Н.А. Каленикова[1]
В.А. Минаев[2]
В.П. Хренов[3]

УСКОРЕНИЕ ФАКТОРИЗАЦИИ В МЕТОДЕ ФЕРМА

Работа посвящена ускорению хорошо известного алгоритма факторизации Ферма. Приведены примеры его реализации и оценка скорости работы.

Ключевые слова: *факторизация, простые числа.*

N.A. Kalenikova
V.A. Minaev
V.P. Khrenov

ACCELERATION OF FERMAT'S METHOD

The paper is devoted to the acceleration of a well known Fermat's method. Examples of its realization and an estimation of algorithm's speed are presented.

Keywords: *factorization, prime numbers.*

Алгоритм факторизации был получен П. Ферма в 1643 г. Основная его идея состоит в том, что составное число C является разностью квадратов, то есть $C = p \cdot q = a^2 - b^2 = (a - b)(a - b)$,

где $a = \frac{p+q}{2}$; $b = \frac{p-q}{2}$.

Поэтому значение a находится последовательным перебором чисел из множества $\left\{E(\sqrt{C})+1, E(\sqrt{C})+2, E(\sqrt{C})+3, ...\right\}$[4] до тех пор, пока не встретится такое a, что значение $a^2 - C$ будет являться точным квадратом, то есть b^2.

Метод Ферма относится к способу факторизации с экспоненциальной сложностью. Р. Леман усовершенствовал алгоритм факторизации Ферма таким образом, что в худшем случае для его выполнения требуется $o(C^{\frac{1}{3}})$ операций [1].

В 1982 году Х. Уильямс предложил метод факторизации с помощью последовательностей чисел Люка. В том же году Д. Поллард предложил свой метод факторизации с $o(B \log B \log^2 N)$ действий (B – максимальный простой делитель). В те же годы А. Ленстра предложил метод факторизации с помощью эллиптических кривых, появились и другие подходы [2].

В связи со сказанным, сложность проблемы факторизации до некоторого времени делала алгоритм шифрования RSA, основанный на произведении двух простых чисел, весьма надежным. Однако после успешного окончания ряда проектов по взлому RSA стало ясно, что разложение на множители не является невыполнимой задачей, и взлом очередного ключа большей длины – вопрос времени.

Таким образом, создание и разработка новых методов факторизации требует пристального внимания тех, кто использует RSA, так как именно этот алгоритм является самым распространенным способом шифрования, используется во множестве отраслей, применяется в защищенных телефонных сетях.

Важно отметить, что знание закона образования простых чисел [3] дает возможность создавать новые методы факторизации, не прибегая к помощи достаточно трудоемких тестов на проверку простоты чисел. Это существенно ускорит разработку новых алгоритмов факторизации.

Именно на знании закона образования простых чисел и основан изложенный в настоящей статье алгоритм факторизации, улучшающий метод Ферма.

Согласно работе [4], в которой описывается закономерность образования простых чисел, множество натуральных чисел образовано единицей, подмножеством из двух простых чисел ${}_1P = \{2, 3\}$, подмножеством простых чисел вида ${}^{-}P\{5, 11, 17, \ldots\}$, полученных путем вычитания единицы от чисел, кратных 6 $\{6n - 1\}$, $n = 1, 2, 3, \ldots$; (назовем их минус-простыми числами ${}^{-}p$ – МПЧ), подмно-

[1] Преподаватель НОУ ВПО «Российский новый университет».

[2] Доктор технических наук, профессор, проректор НОУ ВПО «Российский новый университет».

[3] Заместитель директора Института систем и технологий безопасности НОУ ВПО «Российский новый университет».

[4] Обозначение $E(x)$ введено Лежандром в 1798 году для обозначения функции целая часть от x.

жеством ^{+}P простых чисел {7, 13, 19, …}, образованном при помощи прибавления единицы к числам, кратным 6, {6n – 1}, n = 1, 2, 3, …; (назовем их плюс-простыми числами ^{+}p – ППЧ), подмножествами четных $_{2}C$ и нечетных чисел $_{3}C$ и подмножествами ^{-}C и ^{+}C составных чисел, также получаемых вычитанием либо прибавлением единицы к числам, кратным 6. По аналогии назовем их минус-составными числами (МСЧ) и плюс-составными числами (ПСЧ).

