М І Ф

Математика, Інформатика, Фізика: Наука та Освіта, Том 3, № 2 (2026), с. 237–247.
Mathematics, Informatics, Physics: Science and Education, Volume 3, No. 2 (2026), pp. 237–247.
Journal homepage: https://intranet.vspu.edu.ua/miph

UDC 512.712

Weak Euclidean algorithm and linear representation of GCD

Fedir Sokhatsky

Pidstryhach Institute for Applied Problems for Mechanics and Mathematics,
National Academy of Sciences of Ukraine, Department of algebra, Ukraine
fmsokha@ukr.net
https://orcid.org/0000-0003-4969-5651

Abstract. In a ring with an identity element, the equalities $r_{i-1} = r_i q_i + r_{i+1}$, $i = 1, 2, \ldots, n$, are called a *left Euclidean chain*, and—if $r_n \neq 0$ and $r_{n+1} = 0$—a *weak Euclidean algorithm*. For this left chain, the concept of a *left Bézout sequence* $y_1, y_2, \ldots, y_n$ is introduced here for the first time:

$$y_n := 1, \quad y_{n-1} := -q_{n-1}, \quad y_i := y_{i+2} - q_i y_{i+1}, \quad i = n-2, n-3, \ldots, 2, 1.$$

It is proved that for $r_n \neq 0$, Bézout's equalities hold:

$$r_n = r_i y_{i+2} + r_{i+1} y_{i+1} \quad \text{for all} \quad i = 0, 1, \ldots, n-2.$$

If the left Euclidean chain is a left weak Euclidean algorithm, then $r_n = \gcd_\ell(a, b)$ is the left greatest common divisor of the elements $a = r_0$ and $b = r_1$, and for $i = 0$, we obtain its linear representation $\gcd_\ell(a, b) = ay_2 + by_1$. Analogous properties hold for right divisors. In commutative rings, these concepts coincide.

Keywords: weak Euclidean algorithm, linear representation, Bézout sequence, left greatest common divisor, ring with identity element.

1. Introduction

The study of the Euclidean algorithm remains highly relevant, both due to the need to extend its application to new structures within algebraic rings [1, 2, 3, 4] and in the context of mathematics education [5]. Investigating its computational efficiency is of particular importance; for instance, two notable works address this issue as follows:

"The extended GCD (XGCD) calculation, which computes Bézout coefficients b_a, b_b such that $b_a * a_0 + b_b * b_0 = \mathrm{GCD}(a_0, b_0)$, is a critical operation in many cryptographic applications. In particular, large-integer XGCD is computationally dominant for two applications

e-ISSN 3041-1955 DOI: https://doi.org/10.31652/3041-1955-2026-03-02-11
2020 Mathematics Subject Classification: 11A05, 11R04.
© 2026 Sokhatsky F., Creative Commons Attribution 4.0 International Licence.

of increasing interest: verifiable delay functions that square binary quadratic forms within a class group and constant-time modular inversion for elliptic curve cryptography" [6].

"Euclidean ... constitutes the basis for Rivest, Shamir, and Adleman (RSA) and data encryption standard (DES) algorithms, which are commonly used for security on the Internet. Many versions of the algorithm have been developed for various purposes. These include binary GCD, extended GCD, and GCD for polynomials, to mention a few. However, the algorithm delays convergence, particularly the classical Euclidean algorithm, and the pattern of computing it has mostly been successive division to get the quotient and remainder. All these versions either did not adequately address the convergence delay problem or inconsistently worsened it" [7].

In this article, within a ring R with an identity element, a sequence of equalities $r_{i-1} = r_i q_i + r_{i+1}$ $(i = 1, 2, \dots, n)$ is called a *left Euclidean chain*. If, additionally, $r_n \neq 0$ and $r_{n+1} = 0$, it is called a *weak left Euclidean algorithm* [4]. In this case, r_n is a greatest left divisor of the elements r_0 and r_1. For every left Euclidean chain with $r_n \neq 0$, we introduce a sequence of ring elements $y_1, y_2, \dots, y_n$—termed the *left Bézout sequence*—defined by the recurrence relations:

$$y_n := 1, \quad y_{n-1} := -q_{n-1}, \quad y_i := y_{i+2} - q_i y_{i+1}, \quad i = n-2, n-3, \dots, 2, 1.$$

The main result of this article is an algorithm for expressing the element r_n of the left Euclidean chain in terms of adjacent elements of the Bézout sequence—namely, the Bézout equalities (Theorems 2, 8, and 10).

The author has aimed to present a self-contained paper accessible even to students. Consequently, several well-known yet essential foundational results are included. For all other necessary definitions and background, we refer the reader to [8].

2. Divisibility in a ring

Let R be a ring with an identity element. If $c = ab$, then a is called a *left divisor* of c, and b is called a *right divisor* of c. We denote the set of all left (right) divisors of an element c by $\mathrm{GCD}_\ell(c)$ (respectively, $\mathrm{GCD}_r(c)$). In general, the relations of left and right divisibility are preorders on R, as they are not antisymmetric; for instance, for any x, the element $-x$ is also a divisor of c whenever x is a divisor of c. We denote the set of all greatest left (right) divisors of an element c by $\mathrm{GD}_\ell(c)$ (respectively, $\mathrm{GD}_r(c)$).

