УДК 681

С.О. Яременко
І.А. Клєопа

АЛГОРИТМ ЕВКЛІДА ЯК ПРИКЛАД ОБЧИСЛЮВАЛЬНОЇ ЗАДАЧІ З ТЕОРІЇ ЧИСЕЛ

Вінницький національний технічний університет

Анотація

У роботі досліджується алгоритм Евкліда як фундаментальна обчислювальна задача в контексті елементарної теорії чисел. Розглядаються теоретичні основи алгоритму, його обчислювальна складність, та практичні застосування в криптографії. На конкретних числових прикладах демонструється розв'язання задач пошуку найбільшого спільного дільника, обчислення коефіцієнтів Безу та розв'язання лінійних конгруенцій з використанням систем комп'ютерної математики, зокрема Maple.

Ключові слова: алгоритм Евкліда, найбільший спільний дільник, рівняння Безу, обчислювальна складність, діофантові рівняння, криптографія, система Maple.

Abstract

The paper investigates the Euclidean algorithm as a fundamental computational problem in the context of elementary number theory. The theoretical foundations of the algorithm, its computational complexity, and practical applications in cryptography are considered. Specific numerical examples demonstrate the solution of the problems of finding the greatest common divisor, calculating Bezu coefficients, and solving linear congruences using computer mathematics systems, in particular Maple.

Keywords: Euclidean algorithm, greatest common divisor, Bezu equation, computational complexity, Diophantine equations, cryptography, Maple system.

Вступ

Теорія чисел – це розділ математики, який вивчає властивості цілих чисел, їхню будову, взаємозв’язки та закономірності, зокрема подільність чисел і операції над ними. Одним із ключових понять у теорії чисел є найбільший спільний дільник (НСД) двох або більше чисел, тобто найбільше натуральне число, на яке ці числа діляться без остачі. Для ефективного знаходження НСД у теорії чисел використовується алгоритм Евкліда — класичний і ефективний метод, заснований на ідеї, що НСД двох чисел не змінюється, якщо від більшого числа відняти менше або замінити більше число остачею від ділення на менше, що робить цей алгоритм швидким і зручним для практичного застосування. Метод розв'язання такого завдання викладено в класичній праці давньогрецького математика Евкліда у його монументальній праці «Начала» (The Elements), написаній приблизно 300 років до нашої ери.

Питання обчислювальних аспектів теорії чисел досліджували такі вчені, як Евклід, Карл Фрідріх Гаусс, П’єр Ферма, а в сучасній математиці – Дональд Кнут у праці «Мистецтво програмування» (1968–2011 рр.). Алгоритм Евкліда базується на основній теоремі арифметики: якщо $a > b > 0$, то НСД(a, b) = НСД(b, a mod b), де mod позначає остачу від ділення. Цей процес повторюється, доки не досягне нуля, і останнє ненульове число є НСД. У контексті теорії чисел алгоритм Евкліда не лише знаходить НСД, але й слугує основою для розв’язання лінійних діофантових рівнянь виду $ax + by = c$, де c кратне НСД(a, b).

Попри давність походження, алгоритм залишається одним з найефективніших та найпрактичніших інструментів сучасної обчислювальної математики. Актуальність дослідження обумовлена кількома чинниками. По-перше, алгоритм Евкліда слугує основою для розв'язання широкого класу задач в теорії чисел, включаючи розв'язання лінійних діофантових рівнянь, обчислення модульних обернених та розв'язання лінійних конгруенцій. По-друге, розширений варіант алгоритму має критичне значення для криптографічних алгоритмів, особливо при генерації приватних ключів у методі RSA. По-третє, алгоритм демонструє принципи ефективного обчислення, досягаючи логарифмічної складності відносно розміру вхідних даних, що було доведено французьким математиком Габріелем Ламе у 1844 році.

Метою роботи є аналіз алгоритму Евкліда як обчислювальної задачі з теорії чисел, його математичних основ, обчислювальної складності та практичного застосування, зокрема за допомогою системи комп'ютерної математики Maple.