Числа, к которым может быть эффективно применим метод Ферма, – это элементы множеств МСЧ и ПСЧ. По определению [4], ПСЧ ^{+}C может быть получено как произведение двух ППЧ $^{+}C = {}^{+}p \cdot {}^{+}q$, так и двух МПЧ $^{+}C = {}^{-}p \cdot {}^{-}q$, а МСЧ ^{-}C образуется произведением МПЧ на ППЧ $^{-}C = {}^{-}p \cdot {}^{+}q = {}^{+}p \cdot {}^{-}q$ [3].

Новый алгоритм факторизации

Разложение на множители МСЧ

Если имеется МСЧ $^{-}C = {}^{-}p \cdot {}^{+}q = {}^{+}p \cdot {}^{-}q$, то метод факторизации Ферма можно улучшить не менее чем в 6 раз, руководствуясь следующей процедурой.

1. Вычислить значение $g = \dfrac{^{-}C + 1}{6}$ и, если оно четно, перейти к указанию 2, а если нечетно, то – к указанию 3.

2. Среди чисел вида:
$E(\sqrt{^{-}C}) + 1, E(\sqrt{^{-}C}) + 2, E(\sqrt{^{-}C}) + 3, \ldots$ исследовать на полный квадрат только числа, делящиеся нацело на 6.

3. Среди чисел вида:
$E(\sqrt{^{-}C}) + 1, E(\sqrt{^{-}C}) + 2, E(\sqrt{^{-}C}) + 3, \ldots$ исследовать на полный квадрат только числа, имеющие в остатке 3 при делении на 6.

В общем виде это утверждение выглядит так:

Утверждение 1. Если составное число – число вида $^{-}C = {}^{-}p \cdot {}^{+}q = {}^{+}p \cdot {}^{-}q$, то среднее арифметическое $a = \dfrac{^{+}p + {}^{-}q}{2}$ нацело делится на 6 при четном значении g или имеет в остатке 3 при нечетном значении g.

Доказательство

Для произведения ППЧ и МПЧ, например при $^{+}p = 6x + 1, {}^{-}q = 6y - 1,$ где x, y – натуральные, a и g примут вид:

$$a = \frac{^{+}p + {}^{-}q}{2} = \frac{6x + 1 + 6y - 1}{2} = 3x + 3y;$$

$$g = \frac{(6x + 1)(6y - 1) + 1}{6} = 6xy - x + y.$$

В зависимости от значений x и y возможны следующие случаи:

1) x и y – четные числа: $x = 2m$ и $y = 2n$, имеем:
$a = 3x + 3y = 6m + 6n$, следовательно, a делится на 6 нацело; а число $g = 6 \cdot 2m \cdot 2n - 2m + 2n = 2(12mn - m + n)$ – четное;

2) x и y – нечетные числа вида $x = 2m - 1$ и $y = 2n - 1$, $a = 3x + 3y = 3 \cdot (2m - 1) + 3 \cdot (2n - 1) = 6(m + n - 1)$, то есть a нацело делится на 6.

Так как $g = 6 \cdot (2m - 1)(2n - 1) - 2m + 1 + 2n - 1 = 2(12mn - 7m - 5n + 3)$, то оно, так же как и в случае 1, четное;

3) x – четное, а y – нечетное (или наоборот, что равносильно) числа вида $x = 2m$ и $y = 2n - 1$, тогда $a = 3 \cdot 2m + 3 \cdot (2n - 1) = 6m + 6n - 3$ имеет при делении на 6 в остатке 3, $g = 6 \cdot 2m\,(2n - 1) - 2m + 2n - 1 = 24mn - 14m + 2n - 1$.

Пример 1

Рассмотрим составное число C = 70098131. Выяснить, составное оно или простое, можно легко с помощью линейного генератора простых чисел подряд [5].

Поскольку g = 11683022 – число целое и четное, значит, исходя из выше приведенного доказательства, C является МСЧ.

