УДК

В. М. Михалевич
І.С. Кот

Фрагменти навчального Maple-тренажера для реалізації тесту Міллера–Рабіна

Вінницький національний технічний університет

Анотація

Запропоновано варіант одного з ключових фрагментів навчального програмного тренажера, розробленого в середовищі системи комп'ютерної математики Maple. Тренажер призначено для опанування студентами алгоритму тестування чисел на простоту методом Міллера–Рабіна. Наведено приклади роботи тренажера у вигляді покрокового виведення результатів обчислень, що супроводжуються текстовими коментарями.

Ключові слова: навчальний Maple-тренажер, тест Міллера–Рабіна, прості числа, складені числа, криптографія.

Abstract

A version of a key module of an educational software simulator developed within the Maple computer algebra system is presented. The simulator is intended to help students master primality testing using the probabilistic Miller–Rabin method. Examples of the simulator's operation are provided as step-by-step outputs of computations accompanied by explanatory comments.

Keywords: educational Maple simulator, Miller–Rabin test, prime numbers, composite numbers, cryptography.

Вступ

Безпека сучасних криптосистем критично залежить від використання великих простих чисел. Пряма перевірка чисел на простоту шляхом перебору дільників є ресурсомісткою, тому використання систем комп'ютерної математики (СКМ) у навчальному процесі дозволяє знизити обчислювальне навантаження на студента та підвищити ефективність засвоєння складних алгоритмів теорії чисел.

Одним із таких алгоритмів є тест Міллера–Рабіна, який широко застосовується в сучасній криптографії. Проте традиційні статичні навчальні матеріали у форматах PDF або DOC часто обмежують можливості СКМ, фактично перетворюючи їх на пасивне джерело інформації.

Для подолання цього обмеження в роботі використано концепцію навчальних Maple-тренажерів (НМТ), що реалізує технологію «живих сторінок», де обчислювальний супровід бере на себе система, а студент зосереджується на логіці методу.

Метою роботи є розробка версії ключового фрагмента навчального тренажера в СКМ Maple, що відтворює всі кроки тесту Міллера–Рабіна та супроводжує обчислення текстовими поясненнями, зокрема щодо класифікації числа як «складеного» або «ймовірно простого».

Результати дослідження

Концепція розробки навчальних Maple-тренажерів (НМТ) викладена в [1, 2], технологія «живих сторінок» - в [3]. Різні варіанти реалізації концепції та технології викладено у численних працях, зокрема, [4] – для розв'язання задач лінійного програмування; [5] – для розробки електронних освітніх ресурсів; [6] – для організації самостійної роботи студентів; [7] – для розв'язання задач з математичних основ криптографії.

Розроблений фрагмент НМТ базується на реалізації процедури MilT2, що автоматизує перевірку числа n на простоту за такою схемою:

1. **Представлення числа**: Число $n-1$ подається у вигляді $2^s \cdot d$, де d — непарне число.
2. **Вибір основи**: Обирається випадкове (або задане користувачем) ціле число a (свідок) з діапазону $1 < a < n-1$.

3. **Обчислення послідовності**. Обчислюються значення $a^d(mod\ n), a^{2d}(mod\ n), \dots, a^{2^{s-1}d}(mod\ n)$.
4. **Аналіз результатів**:
   - Якщо перший елемент послідовності дорівнює 1 або будь-який елемент дорівнює -1 $(mod\ n)$, число вважається «ймовірно простим»;
   - в іншому випадку число n є складеним.

Приклади застосування тренажера

```
MilT2(89027,2);
```

$$n = 89027$$

$$n = 2^{(k)}\ (q) + 1$$

$$89027 = 2^{(1)}\ (44513) + 1$$

$$k = 1$$

$$q = 44513$$

Обчислимо члени послідовності:

$$2^{(i\,q)},\ i = 1, 2, \dots, 2^{(0)}$$

$$2^{(2^{(0)}\ (44513))} = (-6730)\ (modp\ n)$$

$$[2^{(2^{(1)}\ (44513))} = (-6730)^{(2)}] = (-21843)\ (modp\ n)$$

В послідовності відсутнє число (-1), отже число n=89027 є складеним.

```
MilT2(89041,2);
```

$$n = 89041$$

$$n = 2^{(k)}\ (q) + 1$$

$$89041 = 2^{(4)}\ (5565) + 1$$

$$k = 4$$

$$q = 5565$$

Обчислимо члени послідовності:

$$2^{(i\,q)},\ i = 1, 2, \dots, 2^{(3)}$$

$$2^{(2^{(0)}\ (5565))} = (5937)\ (modp\ n)$$

$$[2^{(2^{(1)}\ (5565))} = 5937^{(2)}] = (-12267)\ (modp\ n)$$

$$[2^{(2^{(2)}\ (5565))} = (-12267)^{(2)}] = (-1)\ (modp\ n)$$

Число n=89041є, ймовірно, простим.

