УДК 517.962.26

Д.В. Кручинин, Ю.В. Шабля

Программное обеспечение для анализа тестов простоты натурального числа

Предложен инструментарий для анализа тестов простоты числа в виде специализированного программного обеспечения. Указан перечень функциональных возможностей разработанного программного обеспечения. Описано предназначение данного программного средства, показана возможность применения для существующих тестов простоты, а также для новых разрабатываемых критериев простоты на основе свойств композиции двух производящих функций.
Ключевые слова: тесты на простоту числа, производящие функции, программное обеспечение, анализ, сравнение.

Область применения простых чисел. В современном мире при переходе к информационному типу общества ценность такого ресурса, как информация, переходит на первый план. Владение ценной информацией предоставляет преимущества ее владельцу, а утрата или похищение такой информации могут привести к большим проблемам. Вся актуальность тематики в области защиты информации отражена в многочисленных работах и исследованиях, например таких, как [1–5]. Проблемами в области защиты информации занимается целый раздел математики, выделенный в отдельную науку, – криптография.

Простым числом называют натуральное число больше единицы, которое имеет только два различных делителя: единицу и само себя. Простые числа нашли широкое применение в области криптографии с открытым ключом. Многие криптографические алгоритмы используют простые числа, а некоторые даже полностью основаны именно на свойствах простых чисел, например RSA [6], криптографическая сложность которого заключается в проблеме факторизации больших чисел, т.е. в разложении на простые множители.

Еще одной областью применения простых чисел является наличие функций проверки простоты натурального числа в различных математических пакетах, таких как Maxima, MathLab, Maple, Mathematica. Данные функции возвращают положительный либо отрицательный ответ для заданного числа, и положительный ответ говорит о том, что заданное число с большой долей вероятности является простым числом.

Проблема определения простоты натурального числа. История появления простых чисел берет свое начало с древнейших времен. Изучение простых чисел всегда притягивало математиков, и, например, такой известный древнегреческий математик, как Евклид, уже тогда смог предложить доказательство бесконечности множества простых чисел [7].

Несмотря на такую долгую историю существования простых чисел, до сих пор не решена проблема построения простого числа: не существует в каком-либо виде формулы простого числа. Поэтому исследования и разработки в данной области имеют не только практическое значение, но и фундаментальный характер, что придает большую научную значимость.

Сегодня день данную проблему принято решать следующим образом:

1) задается произвольное натуральное число, для которого заранее неизвестно, является оно простым или составным;

2) заданное число поступает на вход алгоритма проверки простоты числа (тест простоты числа), который определяет, простое это число или составное.

Данные действия повторяются до тех пор, пока не будет получено простое число.

Существует два класса тестов простоты числа, которые выделены на основе критерия достоверности полученного результата:

1) детерминированные тесты – выдают гарантированно точный ответ о простоте числа, но имеют большую вычислительную сложность;

2) вероятностные тесты – результат выполнения теста простоты числа является достоверным лишь с некоторой вероятностью, но время проверки гораздо меньше в сравнении с детерминированными тестами.

Детерминированные тесты на простоту числа хоть и дают достоверный результат, но они значительно уступают вероятностным тестам по скорости работы, поэтому в реальных задачах с применением больших чисел используются именно вероятностные тесты на простоту. Но в таком случае становится очень важным показатель вероятности ошибки теста на простоту, который показывает долю псевдопростых чисел среди определенных тестом простых чисел. Псевдопростое число – это составное число, которое в ходе проведения теста простоты числа было ошибочно определено как простое число.

Существует множество тестов проверки натурального числа на простоту. Широко распространенным на данный момент тестом простоты числа является вероятностный тест Рабина–Миллера. Именно тест Рабина–Миллера применяется в криптографической системе RSA, а также в большинстве математических пакетов. Тест Рабина–Миллера, как и многие другие (тест Ферма, тест Соловея–Штрасена, тест Агравала–Каяла–Саксены), опирается на малую теорему Ферма [8]:

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \quad (1)$$

Также в математическом научном кругу постоянно делаются попытки создания новых тестов простоты, в основе которых может лежать не только малая теорема Ферма, а совершенно произвольный критерий простоты числа. Под критерием простоты числа понимается такое необходимое условие, выполнение которого обязательно для простых чисел.

