УДК 511.313

ВЗАИМОСВЯЗЬ ТЕСТА ПРОСТОТЫ ФЕРМА И ТЕОРЕМЫ ВИЛЬСОНА ПРИ ОПРЕДЕЛЕНИИ ПРОСТЫХ ЧИСЕЛ

Приходько А.А.

ФГБОУ ВО «Кубанский государственный аграрный университет им. И.Т. Трубилина», Краснодар, e-mail: kampanus@yandex.ru

Оптимизация алгоритмов для поиска и проверки простых чисел является актуальной задачей, решение которой необходимо для стойкости криптографических систем. В статье рассмотрены основные алгоритмы и тесты определения простых чисел. Истинные тесты простоты чисел имеют высокую степень сложности расчета, а вероятностные тесты не могут определить точно простые числа. В данной статье рассмотрен метод определения простых чисел, основанный на теореме Вильсона. Предложены решения по снижению нагрузки на вычислительную технику, выведена формула определения простого числа. В статье определена взаимосвязь малой теоремы Ферма и теоремы Вильсона. Соотношение истинного теста простоты, основанного на теореме Вильсона, и вероятностного теста Ферма обосновывает появление псевдопростых чисел Ферма и определяет необходимые условия их проверки. При определении параметров простоты числа используется китайская теорема об остатках и теорема В. Серпинского о критерии простого числа. Приведены оптимизационные решения при проверке простого числа по теореме Вильсона. Предложена оптимизация теста простоты Ферма с уменьшением выполнения необходимых операций в два раза, также представлено обоснование такой оптимизации.

Ключевые слова: теорема Вильсона, малая теорема Ферма, простые числа, алгоритм расчета простого числа, метод Эратосфена, китайская теорема об остатках

THE RELATIONSHIP OF FERMAT'S SIMPLICITY TEST AND WILSON'S THEOREM IN DETERMINING PRIME NUMBERS

Prikhodko A.A.

Kuban State Agrarian University, e-mail: kampanus@yandex.ru

Optimization of algorithms for searching and verifying prime numbers is an urgent task, the solution of which is necessary for the stability of cryptographic systems. The article discusses the basic algorithms and tests for determining prime numbers. True number simplicity tests have a high degree of calculation complexity, and probabilistic tests cannot determine exactly prime numbers. This article discusses a method for determining prime numbers based on Wilson's theorem. Solutions to reduce the load on computing equipment are proposed, a formula for determining a prime number is derived. The article defines the relationship between Fermat's small theorem and Wilson's theorem. The ratio of the true simplicity test based on Wilson's theorem and the probabilistic Fermat test justifies the appearance of pseudo-simple Fermat numbers and determines the necessary conditions for their verification. When determining the parameters of the simplicity of a number, the Chinese remainder theorem and V. Serpinsky's theorem on the criterion of a prime number are used. Optimization solutions are given when checking a prime number by Wilson's theorem. The optimization of the Fermat simplicity test with a halving of the necessary operations is proposed, and the rationale for such optimization is also presented.

Keywords: Wilson's theorem, Fermat's small theorem, prime numbers, prime number calculation algorithm, Eratosthenes method, Chinese remainder theorem

Рост вычислительных мощностей для обеспечения требуемого уровня стойкости криптографических систем вызвал необходимость использовать простые числа все большей разрядности. Это привело к необходимости адаптировать трудоемкость вычислительных операций криптографических алгоритмов при нахождении простых чисел [1].

Алгоритмы проверки простых чисел могут быть разделены на две группы: истинные (детерминированные) и вероятностные тесты. Истинные алгоритмы позволяют точно определить простоту числа. Вероятностные тесты позволяют выяснить простое число или нет с определенной вероятностью ошибки [2].

На сегодняшний день существует всего два основных детерминированных алгоритма проверки простого числа, это теорема Вильсона и метод Эратосфена. Метод Эратосфена предполагает простой подбор делителей, что является достаточно сложным из-за большого количества необходимых операций [3]. Проверка простого числа по теореме Вильсона также имеет высокую сложность расчета.

