$ is, however, not recommended because it can be confused with the set of m-adic integers. The ring $\mathbb{Z}/m\mathbb{Z}$ is fundamental to various branches of mathematics (see *§ Applications* below).

For $m > 0$ one has

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{a}_m \mid a \in \mathbb{Z}\} = \left\{\overline{0}_m, \overline{1}_m, \overline{2}_m, \ldots, \overline{m-1}_m\right\}.$$

When $m = 1$, $\mathbb{Z}/m\mathbb{Z}$ is the zero ring; when $m = 0$, $\mathbb{Z}/m\mathbb{Z}$ is not an empty set; rather, it is isomorphic to $\mathbb{Z}$, since $\overline{a}_0 = \{a\}$.

Addition, subtraction, and multiplication are defined on $\mathbb{Z}/m\mathbb{Z}$ by the following rules:

- $\overline{a}_m + \overline{b}_m = \overline{(a+b)}_m$

- $\overline{a}_m - \overline{b}_m = \overline{(a-b)}_m$
- $\overline{a}_m \overline{b}_m = \overline{(ab)}_m$.

The properties given before imply that, with these operations, $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring. For example, in the ring $\mathbb{Z}/24\mathbb{Z}$, one has

$$\overline{12}_{24} + \overline{21}_{24} = \overline{33}_{24} = \overline{9}_{24}$$

as in the arithmetic for the 24-hour clock.

The notation $\mathbb{Z}/m\mathbb{Z}$ is used because this ring is the quotient ring of $\mathbb{Z}$ by the ideal $m\mathbb{Z}$, the set formed by all $k\ m$ with $k \in \mathbb{Z}$.

Considered as a group under addition, $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group, and all cyclic groups are isomorphic with $\mathbb{Z}/m\mathbb{Z}$ for some m.[8]

The ring of integers modulo m is a field if and only if m is prime (this ensures that every nonzero element has a multiplicative inverse). If $m = p^k$ is a prime power with $k > 1$, there exists a unique (up to isomorphism) finite field $\mathrm{GF}(m) = \mathbb{F}_m$ with m elements, which is *not* isomorphic to $\mathbb{Z}/m\mathbb{Z}$, which fails to be a field because it has zero-divisors.

If $m > 1$, $(\mathbb{Z}/m\mathbb{Z})^\times$ denotes the multiplicative group of the integers modulo m that are invertible. It consists of the congruence classes a_m, where a is coprime to m; these are precisely the classes possessing a multiplicative inverse. They form an abelian group under multiplication; its order is $\varphi(m)$, where φ is Euler's totient function

Applications

In pure mathematics, modular arithmetic is one of the foundations of number theory, touching on almost every aspect of its study, and it is also used extensively in group theory, ring theory, knot theory, and abstract algebra. In applied mathematics, it is used in computer algebra, cryptography, computer science, chemistry and the visual and musical arts.

A very practical application is to calculate checksums within serial number identifiers. For example, International Standard Book Number (ISBN) uses modulo 11 (for 10-digit ISBN) or modulo 10 (for 13-digit ISBN) arithmetic for error detection. Likewise, International Bank Account Numbers (IBANs), for example, make use of modulo 97 arithmetic to spot user input errors in bank account numbers. In chemistry, the last digit of the CAS registry number (a unique identifying number for each chemical compound) is a check digit, which is calculated by taking the last digit of the first two parts of the CAS registry number times 1, the previous digit times 2, the previous digit times 3 etc., adding all these up and computing the sum modulo 10.

In cryptography, modular arithmetic directly underpins public key systems such as RSA and Diffie–Hellman, and provides finite fields which underlie elliptic curves, and is used in a variety of symmetric key algorithms including Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and RC4. RSA and Diffie–Hellman use modular exponentiation.

