УДК 511+519.719.2

Ю.В. Шабля, Д.В. Кручинин, А.А. Шелупанов

Генератор критериев простоты натурального числа на основе свойств композиции производящих функций

Рассматриваются математические аспекты криптографических систем, а именно проверка натуральных чисел на простоту. Проведены анализ существующего положения критериев простоты числа и их проблематика, выявлена необходимость и актуальность проводимого исследования. Разработано специализированное программное обеспечение – генератор критериев простоты числа (Primality Criterion Generator). Данное программное обеспечение является важным инструментом для исследования критериев простоты на основе свойств композиции производящих функций.

Ключевые слова: простое число, производящая функция, критерий простоты числа, генератор критериев простоты числа.

Математической основой современной криптографии является теория чисел. Основным понятием теории чисел, применяющимся в области защиты информации, является простое число. 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 [1].

Несмотря на 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 высокую научную ценность.

На сегодняшний день один из способов решения данной проблемы заключается в следующем:

– задается произвольное натуральное число, для которого заранее не известно, является он простым или составным;

– 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.

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

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

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

В реальных задачах с применением больших чисел используются вероятностные тесты простоты числа. Но в таком случае становится очень важным показатель вероятности ошибки теста простоты числа, 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 числа на простоту. Обзором различных тестов простоты числа занимались такие ученые, как А.А. Балабанов [2], О.Н. Василенко [3], А.В. Черемушкин [4], P. Ribenboim [5] и др.

Большинство современных применяемых на практике тестов простоты числа – вероятностные, значит, существует возможность создания теста простоты числа, который будет характеризоваться меньшей вероятностью ошибки. Разработка более быстрых и точных методов проверки натуральных чисел на простоту поможет снизить потребление временных ресурсов и повысить качество криптографических систем при шифровании.

Также стоит отметить тот факт, что в основе современных применяемых на практике тестов простоты числа лежит малая теорема Ферма [6]. Поэтому существует потребность изучения новых критериев простоты числа, так как это позволит получить новые результаты. Под критерием простоты числа понимается такое необходимое условие, выполнение которого обязательно для простых чисел.

Критерий простоты числа. Данная научная статья является продолжением исследований, описанных в работах [7–10]. В работе [9] была рассмотрена композиция обыкновенных производящих функций и были получены свойства, которые можно применить для получения новых критериев простоты числа.

Свойство 1: Для двух обыкновенных производящих функций с целыми коэффициентами $B(x)=\sum_{n\geq 0} b_n x^n$ и $F(x)=\sum_{n>0} f_n x^n$ и композиты $F^{\Delta}(n,k)$ производящей функции $F(x)$ значение выражения

$$\sum_{k=1}^{n-1} \frac{F^{\Delta}(n,k) b_{k-1}}{k} \tag{1}$$

целое для всех простых n.

На основе Свойства 1 можно составить алгоритм построения новых критериев простоты натурального числа на основе свойств композиции производящих функций:

1. Задать производящую функцию $F(x)=\sum_{n>0} f_n x^n$ с целыми коэффициентами и со свободным членом, равным 0.

2. Вычислить композиту $F^{\Delta}(n,k)$ производящей функции $F(x)$.

3. Задать производящую функцию $B(x)=\sum_{n\geq 0} b_n x^n$ с целыми коэффициентами.

4. Вычислить и упростить выражение (1).

Генератор критериев простоты числа. Используя введенный алгоритм построения новых критериев простоты натурального числа на основе свойств композиции производящих функций, становится возможным создание большого набора новых критериев простоты числа.

Составление каждого из критериев простоты числа требует не только использования программного обеспечения для математических вычислений, но и выполнения расчетов вручную. При этом весь процесс создания нового критерия простоты числа управляется и контролируется только человеком-исследователем и отнимает много времени.

В рамках выполнения данной работы процесс создания нового критерия простоты числа был частично автоматизирован путем создания специализированного программного обеспечения – генератора критериев простоты натурального числа на основе свойств композиции производящих функций (Primality Criterion Generator – «PCG»).

