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

УДК 512.712

Слабкий алгоритм Евкліда та лінійне подання НСД

Федір Сохацький

Інститут прикладних проблем механіки і математики імені Я. С. Підстригача
Національної Академії наук України, відділ алгебри, м. Львів, Україна
fmsokha@ukr.net
https://orcid.org/0000-0003-4969-5651

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.

1. Вступ

Вивчення алгоритму Евкліда залишається надзвичайно актуальним — як через необхідність поширення сфери його застосування на нові структури в межах алгебричних кілець [1, 2, 3, 4], так і в контексті математичної освіти [5]. Особливе значення має дослідження його обчислювальної ефективності; зокрема, це питання розглядається у двох важливих працях:

"Обчислення розширеного найбільшого спільного дільника (XGCD) — операція, що визначає коефіцієнти Безу b_a та b_b так, щоб $b_a \cdot a_0 + b_b \cdot b_0 = \text{GCD}(a_0, b_0)$, — є критично

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

важливою для багатьох криптографічних застосувань. Зокрема, обчислення XGCD для великих цілих чисел є найбільш ресурсомістким етапом у двох сферах, що викликають дедалі більший інтерес: у функціях із перевірюваною затримкою (VDF), які виконують піднесення до квадрата бінарних квадратичних форм у групі класів, та в операціях модульного обернення з постійним часом виконання для криптографії на еліптичних кривих" [6].

"Алгоритм Евкліда ... лежить в основі алгоритмів RSA (Рівеста — Шаміра — Адлемана) та DES (стандарту шифрування даних), які широко використовуються для забезпечення безпеки в Інтернеті. Для різних цілей було розроблено чимало варіацій цього алгоритму, зокрема бінарний алгоритм НСД, розширений алгоритм НСД та алгоритм НСД для поліномів. Однак класичний алгоритм Евкліда характеризується повільною збіжністю, а його реалізація зазвичай передбачає послідовне виконання операції ділення для отримання частки та остачі. Наявні модифікації або не вирішували належним чином проблему повільної збіжності, або ж посилювали її." [7]

У цій статті в довільному кільці R з одиницею послідовність рівностей $r_{i-1} = r_i q_i + r_{i+1}$, $i = 1, 2, \ldots, n$, називається *лівим ланцюгом Евкліда*. Якщо до того ж $r_n \neq 0$ та $r_{n+1} = 0$, то її називають *слабким лівим алгоритмом Евкліда* [4]. У цьому випадку r_n є лівим найбільшим дільником елементів r_0 та r_1. Для кожного лівого ланцюга Евкліда при $r_n \neq 0$ вперше означується послідовність $y_1, y_2, \ldots, y_n$ елементів кільця, яку названо *лівою послідовністю Безу* й визначено за допомогою рівностей:

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

Основним результатом статті є алгоритм вираження елемента r_n лівого ланцюга Евкліда через сусідні елементи послідовності Безу, тобто рівності Безу (Теореми 2, 8 та 10).

Автор прагнув написати самодостатню статтю, доступну навіть студентам. Тому тут наведено деякі добре відомі, але вкрай необхідні результати. Усі інші необхідні означення та результати можна знайти в [8].

2. Подільність у кільці

Нехай R — кільце з одиницею. Якщо $c = ab$, то a називають *лівим дільником*, а b — *правим дільником* елемента c. Множину всіх лівих (правих) дільників елемента c позначатимемо через $D_\ell(c)$ (відповідно $D_r(c)$). Загалом, відношення лівої та правої подільності є передпорядками на R, оскільки вони не антисиметричні: для будь-якого лівого дільника x елемент $-x$ також є лівим дільником елемента c. Множину всіх найбільших лівих (правих) дільників елемента c позначатимемо через $\mathrm{GD}_\ell(c)$ та $\mathrm{GD}_r(c)$ відповідно. Для множин спільних дільників використовують такі позначення:

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

Множину найбільших лівих (правих) спільних дільників позначають через $\mathrm{GCD}_\ell(a, b)$ (відповідно $\mathrm{GCD}_r(a, b)$); вона складається з усіх елементів, які діляться на кожен лівий (відповідно правий) спільний дільник елементів a та b.

