IJDIAS International Journal of Discoveries and Innovations in Applied Sciences

| e-ISSN: 2792-3983 | www.openaccessjournals.eu | Volume: 3 Issue: 2

Euclidean Algorithm and Actions on Them

Yuldoshev Mansur Najmiddin ugli
Academic Lyceum of Tashkent State University of Economics lead math science teacher
mansuryuldoshev212901@mail.ru

Abstract. This article covers the basics of the Euclidean algorithm in detail. Euclid proposed an algorithm only for natural numbers and geometric quantities (lengths, areas, volumes).

Keywords: Euclidean algorithm, mathematical properties, polynomials, theorems, proofs, etc.

Euclid's algorithm is an efficient algorithm for finding the greatest common divisor of two integers (or the common measure of two segments). The algorithm is named after the Greek mathematician Euclid (III century BC), who first described it in the VII and X books of the "Beginnings". It is one of the oldest numerical algorithms in use today. At its simplest, Euclid's algorithm is applied to a pair of positive integers and generates a new pair that consists of the smaller number and the difference between the larger and smaller numbers. The process is repeated until the numbers are equal. The found number is the greatest common divisor of the original pair. However, in the 19th century it was generalized to other types of mathematical objects, including Gaussian integers and polynomials in one variable. This led to the appearance in modern general algebra of such a concept as the Euclidean ring. Later, Euclid's algorithm was generalized to other mathematical structures such as knots and multidimensional polynomials. There are many theoretical and practical applications for this algorithm. In particular, it is the basis for the RSA public key cryptographic algorithm, which is widely used in e-commerce. The algorithm is also used in solving linear Diophantine equations, in constructing continued fractions, in the Sturm method. Euclid's algorithm is the main tool for proving theorems in modern number theory, such as Lagrange's four-square theorem and the fundamental theorem of arithmetic. Ancient Greek mathematicians called this algorithm ἀνθυφαίρεσις or ἀνταναίρεσις - "mutual subtraction". This algorithm was not discovered by Euclid, since there is already a mention of it in the Topic of Aristotle (4th century BC) . It is described twice in Euclid's Elements - in Book VII for finding the greatest common divisor of two natural numbers and in Book X for finding the greatest common measure of two homogeneous quantities. In both cases, a geometric description of the algorithm is given to find the "common measure" of two segments.

Historians of mathematics have suggested that it was with the help of Euclid's algorithm (the procedure of successive mutual subtraction) that the existence of incommensurable quantities (the sides and diagonals of a square, or the sides and diagonals of a regular pentagon) was first discovered in ancient Greek mathematics. However, this assumption does not have sufficient documentary evidence. The algorithm for finding the greatest common divisor of two natural numbers is also described in Book I of the ancient Chinese treatise Mathematics in nine books. The computational complexity of the Euclid algorithm has been fully studied. This complexity can be described as the product of the number of division steps required by the algorithm times the computational complexity of one step. The first known analysis of Euclid's algorithm was proposed by Reinaud in 1811. He showed that the number of algorithm steps for a pair of numbers (u, v) is limited to v. He later improved the estimate to v/2 + 2. Émile Léger in 1837 studied the worst case, when successive Fibonacci numbers are used to compute the gcd. Then, in 1841, Pierre Joseph Fink showed that the number of steps in the algorithm does not exceed 2 log2 v + 1. Therefore, the

algorithm runs in polynomial time on the size of the smaller of the pair of numbers (u, v). Fink's analysis was refined by Gabriel Lame in 1844. He showed that the number of steps required to complete the algorithm is no more than five times h - the number of digits in the decimal representation of the smaller of the pair of numbers (u, v).

To find the greatest common divisor of two natural numbers numbers a and b, a>b, often use the Euclidean algorithm, which consists in consecutive divisions of integers defined by the following system of inequalities:

$$\begin{aligned}
a &= bq_1 + r_1, \quad \text{где} \quad 0 < r_1 < b, \\
b &= r_1 q_2 + r_2, \quad \text{где} \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad \text{где} \quad 0 < r_3 < r_2, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad \text{где} \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad \text{где} \quad r_{n+1} = 0.
\end{aligned}$$

The procedure known as the Euclid algorithm arose no later than. 3rd century BC and occurs in the seventh book Euclid (and apparently has an earlier origin). Designed was this algorithm for solving the problem of the commensurability of two segments. The common measure of segments with lengths a and b is such a segment of length d, which can be laid without residue, both in the first segment and in second; it is clear that d = (a, b) is one of the possible solutions (and the only one if you want to find the largest measure). To find the least common multiple of two given numbers, you need to find two as small numbers as possible, such that, multiplying one of them by one given number, and the other by another given number, we get the same product. Therefore, by virtue of the very choice of these numbers, they depend only on ratio of two given numbers.