Согласно доказанному выше алгоритму, если число g – четное, то на полный квадрат необходимо исследовать только числа, делящиеся нацело на 6.

Найдем значения a вида:

$E(\sqrt{^{-}C}) + 1, E(\sqrt{^{-}C}) + 2, E(\sqrt{^{-}C}) + 3, \ldots$:

$E(\sqrt{^{-}C}) = 8372.$

Множество значений a равно множеству {8373, 8374, 8375, …}.

По полученным значениям составим таблицу 1.

Таблица 1

a	8 373	8 374	8 375	8 376	8 377	8 378	8 379
$a^2 - {}^{-}C$	8 998	25 745	42 494	59 245	75 998	92 753	109 510
a	8 380	8 381	8 382	8 383	8 384	8 385	8 386
$a^2 - {}^{-}C$	126 269	143 030	159 793	176 558	193 325	210 094	226 865
a	8 387	8 388	8 389	…	8 464	8 465	8 466
$a^2 - {}^{-}C$	243 638	260 413	277 190	…	1 541 165	1 558 094	1 575 025

Остатки от деления значений a на 6 имеют вид:

$8373 \equiv 3 \pmod 6$
$8374 \equiv 4 \pmod 6$
$8375 \equiv 5 \pmod 6$
$8376 \equiv 0 \pmod 6$
…
$8466 \equiv 0 \pmod 6$

Среди всех значений $a^2 - {}^{-}C$ полным квадратом является число 1575025, то есть $b = \sqrt{a^2 - {}^{-}C} = \sqrt{8466^2 - 70098131} = 1255$.

Теперь, зная a и b, определим сомножители составного числа ${}^{-}C$, простоту которых можно проверить при помощи линейного генератора простых чисел подряд [5]:

$p = 8466 - 1255 = 7211$; $q = 8466 + 1255 = 9721$.

Таким образом, ${}^{-}C = 7211 \cdot 9721$.

Зная, что полный квадрат находится среди чисел, кратных 6, не надо высчитывать подряд все значения $a^2 - {}^{-}C$.

Предложенный в настоящей работе алгоритм позволяет сократить таблицу 1 до таблицы 2.

Таблица 2

a				8 376			
$a^2 - {}^{-}C$				59 245			
a			8 382				
$a^2 - {}^{-}C$			159 793				
a		8 388		…			8 466
$a^2 - {}^{-}C$		260 413		…			1 575 025

Вывод: решая задачу факторизации методом Ферма, необходимо вычислить 93 значения $a^2 - {}^{-}C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 15 значений $a^2 - {}^{-}C$.

Пример 2

Для разложения на простые сомножители МСЧ ${}^{-}C = 58420049$ методом Ферма, необходимо вычислить 213 значений $a^2 - {}^{-}C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 35 значений $a^2 - {}^{-}C$.

Разложение на множители ПСЧ

В случае если раскладывать на множители методом Ферма составное число вида ${}^{+}C$, возможных остатков от деления a на 6 будет больше. Это связано с тем, что оно может быть образовано двумя способами: ${}^{+}C = {}^{-}p \cdot {}^{-}q$ и ${}^{+}C = {}^{+}p \cdot {}^{+}q$. В таком случае улучшить скорость работы факторизации Ферма можно в 3 раза. Соответствующее описание алгоритма выглядит следующим образом.

1. Вычислить значение $f = \dfrac{{}^{+}C - 1}{6}$ и, если оно четно, перейти к указанию 2, а если нечетно, то – к указанию 3.

2. Среди всех возможных значений $a = \dfrac{{}^{-}p + {}^{-}q}{2}$ для нахождения значения, являющегося полным квадратом, необходимо рассматривать только числа, имеющие при делении на 6 в остатке 1 или 5.

3. Среди всех возможных значений $a = \dfrac{{}^{-}p + {}^{-}q}{2}$ для нахождения значения, являющегося полным квадратом, необходимо рассматривать только числа, имеющие при делении на 6 в остатке 2 или 4.

Утверждение 2. Если ${}^{+}C = {}^{-}p \cdot {}^{-}q$, то остаток от деления среднего арифметического $a = \dfrac{{}^{-}p + {}^{-}q}{2}$ на 6 равен 5 при четном значении f и 2 при нечетном f.