The following notation is used for sets of common divisors:

$$D_\ell(a, b) := D_\ell(a) \cap D_\ell(b), \qquad D_r(a, b) := D_r(a) \cap D_r(b).$$

The set of greatest left (right) common divisors is denoted by $\mathrm{GCD}_\ell(a, b)$ (respectively, $\mathrm{GCD}_r(a, b)$); it consists of all elements that is divided on every left (respectively, right) common divisor of the elements a and b. We write $D(c)$, $\mathrm{CD}(a, b)$, and $\mathrm{GCD}(a, b)$ if, respectively, $D_\ell(c) = D_r(c)$, $\mathrm{GD}_\ell(c) = \mathrm{GD}_r(c)$, and $\mathrm{GCD}_\ell(a, b) = \mathrm{GCD}_r(a, b)$. For example, if $R = \mathbb{Z}$, then $\mathrm{GD}(n) = \{-n, n\}$.

Note that there exist commutative rings in which a greatest common divisor does not exist for every pair of elements.

Lemma 1. *Let R be a ring and let $a = bq + r$ for some $a, b, q, r \in R$. Then*

$$D_\ell(a, b) = D_\ell(b, r), \qquad D_r(a, q) = D_r(q, r).$$

Proof. Let $c \in D_\ell(a, b)$; that is, $a = ca'$ and $b = cb'$ for some $a', b' \in R$. Since $a = bq + r$, we have

$$r = a - bq = ca' - cb'q = c(a' - b'q).$$

Thus, $c \in D_\ell(b,r)$, which implies that $D_\ell(a,b) \subseteq D_\ell(b,r)$. Conversely, since $r = b(-q)+a$, it follows that $D_\ell(a,b) \supseteq D_\ell(b,r)$. Hence, $D_\ell(a,b) = D_\ell(b,r)$. The proof of the second equality is analogous. □

2.1. Left weak Euclidean algorithms. Let R be a ring with an identity element, and let $a,b,q,r \in R$ be elements such that

$$a = bq + r. \tag{1}$$

Then a,b,q, and r are called the *dividend*, *divisor*, *left quota*, and *left remnant*, respectively. '*To divide with a left remnant*' means '*to find a left quota and a left remnant when given a dividend and a divisor*'. The terms "quota" and "remnant" become "partial quotient" and "remainder", respectively, when conditions are imposed on how they are found.

Let each of the equalities

$$r_{i-1} = r_i q_i + r_{i+1}, \quad i = 1,2,\ldots,n-1,\ldots \tag{2}$$

be a division with a left remnant. This sequence of equalities is called a *left Euclidean chain* for a and b if $r_0 := a$ and $r_1 := b$; the pair (a,b) is termed a *right Euclidean pair* [9]. The elements $r_0,\ldots,r_n,\ldots$ are called *left remnants*. If, additionally, $r_n \neq 0$ and $r_{n+1} = 0$ (that is, $r_{n-1} = r_n q_n$), then this left Euclidean chain is called a *left weak Euclidean algorithm*.

Note that the initial part of an arbitrary chain is a finite Euclidean chain. Let a_n denote the last non-zero remainder of this chain and we shall call the number n by the *length* of the chain (evidently $n > 2$). Then the elements $y_1, y_2, \ldots, y_n$ defined by

$$y_n := 1, \quad y_{n-1} := -q_{n-1}, \quad y_i := y_{i+2} - q_i y_{i+1}, \quad i = n-2, n-3, \ldots, 2, 1, \tag{3}$$

are called the *left Bézout sequence*, and y_1 is the *left Bézout coefficient* for a and b. If $R = \mathbb{Z}_m$ is the ring of residues modulo m, then the Bézout coefficient y_1 for coprime numbers m and b is the multiplicative inverse of the element b in the ring $\mathbb{Z}_m$.

Theorem 2. *Let R be a ring with an identity element 1, let (2) be a finite left Euclidean chain for the elements $a,b \in R$ with $r_0 = a$ and $r_1 = b$, and let (3) be the corresponding left Bézout sequence. Then:*

(1) *The sets of left common divisors of adjacent remnants in (2) coincide:*

$$\mathrm{GCD}_\ell(a,b) = \mathrm{GCD}_\ell(r_i, r_{i+1}), \qquad i = 0,1,\ldots,n-1; \tag{4}$$

(2) *When the chain (2) is a left weak Euclidean algorithm, r_n is a left greatest common divisor of a and b, and*

$$\mathrm{GCD}_\ell(a,b) = \mathrm{GCD}_\ell(r_i, r_{i+1}) = \mathrm{GD}_\ell(r_n), \qquad i = 0,1,\ldots,n-1; \tag{5}$$

(3) *Bézout's equalities for adjacent remnants in the chain (2) take the form:*

$$r_n = r_i y_{i+2} + r_{i+1} y_{i+1}, \quad i = 0,1,\ldots,n-2. \tag{6}$$

In particular, $r_n = ay_2 + by_1$, where n is the index of the last non-zero remnant in the left Bézout sequence.

Proof. Item 1 follows from Lemma 1.