Ми пишемо $D(c)$, $\mathrm{GD}(c)$ та $\mathrm{GCD}(a, b)$, якщо, відповідно, $D_\ell(c) = D_r(c)$, $\mathrm{GD}_\ell(c) = \mathrm{GD}_r(c)$ та $\mathrm{GCD}_\ell(a, b) = \mathrm{GCD}_r(a, b)$. Наприклад, якщо $R = \mathbb{Z}$, то $\mathrm{GD}(n) = \{-n, n\}$.

Зауважимо, що існують комутативні кільця, в яких найбільший спільний дільник існує не для всіх пар елементів.

Лема 1. *Нехай R — кільце і $a = bq + r$ для деяких $a, b, q, r \in R$. Тоді*

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

Доведення. Нехай $c \in D_\ell(a,b)$, тобто для деяких $a', b' \in R$ маємо $a = ca'$ та $b = cb'$. Оскільки $a = bq + r$, то

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

Отже, $c \in D_\ell(b,r)$, а тому $D_\ell(a,b) \subseteq D_\ell(b,r)$. Оскільки $r = b(-q) + a$, то $D_\ell(a,b) \supseteq D_\ell(b,r)$. Звідси отримуємо $D_\ell(a,b) = D_\ell(b,r)$. Доведення другої рівності аналогічне. □

2.1. Лівий слабкий алгоритм Евкліда. Нехай R — кільце з одиницею, а $a, b, q, r \in R$ — такі елементи, що

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

Тоді a, b, q, r називаються відповідно *діленим*, *дільником*, *лівою квотою* та *лівим залишком*. «*Ділити з лівим залишком*» означає «*знайти ліву квоту та лівий залишок, якщо задано ділене й дільник*». "Квота" і "залишок" відповідно стають "часткою" і "остачею", якщо на них накладаються умови їх знаходження.

Нехай кожна з рівностей

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

є діленням з лівим залишком. Ці рівності називаються *лівим ланцюгом Евкліда* для a та b, якщо $r_0 := a$ і $r_1 := b$. Елементи $r_0, \ldots, r_n, \ldots$ називаються *лівими залишками*. Якщо ж $r_n \neq 0$ та $r_{n+1} = 0$ (тобто $r_{n-1} = r_n q_n$), то лівий ланцюг Евкліда називається *лівим слабким алгоритмом Евкліда*, а пара (a,b) — *правою Евклідовою парою* [9].

Зауважимо, що початкова частина довільного ланцюга Евкліда є скінченним ланцюгом Евкліда. Позначимо через a_n останній ненульовий залишок цього ланцюга і число n назвемо *довжиною* ланцюга (очевидно, що $n > 2$). Тоді елементи $y_1, y_2, \ldots, y_n$, які визначені співвідношеннями

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

називаються *лівою послідовністю Безу*, а y_1 — *лівим коефіцієнтом Безу* для a та b. Якщо $R = \mathbb{Z}_m$ — кільце лишків за модулем m, то коефіцієнт Безу y_1 для взаємно простих чисел m і b є мультиплікативно оберненим елементом до елемента b у кільці $\mathbb{Z}_m$.

Теорема 2. *Нехай R — кільце з одиницею, (2) — скінченний лівий ланцюг Евкліда для елементів $a, b \in R$, а (3) — відповідна ліва послідовність Безу, де $r_0 = a$ і $r_1 = b$. Тоді:*

(1) *Множини лівих спільних дільників сусідніх залишків у (2) збігаються:*

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

(2) *У випадку, коли ланцюг (2) є лівим слабким алгоритмом Евкліда, елемент r_n є лівим найбільшим спільним дільником a та b, і*

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

(3) *Рівності Безу для сусідніх залишків у ланцюзі (2) мають вигляд:*

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

Зокрема, $r_n = ay_2 + by_1$, where n — номер останнього ненульового залишку в лівому ланцюзі Евкліда.

Доведення. Пункт 1 випливає з леми 1.

Пункт 2. Оскільки $r_{n-1} = r_n q_n = r_n q_n + 0$, то згідно з пунктом 1 маємо $D_\ell(r_i, r_{i+1}) = D_\ell(r_n, 0) = D_\ell(r_n)$. Тобто кожен лівий спільний дільник елементів r_i та r_{i+1} ділить

елемент r_n, а отже, r_n є лівим найбільшим спільним дільником r_i та r_{i+1} для всіх $i = 0, 1, \ldots, n-1$.

Пункт 3 доведемо методом математичної індукції за параметром i у порядку спадання.

