Свойства теоретико-числовых алгоритмов в факториальных кольцах и их приложения в криптографии

Авторы работы: Кондратенок Н.В., Прохоров Н.П.
Руководитель: Васьковский М.М.

Целые простые числа в настоящее время достаточно хорошо исследованы. Они применяются во многих приложениях математики, к примеру, в криптографии. Использование же квадратичных чисел не получило пока широкого распространения. Одной из причин этого является отсутствие четкого математического аппарата, описывающего такое свойство этих чисел как их простота.

В целых числах для проверки на простоту широко применяется тест Соловея-Штрассена и тест Миллера-Рабина. Тесты с вероятностью не менее 0,5 позволяют обнаружить составное число за один запуск. В качестве решающего критерия используются малая теорема Ферма и критерий Миллера соответственно. Контроль эффективности работы теста (времени его работы) может быть осуществлен при помощи теорем Кронекера-Валена и Ламе. Такова методика оценки простоты целого числа.

Целью же приведенного исследования являлась разработка методики оценки простоты квадратичных чисел. Для этого модификации подверглись все этапы оригинальной методики.

Что касается тестов на простоту и используемых в них критериев, то в работах [1] и [2] была доказана возможность их применения для квадратичных чисел.

При этом тест Соловея-Штрассена был модифицирован следующим образом:

1. Получен алгоритм вычисления символа Якоби для квадратичных чисел.
2. Доказан критерий простоты квадратичных чисел, основанный на малой теореме Ферма и свойствах символа Якоби (были обобщены в [5]).
3. Модифицирован сам тест Соловея-Штрассена для квадратичных чисел, а именно введена дополнительная проверка для малых значений N (N – проверяемое число).

Тест Миллера-Рабина был обобщен для квадратичных чисел. В отличие от оригинального варианта теста, где все операции проводились над целыми числами, в предлагаемой модификации на шаге 1 используется норма числа. Указанное обобщение стало возможным после доказательства в [2] критерия Миллера для квадратичных чисел.

С целью оценки времени работы обоих тестов (по аналогии с тестами для целых чисел) были использованы теоремы Кронекера-Валена и Ламе. Отличием примененных теорем являлось их предварительное обобщение для квадратичных чисел. Используя [4] в [3] были получены следующие результаты

1. Найден общий класс факториальных колец, в которых верен аналог теорема Кронекера-Валена: *алгоритм Евклида с выбором наименьшего по норме остатка имеет кратчайшую длину.*
2. Следствие из теоремы Ламе. *Алгоритм Евклида в квадратичных евклидовых кольцах имеет логарифмическую сложность относительно нормы чисел.*

Однако стоит заметить, что существуют Евклидовы кольца, для которых аналоги этих теорем не выполняются. Например единственным мнимым факториальным кольцом для которого не выполнен аналог теоремы Кронекера-Валена это кольцо целых алгебраических элементов поля $\mathbb{Q}(\sqrt{-11})$.

По результатам использования обобщений теорем Кронекера-Валена и Ламе была оценена трудоемкость модифицированных тестов Соловея-Штрассена и Миллера-Рабина. Отмечено, что для обоих алгоритмов она не изменилась и составила $O(\log^3 Nm(N))$.

Полученные результаты представляют интерес не только с теоретической точки зрения, но имеют и практическое значение. К примеру, они были использованы для анализа возможности модернизации RSA-алгоритма.

Изначально работа RSA-алгоритма основана на использовании простых целых чисел. В [5] проведена модификация алгоритма и доказана возможность применения в нем простых квадратичных чисел.

В ходе проверки криптостойкости предлагаемой модификации RSA-алгоритма в квадратичных полях был применен “метод повторного шифрования” как наиболее простой и достаточно распространенный способ взлома шифров. Результаты проверки приведены в [5]. Показано, что криптостойкость модифицированного алгоритма при взломе методом повторного шифрования сравнима с уже существующим. Преимущество же заключается в том, что при взломе “грубой силой” количество анализируемых сообщений в предлагаемом варианте алгоритма будет значительно больше, что обеспечит большее время взлома.

Вместе с этим в [5] были получены ограничения на компоненты модифицированной RSA-криптосистемы.

Полученные результаты разработки модифицированного RSA-алгоритма возможно использовать в криптографии, обеспечивая увеличение криптостойкости закрытия данных.

В качестве направлений дальнейших исследований можно выделить расширение перечня применяемых для оценки стойкости алгоритмов взлома, а так же оценку эффективности и скорости работы модифицированной RSA-криптосистемы.

Список публикаций

1. Васьковский М.М., Кондратенок Н.В., Прохоров Н.П. Тест Соловея-Штрассена в квадратичных Евклидовых кольцах // Материалы

Международной математической конференции “XII Белорусская математическая конференция”(5-10 сентября 2016 г.). Часть 5. – С. 15-16

2. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains // Journal of Number Theory. – V. 168, November 2016, P. 101-116.

3. Vaskouski M., Kondratyonok N. Shortest division chains in unique factorization domains // Journal of Symbolic Computation. – V. 77, November-December 2016, P. 175-188.

4. Васьковский М.М., Кондратенок Н.В. Конечные обобщенные цепные дроби в Евклидовых кольцах // Вестник БГУ. Серия 1 “Физика, математика, информатика”. – №3. – 2013 – С.117-123.

5. Vaskouski M., Kondratyonok N. Analogue of the RSA-cryptosystem in quadratic unique factorization domains // Доклады Национальной академии наук Беларуси. – Том 59, № 5, 2015. – С.18-23.

Доклады на международных конференциях:

1. Международная научная конференция «Белорусская математическая конференция 2016» (Беларусь, Минск, 2016)
2. Международная конференция юных ученых INTEL ISEF 2014 (США, Лос-Анджелес, 2014).
3. Международная конференция юных ученых EUCYS 2014 (Польша, Варшава, 2014). Специальный приз Samsung.
4. Международная конференция юных ученых ICYS 2015 (Турция, Стамбул, 2015). Бронзовая медаль и диплом 3-й степени.
5. Балтийский научно-инженерный конкурс 2013. Диплом 1 степени.
6. Балтийский научно-инженерный конкурс 2014. Диплом 1 степени.
7. Балтийский научно-инженерный конкурс 2015. Диплом 1 степени.