In computer algebra, modular arithmetic is commonly used to limit the size of integer coefficients in intermediate calculations and data. It is used in polynomial factorization, a problem for which all known efficient algorithms use modular arithmetic. It is used by the most efficient implementations of polynomial greatest common divisor, exact linear algebra and Gröbner basis algorithms over the integers and the rational numbers. As posted on Fidonet in the 1980s and archived at Rosetta Code, modular arithmetic was used to disprove Euler's sum of powers conjecture on a Sinclair QL microcomputer using just one-fourth of the integer precision used by a CDC 6600 supercomputer to disprove it two decades earlier via a brute force search.[9]

In computer science, modular arithmetic is often applied in bitwise operations and other operations involving fixed-width, cyclic data structures. The modulo operation, as implemented in many programming languages and calculators, is an application of modular arithmetic that is often used in this context. The logical operator XOR sums 2 bits, modulo 2.

The use of long division to turn a fraction into a repeating decimal in any base b is equivalent to modular multiplication of b modulo the denominator. For example, for decimal, b = 10.

In music, arithmetic modulo 12 is used in the consideration of the system of twelve-tone equal temperament, where octave and enharmonic equivalency occurs (that is, pitches in a 1:2 or 2:1 ratio are equivalent, and C-sharp is considered the same as D-flat).

The method of casting out nines offers a quick check of decimal arithmetic computations performed by hand. It is based on modular arithmetic modulo 9, and specifically on the crucial property that $10 \equiv 1 \pmod 9$.

Arithmetic modulo 7 is used in algorithms that determine the day of the week for a given date. In particular, Zeller's congruence and the Doomsday algorithm make heavy use of modulo-7 arithmetic.

More generally, modular arithmetic also has application in disciplines such as law (e.g., apportionment), economics (e.g., game theory) and other areas of the social sciences, where proportional division and allocation of resources plays a central part of the analysis.

Computational complexity

Since modular arithmetic has such a wide range of applications, it is important to know how hard it is to solve a system of congruences. A linear system of congruences can be solved in polynomial time with a form of Gaussian elimination, for details see linear congruence theorem. Algorithms, such as Montgomery reduction, also exist to allow simple arithmetic operations, such as multiplication and exponentiation modulo m, to be performed efficiently on large numbers.

Some operations, like finding a discrete logarithm or a quadratic congruence appear to be as hard as integer factorization and thus are a starting point for cryptographic algorithms and encryption. These problems might be NP-intermediate.

Solving a system of non-linear modular arithmetic equations is NP-complete.[10]

See also

- Boolean ring
- Circular buffer
- Division (mathematics)
- Finite field
- Legendre symbol
- Modular exponentiation
- Modulo (mathematics)
- Multiplicative group of integers modulo n
- Pisano period (Fibonacci sequences modulo *n*)
- Primitive root modulo n
- Quadratic reciprocity
- Quadratic residue
- Rational reconstruction (mathematics)
- Reduced residue system
- Serial number arithmetic (a special case of modular arithmetic)
- Two-element Boolean algebra
- Topics relating to the group theory behind modular arithmetic:
  - Cyclic group
  - Multiplicative group of integers modulo n
- Other important theorems relating to modular arithmetic:
  - Carmichael's theorem
  - Chinese remainder theorem
  - Euler's theorem
  - Fermat's little theorem (a special case of Euler's theorem)
  - Lagrange's theorem
  - Thue's lemma

Notes

1. Sandor Lehoczky; Richard Rusczky (2006). David Patrick (ed.). *the Art of Problem Solving*. Vol. 1 (7 ed.). AoPS Incorporated. p. 44. ISBN 0977304566.
2. Weisstein, Eric W. "Modular Arithmetic" (https://mathworld.wolfram.com/ModularArithmetic.html). *Wolfram MathWorld*. Archived (https://web.archive.org/web/20230714132828/https://mathworld.wolfram.com/ModularArithmetic.html) from the original on 2023-07-14. Retrieved 2020-08-12.
3. Pettofrezzo & Byrkit (1970, p. 90)
4. Long (1972, p. 78)
5. Long (1972, p. 85)
6. It is a ring, as shown below.
7. "2.3: Integers Modulo n" (https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Book%3A_Introduction_to_Algebraic_Structures_(Denton)/02%3A_Groups_I/2.0