Покажемо, що (6) справджується для найбільшого індексу $i = n-2$. Відповідно до (2) маємо $r_n = r_{n-2} - r_{n-1}q_{n-1}$. Отже,

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

Припустімо, що рівність (6) виконується для $i = k$, тобто $r_n = r_k y_{k+2} + r_{k+1}y_{k+1}$, і доведемо її для $i = k-1$. Підставимо $i = k$ у (2) та (3):

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

Звідси

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

Додамо й віднімемо елемент $r_k q_k y_{k+1}$, а потім скористаємося індуктивним припущенням:

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

Отже, співвідношення (6) справджується для $i = k-1$, а тому за індукцією воно виконується для всіх $i = n-2, n-3, \ldots, 1, 0$. □

Наслідок 3. *Нехай R — кільце без дільників нуля з одиницею, і нехай існує лівий слабкий алгоритм Евкліда для елементів $a, b \in R$. Тоді відповідна послідовність Безу для елементів a, b збігається з лівою послідовністю Безу для елементів a/d' та b/d', де d' — лівий дільник елемента $d := \mathrm{GCD}_\ell(a, b)$. Будь-які два сусідні члени відповідної послідовності Безу (3) є взаємно простими справа.*

Доведення. Нехай (2) — лівий алгоритм, де $a = r_0$ та $b = r_1$. Поділивши (2) на d' зліва, отримаємо:

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

У результаті ми отримуємо алгоритм Евкліда для елементів a/d' та b/d'. Оскільки квоти однакові, то й ліва послідовність Безу залишається незмінною. Якщо $d' = r_n$, то з (6) випливає:

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

Отже, кожен правий дільник елементів y_{i+2} та y_{i+1} ділить 1, а тому елементи y_{i+2} та y_{i+1} є взаємно простими справа для всіх $i = 0, 1, \ldots, n-2$. □

Користуючись ідеями Б. В. Забавського з праць [10, Theorem 2] та [11, Proposition 6], отримано критерій для Евклідових пар у кільцях стабільного рангу 1, а саме має місце така теорема.

Теорема 4. [9, теорема 8] *Нехай R — кільце зі стабільним рангом 1. Тоді пара $(a, b) \in R^2$ є евклідовою парою тоді й тільки тоді, коли правий ідеал $aR + bR$ є головним.*

Приклад 5. Нехай $a = 50$ і $b = 20$. Послідовність рівностей

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

є евклідовим ланцюгом для $a = 50$ і $b = 20$. Знайдімо рівність Безу для $a = 50$ і $b = 20$.

Обчислимо послідовність Безу для a та b:

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

Останній відмінний від нуля залишок — $r_4 = -50$, тому довжина ланцюга $n = 4$. Використовуючи означення послідовності Безу, маємо:

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

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

Згідно з теоремою 2, рівність $r_4 = ay_2 + by_1$ має виконуватися, тобто:

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

Приклад 6. Знайти обернений елемент до 11 в полі лишків Z_{9839}.

З малої теореми Ферма випливає, що таким елементом є 11^{9837}. Знайдемо цей елемент, скориставшись отриманими властивостями. Для цього побудуємо алгоритм Евкліда:

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

Коефіцієнт Безу y_1 є оберненим елементом до 11. Довжина ланцюга Евкліда дорівнює 3, тому

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

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

Приклад 7. Побудуймо слабкий лівий алгоритм Евкліда з $n = 4$ у кільці $M_2(\mathbb{Z})$:

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

і знайдемо (r_0, r_1) та відповідне лінійне подання.

Спершу оберімо довільно r_4, q_4, q_3, q_2, q_1 та обчислімо інші параметри:

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

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

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

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

Згідно з пунктом 2 теореми 2 матриця $r_4 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ є лівим найбільшим спільним дільником матриць

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

Щоб знайти рівності Безу, необхідно визначити послідовність Безу y_1, y_2, y_3, y_4:

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

$$y_2 = y_4 - q_2 y_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix},$$
$$y_1 = y_3 - q_1 y_2 = \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ -4 & -3 \end{bmatrix}.$$

З пункту 3 теореми 2 випливають такі рівності Безу:

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

тобто

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 33 & 21 \\ 69 & 43 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} + \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -4 & -3 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} -8 & 13 \\ -16 & 27 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} + \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 5 \\ 1 & 11 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix}.$$

2.2. Правий слабкий алгоритм Евкліда. Нехай R — кільце з одиницею. Послідовність рівностей

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

називатимемо *правим ланцюгом Евкліда* для a та b, якщо $r_0 := a$ і $r_1 := b$.