Основываясь на алгоритме построения новых критериев простоты числа, а также с учетом использования функциональных возможностей дополнительного программного обеспечения (система компьютерной верстки TeX, система компьютерной алгебры Maxima) был описан алгоритм работы генератора критериев простоты числа. Алгоритм работы генератора критериев простоты числа заключается в выполнении следующей последовательности действий:

Вход: $F(x)$, параметры $F(x)$, $F^{\Delta}(n,k)$, b_n, формула числовой последовательности.

Выход: изображение формулы полученного критерия простоты числа и ее запись в формате, применяемом в программе «Maxima».

1. В программу «PCG» загружается информация из файла, который содержит: перечень производящих функций $F(x)$, вычисленные значения композит $F^{\Delta}(n,k)$, используемые параметры.

2. Пользователь выбирает из загруженного списка доступных производящих функций $F(x)$ ту, данные которой будут использоваться для построения критерия простоты числа.

3. С помощью программы «Maxima» выполняются вычисления, и в результате в программе «PCG» отображаются изображения математических формул $F(x)$, f_n и $F^{\Delta}(n,k)$.

4. Пользователь вводит формулу коэффициентов b_n, чтобы на ее основе получить производящую функцию $B(x)$, которая будет использоваться для построения критерия простоты числа.

5. С помощью программы «Maxima» выполняются вычисления и в результате в программе «PCG» отображаются изображения математических формул $B(x)$ и b_n.

6. Программа «PCG» проверяет, что требуемые значения в виде производящих функций $F(x)$ и $B(x)$ подготовлены. Если они не готовы, то возврат к этапу 1.

7. С помощью программы «Maxima» выполняется вычисление критерия простоты числа.

8. Изображение формулы полученного критерия простоты числа и ее запись в формате, применяемом в программе «Maxima», отображаются для пользователя в программе «PCG». Также отображаются значения двух целочисленных последовательностей, с помощью которых можно попробовать вручную упростить выражение критерия простоты числа.

9. Если критерий простоты числа упрощать не надо, то критерий простоты числа готов и его можно сохранить для дальнейшего использования. Если требуется упростить критерий простоты числа, то пользователь вводит формулу, генерирующую одну из двух предложенных в программе «PCG» целочисленных последовательностей.

10. Программа «PCG» проверяет соответствие указанной пользователем формулы целочисленной последовательности. Если формула соответствует, то вычисляется и отображается для пользователя значение упрощенного выражения критерия простоты числа. Если формула не соответствует, то возврат к этапу 9.

