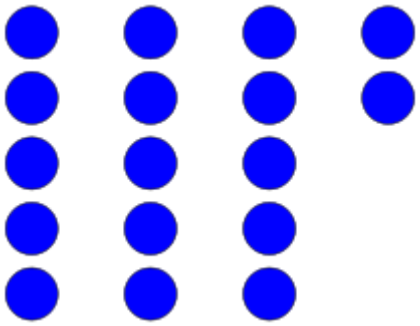
Euclidean division

In arithmetic, **Euclidean division** is the process of division of two integers, which produces a quotient and a remainder smaller than the divisor. Its main property is that the quotient and 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 being long division.

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, and modular arithmetic, for which only remainders are considered. The operation consisting of computing only the remainder is called the *modulo operation*.



17 is divided into 3 groups of 5 with 2 left over. Here the dividend is 17, the divisor is 5, the quotient is 3, and the remainder is 2 (strictly smaller than the divisor 5).
17 = (5 × 3) + 2

Contents

Statement of the theorem

History

Intuitive example

Examples

Proof

- Existence
- Uniqueness
- Other proofs

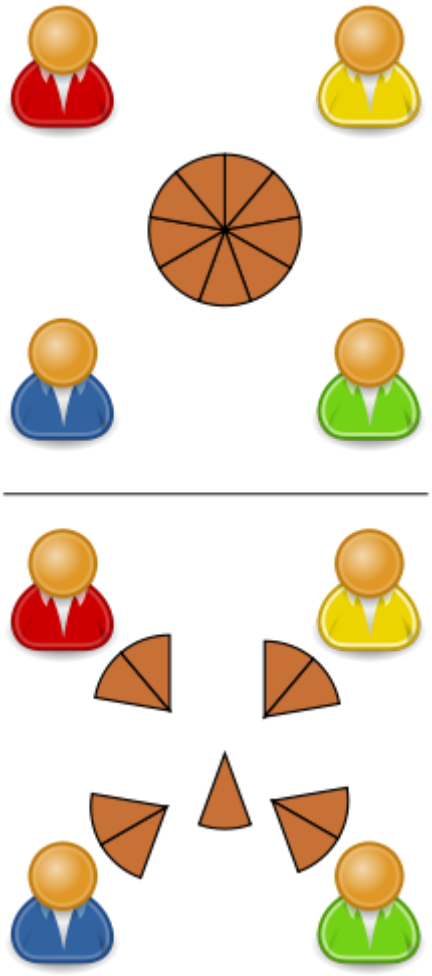
Effectiveness

Generalizations

- In other domains
- Generalized division algorithms
  - First generalization
  - Second generalization

Notes

References



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

Statement of the theorem

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.[1]

The four integers that appear in this theorem have been given names: 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 also provides a simple division algorithm for computing q and r.

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 $0 \le r < |b|$, see § Generalized division algorithms.

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. In fact, the long division algorithm requires this notation.

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 all. 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 b, one can divide the pie evenly among the people such that each person receives q slices (the quotient) and some number of slices $r < b$ are left over (the remainder). Regardless, the equation $a = bq + r$ holds.

If 9 slices were divided among 3 people instead of 4, each would receive 3 and no slices would be left over. In this case the remainder is zero, and it is said that 3 *evenly divides* 9, or that 3 *divides* 9.

Euclidean division can also be extended to negative integers using the same formula; for example $-9 = 4 \times (-3) + 3$, so −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 proof consists of two parts — first, the proof of the existence of q and r, and second, the proof of the uniqueness of q and r.

Existence

Consider first the case $b < 0$. Setting $b' = -b$ and $q' = -q$, the equation $a = bq + r$ may be rewritten $a = b'q' + r$ and the inequality $0 \le r < |b|$ may be rewritten $0 \le r < b'$. This reduces the existence for the case $b < 0$ to that of the case $b > 0$.

Similarly, if $a < 0$ and $b > 0$, setting $a' = -a$, $q' = -q - 1$ and $r' = b - r$, the equation $a = bq + r$ may be rewritten $a' = bq' + r'$ and the inequality $0 \le r < b$ may be rewritten $0 \le r' < b$. Thus the proof of the existence is reduced to the case $a \ge 0$ and $b > 0$ and we consider only this case in the remainder of the proof.

Let q_1 and r_1, both nonnegative, be such that $a = bq_1 + r_1$, for example $q_1 = 0$ and $r_1 = a$. If $r_1 < b$, we are done. Otherwise $q_2 = q_1 + 1$ and $r_2 = r_1 - b$ satisfy $a = bq_2 + r_2$ and $0 \le r_2 < r_1$. Repeating this process one gets eventually $q = q_k$ and $r = r_k$ such that $a = bq + r$ and $0 \le r < b$.

This proves the existence and also gives a simple division algorithm to compute the quotient and the remainder. However this algorithm needs q steps and is thus not efficient.

Uniqueness

Suppose there exists q, q', r, r' with $0 \le r, r' < |b|$ such that $a = bq + r$ and $a = bq' + r'$. Adding the two inequalities $0 \le r < |b|$ and $-|b| < -r' \le 0$ yields $-|b| < r - r' < |b|$, that is $|r - r'| < |b|$.

Subtracting the two equations yields: $b(q' - q) = (r - r')$. Thus $|b|$ divides $|r - r'|$. If $|r - r'| \ne 0$ this implies $|b| \le |r - r'|$, contradicting previous inequality. Thus, $r = r'$ and $b(q' - q) = 0$. As $b \ne 0$, this implies $q = q'$, proving uniqueness.

Other proofs

Some proofs of the algorithm rely on the Well-ordering principle.[2]

Effectiveness

Generally, an existence proof does not provide an algorithm to compute the existing object, but the above proof provides immediately an algorithm (see Division algorithm#Division by repeated subtraction). However this is not a very efficient method, as it requires as many steps as the size of the quotient. This is related to the fact that it only uses addition, subtraction and comparison of the 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 division algorithm. Its generalization to binary notation allows to use it in a computer. However, for large inputs, algorithms that reduce division to multiplication, like Newton–Raphson one, are usually preferred, because they 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.

Generalizations

In other domains

Euclidean domains (also known as **Euclidean rings**)[3] 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**,[4] or **degree function**[3]), there exist q and r in R such that $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$. Unlike in the integer case, q and r need not be unique.

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 Polynomial long division, Polynomial greatest common divisor#Euclidean division and Polynomial greatest common divisor#Pseudo-remainder sequences

Generalized division algorithms

The division algorithm admits a number of generalizations, some of which are listed below

First generalization

Given integers m, a, d with $m > 0$, there exist unique integers q and r with $d \leq r < m + d$ such that $a = mq + r$.

Especially, if $d = -\left\lfloor \frac{m}{2} \right\rfloor$ then $-\left\lfloor \frac{m}{2} \right\rfloor \leq r < m - \left\lfloor \frac{m}{2} \right\rfloor$. In this case, r is called the least absolute remainder. As an application of this generalization, the original Euclidean algorithm for integers can be slightly sped up.

Second generalization

Given integers a, m and R, with $m > 0$ and $\gcd(R, m) = 1$, let R^{-1} be the modular multiplicative inverse of R (that is $0 < R^{-1} < m$, and $R^{-1}R - 1$ is 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).[5]

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

Notes

1. Burton, David M. (2010). *Elementary Number Theory*. McGraw-Hill. pp. 17–19. ISBN 978-0-07-338314-9
2. 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.
3. Rotman 2006, p. 267
4. Fraleigh 1993, p. 376
5. 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.

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