Елементи $r_0, \ldots, r_n, \ldots$ називатимемо *правими залишками*. Якщо $r_{i-1} = q_i r_i + r_{i+1}$ — це евклідове ділення, то r_{i+1} є остачею. Якщо, крім того, $r_n \neq 0$ та $r_{n+1} = 0$ (тобто $r_{n-1} = q_n r_n$), то правий евклідовий ланцюг називається *правим слабким алгоритмом Евкліда*. Елементи $y_1, y_2, \ldots, y_n$, які визначені співвідношеннями

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

називатимемо *правою послідовністю Безу*, а y_1 — *правим коефіцієнтом Безу* для a та b.

Теорема 8. *Нехай R — кільце з одиницею, (7) — скінченний правий ланцюг Евкліда для елементів $a, b \in R$, а (8) — відповідна права послідовність Безу, де $r_0 = a$ і $r_1 = b$. Тоді:*

(1) *Множини правих спільних дільників сусідніх залишків у (7) збігаються:*

$$D_r(a, b) = D_r(r_i, r_{i+1}), \qquad i = 0, 1, \ldots, n-1; \tag{9}$$

(2) *У випадку, коли ланцюг (7) є правим слабким алгоритмом Евкліда, елемент r_n є правим найбільшим спільним дільником a та b, і*

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

(3) *Рівності Безу для сусідніх остач у послідовності (7) мають вигляд:*

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

Зокрема, $r_n = y_2 a + y_1 b$, де n — номер останнього ненульового залишку в правому ланцюгу Евкліда (7).

Наслідок 9. *Нехай R — кільце без дільників нуля з одиницею, і нехай існує правий слабкий алгоритм Евкліда для елементів $a, b \in R$. Тоді відповідна послідовність Безу для елементів a, b збігається з правою послідовністю Безу для елементів $a \backslash d'$ та $b \backslash d'$, де d' — правий дільник елемента $d := \mathrm{GCD}_r(a, b)$. Будь-які два сусідні члени відповідної послідовності Безу (8) є взаємно простими зліва.*

Наслідки для комутативних кілець спрощуються. Теорема 2 та наслідок 3 зумовлюють такі твердження.

Наслідок 10. *Нехай R — комутативне кільце з одиницею, (2) — ланцюг Евкліда для елементів $a, b \in R$ при $b \neq 0$, а (3) — відповідна послідовність Безу. Тоді рівності Безу для сусідніх залишків у ланцюзі (2) мають вигляд:*

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

де n — індекс останнього відмінного від нуля залишку в (2). Зокрема, якщо ланцюг (2) є слабким алгоритмом Евкліда, то

$$(a, b) = a y_2 + b y_1.$$

Наслідок 11. *Нехай R — кільце з одиницею без дільників нуля. Припустимо, що для елементів a та b існує слабкий евклідів алгоритм. Тоді будь-які два сусідні члени послідовності Безу є взаємно простими. Крім того, послідовність Безу для елементів a та b збігається з послідовністю Безу для елементів a/d' та b/d', якщо d' ділить $d := \mathrm{GCD}(a, b)$.*

3. Деякі приклади

Насамкінець згадаймо відому лему про ділення з остачею цілих чисел, а також два елегантні доведення, які, судячи з підручників, не дуже відомі.

‘*Поділити з остачею*’ означає ‘*знайти частку q і остачу r для даного діленого a і дільника b*’, тобто числа, що задовольняють співвідношення:

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

Лема 12 (Евклідове ділення)**.** *Нехай a, b — цілі числа. Якщо $b = 0$, то ділення з остачею неможливе. Якщо $b \neq 0$, то частка q і остача r однозначно визначаються рівностями:*

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

Доведення. Якщо $b = 0$, то нерівність (13) хибна. Отже, остачі не існує, і ділення неможливе.

Далі припустимо, що $b \neq 0$. Нехай виконується (13). Поділивши нерівність (13) на $|b|$, отримаємо $0 \leqslant \frac{r}{|b|} < 1$, тобто $\frac{r}{|b|}$ є невід’ємним дробовим числом. Оскільки $\frac{b}{|b|} q$ є цілим числом, то:

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

Отже, $bq = |b|s$ і $r = a - bq = a - |b|s$, тому (14) виконується.