Критерий простоты на основе свойств композиции производящих функций. В статье [9] был описан новый метод получения критериев простоты натуральных чисел. Данный метод основан на свойствах композиции «логарифмической» производящей функции и производящей функции с целочисленными коэффициентами. В данном случае под «логарифмической» производящей функцией понимается производящая функция, общий вид которой представляется в виде числового ряда:

$$R(x) = \sum_{n=1}^{\infty} \frac{a(n)}{n} x^n . \quad (2)$$

Примером «логарифмической» производящей функцией могут быть:

$$R(x) = \ln\left(\frac{1}{1-x}\right) = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n} x^n , \quad (3)$$

$$R(x) = \ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n , \quad (4)$$

$$R(x) = \mathrm{arctg}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \ldots = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1} x^{2n-1} = \sum_{n=1}^{\infty} \frac{\sin\left(\frac{n\pi}{2}\right)}{n} x^n , \quad (5)$$

$$R(x) = \mathrm{arth}(x) = x + \frac{x^3}{3} + \frac{x^5}{5} + \ldots = \sum_{n=1}^{\infty} \frac{1}{2n-1} x^{2n-1} = \sum_{n=1}^{\infty} \frac{n(\mathrm{mod}2)}{n} x^n . \quad (6)$$

Основное свойство, на котором строится указанный метод генерации критериев простоты числа, заключается в следующем: значение n-го члена композиции $G(x) = R(F(x))$ «логарифмической» производящей функции $R(x)$ и производящей функции с целочисленными коэффициентами $F(x)$ без n-го слагаемого для простого числа n будет целым числом, т.е. значение выражения

$$\sum_{k=1}^{n-1} F^{\Delta}(n,k) \frac{a(k)}{k} \quad (7)$$

является целым для простого числа n.

$F^{\Delta}(n,k)$ – композита производящей функции $F(x)$, необходимая для вычисления коэффициентов композиции производящих функций [10].

На основе указанного метода были построены различные критерии простоты числа, приблизительно оценены характеристики полученных критериев (число ошибок, трудность вычислений). Например, если в качестве внешней производящей функции использовать $R(x) = \mathrm{arctg}(x)$, а внутренней функцией $F(x) = ax + bx^2$, то можно вывести выражение

$$(-1)^{n+1}\frac{\left(a+\sqrt{4b-a^2}\,i\right)^n+\left(a-\sqrt{4b-a^2}\,i\right)^n-(2a)^n}{n2^n}, \quad (8)$$

значение которого при произвольных a, b является целым для простых n.

Продолжение исследований в области получения новых критериев простоты с применением данного метода приводит к накоплению большого количества тестов на простоту, основанных на этих критериях.

Функциональные возможности разработанного программного обеспечения. Имеется большое число различного рода тестов простоты числа, а также разрабатываются все новые тесты простоты. Поэтому чтобы выбрать из них подходящий под конкретную решаемую задачу тест простоты (учитывая требуемое соотношение таких характеристик теста простоты, как время работы и качество результата, т.е. вероятности ошибки), необходимо программное обеспечение, автоматизирующее данный процесс анализа тестов простоты. Также данное программное обеспечение можно активно применять при анализе новых критериев простоты, полученных на основе свойств композиции производящих функций.

Поиск аналогов разработанного программного обеспечения, позволяющих производить сравнительный анализ заданных тестов простоты числа, не показал никаких результатов. То есть такого инструментария не существует на данный момент. Исходя из этого, можно сделать вывод об актуальности и практической значимости выполненной работы.

