Київський національний університет імені Тараса Шевченка

Факультет комп’ютерних наук та кібернетики

Кафедра системного аналізу та теорії прийняття рішень

Звіт

з лабораторної роботи №2

Точна арифметика цілих чисел

Виконав

студент(ка) групи К-23 Флакей Р.Р.

**Постановка задачі:**

Написати клас, що реалізує динамічне подання “довгих” цілих чисел. Довжина

(розрядність) і основа позиційного числення (якщо алгоритм передбачає) вводяться як

параметр.

1. Множення невід’ємних цілих чисел методом Карацуби [Кнут, т.2, с. 336].

2. Множення невід’ємних цілих чисел методом Тоома-Кука [Кнут, т.2, с. 340].

3. Множення невід’ємних цілих чисел методом Шенхаге [Кнут, т.2, с. 344].

4. Множення невід’ємних цілих чисел методом Штрассена [Кнут, т.2, с. 347–350].

5. Обчислення оберненої величини з високою точністю (алгоритм Кука) [Кнут, т.2,

с. 340].

6. Ділення цілих чисел алгоритмом Кука [Кнут, т.2, с. 340].

7. Перевірка простоти числа методом Лемера [Шнайер, с. 297].

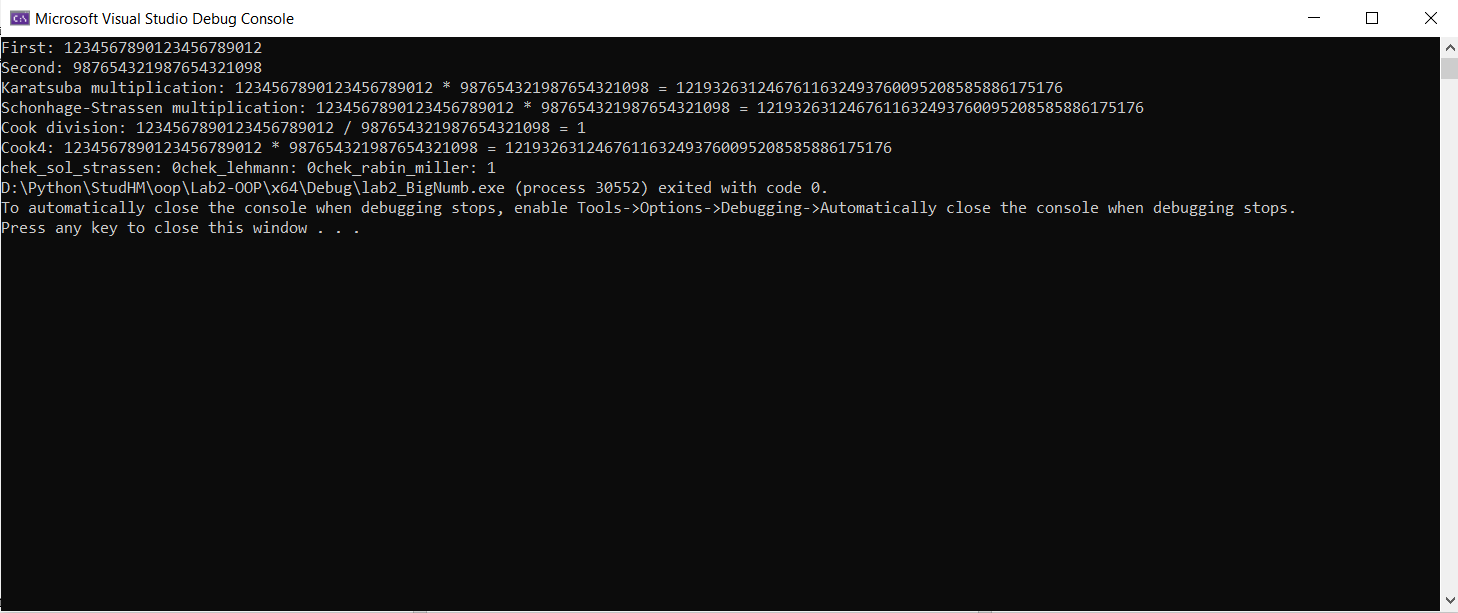
8. Перевірка простоти числа методом Рабіна–Міллера [Шнайер, с. 298].