Item 2. Since $r_{n-1} = r_n q_n = r_n q_n + 0$, by Item 1 we have $D_\ell(r_i, r_{i+1}) = D_\ell(r_n, 0) = D_\ell(r_n)$. This means that each left common divisor of r_i and r_{i+1} divides the element r_n, and so r_n is a left greatest common divisor of r_i and r_{i+1} for all $i = 0,1,\ldots,n-1$.

We prove Item 3 by induction on i in decreasing order.

We first show that the statement holds for the largest index, $i = n-2$. The equalities (2) imply that $r_n = r_{n-2} - r_{n-1}q_{n-1}$. Therefore,

$$r_{n-2}y_n + r_{n-1}y_{n-1} = r_{n-2} \cdot 1 + r_{n-1}(-q_{n-1}) = r_n.$$

Thus, the base case holds.

Suppose the identity (6) is true for $i = k$, i.e., $r_n = r_k y_{k+2} + r_{k+1}y_{k+1}$. We will prove it for $i = k-1$. Substituting $i = k$ into (2) and (3) yields:

$$r_{k-1} = r_k q_k + r_{k+1}, \qquad y_k = y_{k+2} - q_k y_{k+1}.$$

Consequently,

$$r_{k+1} = r_{k-1} - r_k q_k, \qquad y_{k+2} = y_k + q_k y_{k+1}.$$

By adding and subtracting the element $r_k q_k y_{k+1}$ and applying the induction hypothesis, we obtain:

$$\begin{aligned} r_{k-1}y_{k+1} + r_k y_k &= r_k y_k + r_{k-1}y_{k+1} = r_k y_k + r_k q_k y_{k+1} + r_{k-1}y_{k+1} - r_k q_k y_{k+1} = \\ &= r_k(y_k + q_k y_{k+1}) + (r_{k-1} - r_k q_k)y_{k+1} = r_k y_{k+2} + r_{k+1}y_{k+1} = \\ &= r_n. \end{aligned}$$

Hence, (6) is true for $i = k-1$, and by induction, (6) holds for all $i = n-2, n-3, \ldots, 1, 0$. □

Corollary 3. *Let R be a ring without zero divisors, and assume there is a left weak Euclidean algorithm for the elements a and b. Then the corresponding left Bézout sequence for the elements a and b coincides with the left Bézout sequence for the elements a/d' and b/d', where d' is a left divisor of $d := \mathrm{GCD}(a, b)$. Furthermore, any pair of adjacent members of a Bézout sequence are right coprime.*

Proof. Let (2) be a left weak Euclidean algorithm, where $a = r_0$ and $b = r_1$. Dividing (2) by d', we obtain:

$$\frac{r_{i-1}}{d'} = \frac{r_i}{d'}q_i + \frac{r_{i+1}}{d'}, \quad i = 1, 2, \ldots, n, \quad \text{where} \quad \frac{r_{n+1}}{d'} = \frac{0}{d'} = 0.$$

As a result, we obtain a left weak Euclidean algorithm for the elements a/d' and b/d' with the same quotas, and thus the left Bézout sequence is also the same. If $d' = r_n$, then (6) implies:

$$1 = \frac{r_{i-1}}{r_n}y_{i+2} + \frac{r_i}{r_n}y_{i+1}.$$

Therefore, every right divisor of y_{i+2} and y_{i+1} divides 1, which means that the elements y_{i+2} and y_{i+1} are right coprime for all $i = 0, 1, \ldots, n-2$. □

Using an idea of B.V. Zabavsky from [10, Theorem 2] and [11, Proposition 6], the following criterion for Euclidean pairs over rings of stable range 1 is obtained.

Theorem 4. [9, Theorem 8] *Let R be a ring of stable range 1. Then $(a, b) \in R^2$ is a Euclidean pair if and only if the right ideal $aR + bR$ is principal.*

Example 5. Let $a = 50$ and $b = 20$. It is easy to see that the equalities

$$50 = 20 \cdot 3 - 10, \quad 20 = -10 \cdot 2 + 40, \quad -10 = 40 \cdot 1 - 50$$

form a Euclidian chain for $a = 50$, $b = 20$. Find the Bézout equality for $a = 50$, $b = 20$.

Let us calculate the Bézout sequence for a and b:

$$r_0 = a = 50, \quad r_1 = b = 20, \quad r_2 = -10, \quad r_3 = 40, \quad r_4 = -50, \quad q_1 = 3, \quad q_2 = 2, \quad q_3 = 1.$$

The last non-zero remnant is $r_4 = -50$, therefore, the chain length is $n = 4$. Using the definition of the Bézout sequence, we have:

$$y_4 = 1, \qquad y_3 = -q_3 = -1, \qquad y_2 = y_4 - y_3 q_2 = 1 - (-1) \cdot 2 = 3,$$

$$y_1 = y_3 - y_2 q_1 = -1 - 3 \cdot 3 = -10.$$

By Theorem 2, the equality $r_4 = ay_2 + by_1$ must hold; that is,

$$-50 = 50 \cdot 3 + 20 \cdot (-10).$$

Example 6. Find the multiplicative inverse of 11 in the residue field $\mathbb{Z}_{9839}$.

