Тесты на простоту чисел большой разрядности

Дереченик А.А.
ПОИТ, ФКСиС
БГУИР
Минск, Республика Беларусь
e-mail: derechenick@gmail.com

***Аннотация* – В данной работе рассмотрены основные типы алгоритмов проверки числа на простоту, проведен их сравнительный анализ и классификация. Приведены примеры приложений, в которых используются тесты на простоту. В частности уделено внимание тестам, классифицирующимся по признаку детерминизма: тест Люка-Лемера, тест Миллера-Рабина. Разработано программное средство, реализующее тест Люка-Лемера с многопоточной надстройкой для операций длинночисленной арифметики. Произведен сравнительный анализ результатов тестов на простоту для однопоточного и многопоточного случаев.**

Ключевые слова: простые числа; тест на простоту числа; длинночисленная арифметика, многопотоность

I. Введение

Простые числа имеют фундаментальное значение для математики, в общем, и для теории чисел, в частности. Таким образом, большой интерес имеет изучение различных свойств простых чисел. И особенным интересом обладают те свойства, которые позволяют эффективно определять простоту числа. Такие эффективные тесты полезны на практике: определенный перечень криптографических протоколов нуждаются в больших простых числах.

II. Методы тестирования на простоту числа

Определение простого числа уже дает метод для его нахождения: делить число на все значения, не превосходящие его, и если для всех операция присутствовал остаток, то число является простым, в противном случае оно составное. Этот тест был известен со времен древних греков, а его специализация – Решето Эратосфена (240 г. До н. э.), позволяла генерировать все простые числа меньше n. Тем не менее, тест не является эффективным, так как он требует $\sqrt{n}$ шагов для определения простоты. Эффективный тест должен иметь количество шагов сопоставимое со значением $\log n$.

Разделение алгоритмов по детерминистическому признаку основывается на том, что если алгоритм детерминированный, то он со стопроцентной вероятностью дает верный ответ. Самым эффективным тестом этой группы является тест Люка-Лемера, который используется в широкомасштабном проекте распределенных вычислений по поиску простых чисел GIMPS (Great Internet Mersenne Prime Search). Определение простоты числа в общем случае является нетривиальной задачей. Только в 2002 году в статье «PRIMES is in P» впервые был опубликован тест, предложенный индийскими учеными Маниндрой Агравалом, Нираджем Каялом и Нитином Саксеной тест (Аггавала—Каяла—Саксены или тест AKS), который является одновременно универсальным, полиномиальным, детерминированным и безусловным. Таким образом, с появлением вышеуказанной публикации решилась проблема о принадлежности задачи распознавания простоты классу задач P[3].

Тест Люка-Лемера благодаря проекту GIMPS удерживает первенство по поиску самых больших простых чисел. В 2008 году был поставлен новый рекорд и открыто простое число $M_{43112609} = 2^{43112609} - 1$, которое содержит почти тринадцать миллионов знаков.

В некоторых проблемах теории чисел простые числа Мерсенна играют важную роль. Многие генераторы псевдослучайных чисел с большими периодами используют при своем построении простые числа Мерсенна: Вихрь Мерсенна.

Клиентская программа GIMPS, которая для поиска простых чисел использует тест Люка-Лемера, следит за точностью своих вычислений, поэтому данное программное средство нашло свое применение в нагрузочном тестировании аппаратной части компьютера[4]. Пиковые нагрузки позволяют выявлять проблемы с кэшем, памятью, разгоном и перегревом процессора, шиной данных и т.п. В данных тестах расчет производится для уже известных значений простых чисел Мерсенна, а результат вычислений сверяется с эталоном.

Программа GIMPS в своей работе основывается натехнологиираспределенныхвычислений.Любойучастниксетиинтернетможет «пожертвовать» частьювычислительногоресурсацентральногопроцессорасвоегоперсональногокомпьютера.Такимобразом, задействуетсяогромнейшийресурсбольшогоколичестваностольныхкомпьютеровповсемумиру.Данноераспределениевычисленийстановитсявозможнымблагодарянараспараллеливаемостиоперацииумножения, которая занимает почти весь ресурс при выполнении теста Люка-Лемера.

III. Многопоточное тестирование на простоту

В данной работе было предложена реализация распараллеленного умножения для одного компьютера с двухъядерным процессором, поддерживающим технологию Intel Hyper-Threading. Четыре логических процессора исполняли три вычислительных потока. При перемножении двух чисел порядка 2^{500000} сокращение времени операций превысило 50% и составило 55%. Дальнейший рост производительности для данной аппаратной платформы с увеличением порядка множителей не наблюдался. Тестирование для алгоритма Люка-Лемера показало сокращение времени вычислений на 30% для чисел Мерсенна порядка 2^{130000}.

Таким образом, можно сделать заключение, что использование технологий распараллеленных вычислений для длинночисленной арифметики оправдывает себя только при больших значениях множителей, порядка 2^{20000} и выше.

[1] Бараш Л.: Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел – Черноголовка: Институт теоретической физики им. Л.Д. Ландау РАН, 2005

[2] Кнут Д.: Искусство программирования, том 2 – М.: Вильямс, 2000

[3] Manindra Agrawal, Neeraj Kayal, Nitin Saxena: PRIMES is in P // Annals of Mathematics. —Princeton University, 2004.

[4] GIMPS, Great Internet Mersenne Prime Search. [Электронный ресурс] – Электронные данные. – Режим доступа: http://mersenne.org/

[5] Agrawal, M. PRIMES is in P / M. Agrawal, N. Kayal, N. Saxena // Annals of Mathematics. – 2004. – T.160.– №2. – C. 781–793.

[6] Rivest, R. L. A method for obtaining digital signatures and public key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Commun ACM. – 1978. – T.21. – №2. – C. 120-126.

[7] Винберг, Э. Б. Курс алгебры / Э. Б. Винберг. – М.: Факториал, 1999.

[8] Карацуба, А.А. Основы аналитической теории чисел / А.А. Карацуба. – М. : Наука, 1972.

[9] Alford, W. R. There are infinitely many Carmichael numbers / W. R. Alford, A. Granville, C. Pomerance // Annals of Mathematics. – 1994. – T.140. – C. 703-722.