3%3A_Integers_Modulo_n). *Mathematics LibreTexts*. 2013-11-16. Archived (https://web.archive.org/web/20210419035455/https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Book%3A_Introduction_to_Algebraic_Structures_(Denton)/02%3A_Groups_I/2.03%3A_Integers_Modulo_n) from the original on 2021-04-19. Retrieved 2020-08-12.

8. Sengadir T., *Discrete Mathematics and Combinatorics (https://books.google.com/books?id=nglisrt9IewC&pg=PA293&dq=%22Zn+is+generated+by+1%22)*, p. 293, at Google Books
9. "Euler's sum of powers conjecture" (https://rosettacode.org/wiki/Euler%27s_sum_of_powers_conjecture#QL_SuperBASIC). *rosettacode.org*. Archived (https://web.archive.org/web/20230326025754/https://rosettacode.org/wiki/Euler%27s_sum_of_powers_conjecture#QL_SuperBASIC) from the original on 2023-03-26. Retrieved 2020-11-11.
10. Garey, M. R.; Johnson, D. S. (1979). *Computers and Intractability, a Guide to the Theory of NP-Completeness* (https://archive.org/details/computersintract0000gare). W. H. Freeman. ISBN 0716710447.

References

- John L. Berggren. "modular arithmetic" (https://www.britannica.com/EBchecked/topic/920687/modular-arithmetic). Encyclopædia Britannica.
- Apostol, Tom M. (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, ISBN 978-0-387-90163-3, MR 0434929 (https://mathscinet.ams.org/mathscinet-getitem?mr=0434929), Zbl 0335.10001 (https://zbmath.org/?format=complete&q=an:0335.10001). See in particular chapters 5 and 6 for a review of basic modular arithmetic.
- Maarten Bullynck "Modular Arithmetic before C.F. Gauss. Systematisations and discussions on remainder problems in 18th-century Germany (https://web.archive.org/web/20131102014013/http://www.kuttaka.org/Gauss_Modular.pdf)"
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.3: Modular arithmetic, pp. 862–868.
- Anthony Gioia (http://genealogy.math.ndsu.nodak.edu/id.php?id=3545), *Number Theory, an Introduction* Reprint (2001) Dover. ISBN 0-486-41449-3.
- Long, Calvin T. (1972). *Elementary Introduction to Number Theory* (2nd ed.). Lexington: D. C. Heath and Company. LCCN 77171950 (https://lccn.loc.gov/77171950).
- Pettofrezzo, Anthony J.; Byrkit, Donald R. (1970). *Elements of Number Theory* (https://archive.org/details/elementsofnumber0000pett). Englewood Cliffs: Prentice Hall. ISBN 9780132683005. LCCN 71081766 (https://lccn.loc.gov/71081766).
- Sengadir, T. (2009). *Discrete Mathematics and Combinatorics*. Chennai, India: Pearson Education India. ISBN 978-81-317-1405-8. OCLC 778356123 (https://search.worldcat.org/oclc/778356123).

External links

- "Congruence" (https://www.encyclopediaofmath.org/index.php?title=Congruence), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- In this modular art (https://web.archive.org/web/20060101075602/http://britton.disted.camosun.bc.ca/modart/jbmodart.htm) article, one can learn more about applications of modular arithmetic in art.
- An article (https://web.archive.org/web/20160220061222/http://mersennewiki.org/index.php/Modular_arithmetic) on modular arithmetic on the GIMPS wiki

- Modular Arithmetic and patterns in addition and multiplication tables (http://www.cut-the-knot.org/blue/Modulo.shtml)