It follows from Fermat's Little Theorem that 11^{9837} is such an element. Let us find this element by utilizing the properties we have obtained. To do this, we will construct the Euclidean algorithm:

$$\underbrace{9839}_{r_0} = \underbrace{11}_{r_1} \cdot \underbrace{894}_{q_1} + \underbrace{5}_{r_2}, \qquad \underbrace{11}_{r_1} = \underbrace{5}_{r_2} \cdot \underbrace{2}_{q_2} + \underbrace{1}_{r_3},$$

The Bézout coefficient corresponds to the multiplicative inverse of 11. The length of the Euclidean chain is 3; therefore,

$$y_3 = 1, \qquad y_2 = -q_2 = -2, \qquad y_1 = y_3 - y_2 q_1 = 1 - (-2)894 = 1789.$$

Thus, $11 \cdot 1789 \equiv 1 \pmod{9839}$.

Example 7. Let us construct a weak left Euclidean algorithm with $n = 4$ in the ring $M_2(\mathbb{Z})$:

$$r_0 = r_1 q_1 + r_2, \quad r_1 = r_2 q_2 + r_3, \quad r_2 = r_3 q_3 + r_4, \quad r_3 = r_4 q_4,$$

and find $\gcd(r_0, r_1)$ along with its respective linear representation.

First, let us choose r_4, q_4, q_3, q_2, and q_1 arbitrarily and calculate the remaining parameters:

$$r_4 := \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad q_4 := \begin{bmatrix} -1 & 1 \\ 1 & 2 \end{bmatrix}, \quad r_3 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 1 & 11 \end{bmatrix},$$

$$q_3 := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \qquad r_2 = \begin{bmatrix} 1 & 5 \\ 1 & 11 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix},$$

$$q_2 := \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}, \quad r_1 = \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 5 \\ 1 & 11 \end{bmatrix} = \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix},$$

$$q_1 := \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix}, \quad r_0 = \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} = \begin{bmatrix} 33 & 21 \\ 69 & 43 \end{bmatrix}.$$

By item 2 of Theorem 2 the matrix $r_4 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is a left greatest common divisor of the matrices

$$r_0 = \begin{bmatrix} 33 & 21 \\ 69 & 43 \end{bmatrix} \quad \text{and} \quad r_1 = \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix}.$$

To find Bézout equalities, we have to determine the Bézout sequence y_1, y_2, y_3, y_4:

$$y_4 = E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad y_3 = -q_3 = \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix},$$

$$y_2 = y_4 - q_2 y_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix},$$

$$y_1 = y_3 - q_1 y_2 = \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ -4 & -3 \end{bmatrix}.$$

The item 3 of Theorem 2 implies the following Bézout equalities:

$$r_4 = r_0 y_2 + r_1 y_1, \quad r_4 = r_1 y_3 + r_2 y_2, \quad r_4 = r_2 y_4 + r_3 y_3,$$

i.e.,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 33 & 21 \\ 69 & 43 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} + \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -4 & -3 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} + \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 5 \\ 1 & 11 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix}.$$

2.2. Right weak Euclidean algorithms. Let R be a ring with identity element. A sequence of equalities

$$r_{i-1} = q_i r_i + r_{i+1}, \quad i = 1, 2, \dots, n-1, \dots \tag{7}$$

is called a *right Euclidean chain* for a and b if $r_0 := a$ and $r_1 := b$.

The elements $r_0, \dots, r_n, \dots$ are called *right remnants*. If $r_{i-1} = q_i r_i + r_{i+1}$ is a Euclidean division in $\mathbb{Z}$, then r_{i+1} is a remainder. If, additionally, $r_n \neq 0$ and $r_{n+1} = 0$ (that is, $r_{n-1} = q_n r_n$), then the right Euclidean chain is called a *right weak Euclidean algorithm*. The elements $y_1, y_2, \dots, y_n$ defined by

$$y_n := 1, \quad y_{n-1} := -q_{n-1}, \quad y_i := y_{i+2} - y_{i+1} q_i, \quad i = n-2, n-3, \dots, 2, 1, \tag{8}$$

are called the *right Bézout sequence*, and y_1 is the *right Bézout coefficient* for a and b.

Theorem 8. *Let R be a ring with an identity element, let (7) be a finite right Euclidean chain for the elements $a, b \in R$, and let (8) be the respective right Bézout sequence. Then:*

(1) *The sets of right common divisors of adjacent remnants in (7) coincide:*

$$\mathrm{GCD}_r(a, b) = \mathrm{GCD}_r(r_i, r_{i+1}), \qquad i = 0, 1, \dots, n-1; \tag{9}$$

(2) *When the chain (7) is a right weak Euclidean algorithm, r_n is a right greatest common divisor of a and b, and*

$$\mathrm{GCD}_r(a, b) = \mathrm{GCD}_r(r_i, r_{i+1}) = \mathrm{GD}_r(r_n), \qquad i = 0, 1, \dots, n-1; \tag{10}$$

(3) *Bézout's equalities for adjacent remnants in (7) take the following form:*

$$r_n = y_{i+2} r_i + y_{i+1} r_{i+1}, \quad i = 0, 1, \dots, n-2. \tag{11}$$

In particular, $r_n = y_2 a + y_1 b$, where n is the index of the final non-zero remnant in the right Bézout sequence (7).