Для досягнення мети були вирішені такі задачі:

- Визначити ключові математичні властивості алгоритму Евкліда та його історичний контекст.
- Розробити практичні приклади застосування алгоритму Евкліда для розв'язання діофантових рівнянь, лінійних конгруенцій та в криптографії.
- Продемонструвати можливості реалізації алгоритму за допомогою системи Maple на конкретних числових прикладах.

Результати дослідження

Найбільший спільний дільник двох натуральних чисел a і b визначається як найбільше натуральне число, на яке одночасно ділиться без залишку як число a, так і число b.

Наприклад, НСД(252, 105) = 21, оскільки 21 ділить як 252 = 21 × 12, так і 105 = 21 × 5, і ніякого більшого спільного дільника не існує.

Перевірка НСД в середовищі Maple виконується за допомогою команди gcd(a,b):

```
gcd(252, 105);
```

21

Алгоритм базується на фундаментальному властивості: якщо натуральне число g ділить числа a і b, то g також ділить їх різницю a - b. Більш ефективна форма алгоритму використовує операцію ділення з залишком. Якщо $a = bq + r$, де $0 \le r < b$ (q – неповна частка, r – залишок), то НСД(a, b) = НСД(b, r). Процес повторюється доти, доки залишок не дорівнює нулю.

Розширений алгоритм Евкліда реалізується шляхом послідовного ділення з остачею з одночасним обчисленням коефіцієнтів x_i та y_i, для яких виконується рівність $r_i=x_ia+y_i$. На кожному кроці визначається частка $q_i=[r_{i-1}/r_i]$, після чого нові значення залишку та коефіцієнтів обчислюються за формулами:

$$r_{i+1}=r_{i-1}-q_ir_i$$
$$x_{i+1}=x_{i-1}-q_ix_i$$
$$y_{i+1}=y_{i-1}-q_iy_i$$

Процес триває до нульового залишку, а останні ненульові коефіцієнти задають розв'язок рівняння ax+by=НСД(a,b). Це співвідношення відоме як рівняння або теорема Безу – одна з найважливіших теорем елементарної теорії чисел, названа на честь французького математика Етьєна Безу, хоча результат був відомий й раніше.

Приклад 1. Знайти НСД(803, 154). За допомогою теореми Безу необхідно виразити результат як 803s + 154t для деяких цілих s та t. Розширений алгоритм показує, що НСД(803, 154) = 11, і одна з можливих пар коефіцієнтів: 803 × 5 + 154 × (−26) = 11.

В Maple даний приклад можна розрахувати розширеним алгоритмом Евкліда, який матиме вигляд [7]:

```
My_Euclid := proc(a::integer, b::integer)
local r, q, x, y, i;
printf("a = %d, b = %d\n\n", a, b);
r[0] := a;  x[0] := 1;  y[0] := 0;
printf("'r'_0 = %d, 'x'_0 = %d, 'y'_0 = %d, [ %d = (%d) ]\n\n", r[0],
x[0], y[0], r[0], a);
r[1] := b;  x[1] := 0;  y[1] := 1;
printf("'q'_1 = 1, 'r'_1 = %d, 'x'_1 = %d, 'y'_1 = %d, [ %d = (%d)
]\n\n", r[1], x[1], y[1], r[1], b);
i := 1;
while r[i] <> 0 do
q[i] := floor(r[i-1]/r[i]);
r[i+1] := r[i-1] - q[i]*r[i];
x[i+1] := x[i-1] - q[i]*x[i];
y[i+1] := y[i-1] - q[i]*y[i];
```

```
  if r[i+1] <> 0 then
  printf("'q'_%d = %d, 'r'_%d = %d, 'x'_%d = %d, 'y'_%d = %d, [ %d =
%d(%d) - %d(%d) ]\n\n",
  i+1, q[i], i+1, r[i+1], i+1, x[i+1], i+1, y[i+1],
  r[i+1], 1, a, q[i], b);
  end if;
  i := i+1;
  end do;
  printf("gcd = %d, %d(%d) + %d(%d) = %d\n",
  r[i-1], x[i-1], a, y[i-1], b, r[i-1]);
  end proc:
  My_Euclid(803, 154);
```

```
                          a = 803, b = 154

          'r'_0 = 803, 'x'_0 = 1, 'y'_0 = 0, [ 803 = (803) ]

      'q'_1 = 1, 'r'_1 = 154, 'x'_1 = 0, 'y'_1 = 1, [ 154 = (154) ]

  'q'_2 = 5, 'r'_2 = 33, 'x'_2 = 1, 'y'_2 = -5, [ 33 = 1(803) - 5(154) ]

   'q'_3 = 4, 'r'_3 = 22, 'x'_3 = -4, 'y'_3 = 21, [ 22 = 1(803) - 4(154)
                                    ]

   'q'_4 = 1, 'r'_4 = 11, 'x'_4 = 5, 'y'_4 = -26, [ 11 = 1(803) - 1(154)
                                    ]

                    gcd = 11, 5(803) + -26(154) = 11
```

