УДК 511+519.719.2

Д.В. Кручинин

Метод построения рекуррентных вероятностных генераторов простых чисел

Предложен метод построения рекуррентных вероятностных генераторов простых чисел с применением аппарата обыкновенных производящих функций и операции суперпозиции функций $\ln(1+F(x))$, где $F(x)$ является обыкновенной производящей функцией с целыми коэффициентами. Рассмотрены примеры построения таких генераторов с использованием предложенного метода.

Ключевые слова: генератор простых чисел, рекуррентные выражения, простые числа, производящие функции, суперпозиция производящих функций**.**

Простые числа имеют фундаментальное значение в математике в целом и в теории чисел в частности. Таким образом, это представляет большой интерес для изучения различных свойств простых чисел. На практике простые числа играют важную роль в современной криптографии и защите информации. Многие современные криптографические системы строятся на базе простого числа. Поэтому алгоритмы генерации простых чисел и проверки на простоту сформированного числа являются важными инструментами при создании криптографической системы.

Так, в хорошо известной криптографической системе с открытым ключом RSA потребность в выборе простых чисел имеет основополагающую позицию. Каждый пользователь RSA вырабатывает свою пару открытых и секретных ключей. Для этого ему необходимо сгенерировать два больших простых числа p и q и вычислить произведение $n=pq$. Затем требуется взять случайное число e, взаимно простое с $\varphi(n)=(p-1)(q-1)$, и найти число d из условия $ed\equiv 1(\mathrm{mod}\varphi(n))$. Пара (n,e) объявляется открытым ключом и помещается в открытый каталог. Остальные числа $(p,q,\varphi(n),d)$ образуют секретный ключ. Для расшифровки достаточно знать пару (n,d). Поскольку успешное решение задачи факторизации (разложения) числа n позволяет полностью дешифровать схему RSA и определить секретный ключ, то выбор простых чисел p и q во многом определяет стойкость шифрования [1].

В данной работе рассматривается задача генерации простых чисел, в том числе в заданном числовом промежутке.

Генерация простых чисел

Одним из методов получения простых чисел является использование какой-нибудь формулы, порождающей простые числа. Например, еще Л. Эйлер предложил многочлен

$$p(x)=x^2+x+41, \qquad (1)$$

значения которого в первых 40 членах натурального ряда дают простые числа.

Впрочем, есть гораздо более сильный результат Ю. Матиясевича (1970), который доказал, что существует многочлен с целыми коэффициентами от нескольких переменных, значениями которого будут в точности все простые числа [2].

Генерация простых чисел, основанная на тесте Поклингтона.

Теорема Поклингтона. Пусть $n=pR+1$, и полное разложение множителя R на простые множители известно. Тогда если для некоторого $a < n$ выполняются условия:

1) $a^{n-1}\equiv 1 \bmod n$,

2) $НОД(a^{(n-1)/q},n)\neq 1$ для любого $q\,|\,R$, то любой делитель числа n сравним с 1 по модулю R.

Пусть задано простое число p:

1. Выбирается случайным образом чётное число R на промежутке $p\le R\le 4p+2$ и определяется $n=pR+1$.

2. Проверяется получившееся число n на отсутствие малых простых делителей.

3. Проверка простоты числа n с помощью теста Рабина–Миллера для различных значений $a < p$. Если число определяется как составное число, то выбирается новое значение R.

Оценка эффективности этого метода зависит от плотности распределения простых чисел и расстояния между соседними простыми числами [2].

На основе теоремы Поклингтона строится алгоритм построения простых чисел, изложенный в Стандарте (ГОСТ Р34.10–94) «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

Также существуют методы построения больших простых чисел, использующие не только простые делители $n-1$, но и делители чисел $n+1, n^2+1, n^2+n+1$. В основе их лежит использование последовательностей целых чисел, удовлетворяющих линейным рекуррентным уравнениям различных порядков.

Генерация простых чисел с использованием решета Аткина

Решето Аткина – быстрый современный алгоритм нахождения всех простых чисел до заданного целого числа. Основная идея алгоритма состоит в использовании неприводимых квадратичных форм (представление чисел в виде $ax^2 + by^2$). Это оптимизированная версия старинного решета Эратосфена: решето Аткина проделывает некоторую предварительную работу, а затем вычеркивает числа, кратные квадрату.

Алгоритм имеет асимптотическую сложность – $O(n/\log\log n)$ и требует $n^{1/2+o(1)}$ бит памяти, это схоже по сложности с уже известными алгоритмами, но требование памяти существенно ниже в решете Аткина [3].