Corollary 9. *Let R be a ring without zero divisors with an identity element, and assume there is a right weak Euclidean algorithm for the elements a and b. Then the respective right Bézout sequence for the elements a and b coincides with the right Bézout sequence for the elements $a\backslash d'$ and $b\backslash d'$, where d' is a right divisor of $d := \mathrm{GCD}(a, b)$. Furthermore, any pair of adjacent members of a Bézout sequence are left coprime.*

The consequences for commutative rings are simplified. Theorem 2 and Corollary 3 imply the following statements.

Corollary 10. *Let R be a commutative ring with an identity element, let (2) be a Euclidean chain for the elements $a, b \in R$ with $b \neq 0$, and let (3) be the respective Bézout sequence. Then the Bézout equalities for the neighboring remnants in (2) take the following form:*

$$r_n = r_i y_{i+2} + r_{i+1} y_{i+1}, \quad i = 0, 1, \ldots, n-2, \tag{12}$$

where n is the index of the final non-zero remnant in (2). In particular, if (2) is a weak Euclidean algorithm, then

$$\mathrm{GCD}(a, b) = a y_2 + b y_1.$$

Corollary 11. *Let R be a ring without zero divisors with an identity element, and assume there is a weak Euclidean algorithm for the elements a and b. Then any pair of neighboring members of a Bézout sequence are coprime. Furthermore, the Bézout sequence for the elements a and b coincides with the Bézout sequence for a/d' and b/d' if d' divides $d := \mathrm{GCD}(a, b)$.*

3. Some examples

Finally, let us recall the well-known lemma on division with remainder, as well as two elegant proofs that, judging by textbooks, are not widely known.

'*To divide with a remainder*' means '*to find a quotient q and a remainder r for a given dividend a and divisor b*' satisfying the relations:

$$a = bq + r, \qquad 0 \leqslant r < |b|. \tag{13}$$

Lemma 12 (Euclidean division)**.** *Let a and b be integers. If $b = 0$, then division with a remainder is impossible. If $b \neq 0$, then the quotient q and the remainder r are uniquely determined by:*

$$q = \frac{|b|}{b} s, \quad r = a - |b| s, \quad \textit{where} \quad s := \left\lfloor \frac{a}{|b|} \right\rfloor. \tag{14}$$

Proof. If $b = 0$, then the inequality in (13) is false. Therefore, the remainder does not exist, and division is impossible. Henceforth, suppose $b \neq 0$.

Let (13) hold. Dividing the inequality in (13) by $|b|$, we obtain $0 \leqslant \frac{r}{|b|} < 1$; that is, $\frac{r}{|b|}$ is a non-negative fractional number. Since $\frac{b}{|b|} q$ is an integer, we have:

$$s = \left\lfloor \frac{a}{|b|} \right\rfloor = \left\lfloor \frac{bq + r}{|b|} \right\rfloor = \left\lfloor \frac{b}{|b|} q + \frac{r}{|b|} \right\rfloor = \frac{b}{|b|} q.$$

Therefore, $bq = |b|s$ and $r = a - bq = a - |b|s$, and thus (14) holds.

Conversely, let (14) be true. Consequently, $|b|s = bq$, $a = |b|s + r = bq + r$, and

$$\frac{r}{|b|} = \frac{a - |b|s}{|b|} = \frac{a}{|b|} - s = \frac{a}{|b|} - \left\lfloor \frac{a}{|b|} \right\rfloor.$$

By definition, $\frac{r}{|b|}$ is the fractional part of the rational number $\frac{a}{|b|}$. Therefore,

$$0 \leqslant \frac{r}{|b|} < 1, \quad \text{that is,} \quad 0 \leqslant r < |b|.$$

Hence, (13) holds, which proves the lemma.

Another proof of existence and uniqueness. Consider the set $M_{a,b} := \{a - bx \mid x \in \mathbb{Z}\}$ equipped with the linear order $\leqslant$. Each successive element is greater by $|b|$. The inequality $0 \leqslant r < |b|$ can be written as $r \geqslant 0$ and $r - |b| < 0$, which means that r is the least element in the subset $M^{\geqslant 0}_{a,b}$ of non-negative elements within $M_{a,b}$. Since the set of all non-negative

integers is well-ordered, the set $M_{a,b}^{\geqslant 0}$ must have a least element, provided that it is non-empty (indeed, $M_{a,b}^{\geqslant 0}$ contains $a + b^2|a|$). Thus, the remainder exists and is unique, as is the corresponding quotient. □

Example 13. Find the greatest common divisor of 9367 and 4318, along with the respective Bézout equalities.

