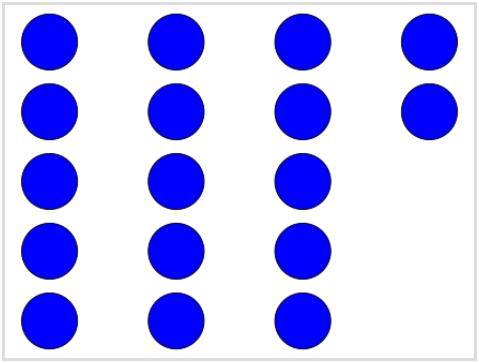
WIKIPEDIA
The Free Encyclopedia

Euclidean division

In arithmetic, **Euclidean division** – or **division with remainder** – is the process of dividing one integer (the dividend) by another (the divisor), in a way that produces an integer quotient and a natural number remainder strictly smaller than the absolute value of the divisor. A fundamental property is that the quotient and the remainder exist and are unique, under some conditions. Because of this uniqueness, *Euclidean division* is often considered without referring to any method of computation, and without explicitly computing the quotient and the remainder. The methods of computation are called integer division algorithms, the best known of which being long division.



17 is divided into 3 groups of 5, with 2 as leftover. Here, the dividend is 17, the divisor is 3, the quotient is 5, and the remainder is 2 (which is strictly smaller than the divisor 3), or more symbolically, 17 = (3 × 5) + 2.

Euclidean division, and algorithms to compute it, are fundamental for many questions concerning integers, such as the Euclidean algorithm for finding the greatest common divisor of two integers,[1] and modular arithmetic, for which only remainders are considered.[2] The operation consisting of computing only the remainder is called the *modulo operation*,[3] and is used often in both mathematics and computer science.

Division theorem

Euclidean division is based on the following result, which is sometimes called **Euclid's division lemma**.

Given two integers a and b, with $b \neq 0$, there exist unique integers q and r such that

$$a = bq + r$$

and

$$0 \leq r < |b|,$$

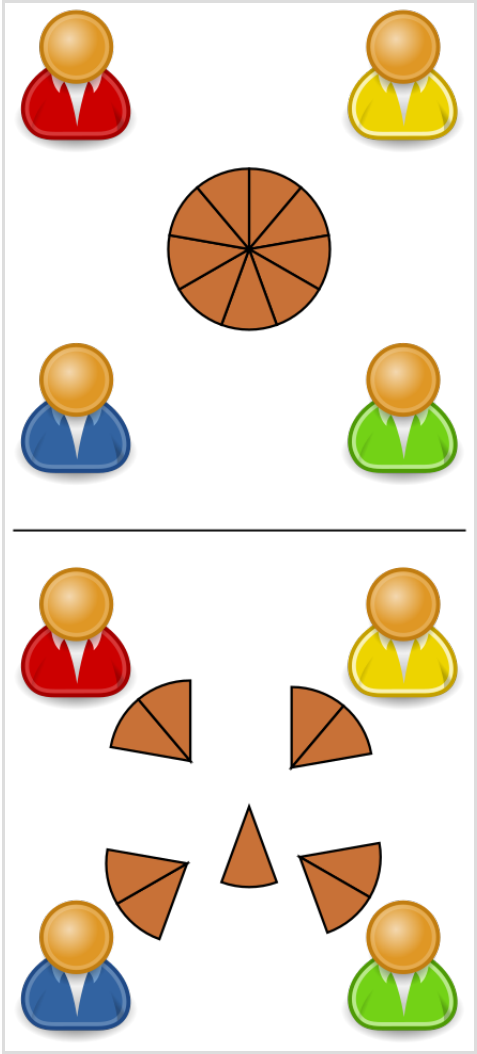
where $|b|$ denotes the absolute value of b.[4]

In the above theorem, each of the four integers has a name of its own: a is called the *dividend*, b is called the *divisor*, q is called the *quotient* and r is called the *remainder*.

The computation of the quotient and the remainder from the dividend and the divisor is called *division*, or in case of ambiguity, *Euclidean division*. The theorem is frequently referred to as the *division algorithm* (although it is a theorem and not an algorithm), because its proof as given below lends itself to a simple division algorithm for computing q and r (see the section Proof for more).

Division is not defined in the case where $b = 0$; see division by zero.

For the remainder and the modulo operation, there are conventions other than $0 \leq r < |b|$, see § Other intervals for the remainder.



The pie has 9 slices, so each of the 4 people receives 2 slices and 1 is left over.

Generalization

Although originally restricted to integers, Euclidean division and the division theorem can be generalized to univariate polynomials over a field and to Euclidean domains.

In the case of polynomials, the main difference is that the inequalities $0 \leq r < |b|$ are replaced with

$$\deg r < \deg b,$$

where **deg** denotes the polynomial degree.

In the generalization to Euclidean domains, the inequality becomes

$$f(r) < f(b),$$

where f denote a specific function from the domain to the natural numbers called a "Euclidean function".