Навпаки, нехай (14) істинне. Отже, $|b|s = bq$, $a = |b|s + r = bq + r$ і

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

За означенням, $\frac{r}{|b|}$ є дробовою частиною числа $\frac{a}{|b|}$, тому:

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

Отже, (13) виконується, і лему доведено.

Ще одне доведення існування та єдиності. Розглянемо множину $M_{a,b} := \{a - bx \mid x \in \mathbb{Z}\}$ з лінійним порядком $\leqslant$. Кожне наступне число більше на $|b|$. Нерівність $0 \leqslant r < |b|$ можна записати як $r \geqslant 0$ і $r - |b| < 0$, що означає, що r є найменшим елементом у підмножині $M_{a,b}^{\geqslant 0}$ цілих невід'ємних чисел множини $M_{a,b}$. Оскільки множина всіх невід'ємних цілих чисел є цілком впорядкованою, то множина $M_{a,b}^{\geqslant 0}$ має найменший елемент, позаяк вона непорожня ($M_{a,b}^{\geqslant 0}$ містить $a + b^2|a|$). Оскільки найменший елемент існує і єдиний, то й остача існує і єдина, а з нею і відповідна частка. □

Приклад 13. Знайти рівності Безу для чисел 9367 та 4318.

Розв'язання. Застосуємо алгоритм Евкліда:

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

Отже, $d := (9367, 4318) = 17$. Щоб знайти рівності Безу, випишемо всі остачі та частки:

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

Номер останньої ненульової остачі в алгоритмі дорівнює 6, тому $n = 6$. Для обчислення відповідної послідовності Безу використовуємо формулу (3):

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

Тому отримуємо:

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

Використовуючи (12) для $i = 0, 1, 2, 3, 4$, отримуємо п'ять рівностей Безу:

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

Δ

Приклад 14. Знайдіть рівності Безу для ланцюга Евкліда:

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

Усі квоти цього ланцюга Евкліда такі:

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

Номер останнього ненульового залишку в ланцюгу Евкліда дорівнює 4 ($r_4 = 68$); тому $n = 4$. Обчислимо відповідну послідовність Безу за формулою (3):

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

Використовуючи (12) для $i = 0, 1, 2$, отримуємо три рівності:

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

Приклад 15. У кільці гауссових чисел знайти рівності Безу для чисел $62+21i$ та $16+18i$, користуючись рівностями:

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

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

Оскільки $r_5=0$, то заданий ланцюг Евкліда є слабким алгоритмом Евкліда. Позаяк останній відмінний від нуля залишок — $r_4=2+i$, то

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

Користуючись формулами (3), знайдемо послідовність Безу:

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

З теореми 2 отримуємо $r_4=r_jy_{j+2}+r_{j+1}y_{j+1}$ для всіх $j=0,1,2$. Отже,

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

Приклад 16. У кільці гауссових чисел знайти рівності Безу для чисел $36+30i$ та $16+3i$, користуючись ланцюгом Евкліда:

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

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

Останній відмінний від нуля залишок — $r_5=2-3i$, тому $n=5$. Знайдемо послідовність Безу, користуючись формулами (3):

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

З теореми 2 отримуємо $r_5=r_jy_{j+2}+r_{j+1}y_{j+1}$ для всіх $j=0,1,2,3$. Отже,

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

Висновки. Запропонований метод знаходження рівностей Безу (теореми 2 і 8) дозволяє ефективно проводити дослідження за допомогою слабкого алгоритму Евкліда як в комутативних (приклади 7, 15, 16), так і в некомутативних кільцях (приклад 7). А також отриманий метод результативніше використовує сам алгоритм Евкліда в довільних Евклідових кільцях (приклади 15, 16). Зокрема, знаходити обернений елемент в кільці $\mathbb{Z}_m$ (приклад 6).

Конфлікт інтересів і етика. Автор є членом редакційної колегії цього журналу. Для уникнення конфлікту інтересів, рукопис пройшов відповідну процедуру рецензування незалежними рецензентами, а прийняття рішення про публікацію здійснювалося незалежним редактором. Автор також заявляє про повне дотримання всіх правил етики журнальних досліджень.

Подяки. Автор висловлює щиру подяку рецензентам за слушні зауваження. Автор заявляє про відсутність спеціального фінансування цієї роботи.

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

UDC 512.712

Weak Euclidean algorithm and linear representation of gcd

Fedir Sokhatsky

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.

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

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