Для нахождения простых чисел, следующих за заданным числом x, можно использовать следующий алгоритм:

1. Выписывается множество чисел $\{n, n+2, n+4, ..., n+2m\}$, где $n \geq x$ – наименьшее нечетное число, $n+2m$ – верхняя граница интервала.

2. Выполняется просеивание этого интервала с использованием решета Эратосфена или Аткина с помощью множества небольших простых чисел $\{3,5,...,p_k\}$, ограниченного сверху границей B. При $B=10$ отсеется примерно половина кандидатов. При $p_k < 1000$ отсеется $5/6$ всех кандидатов.

3. Проверяются оставшиеся кандидаты с помощью теста Рабина–Миллера [2].

В 2008 г. Э. Роуланд получил рекуррентную последовательность, состоящую только из простых чисел, что делает возможным построение рекуррентного генератора простых чисел [4].

Последовательность задается следующим образом:

Пусть $a_1 = 7$ и для всех $n > 1$ $a_n = a_{n-1} + НОД(n, a_{n-1})$, то для всех $n > 1$ выражение $b_n = a_n - a_{n-1}$ принимает только 1 и простые значения.

Недостатки данного метода генерации заключаются в следующем:

- генерация происходит при помощи дополнительной операции отыскания наибольшего общего делителя;
- генерируются простые числа не подряд;
- множественные повторения простых чисел, особенно числа 1;
- неизвестно, генерируются ли все простые числа.

Построение рекуррентных выражений для определения простоты числа

Для построения рекуррентных выражений, определяющих простоту числа, рассмотрим следующую суперпозицию производящих функций:

$$G(x) = R(F(x)), \tag{2}$$

где внешней функцией является производящая функция $R(x) = \ln(\frac{1}{1-x})$, а внутренней – обыкновенная производящая функция $F(x)$ с целыми коэффициентами.

Известно [5], что данная суперпозиция $G(x) = \sum_{n \geq 1} g(n)x^n$ обладает следующим свойством:

- для любых значений $n > 0$, значения выражения $ng(n)$ являются целыми числами.

Для последовательности, задаваемой целочисленной функцией $ng(n)$, возможно построение рекуррентных функций, также однозначно определяющих заданную последовательность.

Рассмотрим еще одно свойство суперпозиции $G(x)=\sum_{n\geq 1} g(n)x^n$ **:**

- для любых простых значений n, значения выражения

$$\frac{ng(n)-f(1)^n}{n} \tag{3}$$

являются целыми числами [5].

Приводя полученную рекуррентную функцию к виду (3), получаем рекуррентную функцию, которая генерирует последовательность чисел. Причем при простых значениях n элемент последовательности однозначно будет целым. Обратное утверждение неверно.

Рассмотрим ряд примеров, характеризующих вышеописанные утверждения.

Пример 1

Пусть $F(x)=x+x^2$, тогда функция коэффициентов $g(n)$ суперпозиции $G(x)=\ln\left(\frac{1}{1-x-x^2}\right)$ имеет вид

$$g(n)=\sum_{k=1}^{n}\binom{k}{n-k}\frac{1}{k}, \tag{4}$$

$$ng(n)=[1,3,4,7,11,18,29,47,76,123,199,322,521,843...].$$

Это последовательность чисел Люка, где числа Люка определяются следующим образом:

$$L(n)=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

или рекуррентная формула

$$L(n)=L(n-1)+L(n-2).$$

Приводя рекуррентную формулу к виду (3), получаем выражение

$$\frac{L(n-1)+L(n-2)-1}{n}, \tag{5}$$

генерирующее последовательность чисел от 1 до n, такую, что при простых значениях n элемент последовательности однозначно будет целым.

Рекуррентная формула n-го члена последовательности определяется следующим образом:

$$b(n)=\frac{a(n)}{n},$$
$$\text{где } a(n)=a(n-1)+a(n-2)+1, \tag{6}$$
$$a(1)=0, a(1)=2.$$

Для $n=23$ последовательность будет следующая:

$$0,1,1,\frac{3}{2},2,\frac{17}{6},4,\frac{23}{4},\frac{25}{3},\frac{61}{5},18,\frac{107}{4},40,\frac{421}{7},\frac{1363}{15},\frac{1103}{8},210,\frac{5777}{18},492,\frac{7563}{10},\frac{24475}{21},\frac{19801}{11},2786.$$

Видно, что для $n\leq 23$ целые значения принимают только элементы при простых порядковых номерах. К сожалению, в общем виде существуют и псевдопростые числа n, элементы при которых также целые числа. Так, для $n<150000$ существуют 31 псевдопростое число, называемое псевдопростыми числами Люка:

705, 2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201, 15251, 24465,29281, 34561, 35785, 51841, 54705, 64079, 64681, 67861, 68251, 75077, 80189, 90061, 96049, 97921, 100065, 100127,105281, 113573, 118441, 146611.