При определении простых чисел высоких порядков в основном используют тест Ферма, который является вероятностным. Благодаря быстрым алгоритмам, основанным на китайской теореме об остатках [4], проверку числа можно осуществить достаточно быстро, но данный тест не позволяет проверить псевдопростые числа Ферма, которые обладают некоторыми свойствами простых чисел, но не являются ими.

Целью данной работы было найти взаимосвязь теста Ферма и теоремы Вильсона, так как нет понимания, почему тест Ферма не распознает псевдопростые числа. На сегодняшний день считается, что эти две теоремы не связаны между собой и имеют совершенно разные принципы расчета. В данной статье представлены результаты исследований, которые наглядно показывают, каким образом тест Ферма соотносится с теоремой Вильсона, что имеет большое значение для дальнейшей адаптации алгоритма поиска и проверки простых чисел.

Теорема Вильсона формулируется следующим образом: Если p простое число, то имеет место сравнение $(p - 1)! + 1 \equiv 0 \pmod p$ (1). Так же справедлива обратная теорема: Если для целого положительного p имеет место соотношение (1), то p число простое, т.е. если сумма $(p - 1)! + 1$ делится на p без остатка, то число p является простым числом. Проблема заключается в том, что даже при небольших числах n, число $(n - 1)! + 1$ очень большое число. Например, если по данному алгоритму проверить, является ли число 997 простым, то надо проверить делимость числа 996! + 1 на 997. Данное число содержит 2556 десятичных знаков, что существенно усложняет проверку [5]. Поэтому алгоритм проверки простого числа по теореме Вильсона имеет в основном теоретическое значение и не применяется на практике.

Оптимизация алгоритма по теореме Вильсона заключается в использовании китайской теоремы об остатках. При расчете факториала предположительно простого числа p на каждом этапе находится остаток от деления на p и последующее умножение производится уже этого остатка. Пример расчета числа 97 по данному алгоритму представлен в табл. 1.

Первые четыре числа не отличаются от стандартного расчета факториала. Пятое число больше числа p и равно 120, поэтому берется остаток от деления на 97, что составляет 23. Шестое число находится произведением 23 на 6 и аналогично находится остаток от деления данного числа на 97. Число с порядковым номером 96 действительно равно 96 (или p–1), что является доказательством простого числа p по теореме Вильсона. Таким образом, чтобы определить остаток от деления факториала 97, вычисление самого факториала не требуется. Более того, если последовательно перемножить числа получившегося ряда и аналогично выделять остаток от деления после каждой операции, то в результате найдем остаток от деления суперфакториала проверяемого числа.

Таблица 1

Пример расчета по алгоритму числа 97

№ п/п	n (mod p)	№ п/п	n (mod p)	№ п/п	n (mod p)	№ п/п	n (mod p)	№ п/п	n (mod p)
1	1	21	47	41	76	61	4	81	11
2	2	22	64	42	88	62	54	82	29
3	6	23	17	43	1	63	7	83	79
4	24	24	20	44	44	64	60	84	40
5	23	25	15	45	40	65	20	85	5
6	41	26	2	46	94	66	59	86	42
7	93	27	54	47	53	67	73	87	65
8	65	28	57	48	22	68	17	88	94
9	3	29	4	49	11	69	9	89	24
10	30	30	23	50	65	70	48	90	26
11	39	31	34	51	17	71	13	91	38
12	80	32	21	52	11	72	63	92	4
13	70	33	14	53	1	73	40	93	81
14	10	34	88	54	54	74	50	94	48
15	53	35	73	55	60	75	64	95	1
16	72	36	9	56	62	76	14	96	96
17	60	37	42	57	42	77	11	97	0
18	13	38	44	58	11	78	82	98	0
19	53	39	67	59	67	79	76	99	0
20	90	40	61	60	43	80	66	100	0

Таблица 2

Пример расчета по алгоритму числа 57

№ п/п	n (mod p)	№ п/п	n (mod p)	№ п/п	n (mod p)	№ п/п	n (mod p)
1	1	16	9	31	0	46	0
2	2	17	39	32	0	47	0
3	6	18	18	33	0	48	0
4	24	19	0	34	0	49	0
5	6	20	0	35	0	50	0
6	36	21	0	36	0	51	0
7	24	22	0	37	0	52	0
8	21	23	0	38	0	53	0
9	18	24	0	39	0	54	0
10	9	25	0	40	0	55	0
11	42	26	0	41	0	56	0
12	48	27	0	42	0	57	0
13	54	28	0	43	0		
14	15	29	0	44	0		
15	54	30	0	45	0		

Рассмотрим проверку составного числа по данному алгоритму. Выполним расчет по числу 57. Результаты приведены в табл. 2.