9. Перевірка простоти числа методом Соловея–Штрассена [Шнайер, с. 298].

~~10.Перевірка простоти числа методом Фробеніуса~~

~~(https://en.wikipedia.org/wiki/Quadratic\_Frobenius\_test).~~

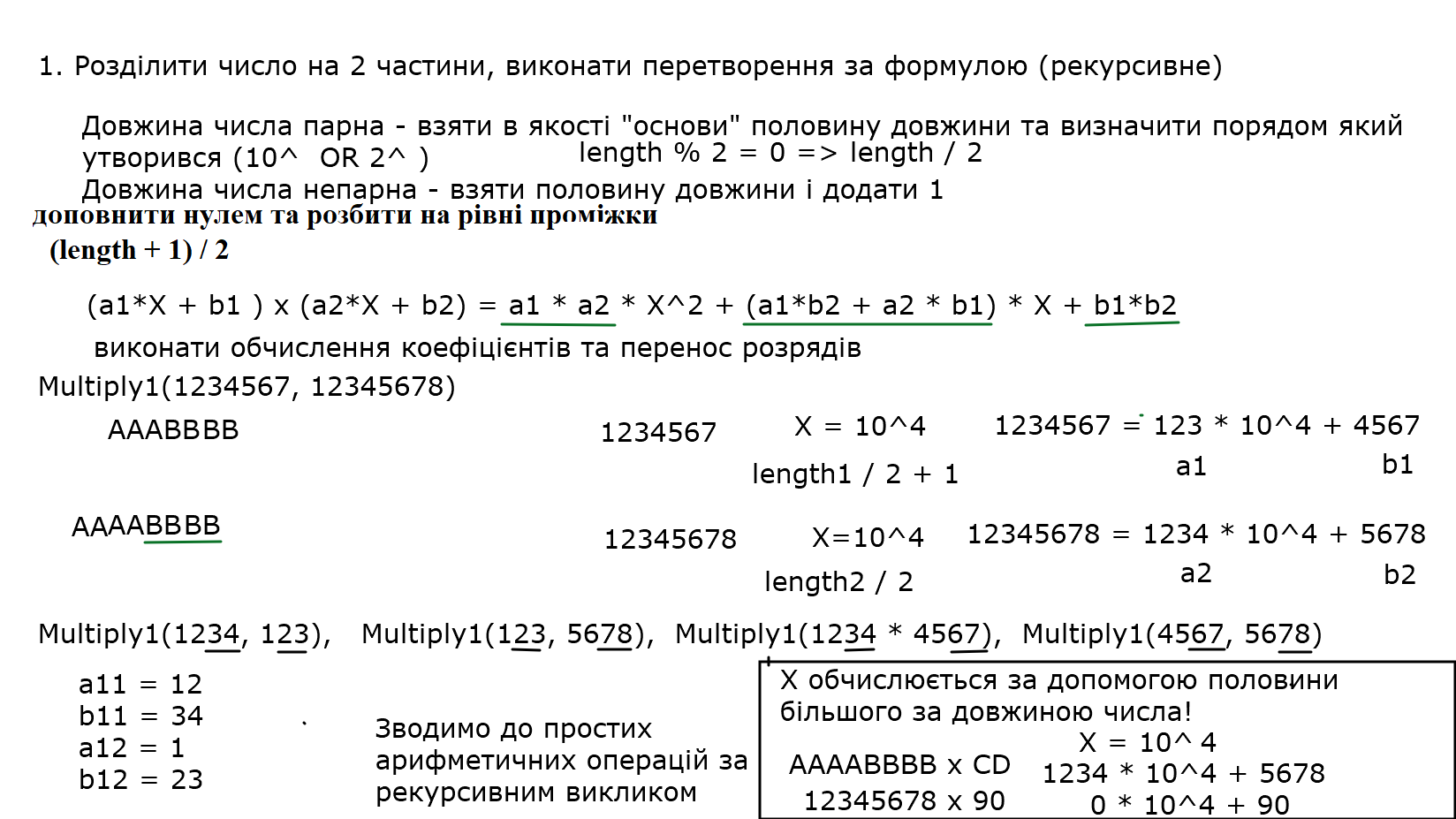
**Обрані великі числа:**



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *m* | = | 12 | 3456 | 7890 | 1234 | 5678 | 9012 |
| *n* | = | 9 | 8765 | 4321 | 9876 | 5432 | 1098. |
|  |  |  |  |  |  |  |  |