Пример 2

Пусть $F(x)=\frac{1}{1-x}$, тогда функция коэффициентов $g(n)$ суперпозиции $G(x)=\ln\left(\frac{1-x}{x}\right)$ имеет вид

$$g(n)=\sum_{k=1}^{n}\frac{1}{k}\binom{n-1}{k-1}=\frac{2^n-1}{n}, \tag{7}$$

$$ng(n)=[1,3,7,15,31,63,127,255,511,1023,2047,4095,8191,16383,...].$$

Это последовательность чисел Мерсенна, рекуррентная формула которых имеет следующий вид:

$$M(n)=M(n-1)+2M(n-2)+2, \tag{8}$$

Приводя рекуррентную формулу к виду (3), получим выражение, генерирующее последовательность чисел от 1 до n, такую, что при простых значениях n элемент последовательности однозначно будет целым.

Рекуррентная формула n-го члена последовательности определяется следующим образом:

$$b(n)=\frac{a(n)}{n},$$
$$\text{где } a(n)=2a(n-1)+2, \tag{9}$$
$$a(1)=0.$$

Для $n=20$ последовательность будет следующая:

$$0,1,2,\frac{7}{2},6,\frac{31}{3},18,\frac{127}{4},\frac{170}{3},\frac{511}{5},186,\frac{2047}{6},630,\frac{8191}{7},\frac{10922}{5},\frac{32767}{8},7710,\frac{131071}{9},27594,\frac{524287}{10}.$$

Видно, что для $n\le 20$ целые значения принимают только элементы при простых порядковых номерах. К сожалению, в общем виде существуют и псевдопростые числа n, элементы при которых также целые числа, они называются числа Сарруса. Так, для $n<10000$ существует гораздо больше чисел Сарруса, чем псевдопростых чисел Люка:

341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277,

4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911.

Использование полученных рекуррентных выражений

Используя полученные рекуррентные выражения, возможно построение вероятностных генераторов простых чисел. В зависимости от подставляемых производящих функций генераторы простых чисел имеют различную точность определения простоты. Используя данный метод, можно находить множество чисел от 1 до n, в котором находятся все простые числа в этом интервале и некоторые составные числа, удовлетворяющие условию генерации, количество которых определяется суперпозицией имеющихся производящих функций. Для подсчета вероятности и понятия адекватности использования получаемых генераторов простых чисел можно использовать функции подсчета количества простых чисел в заданном интервале. Сравнивая количество псевдопростых чисел, полученных с помощью рекуррентного генератора, и результат функции подсчета простых чисел, можно сделать заключение о состоятельности рекуррентного генератора и о его дальнейшем практическом применении.

Преимущество использования рекуррентных генераторов заключаются в том, что при знании некоторых необходимых элементов $a(k)$ определенной размерности возможно дальнейшее построение простых чисел в интервале от k до n. То есть если хранить необходимое количество элементов последовательности $a(n)$, заданной большой размерности, то с легкостью можно отыскать множество псевдопростых чисел, больших, чем заданные значения n. В этом случае вся сложность генерации будет заключаться в операции деления на порядковый номер n и хранении нижней границы значений $a(n)$ необходимого порядка.

Применение рекуррентных генераторов простых чисел целесообразно для построения простых чисел в заданном интервале некоторой допустимой погрешностью либо для построения или уменьшения размера последовательности чисел, необходимых для отыскания простых чисел с помощью проверок простоты. То есть строится некоторая последовательность псевдопростых чисел и для чисел данной последовательности применяются некоторые тесты на простоту до тех пор, пока не найдется среди них простое число.

Литература

1. Rivest R. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21(2). – P. 120–126.

2. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учеб. пособие. – Казань: Казан. ун., 2011. – 190 с.

3. Atkin A.O.L. Prime sieves using binary quadratic forms / A.O.L. Atkin, D.J. Bernstein // Mathematics of Computation. – 2004. – Vol. 73. – P. 1023–1030.

4. Rowland E.S. A Natural Prime-Generating Recurrence // Journal of Integer Sequences. – 2008. – Vol. 11, article 08.2.8. – P. 1–13.

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

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

Kruchinin D.V.

The method of constructing probabilistic recurrence generators of prime numbers

A method for constructing probabilistic recurrence generators of prime numbers proposed by using the apparatus of ordinary generating functions and operations of superposition of generating functions $\ln(1 + F(x))$, where $F(x)$ is a ordinary generating function with integer coefficients. Examples of the construction of prime number generators considered by using the proposed method.

Keywords: prime number generator, recurrence expressions, prime numbers, generating functions, superposition of generating functions.
