Исследование алгоритмов проверки числа на простоту с целью улучшения криптографических методов защиты информации

Ю.В. Шабля, студент каф. КИБЭВС
Научный руководитель Д.В. Кручинин, аспирант каф. КИБЭВС
Проект ГПО КИБЭВС-1205 – Математические основы защиты информации

В последние годы все больше и больше уделяется внимание информатизации общества, а сама информация теперь воспринимается как достаточно ценный ресурс. Вследствие чего необходима реализация защиты конфиденциальной информации. Решением данной проблемы занимается такая наука, как криптография.

Математической основой современной криптографии является теория чисел. Основным понятием теории чисел, применяющимся в области защиты информации, является простое число. Простым числом p называется натуральное число большее единицы, имеющее только два различных натуральных делителя: единицу и само себя. Изучение простых чисел и их свойств ведёт своё начало с древнейших времён. Например, хорошо известны труды древнегреческого математика Евклида, который уже тогда смог предложить доказательство того, что множество простых чисел бесконечно [1].

К сожалению, на сегодняшний день вопрос простых чисел является основной нерешённой проблемой целочисленной арифметики и исследования в данной области имеют высокую научную ценность. Можно выделить три основных вопроса в данной проблеме простых чисел:

- как построить простое число (актуально при построении огромных простых чисел, используемых в качестве секретных ключей шифрования в некоторых криптографических системах);
- как проверить натуральное число на простоту (поиск наиболее эффективного и точного метода тестирования числа на простоту);
- как получить факторизацию числа (разложение числа на простые множители).

Методы тестирования числа на простоту очень востребованы в криптографических алгоритмах. Поэтому решение именно второго вопроса имеет наибольшее техническое и экономическое значение, так как не существует единого эффективного способа быстрого определения простоты числа и это замедляет работу криптографических алгоритмов. Исследования в этой области проводятся и на данный момент, например, одной из последних значительных разработок стал полиномиальный детерминированный тест простоты числа AKS [2].

На практике различные методы проверки на простоту натурального числа применяются в разных криптографических алгоритмах, например, в криптографической системе с открытым ключом RSA [3]. Данный криптографический алгоритм основан на том, что факторизация больших натуральных чисел – очень трудная вычислительная операция. Благодаря этому данный алгоритм до сих пор остаётся наиболее эффективным и часто применяемым при шифровании для защиты информации. Но скорость выполнения данного алгоритма шифрования и его криптографическая устойчивость целиком и полностью зависят от выбора пары достаточно больших простых чисел, на основе которых собственно и будет осуществляться процесс шифрования данных.

Также существует множество критериев, по которым классифицируют алгоритмы проверки случайного натурального числа на простоту, но основным является критерий достоверности полученного результата. Согласно данному критерию алгоритмы делятся на детерминированные и вероятностные.

Особенность детерминированных тестов заключается в том, что они гарантированно выдают точный ответ: простое или составное заданное натуральное число. Но главный недостаток существующих детерминированных тестов – это огромная вычислительная сложность, и, следовательно, невозможность их применения при больших числах, которые

востребованы на практике. Данные тесты рационально применять только на достаточно малых числах.

Вероятностные тесты характеризуются значительно меньшим временем выполнения тестирования числа, поэтому именно такого типа тесты применяются на практике. Но результат, который получается после выполнения теста, является достоверным лишь с некоторой вероятностью, если он положительный (исследуемое число является простым), или полностью достоверным при отрицательном результате (исследуемое число является составным).

В нашем проекте рассматривается новый метод генерации алгоритмов проверки на простоту натурального числа, основанный на теории производящих функций [4-5]. В данных работах рассмотрена композиция с использованием логарифмической производящей функции, но применение такого метода возможно и с применением композиции других производящих функций, которые можно привести к требуемому виду (например, функция арктангенса, арктангенса гиперболического). Данный метод позволяет генерировать вероятностные критерии на простоту.

Представленный метод уже был использован для получения критериев простоты с применением в качестве внешней производящей функции композиции производящих функций функции вида ln(1+F(x)). На данный момент проводится работа по построению критериев простоты числа с применением в качестве внешней функции функций вида arctg(F(x)) и arth(F(x)).

Например, на основе внешней производящей функции R(x)=arctg(F(x)) и внутренней функции $F(x)=ax+bx^2$ можно вывести выражение следующего вида:

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

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

Генерируя данным способом различные критерии и оценивая количество ошибок и скорость выполнения, появляется возможность создания более эффективных и точных методов проверки натуральных чисел на простоту, в чем и заключается актуальность проекта.

Список использованных источников

1 Евклид. Начала Евклида. Книги VII-X: Перевод с греческого и комментарии Д.Д. Мордухай-Болтовского. – М.-Л.: ГИТТЛ. – 1949. – P. 510.

2 Agrawal M., Kayal N., Saxena N. Primes is in p // Annals of mathematics. – 2004. – P. 781-793.

3 Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and publickey cryptosystems // Communications of the ACM. 1978. Vol. 21, №2, P. 120–126.

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

5 Кручинин Д.В. О свойствах коэффициентов суперпозиции некоторых производящих функций // Прикладная дискретная математика. – 2012. – №1(15). – С. 55-59.