Число не прошло проверку, так как после восемнадцатого числа остаток от деления составил ноль. Соответственно, последующее число алгоритм рассчитывает как 0 × 20 = 0. Все последующие числа будут также равны нулю, поэтому условие $(p-1)! + 1 \equiv 0 \pmod p$ не выполняется.

Метод Эратосфена и теорема Вильсона основаны на разных принципах проверки. В первом случае происходит деление проверяемого числа на возможные множители. Теорема Вильсона основана на том принципе, что если у числа есть делители, то их произведение, умноженное на любое число, будет делить без остатка исходное число. Например, если число 35 делится на 7 и 5, то произведение $7\times5\times n$, при любом целочисленном значении n, будет делиться без остатка на число 35. Минимальный возможный делитель для нечетного числа это 3, поэтому проверку по данному алгоритму необходимо и достаточно выполнить до числа равного $p/3$. По количеству необходимых операций предложенный вариант уступает методу Эратосфена, где достаточно проверить $\sqrt{p}$ чисел [6], однако деление несопоставимых по разряду чисел требует больше времени, чем близких по количеству десятичных знаков.

На данном этапе алгоритм возможно оптимизировать, понимая особенности десятичной системы счисления. Если проверку проходит число, которое оканчивается на три, то оно может быть получено только умножением чисел вида $x1 \times x3$ или $x7 \times x9$. Таким образом при возведении факториала количество чисел возможно сократить.

Особенность данного метода в том, что в процессе возведения факториала есть возможность привести число p к виду $p / 2^n$ и результат расчета останется верным. При делении на другие числа алгоритм не работает корректно, что уже говорит о тесной взаимосвязи теоремы Вильсона и чисел вида 2^n. В качестве примера приведен расчет числа 97, которое в процессе проверки в произвольном порядке делится на различные 2^n. Результаты возведения факториала представлены в табл. 3.

Данный алгоритм основан на китайской теореме об остатках и широко применяется в программировании. Если необходимо узнать остаток от деления от произведения нескольких чисел, то на любом этапе умножения допустимо складывать и отнимать исходное число любое количество раз, и это не влияет на результат. На основании данного правила число n допустимо привести к виду $n - p$, если необходимо узнать остаток от деления числа p.

Рассмотрим проверку простого числа 5 по теореме Вильсона. Для этого необходимо рассчитать 4!. Расчет представляет собой вид: 1×2×3×4. Используя китайскую теорему об остатках, выражение допустимо привести к виду: $1\times2\times(3-5)\times(4-5) = 1\times2\times(-2)\times(-1) = -(1^2)\times-(2^2)=4$.