Construct the Euclidean algorithm:

$$9367 = 4318 \cdot 2 + 731; \quad 4318 = 731 \cdot 5 + 663; \quad 731 = 663 \cdot 1 + 68;$$
$$663 = 68 \cdot 9 + 51; \qquad 68 = 51 \cdot 1 + \mathbf{17}; \qquad 51 = 17 \cdot 3 + 0.$$

Hence, $d := \mathrm{GCD}(9367, 4318) = 17$. To find the Bézout equalities, we identify all remainders and quotients:

$$r_0 = 9367, \quad r_1 = 4318, \quad r_2 = 731, \quad r_3 = 663, \quad r_4 = 68, \quad r_5 = 51, \quad r_6 = 17, \quad r_7 = 0;$$
$$q_1 = 2, \qquad q_2 = 5, \qquad q_3 = 1, \qquad q_4 = 9, \qquad q_5 = 1, \qquad q_6 = 3.$$

The index of the final non-zero remainder in the Bézout algorithm is 6; therefore, $n = 6$. To calculate the corresponding Bézout sequence, we use formula (3):

$$y_6 := 1, \qquad y_5 := -q_5, \qquad y_i := y_{i+2} - y_{i+1} \cdot q_i, \quad i = 4, 3, 2, 1.$$

Thus, we have:

$$y_6 = 1, \qquad y_5 = -q_5 = -1, \qquad y_4 = y_6 - y_5 \cdot q_4 = 1 - (-1) \cdot 9 = 10,$$
$$y_3 = y_5 - y_4 q_3 = -1 - 10 \cdot 1 = -11, \qquad y_2 = y_4 - y_3 \cdot q_2 = 10 - (-11) \cdot 5 = 65,$$
$$y_1 = y_3 - y_2 \cdot q_1 = -11 - 65 \cdot 2 = -141.$$

Using (12) for $i = 0, 1, 2, 3, 4$, we obtain five Bézout equalities:

$$17 = 9367 \cdot 65 + 4318 \cdot (-141), \quad 17 = -11 \cdot 4318 + 65 \cdot 731, \quad 17 = 10 \cdot 731 + (-11) \cdot 663,$$
$$17 = -1 \cdot 663 + 10 \cdot 68, \quad 17 = 1 \cdot 68 + (-1) \cdot 51.$$

Δ

Example 14. Find the Bézout equalities for the Euclidean chain:

$$\underbrace{9367}_{r_0} = \underbrace{4318}_{r_1} \cdot 2 + \underbrace{731}_{r_2}; \quad 4318 = 731 \cdot 5 + \underbrace{663}_{r_3}; \quad 731 = 663 \cdot 1 + \underbrace{68}_{r_4}.$$

All quotas of this Euclidean chain are given by:

$$q_1 = 2, \qquad q_2 = 5, \qquad q_3 = 1.$$

The index of the final non-zero remnant in the Euclidean chain is 4 ($r_4 = 68$); therefore, $n = 4$. We calculate the corresponding Bézout sequence using formula (3):

$$y_4 = 1, \qquad y_3 = -q_3 = -1, \qquad y_2 = y_4 - y_3 \cdot q_2 = 1 - (-1) \cdot 5 = 6,$$
$$y_1 = y_3 - y_2 \cdot q_1 = -1 - 6 \cdot 2 = -13.$$

Using (12) for $i = 0, 1, 2$, we obtain three equalities:

$$68 = 9367 \cdot 6 + 4318 \cdot (-13), \quad 68 = -1 \cdot 4318 + 6 \cdot 731, \quad 68 = 1 \cdot 731 + (-1) \cdot 663.$$

Example 15. In the ring of Gaussian integers, find Bézout's identities for the numbers $62+21i$ and $16+18i$ using the equalities:

$$\underbrace{62+21i}_{r_0}=(\underbrace{16+18i}_{r_1})(\underbrace{2-i}_{q_1})+(\underbrace{12+i}_{r_2}),\qquad \underbrace{16+18i}_{r_1}=(\underbrace{12+i}_{r_2})(\underbrace{1+i}_{q_2})+(\underbrace{5+5i}_{r_3}),$$

$$\underbrace{12+i}_{r_2}=(\underbrace{5+5i}_{r_3})(\underbrace{1-i}_{q_3})+(\underbrace{2+i}_{r_4}),\qquad \underbrace{5+5i}_{r_3}=(\underbrace{2+i}_{r_4})(\underbrace{3+i}_{q_4})+\underbrace{0}_{r_5}.$$

Since $r_5=0$, the given Euclidean chain is a weak Euclidean algorithm. The last non-zero remnant is $r_4=2+i$; hence,

$$n=4,\qquad \mathrm{GCD}(62+21i,16+18i)=r_4=2+i.$$

Using formulas (3), we find the Bézout sequence:

$$y_4=1,\qquad y_3=-q_3=-1+i,\qquad y_2=y_4-q_2y_3=1-(1+i)(-1+i)=3,$$
$$y_1=y_3-q_1y_2=-1+i-(2-i)3=-7+4i.$$

From Theorem 2, we obtain $r_4=r_jy_{j+2}+r_{j+1}y_{j+1}$ for all $j=0,1,2$. Therefore,

$$\begin{aligned}2+i=\mathrm{GCD}(62+21i,16+18i)&=(62+21i)3+(16+18i)(-7+4i)\\&=(16+18i)(-1+i)+(12+i)3\\&=(12+i)1+(5+5i)(-1+i).\end{aligned}$$

Example 16. In the ring of Gaussian integers, find Bézout's identities for the numbers $36+30i$ and $16+3i$ using the Euclidean algorithm:

$$\underbrace{36+30i}_{r_0}=(\underbrace{16+3i}_{r_1})(\underbrace{2+i}_{q_1})+(\underbrace{7+8i}_{r_2}),\qquad \underbrace{16+3i}_{r_1}=(\underbrace{7+8i}_{r_2})(\underbrace{1-i}_{q_2})+(\underbrace{1+2i}_{r_3}),$$

$$\underbrace{7+8i}_{r_2}=(\underbrace{1+2i}_{r_3})(\underbrace{3-i}_{q_3})+(\underbrace{2+3i}_{r_4}),\qquad \underbrace{1+2i}_{r_3}=(\underbrace{2+3i}_{r_4})(\underbrace{1+i}_{q_4})+\underbrace{2-3i}_{r_5}.$$