**1. Множення невід’ємних цілих чисел методом Карацуби [Кнут, т.2, с. 336].**

**Множення Карацуби**— метод швидкого [множення](https://uk.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F), який дозволяє перемножувати два [*n*-значних](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B7%D0%B8%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F) числа зі складністю обчислення:

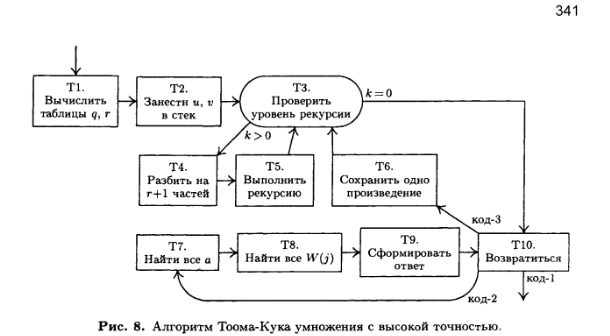
{\displaystyle M(n)=O(n^{\log \_{2}3}),\quad \log \_{2}3\approx 1{,}5849\ldots }

First: 1234567890123456789012

Second: 987654321987654321098

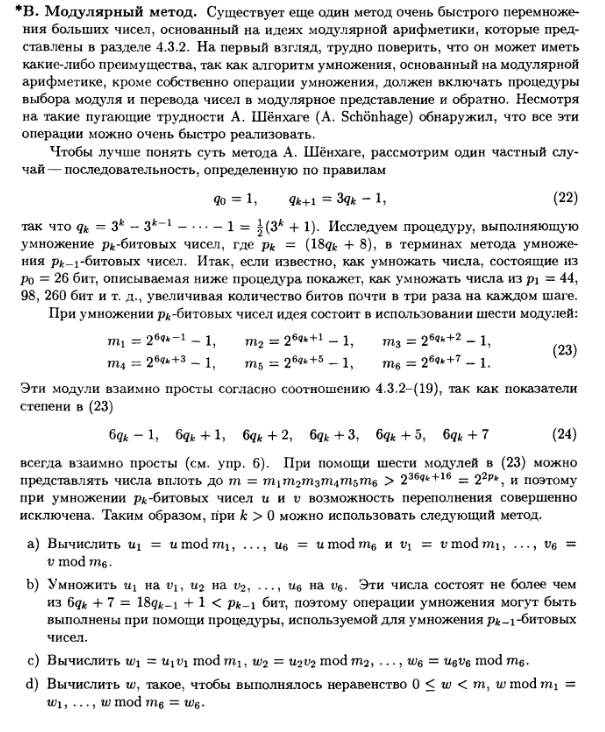
Karatsuba multiplication: 1234567890123456789012 \* 987654321987654321098 = 1219326312467611632493760095208585886175176

**2. Множення невід’ємних цілих чисел методом Тоома-Кука [Кнут, т.2, с. 340].**

****

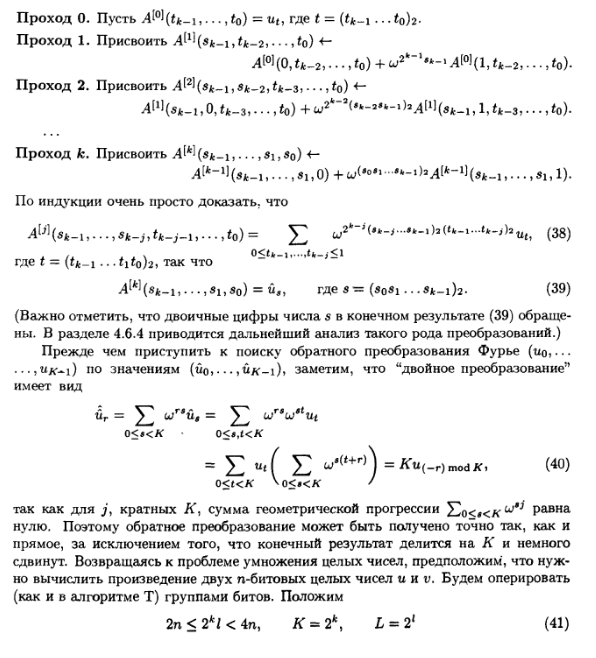
Toom-Cook: 1234567890123456789012 \* 987654321987654321098 = 1219326312467611632493760095208585886175176