Особливістю тренажера є інтерактивне відтворення кожного кроку піднесення до степеня за модулем. Це дає змогу студенту не лише отримати кінцевий результат, а й простежити момент порушення умов простоти (наприклад, появу «нетривіального квадратного кореня з одиниці»), що є принципово важливим для розуміння математичної суті тесту.

Висновки

Запропонований фрагмент навчального Maple-тренажера пройшов апробацію під час лекційних і лабораторних занять, а також у процесі самостійної роботи студентів факультету інформаційних технологій і комп'ютерної інженерії ВНТУ. Практичне впровадження інструменту отримало позитивні відгуки здобувачів освіти, які відзначили зручність його використання, інформативність покрокової візуалізації алгоритму Міллера–Рабіна та зрозумілість текстових пояснень, що супроводжують обчислення. Отримані результати підтверджують ефективність використання СКМ Maple для подолання обчислювального бар'єра при вивченні складних, зокрема ймовірнісних методів. Застосування такого тренажера дозволяє змістити акцент із рутинних обчислень на глибше розуміння математичних основ криптографічного захисту інформації, що є важливим для підготовки майбутніх фахівців.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Михалевич В. М. Навчально-контролюючий Maple — комплекс з вищої математики / В. М. Михалевич // Інформаційні технології та комп'ютерна інженерія. — 2004. — № 1. — С. 74–78.
2. Михалевич В. М. Розвиток системи Maple у навчанні вищої математики майбутніх інженерів-механіків : монографія / В. М. Михалевич, Я. В. Крупський. — Вінниця: ВНТУ, 2013. — 236 с. ISBN. — 978-966-641-539-7.
3. Михалевич В.М. Реалізації технології "живих сторінок" в Maple, MathCad, Excel // Вісник ВПІ. – 2004. - № 3. – С. 90-95.
4. Михалевич В. М. Використання системи комп'ютерної алгебри для висвітлення ключових ідей симплекс-алгоритму / В. М. Михалевич, О. І. Тютюнник // Теорія та методика навчання математики, фізики, інформатики : [зб. наук. праць]. — Випуск IX. — Кривий3 Ріг : Видавничий відділ НМетАУ, 2011. — С.113–118.
5. Михалевич В. М. Розробка електронних освітніх ресурсів в середовищі СКМ Maple [Текст] / В. М. Михалевич, Я. В. Крупський, Ю. В. Добранюк // Математика та інформатика у вищій школі: виклики сучасності : зб. наук. праць за матеріалами Всеукр. наук.-практ. конф., 18-19 травня 2017 р. / М-во освіти і науки України, Вінницький державний педагогічний університет імені Михайла Коцюбинського [та ін.]. - Вінниця : ФОП Рогальська І. О., 2017.- С. 69-72.
6. Михалевич В. М. Організація самостійної роботи студентів шляхом використання системи комп'ютерної математики Maple / В. М. Михалевич, Я. В. Крупський, О. І. Тютюнник // Вісник Вінницького політехнічного інституту. - 2014. - № 3. - С. 114-118.
7. Mykhalevych V., Maidanevych L. Use of the maple system in mathematical problems of cryptography. Part 1. Elementary theory of numbers. Information technology and computer engineering. 2024. Т. 59, № 1. С. 105–118. URL: https://doi.org/10.31649/1999-9941-2024-59-1-105-118.

***Іларія Сергіївна Кот**– студентка групи 1ЕХКБ-25Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ilariakot09@gmail.com*

Науковий керівник: ***Володимир Маркусович Михалевич***— д-р техн. наук, професор, завідувач кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: mykhalevych@vntu.edu.ua

Kot Ilaria S. *– student of group 1EHKB-25B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ilariakot09@gmail.com*

Supervisor: ***Mykhalevych Volodymyr M.*** —Dr. Sc. (Eng.), Professor, Head of the Chair for Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, mykhalevych@vntu.edu.ua