Таблица 3

Пример проверки числа 97 с различными делителями вида 2^n

№ п/п	n (mod p)	p / 2^n	№ п/п	n (mod p)	p / 2^n	№ п/п	n (mod p)	p / 2^n
1	1	3,03125	34	15,25	24,25	67	24,5	48,5
2	2	3,03125	35	0,25	24,25	68	17	48,5
3	2,96875	3,03125	36	9	24,25	69	9	48,5
4	2,78125	3,03125	37	42	48,5	70	48	48,5
5	1,78125	3,03125	38	44	48,5	71	13	48,5
6	1,59375	3,03125	39	18,5	48,5	72	14,5	48,5
7	2,0625	3,03125	40	12,5	48,5	73	40	48,5
8	1,34375	3,03125	41	27,5	48,5	74	1,5	48,5
9	3	3,03125	42	39,5	48,5	75	15,5	48,5
10	5,75	12,125	43	1	48,5	76	14	48,5
11	2,625	12,125	44	44	48,5	77	11	97
12	7,25	12,125	45	40	48,5	78	82	97
13	9,375	12,125	46	45,5	48,5	79	76	97
14	10	12,125	47	4,5	48,5	80	66	97
15	4,5	12,125	48	22	48,5	81	11	97
16	11,375	12,125	49	11	48,5	82	29	97
17	11,5	12,125	50	16,5	48,5	83	79	97
18	0,875	12,125	51	17	48,5	84	40	97
19	16,625	24,25	52	11	48,5	85	5	97
20	17,25	24,25	53	1	48,5	86	42	97
21	22,75	24,25	54	5,5	48,5	87	65	97
22	15,5	24,25	55	11,5	48,5	88	94	97
23	17	24,25	56	13,5	48,5	89	24	97
24	20	24,25	57	42	48,5	90	26	97
25	15	24,25	58	11	48,5	91	38	97
26	2	24,25	59	18,5	48,5	92	4	97
27	5,5	24,25	60	43	48,5	93	81	97
28	8,5	24,25	61	4	48,5	94	48	97
29	4	24,25	62	5,5	48,5	95	1	97
30	23	24,25	63	7	48,5	96	96	97
31	9,75	24,25	64	11,5	48,5	97	0	0
32	21	24,25	65	20	48,5	98	0	0
33	14	24,25	66	10,5	48,5	99	0	0

При четном количестве множителей результат положительный, при нечетном – отрицательный. Если результат получается отрицательным, то необходимо брать остаток от деления отрицательного числа, то есть принцип расчета не меняется. Теорема В. Серпинского о критерии простого числа хорошо описывает данное правило [7].

Как было рассмотрено выше, доказательством того, что число простое, является наличие положительного остатка от числа $\left(\frac{p-1}{2}\right)!$ Используем китайскую теорему об остатках для записи следующего равенства, на примере числа 5: $1\times2 \equiv (-4)\times(-3) \equiv 2$ (*mod* 5). Запишем выражение в общем виде:

$$1\times2\times\ldots\left(\frac{p-1}{2}\right) \equiv (1-p)\times(2-p)\times\ldots\left(\frac{p-1}{2}\right)-p \equiv n\ (mod\ p).$$

Если число *p* простое, выполняется следующее условие:

$$\frac{(1-p)\times(2-p)\ldots\left(\frac{p-1}{2}\right)-p}{1\times 2\times\ldots\left(\frac{p-1}{2}\right)}\equiv 1(mod\ p).$$

Преобразуем выражение в следующий вид:

$$\left(1-\frac{p}{1}\right)\times\left(1-\frac{p}{2}\right)\times\ldots\left(1-\frac{p}{\left(\frac{p-1}{2}\right)}\right)\equiv 1(mod\ p).$$

Проверим выражение на примере числа 11:

$$\left(1-\frac{11}{1}\right)\times\left(1-\frac{11}{2}\right)\times\left(1-\frac{11}{3}\right)\times\left(1-\frac{11}{4}\right)\times\left(1-\frac{11}{5}\right)=-252\equiv 1\ (mod\,11).$$

Число 11 удовлетворяет условию, значит, данное простое. Эта формула хорошо известна, но имеет свои недостатки [8]. При расчете больших чисел появляется ошибка, вызванная приближенными значениями множителей.

Рассмотрим детально, как выполняется расчет:

$$\frac{-6\times-7\times-9\times-10}{1\times 2\times 3\times 4\times 5}=-252\cdot$$

Как видно, все числа из знаменателя сокращаются с числителем, умножение производится уже оставшихся значений: -3×-7×-2×-3×-2 = – 252. Дробных чисел при таком расчете получиться не может, так как знаменатель всегда будет сокращаться с числителем.

Чтобы понять закономерность, по которой формируется итоговое число, рассмотрим более высокое простое число, например 23:

$$\frac{-22\times-21\times-20\times-19\times-18\times-17\times-16\times-15\times-14\times-13\times-12}{1\times 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10\times 11}\equiv 1\ (mod\,23).$$

Разобьем выражение на два. Рассмотрим отдельно четные и нечетные числа по знаменателю.

$$\frac{-22\times-20\times-18\times-16\times-14\times-12}{1\times 3\times 5\times 7\times 9\times 11}\times\frac{-21\times-19\times-17\times-15\times-13}{2\times 4\times 6\times 8\times 10}\equiv 1\ (mod\,23).$$