Разработанное программное обеспечение для анализа и сравнения тестов простоты числа обладает следующим набором функциональных возможностей:

– *Анализ теста простоты числа.* Заключается в выборе теста простоты (либо из имеющегося списка существующих тестов простоты числа, записанных в самой программе, либо путем ввода нового критерия простоты, полученного при исследовании свойств композиции производящих функций).

– *Проверка одного числа или интервала чисел.* При проверке тест простоты применяется либо для одного заданного пользователем числа n, либо для указанного интервала натуральных чисел $[n_1,n_2]$. Проверка одного числа необходима для проверки простоты заданного числа указанным тестом простоты числа, а проверка интервала чисел используется для анализа указанного теста простоты числа.

– *Сравнение тестов простоты числа.* Возможность выбора двух различных тестов простоты числа (либо из имеющегося списка существующих тестов простоты числа, записанных в самой программе, либо путем ввода нового критерия простоты, полученного при исследовании свойств композиции производящих функций) с последующим проведением анализа данных тестов простоты на одинаковых входных данных. Это обеспечит возможность сравнения двух указанных пользователем тестов простоты числа между собою.

– *Вывод сравнительной таблицы.* При проведении анализа теста происходит вычисление параметров исследуемого теста (время выполнения теста простоты числа, подсчет числа совершенных ошибок в сравнении с другим тестом простоты, вероятность ошибки), которые отображаются в виде сравнительной таблицы. Данная таблица позволяет наглядно представить лучшие стороны сравниваемых тестов простоты числа относительно друг друга.

– *Комбинирование двух тестов простоты числа.* Использование двух различных тестов простоты на одних и тех же входных данных с возможностью перекрытия множеств ошибок данных тестов за счет увеличения времени работы. Наличие такой функции в программе позволяет получать новый тест простоты числа с новыми свойствами и параметрами на основании двух других тестов простоты числа.

Наличие данного набора функциональных возможностей отражено на рис. 1.

Указанный набор функциональных возможностей программы делает возможным ее использование при решении задачи поиска эффективного способа проверки на простоту.

Заключение. В ходе выполненного исследования показана научная и практическая значимость выполненной разработки программного обеспечения для проведения анализа и сравнения тестов простоты числа. Реализация программного обеспечения с указанным набором функциональных возможностей позволяет значительно облегчить процесс анализа тестов простоты числа за счет ав-

томатизации данного процесса и представления итоговой информации в удобной для понимания и сравнения форме. Также данное программное обеспечение можно применять и при простом выполнении тестирования на простоту заданного числа.