History

Although "Euclidean division" is named after Euclid, it seems that he did not know the existence and uniqueness theorem, and that the only computation method that he knew was the division by repeated subtraction.

Before the discovery of Hindu–Arabic numeral system, which was introduced in Europe during the 13th century by Fibonacci, division was extremely difficult, and only the best mathematicians were able to do it. Presently, most division algorithms, including long division, are based on this notation or its variants, such as binary numerals. A notable exception is Newton–Raphson division, which is independent from any numeral system.

The term "Euclidean division" was introduced during the 20th century as a shorthand for "division of Euclidean rings". It has been rapidly adopted by mathematicians for distinguishing this division from the other kinds of division of numbers.

Intuitive example

Suppose that a pie has 9 slices and they are to be divided evenly among 4 people. Using Euclidean division, 9 divided by 4 is 2 with remainder 1. In other words, each person receives 2 slices of pie, and there is 1 slice left over.

This can be confirmed using multiplication, the inverse of division: if each of the 4 people received 2 slices, then $4 \times 2 = 8$ slices were given out in total. Adding the 1 slice remaining, the result is 9 slices. In summary: $9 = 4 \times 2 + 1$.

In general, if the number of slices is denoted a and the number of people is denoted b, then one can divide the pie evenly among the people such that each person receives q slices (the quotient), with some number of slices $r < b$ being the leftover (the remainder). In which case, the equation $a = bq + r$ holds.

If 9 slices were divided among 3 people instead of 4, then each would receive 3 and no slice would be left over, which means that the remainder would be zero, leading to the conclusion that 3 *evenly divides* 9, or that 3 *divides* 9.

Euclidean division can also be extended to negative dividend (or negative divisor) using the same formula; for example $-9 = 4 \times (-3) + 3$, which means that −9 divided by 4 is −3 with remainder 3.

Examples

- If $a = 7$ and $b = 3$, then $q = 2$ and $r = 1$, since $7 = 3 \times 2 + 1$.
- If $a = 7$ and $b = -3$, then $q = -2$ and $r = 1$, since $7 = -3 \times (-2) + 1$.
- If $a = -7$ and $b = 3$, then $q = -3$ and $r = 2$, since $-7 = 3 \times (-3) + 2$.
- If $a = -7$ and $b = -3$, then $q = 3$ and $r = 2$, since $-7 = -3 \times 3 + 2$.

Proof

The following proof of the division theorem relies on the fact that a decreasing sequence of non-negative integers stops eventually. It is separated into two parts: one for existence and another for uniqueness of q and r. Other proofs use the well-ordering principle (i.e., the assertion that every non-empty set of non-negative integers has a smallest element) to make the reasoning simpler, but have the disadvantage of not providing directly an algorithm for solving the division (see § Effectiveness for more).[5]

Existence

For proving the existence of Euclidean division, one can suppose $b > 0$, since, if $b < 0$, the equality $a = bq + r$ can be rewritten $a = (-b)(-q) + r$. So, if the latter equality is a Euclidean division with $-b > 0$, the former is also a Euclidean division.

Given $b > 0$ and a, there are integers q_1 and $r_1 \geq 0$ such that $a = bq_1 + r_1$; for example, $q_1 = 0$ and $r_1 = a$ if $a \geq 0$, and otherwise $q_1 = a$ and $r_1 = a - ab$.

Let q and r be such a pair of numbers for which r is nonnegative and minimal. If $r < b$. we have Euclidean division. Thus, we have to prove that, if $r \geq b$, then r is not minimal. Indeed, if $r \geq b$, one has $a = b(q + 1) + (r - b)$, with $0 \leq r - b < r$, and r is not minimal

This proves the existence in all cases. This provides also an algorithm for computing the quotient and the remainder, by starting from $q = 0$ (if $a \geq 0$) and adding 1 to it until $a - bq < b$. However, this algorithm is not efficient, since its number of steps is of the order of a/b

Uniqueness

The pair of integers r and q such that $a = bq + r$ is unique, in the sense that there can be no other pair of integers that satisfy the same condition in the Euclidean division theorem. In other words, if we have another division of a by b, say $a = bq' + r'$ with $0 \leq r' < |b|$, then we must have that

$$q' = q \text{ and } r' = r.$$

To prove this statement, we first start with the assumptions that

$$0 \leq r < |b|$$
$$0 \leq r' < |b|$$
$$a = bq + r$$
$$a = bq' + r'$$

Subtracting the two equations yields

$$b(q - q') = r' - r.$$

So b is a divisor of $r' - r$. As

$$|r' - r| < |b|$$

by the above inequalities, one gets

$$r' - r = 0,$$

and

$$b(q - q') = 0.$$

Since $b \neq 0$, we get that $r = r'$ and $q = q'$, which proves the uniqueness part of the Euclidean division theorem.