Using the Euclidean algorithm, the greatest common divisor of numbers a and b can be represented as a linear combination of these numbers, namely, there are integers x0, y0 such that x0a+y0b = gcd(a, b). Such a representation is called a linear expansion of the greatest common divisor of numbers a, b. Let us present an algorithm for finding a decomposition for two numbers. Euclid's algorithm is an efficient algorithm for finding the greatest common divisor of two integers (or the common measure of two segments). The algorithm is named after the Greek mathematician Euclid, who first described it in Books VII and X of the Elements. At its simplest, Euclid's algorithm is applied to a pair of positive integers and generates a new pair that consists of the smaller number and the difference between the larger and smaller numbers. The process is repeated until the numbers are equal. The found number is the greatest common divisor of the original pair. The first description of the algorithm is in Euclid's Elements (circa 300 BC), making it one of the oldest numerical algorithms in use today. The original algorithm was proposed only for natural numbers and geometric lengths (real numbers). However, in the 19th century it was generalized to other types of numbers, such as Gaussian integers and polynomials in one variable. This led to the appearance in modern general algebra of such a concept as the Euclidean ring. Later, Euclid's algorithm was also generalized to other mathematical structures such as knots and multidimensional polynomials. There are many theoretical and practical applications for this algorithm. In particular, it is the basis for the RSA public key cryptographic algorithm, which is widely used in e-commerce. The algorithm is also used in solving linear Diophantine equations, in constructing continued fractions, in the Sturm method. Euclid's algorithm is the main tool for proving theorems in modern number theory, such as Lagrange's four-square theorem and the fundamental theorem of arithmetic.

Ancient Greek mathematicians called this algorithm or - "mutual subtraction". This algorithm was not discovered by Euclid, since there is already a mention of it in the Topic of Aristotle. In Euclid's

Elements, it is described twice - in Book VII for finding the greatest common divisor of two natural numbers and in Book X for finding the greatest common measure of two homogeneous quantities. In both cases, a geometric description of the algorithm is given to find the "common measure" of two segments. Historians of mathematics have suggested that it was with the help of Euclid's algorithm (the procedure of successive mutual subtraction) that the existence of incommensurable quantities (the sides and diagonals of a square, or the sides and diagonals of a regular pentagon) was first discovered in ancient Greek mathematics. However, this assumption does not have sufficient documentary evidence. The algorithm for finding the greatest common divisor of two natural numbers is also described in Book I of the ancient Chinese treatise Mathematics in nine books.

References:

1. Hojiyev J ,Faynleyb A.S. ,,Algebra va sonlar nazariyasi kursi “ , Toshkent, Uzbekiston 2001 y
2. D.Yunusova, A.Yunusov ,, Algebra va sonlar nazariyasi “ Toshkent 2007 y
3. Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev, F.H.Haydarov ,, Algebra va sonlar nazariyasi “ o‟quv qo‟llanma Toshkent 2019
4. Maxmudova D.M. , Do‟stmurodova G.X. , Eshmamatova I.A. ,, Algebra va sonlar nazariyasi “ Toshkent 2020 y
5. B.Z.Usmonov, G.Sh.Togayeva, M.A.Davlatova “O'zgarmas koeffitsientli ikkinchi tartibli bir jinsli differentsial tenglamalarini o'qitishda matematik paketlarni o'rni”./ACADEMIC RESEARCH IN EDUCATIONAL SCIENCES VOLUME 2 | ISSUE 3 | 2021 ISSN: 2181-1385 Scientific Journal Impact Factor (SJIF) 2021: 5.723
6. G.U.Suyunova., B.Z.Usmonov. “BIOLOGIYA FANINI O'RGATISHDA AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARI O'RNI VA VAZIFALARI”. /ACADEMIC RESEARCH IN EDUCATIONAL SCIENCES VOLUME 2 | ISSUE 3 | 2021 ISSN: 2181-1385 Scientific Journal Impact Factor (SJIF) 2021: 5.723