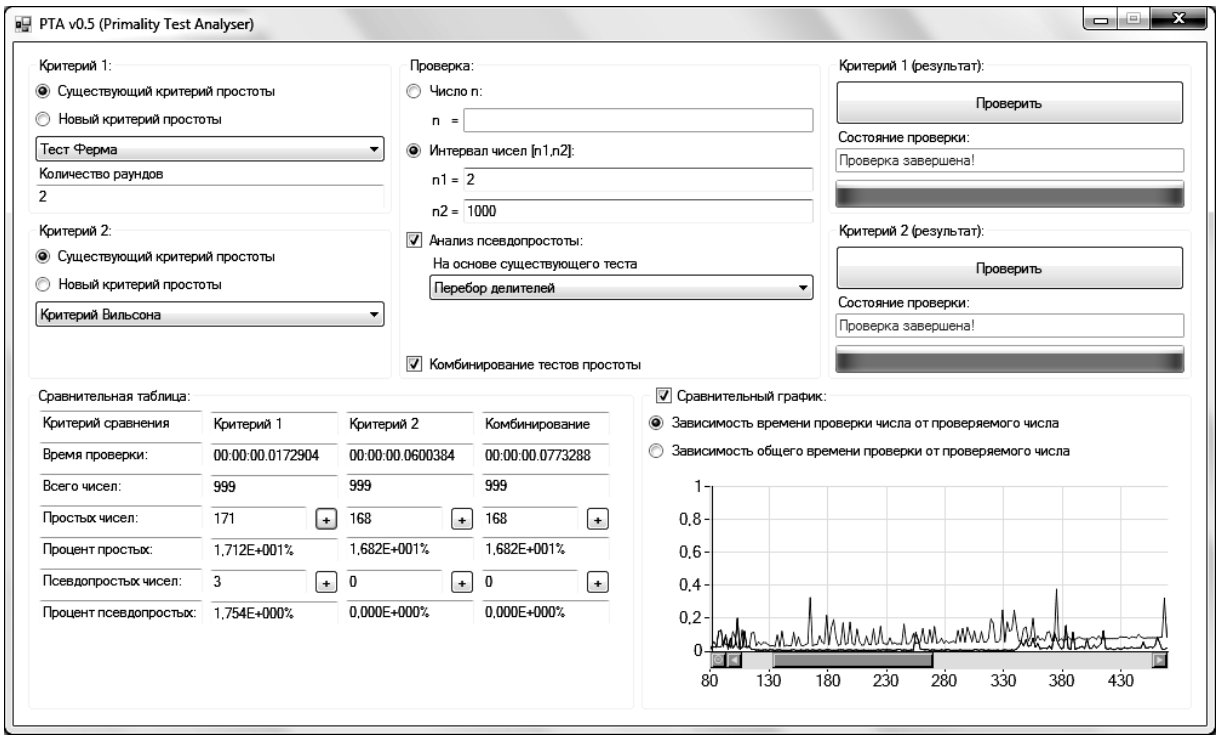

Рис. 1. Интерфейс программного обеспечения

Стоит отметить и тот фактор, что аналогов в виде готового программного обеспечения не было обнаружено, поэтому разработка такого программного обеспечения характеризуется своей новизной и актуальностью.

Литература

1. Основы информационной безопасности: учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2011. – 558 с.

2. Мещеряков Р.В. Специальные вопросы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов. – Томск: Изд-во Ин-та оптики атмосферы, 2003. – 243 с.

3. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 349 с.

4. Евсютин О.О. Моделирование в информационной безопасности и обработке данных с использованием математического аппарата дискретных динамических систем / О.О. Есютин, В.Г. Миронова // Ползуновский вестник (Барнаул, АлтГТУ). – 2012. – С. 222–226.

5. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – Благовещенск: Изд-во Амурского гос. ун-та, 2012. – С. 28–35.

6. Rivest R. A method for obtaining digital signatures and public-key cryptosystems / R. Rivest, A. Shamir, L. Adleman // Communications of the ACM (New York). – 1978. – Vol. 21, № 2. – P. 120–126.

7. Начала Евклида. Книги VII–X / пер. с греч. и комментарии Д.Д. Мордухай-Болтовского при редакционном участии И.Н. Веселовского. – М.; Л.: ГИТТЛ, 1949. – 511 с.

8. Agrawal M. Primality tests based on Fermat's little theorem // Lecture notes in computer science. – 2006. – Vol. 4308. – P. 288–293.

9. Кручинин Д.В. Метод построения алгоритмов проверки простоты натуральных чисел для защиты информации / Д.В. Кручинин, В.В. Кручинин // Доклады ТУСУРа. – 2011. – № 2(24). – С. 247–251.

10. Кручинин В.В. Комбинаторика композиций и ее приложения. – Томск: В-Спектр, 2010. – 156 с.

Кручинин Дмитрий Владимирович
Мл. науч. сотрудник каф. комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: +7-913-845-99-04
Эл. почта: kdv@keva.tusur.ru

Шабля Юрий Васильевич
Инженер каф. КИБЭВС
Тел.: +7-906-949-03-07
Эл. почта: shablya-yv@mail.ru

Kruchinin D.V., Shablya Y.V.
Analysis software for primality tests

We developed the software for primality tests analysis. The purpose of this software tool is to show the possibility of using it for existing primality tests, and for newly developed primality criteria based on the composition of generating functions.
Keywords: primality tests, generating functions, software, analysis, comparison.