Перевірити результат також можна перевірити командою igcdex(a,b,'s','t');s,t;

```
> igcdex(803,154,'s','t');s,t;
```

```
                                  11
                               5, -26
```

Функція igcdex (integer gcd extender) є вбудованою процедурою в пакеті numtheory системи Maple. Вона повертає НСД та присвоює змінним s та t коефіцієнти Безу (s = 5, t =-26). Це дозволяє швидко й надійно розв'язувати такі задачі навіть для дуже великих чисел, де ручні обчислення стали б практично неможливими.

Діофантовим рівнянням називається рівняння вигляду $ax + by = c$, де a, b, c – цілі числа, а розв'язками є цілі числа x та y. Алгоритм Евкліда дозволяє розв'язати такі рівняння, якщо НСД(a, b) ділить c.

Приклад 2: Знайти найбільший спільний дільник чисел 1071 і 462, а також представити його у вигляді лінійної комбінації цих чисел.

Розв'язання за допомогою алгоритму Евкліда [7] :

$$1071 = 462 \times 2 + 147$$
$$462 = 147 \times 3 + 21$$
$$147 = 21 \times 7 + 0$$

Отже, НСД(1071, 462) = 21. Для знаходження коефіцієнтів виконуємо зворотний хід:

$$21 = 462 - 147 \times 3$$
$$21 = 462 - (1071 - 462 \times 2) \times 3$$
$$21 = 462 - 1071 \times 3 + 462 \times 6$$
$$21 = 462 \times 7 + 1071 \times (-3)$$

Таким чином, $1071 \times (-3) + 462 \times 7 = 21$.

Реалізація в системі Maple:

```
  My_Euclid(1071, 462);
```

```
                          a = 1071, b = 462
```

```
'r'_0 = 1071, 'x'_0 = 1, 'y'_0 = 0, [ 1071 = (1071) ]

'q'_1 = 1, 'r'_1 = 462, 'x'_1 = 0, 'y'_1 = 1, [ 462 = (462) ]

'q'_2 = 2, 'r'_2 = 147, 'x'_2 = 1, 'y'_2 = -2, [ 147 = 1(1071) -
2(462) ]

'q'_3 = 3, 'r'_3 = 21, 'x'_3 = -3, 'y'_3 = 7, [ 21 = 1(1071) - 3(462)
]

gcd = 21, -3(1071) + 7(462) = 21
```

```
igcdex(1071,462,'s','t');s,t;
```

```
21
-3, 7
```

Однією з найпрактичніших задач, де використовується алгоритм Евкліда, є розв'язання лінійних конгруенцій вигляду $ax \equiv b \pmod m$. Таке рівняння має розв'язок тоді й тільки тоді, коли НСД(a, m) ділить b.

Приклад 3: Розв'язати конгруенцію $17x \equiv 3 \pmod{29}$.

Спочатку знаходимо модульний мультиплікативний обернений: число v таке, що $17v \equiv 1 \pmod{29}$. Використовуючи розширений алгоритм Евкліда:

$$29 = 17 \times 1 + 12$$
$$17 = 12 \times 1 + 5$$
$$12 = 5 \times 2 + 2$$
$$5 = 2 \times 2 + 1$$
$$2 = 1 \times 2 + 0$$

Зворотний хід дає: $1 = 5 - 2 \times 2 = 5 - 2 \times (12 - 5 \times 2) = \ldots = 12 \times 17 + (-7) \times 29$. Отже, $17 \times 12 \equiv 1 \pmod{29}$, тобто модульний обернений дорівнює 12. Тоді $x \equiv 3 \times 12 \equiv 36 \equiv 7 \pmod{29}$.