**3. Множення невід’ємних цілих чисел методом Шенхаге [Кнут, т.2, с. 344].**

****

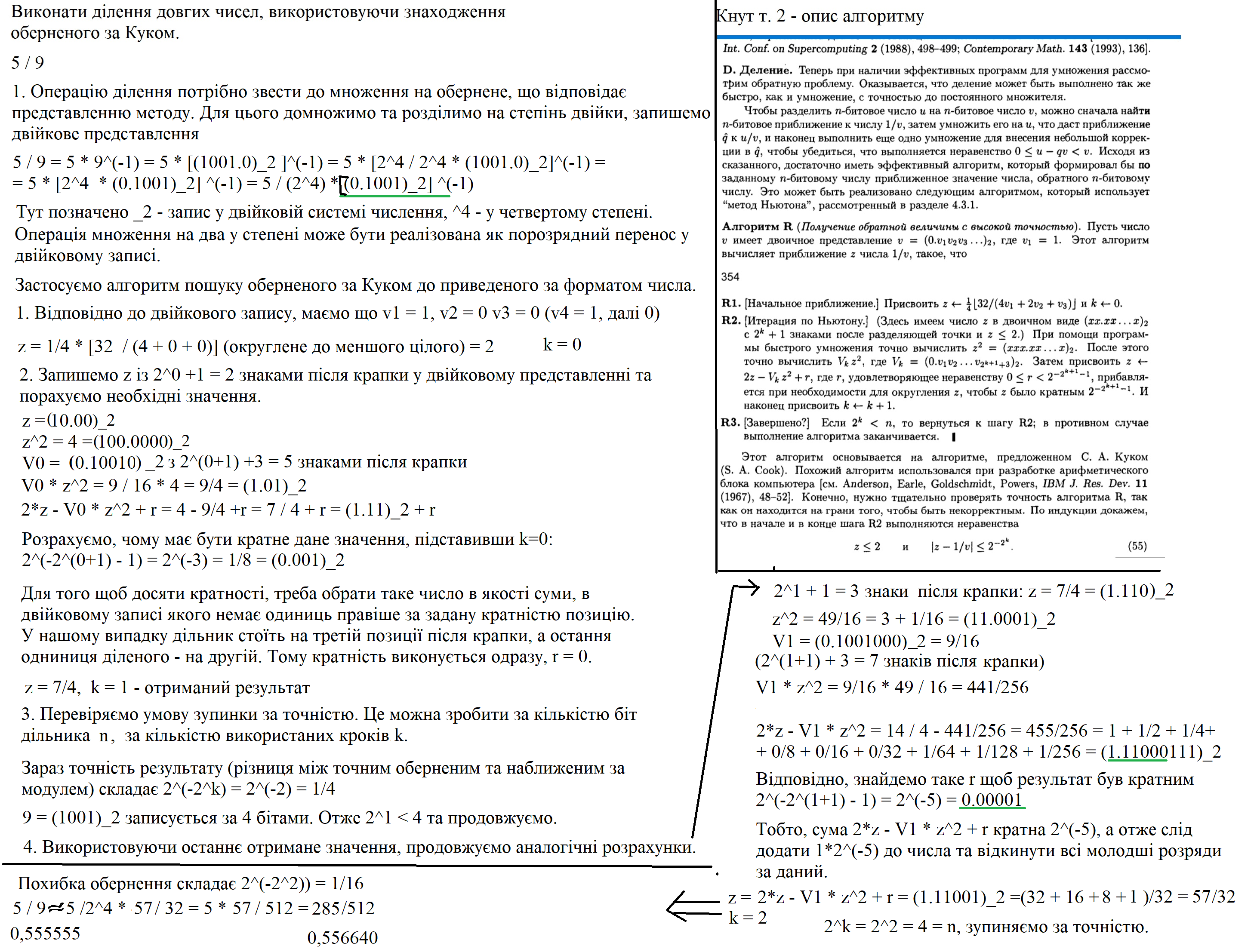
**Schonhage multiplication: 1234567890123456789012 \* 987654321987654321098 = 1219326312467611632493760095208585886175176**