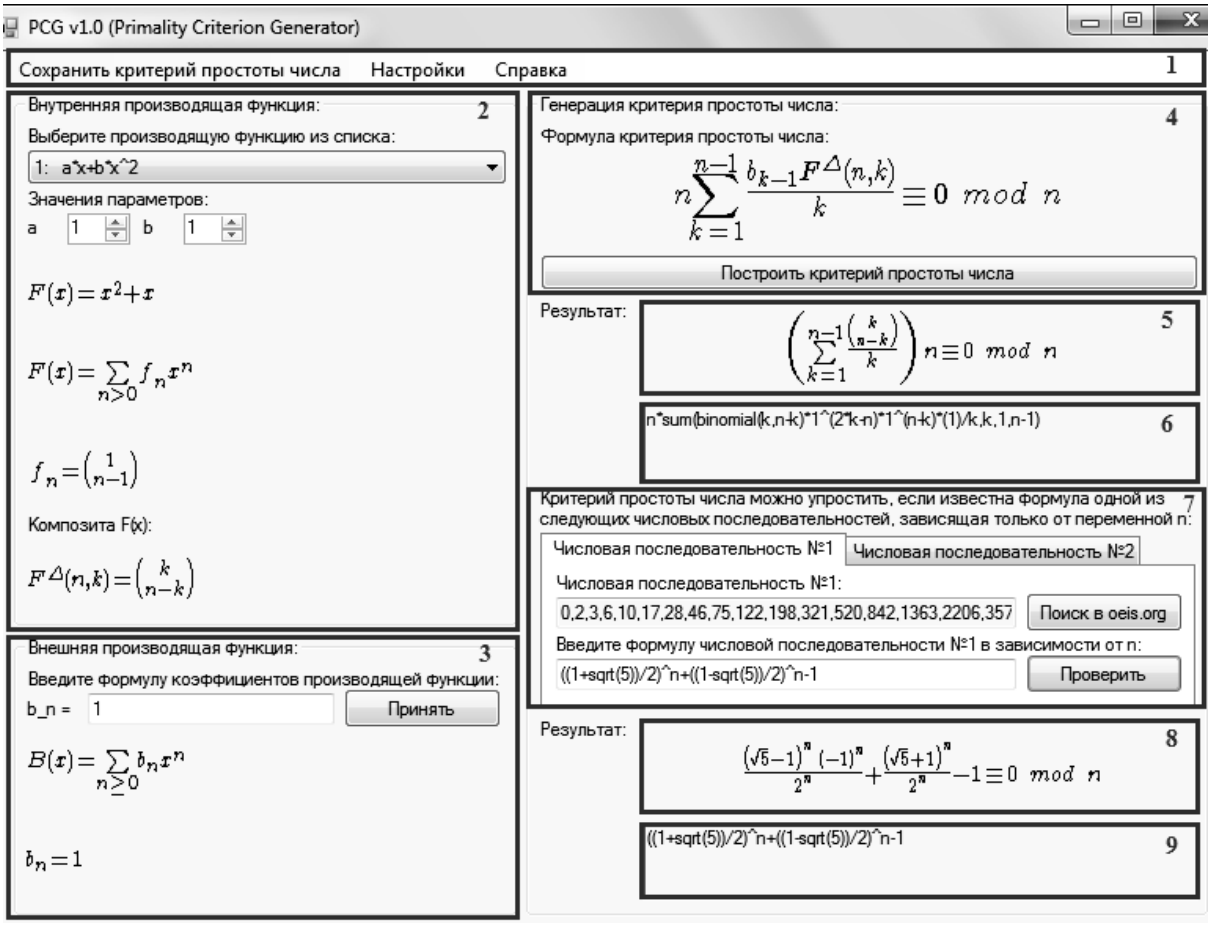

Рис. 1. Графический пользовательский интерфейс программы «PCG»

Графический пользовательский интерфейс главной формы программы «PCG» состоит из нескольких рабочих областей (рис. 1), каждая из которых предназначена для выполнения конкретной задачи:

1. Область меню, из которой можно сохранить полученные результаты, запустить окно настроек и запустить окно справки.

2. Область, предназначенная для введения и отображения данных, касающихся производящей функции $F(x)$.

3. Область, предназначенная для введения и отображения данных, касающихся производящей функции $B(x)$.

4. Область, предназначенная для запуска процесса построения критерия простоты числа.

5. Область результатов, отображающая полученный критерий простоты числа в виде изображения математической формулы.

6. Область результатов, отображающая полученный критерий простоты числа в виде записи в формате, применяемом в программе «Maxima».

7. Область, отображающая полученные целочисленные последовательности, с помощью которых можно упростить критерий простоты числа.

8. Область результатов, отображающая полученный упрощенный критерий простоты числа в виде изображения математической формулы.

9. Область результатов, отображающая полученный упрощенный критерий простоты числа в виде записи в формате, применяемом в программе «Maxima».

Также на рис. 1 представлен пример работы с программой «PCG».

На вход программы «PCG» поданы следующие данные:

– $F(x)=ax+bx^2=x+x^2$, $a=1$, $b=1$ (см. рис. 1, область 2);

– $B(x)=\sum_{n\geq 0}b_n x^n=\sum_{n\geq 0}x^n$ (см. рис. 1, область 3).

В результате выполнения вычислений программа «PCG» выдала следующую информацию:

– критерий простоты числа: $n\sum_{k=1}^{n-1}\frac{\binom{k}{n-k}}{k}\equiv 0 \bmod n$ (см. рис. 1, область 5 и область 6);

– числовая последовательность №1: $[0,2,3,6,10,17,28,46,75,...]$ (см. рис. 1, область 7).