Effectiveness

In general, an existence proof does not provide an algorithm for computing the existing quotient and remainder, but the above proof does immediately provide an algorithm (see Division algorithm#Division by repeated subtraction), even though it is not a very efficient one as it requires as many steps as the size of the quotient. This is related to the fact that it uses only additions, subtractions and comparisons of integers, without involving multiplication, nor any particular representation of the integers such as decimal notation.

In terms of decimal notation, long division provides a much more efficient algorithm for solving Euclidean divisions. Its generalization to binary and hexadecimal notation provides further flexibility and possibility for computer implementation. However, for large inputs, algorithms that reduce division to multiplication, such as Newton–Raphson, are usually preferred, because they only need a time which is proportional to the time of the multiplication needed to verify the result —independently of the multiplication algorithm which is used (for more, see Division algorithm#Fast division methods).

Variants

The Euclidean division admits a number of variants, some of which are listed below.

Other intervals for the remainder

In Euclidean division with d as divisor, the remainder is supposed to belong to the interval $[0, d)$ of length $|d|$. Any other interval of the same length may be used. More precisely, given integers m, a, d with $m > 0$, there exist unique integers q and r with $d \leq r < m + d$ such that $a = mq + r$.

In particular, if $d = -\left\lfloor \frac{m}{2} \right\rfloor$ then $-\left\lfloor \frac{m}{2} \right\rfloor \leq r < m - \left\lfloor \frac{m}{2} \right\rfloor$. This division is called the *centered division*, and its remainder r is called the *centered remainder* or the least absolute remainder.

This is used for approximating real numbers: Euclidean division defines truncation, and centered division defines rounding.

Montgomery division

Given integers a, m and R, with $m > 0$ and $\gcd(R, m) = 1$, let R^{-1} be the modular multiplicative inverse of R (i.e., $0 < R^{-1} < m$ with $R^{-1}R - 1$ being a multiple of m), then there exist unique integers q and r with $0 \leq r < m$ such that $a = mq + R^{-1} \cdot r$. This result generalizes Hensel's odd division (1900).[6]

The value r is the N-residue defined in Montgomery reduction.

In Euclidean domains

Euclidean domains (also known as **Euclidean rings**)[7] are defined as integral domains which support the following generalization of Euclidean division:

> Given an element a and a non-zero element b in a Euclidean domain R equipped with a **Euclidean function** d (also known as a **Euclidean valuation**[8] or **degree function**[7]), there exist q and r in R such that $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$.

Uniqueness of q and r is not required.[1] It occurs only in exceptional cases, typically for univariate polynomials, and for integers, if the further condition $r \geq 0$ is added.

Examples of Euclidean domains include fields, polynomial rings in one variable over a field, and the Gaussian integers. The Euclidean division of polynomials has been the object of specific developments.

See also

- Euclid's lemma
- Euclidean algorithm

Notes

1. "Division and Euclidean algorithms" (https://web.archive.org/web/20210506140331/http://www-groups.mcs.st-andrews.ac.uk/~john/MT4517/Lectures/L6.html). *www-groups.mcs.st-andrews.ac.uk*. Archived from the original (http://www-groups.mcs.st-andrews.ac.uk/~john/MT4517/Lectures/L6.html) on 2021-05-06. Retrieved 2019-11-15.
2. "What is modular arithmetic?" (https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic). *Khan Academy*. Retrieved 2019-11-15.
3. "Fun With Modular Arithmetic – BetterExplained" (https://betterexplained.com/articles/fun-with-

modular-arithmetic/). *betterexplained.com*. Retrieved 2019-11-15.
4. Burton, David M. (2010). *Elementary Number Theory*. McGraw-Hill. pp. 17–19. ISBN 978-0-07-338314-9.
5. Durbin, John R. (1992). *Modern Algebra : an Introduction* (http://www.wiley.com/WileyCDA/WileyTitle/productCd-EHEP000258.html) (3rd ed.). New York: Wiley. p. 63. ISBN 0-471-51001-7.
6. Haining Fan; Ming Gu; Jiaguang Sun; Kwok-Yan Lam (2012). "Obtaining More Karatsuba-Like Formulae over the Binary Field". *IET Information Security*. **6** (1): 14–19. CiteSeerX 10.1.1.215.1576 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.215.1576). doi:10.1049/iet-ifs.2010.0114 (https://doi.org/10.1049%2Fiet-ifs.2010.0114).
7. Rotman 2006, p. 267
8. Fraleigh 1993, p. 376

References

- Fraleigh, John B. (1993), *A First Course in Abstract Algebra* (5th ed.), Addison-Wesley, ISBN 978-0-201-53467-2
- Rotman, Joseph J. (2006), *A First Course in Abstract Algebra with Applications* (3rd ed.), Prentice-Hall, ISBN 978-0-13-186267-8

Retrieved from "https://en.wikipedia.org/w/index.php?title=Euclidean_division&oldid=1214273580"