**4. Множення невід’ємних цілих чисел методом Штрассена [Кнут, т.2, с. 347–350].**

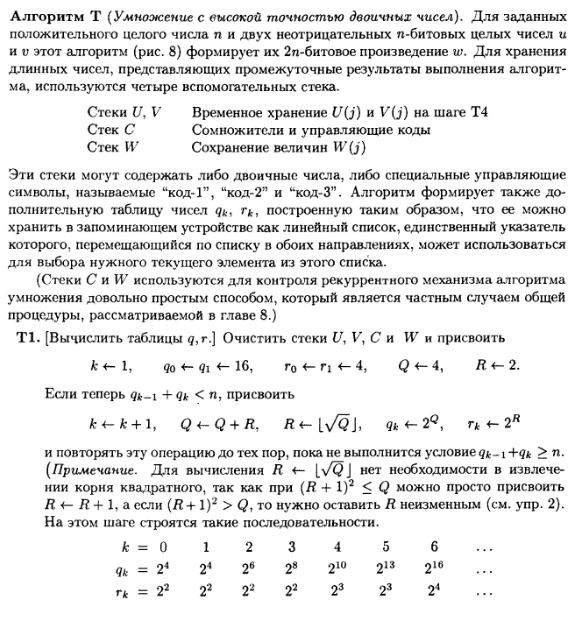
****

**Strassen multiplication: 1234567890123456789012 \* 987654321987654321098 = 1219326312467611632493760095208585886175176**