Далее посчитаем результат по первой части:

$$\frac{-22\times-20\times-18\times-16\times-14\times-12}{1\times 3\times 5\times 7\times 9\times 11}=2048=2^{11}\equiv 1\ (mod\,11).$$

Результатом деления получилось число вида 2^n. Данный результат не является случайным и имеет закономерность, при $p > 8$:

$$\frac{(1-p)\times(3-p)\times(5-p)\ldots\left(\left(\frac{p-1}{2}\right)-p\right)}{1\times 3\times 5\times\ldots\left(\frac{p-1}{2}\right)}=2^{\left(\frac{p-1}{2}\right)}.$$

В расчете может получиться как положительное, так и отрицательное число. Принцип не меняется: если число отрицательное, то остаток от деления вычисляется от отрицательного числа. Наглядно видна связь данного выражения с малой теоремой Ферма: Если p – простое число, то оно удовлетворяет сравнению $a^{p-1} \equiv (mod\ p)$. Как правило, проверка простых чисел ведется именно по основанию 2, так как это наименьшее число. Выведенная формула позволяет оптимизировать выражение до вида

$$2^{\left(\frac{p-1}{2}\right)}+1 \equiv 0\left(mod\ p\right),$$ если число p – простое число вида $8k + 3$ или $8k + 5$.

$$2^{\left(\frac{p-1}{2}\right)}-1 \equiv 0\left(mod\ p\right),$$ если число p – простое число вида $8k + 1$ или $8k + 7$.

Разделение проверяемых чисел на две группы обусловлено количеством умножений отрицательных чисел, что наглядно видно из расчета, приведенного выше.

Данное условие является необходимым, но не достаточным признаком простого числа. Для полного доказательства простого числа необходимо решить вторую часть уравнения и доказать, что

$$\frac{(2-p)\times(4-p)\times(6-p)\ldots\left(\left(\frac{p-1}{2}\right)-p\right)}{2\times4\times6\times\ldots\left(\frac{p-1}{2}\right)}\times 2^{\left(\frac{p-1}{2}\right)} \equiv 1\left(mod\ p\right).$$

Доказательство данной части формулы требует расчета факториала, что затрудняет вычислительный процесс. Адаптация этой части уравнения остается открытым вопросом.

Предложенная формула значительно облегчает доказательство простых чисел, так как сокращает количество необходимых операций при прохождении теста простоты Ферма в два раза. Выведенное выражение раскрывает взаимосвязь малой теоремы Ферма и теоремы Вильсона, что открывает новые возможности изучения простых и псевдопростых чисел Ферма.

Список литературы

1. Коломийцева С.В., Соколова К.Н. Сравнительный анализ алгоритмов проверки чисел на простоту // Информационные технологии и высокопроизводительные вычисления: материалы V Международной научно-практической конференции. 2019. С. 90–96.

2. Дмитриев Е.А. Тест Вильсона // Приоритетные направления развития образования и науки: сборник материалов II Международной научно-практической конференции. В 2-х т. 2017. С. 54.

3. Певный А.Б., Юркина М.Н. Сложность решета Эратосфена и распределение простых чисел // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2020. № 4 (37). С. 66–72.

4. Чопик А.А. Применение китайской теоремы об остатках // Актуальные направления научных исследований XXI века: теория и практика. 2015. Т. 3. № 8–3 (19–3). С. 446–448.

5. Мамараимов М.Т., Уштенов Е.Р. Проблемы простых чисел и теорема о критерии простого числа. Theory and practice inthe physical, mathematical andtechnical sciences. 2012. С. 16.

6. Сикорская Г.А., Галушкин Д.А., Данильчук М.В. О методах проверки числа на простоту // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всероссийской научно-методической конференции (с международным участием). 2020. С. 1560.

7. Акылбаев М.И., Уштенов Е.Р. Новая теорема о критерии простого числа // Международный журнал прикладных и фундаментальных исследований. 2014. № 1–2. С. 255–257.

8. Дмитриев А.П., Рагило П.Ю., Вайтюль И.В. О распределении простых чисел // Тезисы докладов 51-й международной научно-технической конференции преподавателей и студентов. 2018. С. 124.