The last non-zero remnant is $r_5=2-3i$; therefore, $n=5$. Let us find the Bézout sequence using formula (3):

$$\begin{aligned}&y_5=1,\qquad y_4=-q_4=-(1+i),\\&y_3=y_5-q_3y_4=1-(3-i)\big(-(1+i)\big)=5+2i,\\&y_2=y_4-q_2y_3=-(1+i)-(1-i)(5+2i)=-8+2i,\\&y_1=y_3-q_1y_2=(5+2i)-(2+i)(-8+2i)=23+6i.\end{aligned}$$

From Theorem 2, we obtain $r_5=r_jy_{j+2}+r_{j+1}y_{j+1}$ for all $j=0,1,2,3$. Therefore,

$$\begin{aligned}2-3i&=r_0y_2+r_1y_1=(36+30i)(-8+2i)+(16+3i)(23+6i)\\&=r_1y_3+r_2y_2=(16+3i)(5+2i)+(7+8i)(-8+2i)\\&=r_2y_4+r_3y_3=(7+8i)(-(1+i))+(1+2i)(5+2i)\\&=r_3y_5+r_4y_4=(1+2i)(1)+(2+3i)(-(1+i)).\end{aligned}$$

Conclusions. The proposed method for finding Bézout identities (Theorems 2 and 8) enables efficient analysis using a weak Euclidean algorithm in both commutative (Examples 7, 15, 16) and non-commutative rings (Example 7). Furthermore, this method makes more effective use of the Euclidean algorithm itself within arbitrary Euclidean rings (Examples 15, 16) — for instance, in finding the multiplicative inverse of an element in the ring $\mathbb{Z}_m$ (Example 6).

Conflict of interest and ethics. The author is a member of the editorial board of this journal. To avoid a conflict of interest, the manuscript underwent an appropriate peer-review process by independent reviewers, and the decision on publication was made by an independent editor. The author also declares full adherence to all journal research ethics policies.

Acknowledgements. The author expresses sincere gratitude to the reviewers for their valuable comments. The author declares no special funding for this work.

References

1. Lemmermeyer, F. (2004). *The Euclidean algorithm in algebraic number fields (Online survey)*. http://www.fen.bilkent.edu.tr/~franz/publ/survey.pdf
2. Lemmermeyer, F. (2026). *Euclidean Rings, preprint arXiv:2608.23216*, 314. https://arxiv.org/abs/2608.23216v1
3. Romaniv, Andrii (2025). *The relationships between common multiples of matrices over commutative Bézout domain of stable range 1.5*, Buletinul Academiei de Ştiinţe a Republicii Moldova. Matematica, **2(108)–3(109)**, 50–61. https://doi.org/10.56415/basm.y2025.i2-3.p62
4. Salce, L., Zanardo, P. (2014). *Products of elementary and idempotent matrices over integral domains*, Linear Algebra Appl., **452**, 130–152. https://doi.org/10.1016/j.laa.2014.03.042
5. Levrie, P., Penne, R. (2016). *The extended Euclidean Algorithm made easy*, Math. Gazette, **100** (547), 147–149. https://doi.org/10.1017/mag.2016.25
6. Sreedhar, K., Horowitz, M., Torng, C. (2022). *A Fast Large-Integer Extended GCD Algorithm and Hardware Design for Verifiable Delay Functions and Modular Inversion*, IACR Trans. Cryptogr. Hardware Embed. Syst., **2022** (4), 163–187. https://doi.org/10.46586/tches.v2022.i4.163-187
7. Erho, J. A., Okrinya, A. B. (2026). *Novel approach to shortening convergence of Euclidean's greatest common divisor algorithm*, Math. Open, **5**, Article 2550022. https://doi.org/10.1142/s2811007225500221
8. Shchedryk, V. P. (2021). *Arithmetic of Matrices over Rings*, Akademperiodyka, Kyiv. https://doi.org/10.15407/akademperiodika.430.278
9. Alahmadi, A., Jain, S. K., Lam, T. Y., Leroy, A. (2014). *Euclidean pairs and quasi-Euclidean rings*, J. Algebra, **406**, 154–170. https://doi.org/10.1016/j.jalgebra.2014.02.009
10. Zabavsky, B. V. (2003). *Reduction of matrices over Bezout rings with stable rank not higher than 2*, Ukrainian Math. J., **55** (4), 550–554. https://doi.org/10.1023/B:UKMA.0000010166.70532.41
11. Zabavsky, B. V. (2005). *Diagonalizability theorems for matrices over rings with finite stable range*, Algebra Discrete Math., **1**, 151–165. https://admjournal.luguniv.edu.ua/index.php/adm/article/view/923/452
12. Bovdi, V., Zabavsky, B. (2025). *Rings of the right (left) almost stable range 1*, Carpathian Math. Publ., **17** (2), 463–471. https://doi.org/10.15330/cmp.17.2.461-471