**5. Обчислення оберненої величини з високою точністю (алгоритм Кука) [Кнут, т.2,**

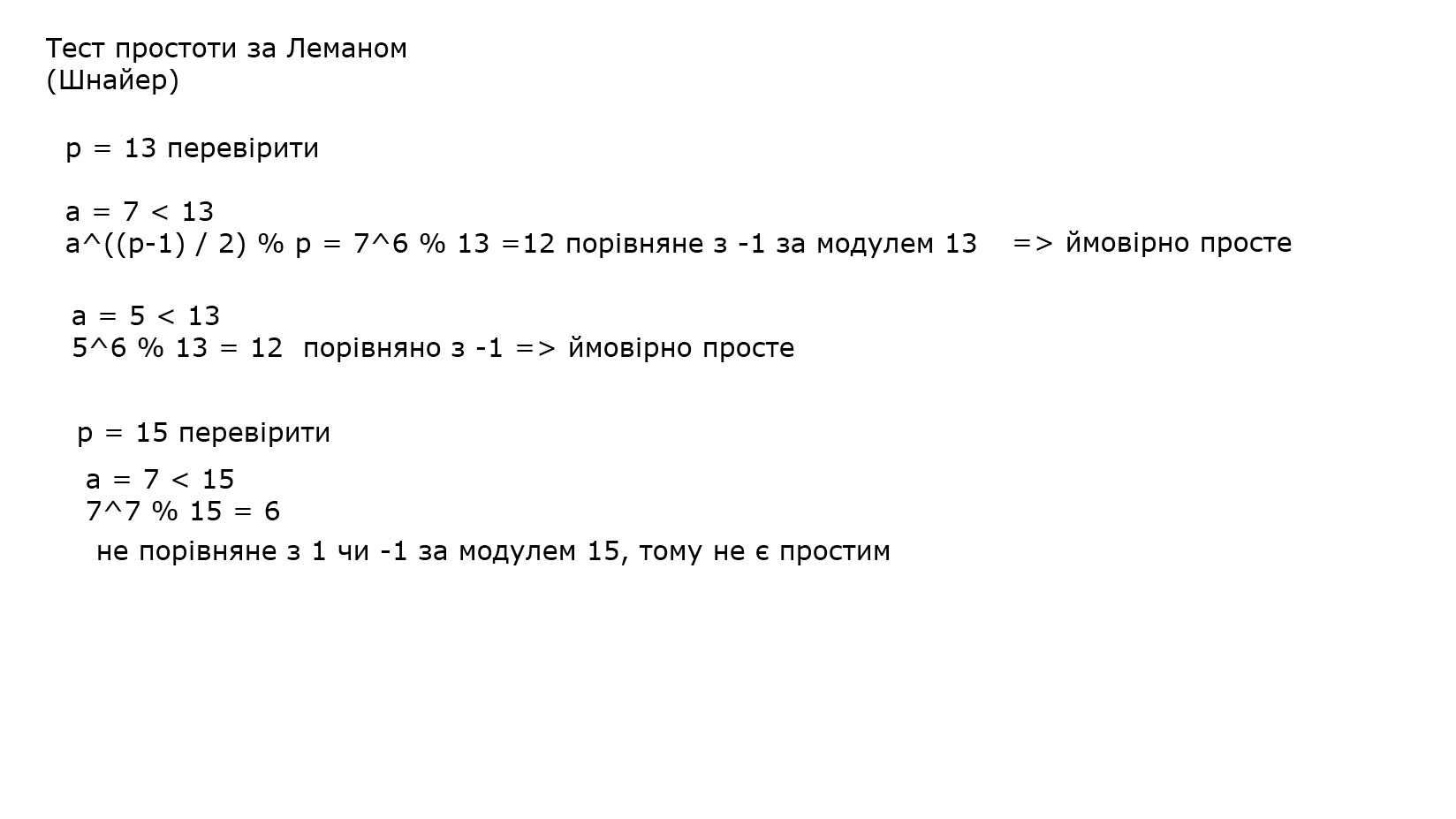


**6. Ділення цілих чисел алгоритмом Кука [Кнут, т.2, с. 340].**



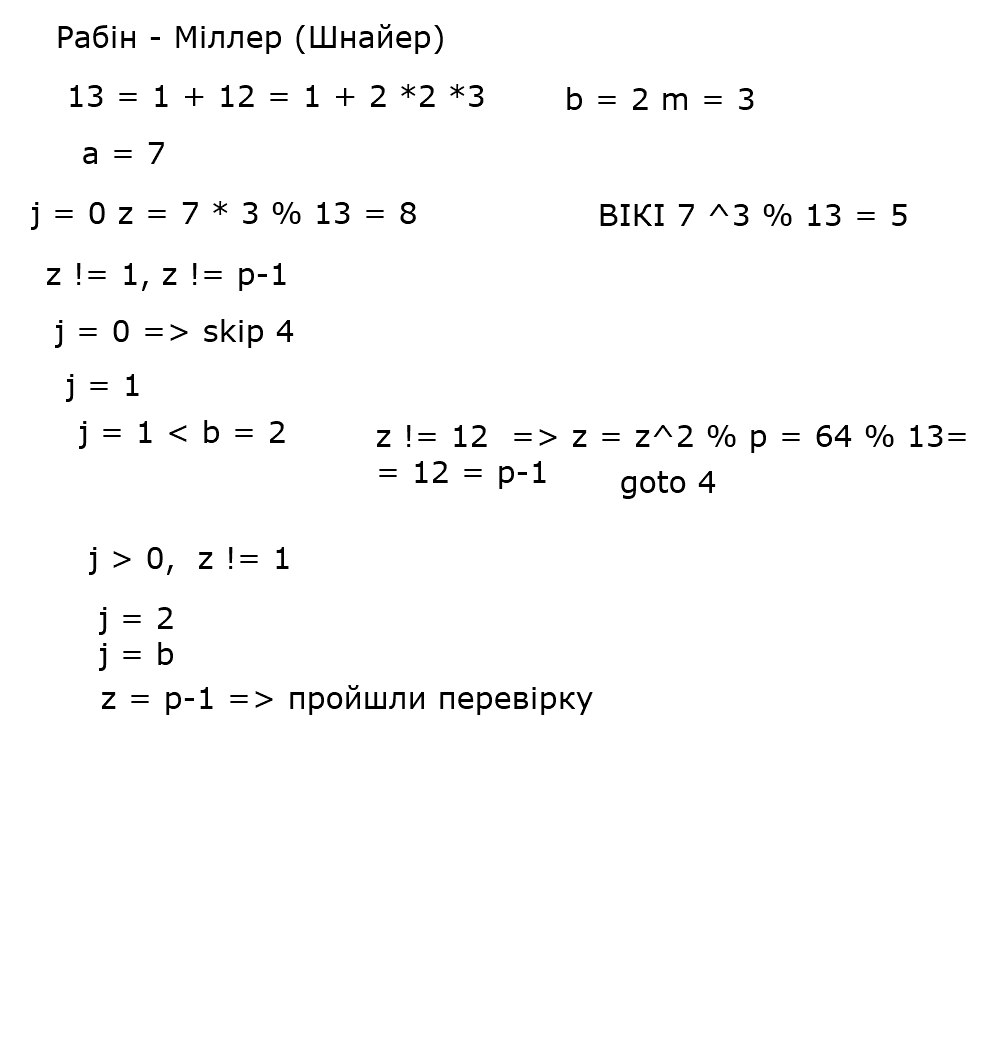
Cook division: 1234567890123456789012 / 987654321987654321098 = 1

