**Eucliean division**

PHAM NHU QUYNH

Quynhquych09@gmail.com

ARTICLE INFO ABSTRACT

------------------------ ----------------------------------------------------

Keyword:

Eucliean division

Keywords:

Euclid’s division algorithm suggests a method that deals with the divisibility of integers. In simple words, it says any positive integer *a* can be divided by another positive integer *b* in such a way that the remainder *r*obtained is smaller than *b*.

Eucliean division

1. **Introduction**

Euclidean algorithm, procedure for finding the greatest common divisor (GCD) of two numbers, described by the Greek mathematician Euclid [1]in his Elements (c. 300 BC) . The method is computationally efficient and, with minor modifications, is still used by computers.

Before the discovery of Hindu–Arabic numeral system, which was introduced in Europe during the 13th century by Fibonacci [2], 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.

Eucliean is about division of integers. For polynomials, see Euclidean division of polynomials. For other domains, see Euclidean domain.

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.

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,[3] and modular arithmetic, for which only remainders are considered.[4] The operation consisting of computing only the remainder is called the modulo operation,[5] and is used often in both mathematics and computer science.

## Background

*Division* is one of the four basic operations of arithmetic. The other operations are addition, subtraction, and multiplication.

At an elementary level the division of two natural numbers is, among other possible interpretations, the process of calculating the number of times one number is contained within another.This number of times need not be an integer. For example, if 20 apples are divided evenly between 4 people, everyone receives 5 apples .

The division with remainder or Euclidean division of two natural numbers provides an integer quotient, which is the number of times the second number is completely contained in the first number, and a remainder, which is the part of the first number that remains, when in the course of computing the quotient, no further full chunk of the size of the second number can be allocated. For example, if 21 apples are divided between 4 people, everyone receives 5 apples again, and 1 apple remains.

For division to always yield one number rather than a quotient plus a remainder, the natural numbers must be extended to rational numbers or real numbers. In these enlarged number systems, division is the inverse operation to multiplication, that is a = c / b means a × b = c, as long as b is not zero. If b = 0, then this is a division by zero, which is not defined.In the 21-apples example, everyone would receive 5 apple and a quarter of an apple, thus avoiding any leftover.

Both forms of division appear in various algebraic structures, different ways of defining mathematical structure. Those in which a Euclidean division (with remainder) is defined are called Euclidean domains and include polynomial rings in one indeterminate (which define multiplication and addition over single-variabled formulas). Those in which a division (with a single result) by all nonzero elements is defined are called fields and division rings. In a ring the elements by which division is always possible are called the units (for example, 1 and −1 in the ring of integers). Another generalization of division to algebraic structures is the quotient group, in which the result of "division" is a group rather than a number.

1. **Main Results**

**3.1 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 ≠ 0, there exist unique integers q and r such that

a = bq + r

and

0 ≤ r < |b|,

where |b| denotes the absolute value of b.

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.

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 ≤ r < |b|.

**3.2 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 × 2 = 8 slices were given out in total. Adding the 1 slice remaining, the result is 9 slices. In summary: 9 = 4 × 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](https://en.wikipedia.org/wiki/Divides" \o "Divides)* 9.

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

**3.3 Examples**

If a = 7 and b = 3, then q = 2 and r = 1, since 7 = 3 × 2 + 1.

If a = 7 and b = −3, then q = −2 and r = 1, since 7 = −3 × (−2) + 1.

If a = −7 and b = 3, then q = −3 and r = 2, since −7 = 3 × (−3) + 2.

If a = −7 and b = −3, then q = 3 and r = 2, since −7 = −3 × 3 + 2.

**3.4 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.

* + 1. **Existence**

Consider first the case b < 0. Setting b' = –b and q' = –q, the equation a = bq + r may be rewritten as a = b'q' + r and the inequality 0 ≤ r < |b| may be rewritten as 0 ≤ 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 as a' = bq' + r′, and the inequality 0 ≤ r < |b| may be rewritten as 0 ≤ r' < |b|. Thus the proof of the existence is reduced to the case a ≥ 0 and b > 0 — which will be considered in the remainder of the proof.

Let q1 = 0 and r1 = a, then these are non-negative numbers such that a = bq1 + r1. If r1 < b then the division is complete, so suppose r1 ≥ b. Then defining q2 = q1 + 1 and r2 = r1 – b, one has a = bq2 + r2 with 0 ≤ r2 < r1. As there are only r1 non-negative integers less than r1, one only needs to repeat this process at most r1 times to reach the final quotient and the remainder. That is, there exist a natural number k ≤ r1 such that a = bqk + rk and 0 ≤ rk < |b|.

This proves the existence and also gives a simple division algorithm for computing the quotient and the remainder. However, this algorithm is not efficient, since its number of steps is of the order of a/b.

* + 1. **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 ≤ r' < |b|, then we must have that

q' = q and r' = r.

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

0 ≤ r < |b|

0 ≤ 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 ≠ 0, we get that r = r′ and q = q′, which proves the uniqueness part of the Euclidean division theorem.

* + 1. **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 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 more.

1. **Conclusion**

In this article, we have studied the introduction and definition of Euclid’s division lemma. We also studied Euclid’s division algorithm. Euclid’s Division Lemma is the proven statement, that is used in the division of integers. Euclid’s division lemma is used to find the HCF of numbers. It is also important to note that, Lemma is also helpful in finding properties of numbers such as cube numbers, square numbers, even and odd numbers, etc. We discussed the various uses of Euclid’s division lemma, such as finding the HCF of numbers using Euclid’s division lemma and discussing the properties of even and odd numbers.

**\*References**

[1] <https://www.britannica.com/biography/Euclid-Greek-mathematician>

[2] <https://www.britannica.com/biography/Fibonacci>

[3] "Division and Euclidean algorithms". www-groups.mcs.st-andrews.ac.uk. Retrieved 2019-11-15.

[4] "What is modular arithmetic?". Khan Academy. Retrieved 2019-11-15.

[5] "Fun With Modular Arithmetic – BetterExplained". betterexplained.com. Retrieved 2019-11-15.