UDC 512.712

Слабкий алгоритм Евкліда та лінійне подання НСД

Федір Сохацький

Анотація. У кільці з одиницею рівності $r_{i-1} = r_i q_i + r_{i+1}$, $i = 1, 2, \ldots, n$, називаються *лівим ланцюгом Евкліда*, а за умов $r_n \neq 0$ та $r_{n+1} = 0$ — *слабким алгоритмом Евкліда*. Для цього лівого ланцюга вперше вводиться поняття *лівої послідовності Безу* $y_1, y_2, \ldots, y_n$:

$$y_n := 1, \quad y_{n-1} := -q_{n-1}, \quad y_i := y_{i+2} - q_i y_{i+1}, \quad i = n-2, n-3, \ldots, 2, 1.$$

Доведено, що за умови $r_n \neq 0$ виконуються рівності Безу:

$$r_n = r_i y_{i+2} + r_{i+1} y_{i+1} \quad \text{для всіх} \quad i = 0, 1, \ldots, n-2.$$

Якщо лівий ланцюг Евкліда є лівим слабким алгоритмом Евкліда, то $r_n = \text{НСД}_\ell(a,b)$ є лівим найбільшим спільним дільником елементів $a = r_0$ та $b = r_1$, а при $i = 0$ отримуємо його лінійне подання $\text{НСД}_\ell(a,b) = ay_2 + by_1$. Аналогічні властивості виконуються і для правих дільників. У комутативних кільцях ці поняття збігаються.

Ключові слова: слабкий алгоритм Евкліда, лінійне подання, послідовність Безу, ланцюг Евкліда, лівий найбільший спільний дільник, кільце з одиницею.

Список використаних джерел

1. Lemmermeyer F. The Euclidean algorithm in algebraic number fields (Online survey), 2004. URL: http://www.fen.bilkent.edu.tr/~franz/publ/survey.pdf
2. Lemmermeyer F. Euclidean Rings. *Preprint arXiv:2608.23216*. 2026. 314 p. URL: https://arxiv.org/abs/2608.23216v1
3. Andrii Romaniv, The relationships between common multiples of matrices over commutative Bézout domain of stable range 1.5, Buletinul Academiei de Ştiinţe a Republicii Moldova. Matematica, 2025, 2(108)–3(109), 50–61, DOI: https://doi.org/10.56415/basm.y2025.i2-3.p62
4. Salce L., Zanardo P. Products of elementary and idempotent matrices over integral domains. *Linear Algebra Appl.* 2014. Vol. 452. P. 130–152. DOI: https://doi.org/10.1016/j.laa.2014.03.042
5. Levrie P., Penne R. The extended Euclidean Algorithm made easy. *Math. Gazette*. 2016. Vol. 100, No. 547. P. 147–149. DOI: https://doi.org/10.1017/mag.2016.25
6. Sreedhar K., Horowitz M., Torng C. A Fast Large-Integer Extended GCD Algorithm and Hardware Design for Verifiable Delay Functions and Modular Inversion. *IACR Trans. Cryptogr. Hardware Embed. Syst.* 2022. Vol. 2022, No. 4. P. 163–187. DOI: https://doi.org/10.46586/tches.v2022.i4.163-187
7. Erho J. A., Okrinya A. B. Novel approach to shortening convergence of Euclidean's greatest common divisor algorithm. *Math. Open*. 2026. Vol. 5. Article 2550022. DOI: https://doi.org/10.1142/s2811007225500221
8. Shchedryk V. P. Arithmetic of Matrices over Rings. Kyiv: Akademperiodyka, 2021. 278 p. https://doi.org/10.15407/akademperiodika.430.278
9. Alahmadi A., Jain S. K., Lam T. Y., Leroy A. Euclidean pairs and quasi-Euclidean rings. *J. Algebra*. 2014. Vol. 406. P. 154–170. https://doi.org/10.1016/j.jalgebra.2014.02.009
10. Zabavsky B. V. Reduction of matrices over Bezout rings with stable rank not higher than 2. *Ukrainian Math. J.* 2003. Vol. 55, No. 4. P. 550–554. DOI: https://doi.org/10.1023/B:UKMA.0000010166.70532.41
11. Zabavsky B. V. Diagonalizability theorems for matrices over rings with finite stable range. *Algebra Discrete Math.* 2005. No. 1. P. 151–165. URL: https://admjournal.luguniv.edu.ua/index.php/adm/article/view/923/452
12. Bovdi V., Zabavsky B. Rings of the right (left) almost stable range 1. *Carpathian Math. Publ.* 2025. Vol. 17, No. 2. P. 463–471. DOI: https://doi.org/10.15330/cmp.17.2.461-471

Про автора / About the author

Федір Сохацький, доктор фізико-математичних наук, старший науковий співробітник, відділ алгебри, Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача Національної академії наук України, вул. Наукова, 3 Б, м. Львів, 79060, Україна;

Fedir Sokhatsky, Doctor of Science in Physics and Mathematics, Senior Researcher, Department of Algebra, Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine, 3-b Naukova Str., Lviv 79060, Ukraine.

Отримано / Received 30.09.2026
Прийнято до друку / Accepted 03.11.2026
Опубліковано / Published 25.11.2026