**7. Перевірка простоти числа методом Лемера [Шнайер, с. 297].**



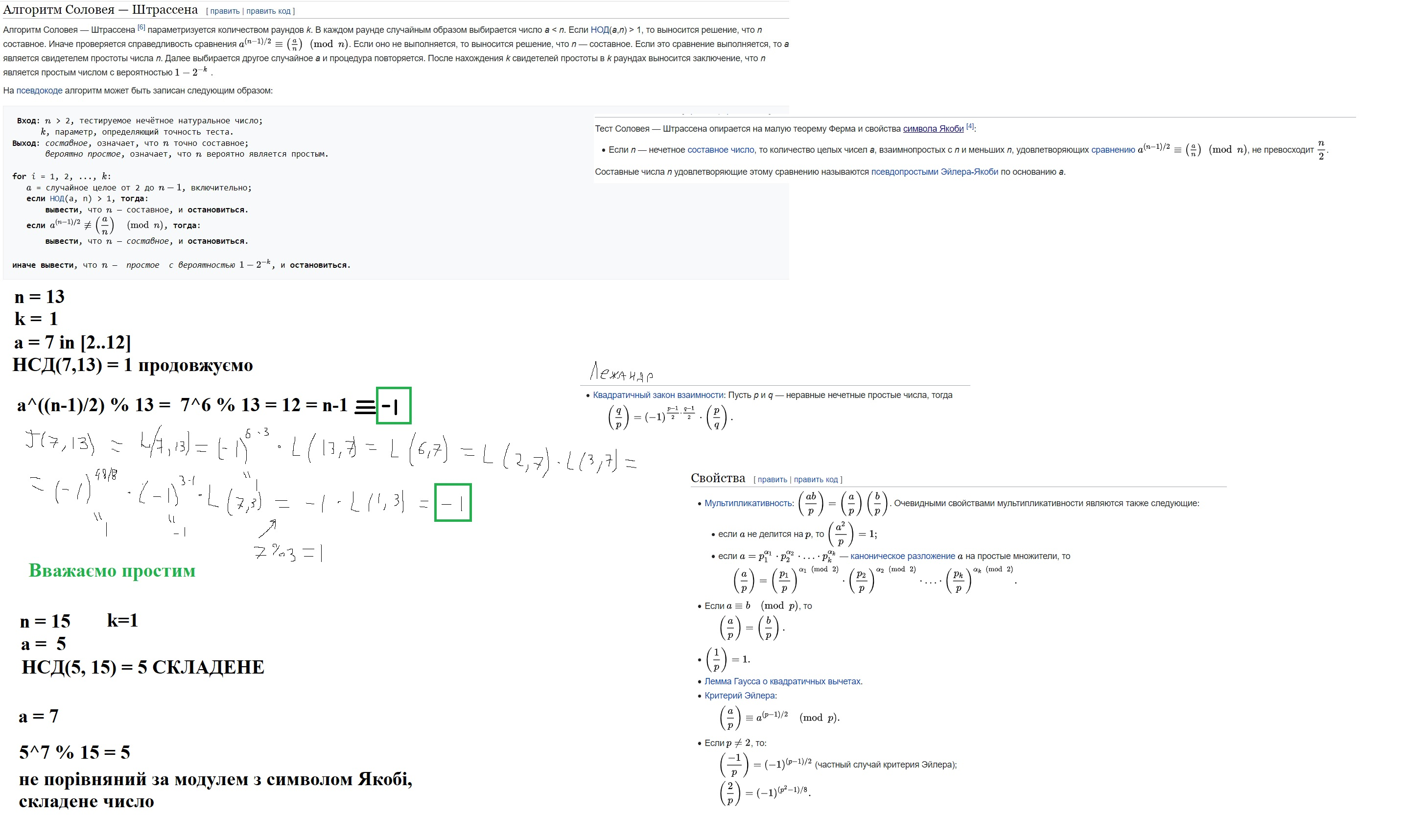
lehmann: 1

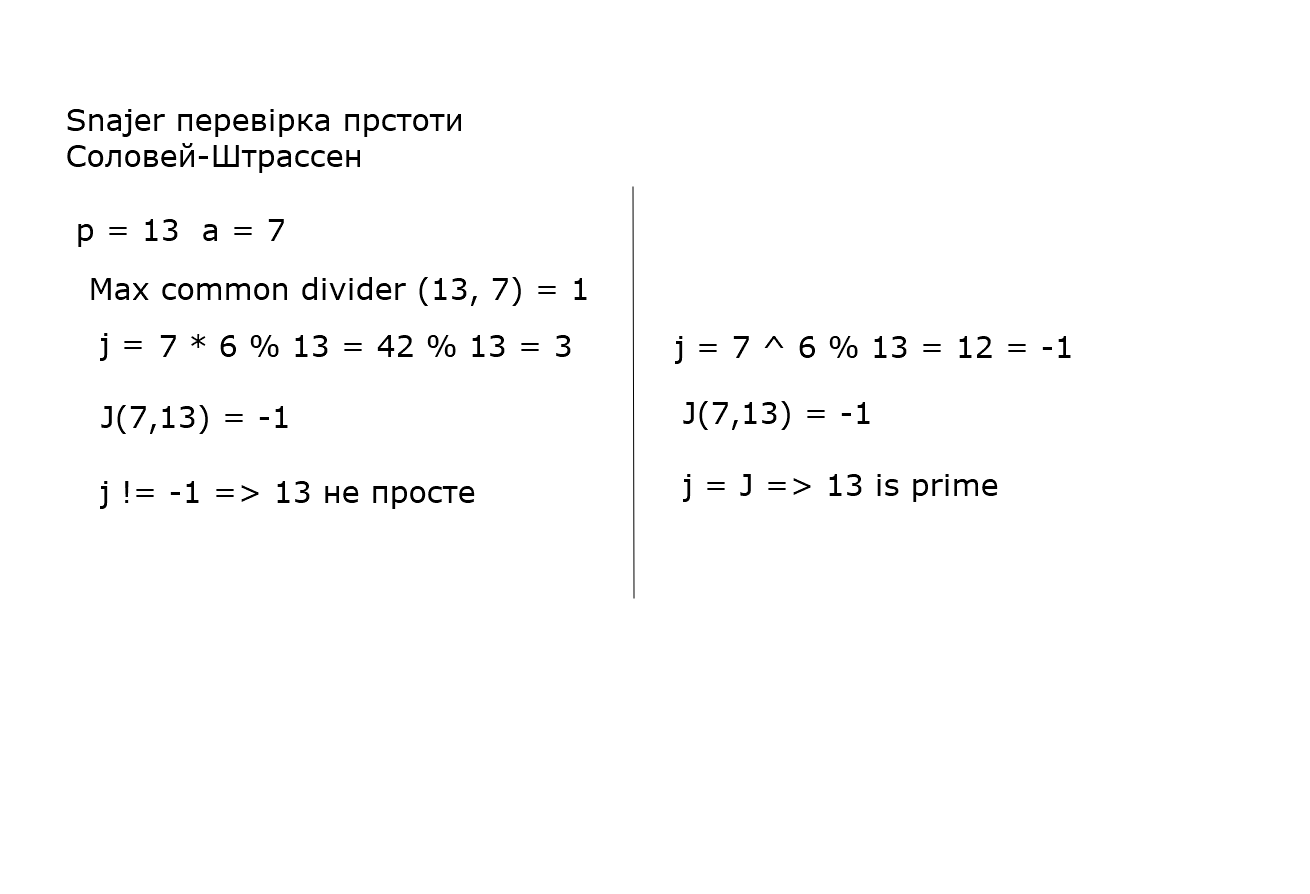
**8. Перевірка простоти числа методом Рабіна–Міллера [Шнайер, с. 298].**



rabin\_miller: 1

**9. Перевірка простоти числа методом Соловея–Штрассена [Шнайер, с. 298].**



 sol\_strassen: 1