Если ввести формулу полученной числовой последовательности, зависящую только от переменной n, то программа «PCG» предложит упрощенный критерий простоты (см. рис. 1, области 8 и 9):

$$\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n\equiv 1 \bmod n. \qquad (2)$$

Данный критерий простоты числа соответствует сравнению:

$$L_n\equiv 1 \bmod n, \qquad (3)$$

где L_n – числа Люка (числовая последовательность A000032 в Онлайн-энциклопедии целочисленных последовательностей [11]).

Заключение. В результате выполнения работы было разработано специализированное программное обеспечение – генератор критериев простоты числа (Primality Criterion Generator – «PCG»). Программа «PCG» позволяет получать множество различных критериев простоты числа, применяя полученные в статье [10] свойства композиции обыкновенных производящих функций.

Благодаря полученным результатам появляется возможность эффективного исследования новых критериев простоты числа. Поскольку существует возможность использования генератора критериев простоты числа в комплексе с программой, предназначенной для проведения анализа и сравнения тестов и критериев простоты числа (Primality Test Analyser – «PTA»), описание которой представлено в статье [11]. Программы «PCG» и «PTA» составляют комплекс программ и являются удобным средством исследования критериев простоты числа для дальнейшего поиска эффективного теста простоты числа.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части Государственного задания ТУСУР на 2015 год (проект № 3657).

Литература

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

2. Балабанов А.А. Алгоритм быстрой генерации ключей в криптографической системе RSA / А.А. Балабанов, А.Ф. Агафонов, В.А. Рыку // Вестник научно-технического развития. – 2009. – № 7 (23). – С. 11–17.

3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – МНЦМО, 2003. – 326 с.

4. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин. – МНЦМО, 2002. – 104 с.

5. Ribenboim P. The little book of bigger primes / P. Ribenboim. – Springer, 2004. – 356 p.

6. Agrawal M. Primality tests based on Fermat's little theorem / M. Agrawal // Distributed Computing and Networking. – Springer, 2006. – Vol. 4308. – P. 288–293.

7. 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.

8. Кручинин Д.В. Метод построения рекуррентных вероятностных генераторов простых чисел / Д.В. Кручинин // Доклады ТУСУРа. – 2012. – № 1(25). – Ч. 2. – С. 131–135.

9. Kruchinin D.V. New properties for a composition of some generating functions for primes [Электронный ресурс] / D.V. Kruchinin. Y.V. Shablya. – Режим доступа: http://arxiv.org/abs/1109.1683, свободный (дата обращения: 19.06.2015).

10. Кручинин Д.В. Программное обеспечение для анализа тестов простоты натурального числа / Д.В. Кручинин, Ю.В. Шабля // Доклады ТУСУРа. – 2014. – № 4(34). – С. 95–99.

11. The on-line encyclopedia of integer sequences [Электронный ресурс]. – Режим доступа: http://oeis.org, свободный (дата обращения: 19.06.2015).

Шабля Юрий Васильевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: +7-906-949-03-07
Эл. почта: shablya-yv@mail.ru

Кручинин Дмитрий Владимирович
Младший науч. сотрудник каф. КИБЭВС ТУСУРа
Тел.: +7-913-845-99-04
Эл. почта: kdv@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, зав. каф. КИБЭВС ТУСУРа
Тел.: +7 (382-2) 70-15-29
Эл. почта: saa@keva.tusur.ru

Shablya Y.V., Kruchinin D.V., Shelupanov A.A.

Generator of primality criteria based on properties of the composition of generating functions

In this paper are considered the mathematical aspects of cryptographic systems, i.e. checking of natural numbers for primality. The current situation of the primality criteria and its problems were analysed, and the necessity and the relevance of the study was identified. During the study an algorithm for constructing the new primality criteria based on the properties of the composition of ordinary generating functions with integer coefficients was introduced. Also, a software that will be used to search for new effective primality tests named Primality Criterion Generator was developed.

Keywords: prime, generating function, primality criterion, primality criterion generator.