Перевірка:

```
My_Euclid(17, 29);
```

```
a = 17, b = 29

'r'_0 = 17, 'x'_0 = 1, 'y'_0 = 0, [ 17 = (17) ]

'q'_1 = 1, 'r'_1 = 29, 'x'_1 = 0, 'y'_1 = 1, [ 29 = (29) ]

'q'_2 = 0, 'r'_2 = 17, 'x'_2 = 1, 'y'_2 = 0, [ 17 = 1(17) - 0(29) ]

'q'_3 = 1, 'r'_3 = 12, 'x'_3 = -1, 'y'_3 = 1, [ 12 = 1(17) - 1(29) ]

'q'_4 = 1, 'r'_4 = 5, 'x'_4 = 2, 'y'_4 = -1, [ 5 = 1(17) - 1(29) ]

'q'_5 = 2, 'r'_5 = 2, 'x'_5 = -5, 'y'_5 = 3, [ 2 = 1(17) - 2(29) ]

'q'_6 = 2, 'r'_6 = 1, 'x'_6 = 12, 'y'_6 = -7, [ 1 = 1(17) - 2(29) ]

gcd = 1, 12(17) + -7(29) = 1
```

```
3*12 mod 29;
```

```
7
```

```
17*7 mod 29;
```

```
3
```

Висновок

1. Показано актуальність алгоритму Евкліда, описаного понад дві тисячі років тому в його праці «Начала», та його практичну цінність у сучасну інформаційну епоху; підтверджено ефективність алгоритму;

2. Встановлено необхідність глибокого розуміння математичних алгоритмів для побудови надійних криптографічних систем і розв'язання прикладних обчислювальних задач; відзначено роль систем комп'ютерної математики, зокрема Maple, у формуванні обчислювального мислення.

3. Окреслено перспективи подальших досліджень, зокрема вивчення варіацій алгоритму Евкліда для многочленів, аналіз його поведінки в різних числових системах, дослідження застосувань у сучасній криптографії, а також оптимізацію обчислень для великих чисел за допомогою модифікованих алгоритмів.

Список літератури

1. Вікіпедія. Алгоритм Евкліда https://en.wikipedia.org/wiki/Euclidean_algorithm
2. Вікіпедія. Розширений алгоритм Евкліда https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm
3. Алгоритм Евкліда для обчислення найбільшого спільного дільника. CP-Algorithms. https://cp-algorithms.com/algebra/euclid-algorithm.html
4. Розширений алгоритм Евкліда. CP-Algorithms. https://cp-algorithms.com/algebra/extended-euclid-algorithm.html
5. Вікіпедія. Рівняння Безу https://uk.wikipedia.org/wiki/%D0%A0%D1%96%D0%B2%D0%BD%D1%8F%D0%BD%D0%BD%D1%8F_%D0%91%D0%B5%D0%B7%D1%83
6. Лінійні діофантові рівняння. CP-Algorithms. https://cp-algorithms.com/algebra/linear-diophantine-equation.html
7. В. М. Михалевич, Л. О. Майданевич, Використання системи MAPLE у математичних задачах криптографії. Повідомлення 1. Елементарна теорія чисел. с. 105–118, 2024.

Яременко Софія Олександрівна – студентка групи 2 КІТС – 25б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: sofiaaremenko339@gmail.com

Науковий керівник: ***Клєопа Ірина Анатоліївна*** – pHd, доцент, кафедра вищої математики, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: paceka08@vntu.edu.ua

Yaremenko Sofiia Oleksandrivna – student of group 2CITS – 25b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: sofiaaremenko339@gmail.com

Scientific supervisor: ***Klieopa Iryna Anatoliivna*** – PhD, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: paceka08@vntu.edu.ua