Доказательство

Для произведения МПЧ на МПЧ ${}^{-}p = 6x - 1$ и ${}^{-}q = 6y - 1$, где x, y – натуральные,

$$a = \frac{{}^{-}p + {}^{-}q}{2} = \frac{6x - 1 + 6y - 1}{2} = 3x + 3y - 1;\ f = 6xy - x - y.$$

В зависимости от значений x и y возможны следующие случаи:

1) x и y – четные числа: $x = 2m$, $y = 2n$, имеем: $a = 6m + 6n - 1$.

Таким образом, остаток от деления a на 6 равен 5. При этом:

$f = 6 \cdot 2m \cdot 2n - 2m - 2n = 2(12mn - m - n)$, то есть f – четное число;

2) когда x и y – нечетные числа вида $2m - 1$ и $2n - 1$, соответственно:

$a = 6m + 6n - 7$, и остаток от деления a на 6 равен 5. При этом:

$f = 6(2m - 1)(2n - 1) - 2m + 1 - 2n + 1 = 2(12mn - 7m - 7n + 4)$ – четное число;

3) для сочетания, когда x – четное, а y – нечетное, или наоборот:

$a = 6m + 6n - 4$. При делении a на 6 остаток равен 2. При этом:

$f = 6 \cdot 2m(2n - 1) - 2m - 2n + 1 = 24mn - 14m - 2n + 1$ – нечетное число, так как при делении на 2 имеет в остатке единицу.

Утверждение 3. Если $^{+}C = {}^{+}p \cdot {}^{+}q$, то среднее арифметическое $a = \dfrac{{}^{+}p + {}^{+}q}{2}$ имеет в остатке 1 при делении на 6, если значение f четно, или остаток равен 4 при нечетном значении f.

Доказательство утверждения аналогично двум предыдущим.

Пример 3

Для разложения на простые сомножители ПСЧ ^{+}C = 71396707 методом Ферма необходимо вычислить 116 значений $a^2 - {}^{-}C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 39 значений $a^2 - {}^{-}C$.

Стоит отметить, что в алгоритме RSA простые p и q рекомендуется выбирать таким образом, чтобы задача разложения числа C была достаточно сложна в вычислительном плане. Одним из требований, предъявляемым к используемым в RSA простым числам, является небольшая величина наибольшего общего делителя чисел $p - 1$ и $q - 1$; желательно, чтобы НОД$(p - 1, q - 1) = 2$ [10].

Легко показать, используя закон формирования простых чисел [3], что НОД$(p - 1, q - 1) = 2$ только в двух случаях: когда p представимо в виде $6n + 1$ и q в виде $6m - 1$ или при $p = 6n - 1$ и $q = 6m - 1$, то есть составное число может быть как ПСЧ, так и МСЧ, но ПСЧ в этом случае формируется только как произведение МПЧ на МПЧ.

Таким образом, из рассмотренных выше утверждений практическое приложение для алгоритма факторизации применительно к RSA могут быть только первые два. Их можно объединить в следующую систему указаний:

1) выяснить, элементом какого множества число является C: ПСЧ или МСЧ;

2) если C – МСЧ, нужно воспользоваться ***утверждением 1***, иначе – ***утверждением 2***.

Итак, в связи с тем, что в шифровании методом RSA не участвуют одновременно два ППЧ, предложенный в работе алгоритм, применимый к криптосистеме RSA, эффективнее метода факторизации Ферма не менее чем в 6 раз.

Отметим, что при последовательном вычислении скорость работы предложенного алгоритма не может конкурировать со способами факторизации с субэкспоненциальной сложностью. Наиболее эффективным из них на данный момент считается алгоритм решета числового поля, эвристическая оценка сложности которого составляет $e^{(k+o(1))(\log C)^{\frac{1}{3}}(\log\log C)^{\frac{2}{3}}}$ арифметических операций при некоторой постоянной k [2].

Построим модель вычислений, чтобы провести анализ и оценить возможность параллелизма улучшенного алгоритма. Модель нашего алгоритма представлена в виде графа «операции – операнд» на рис. 1.

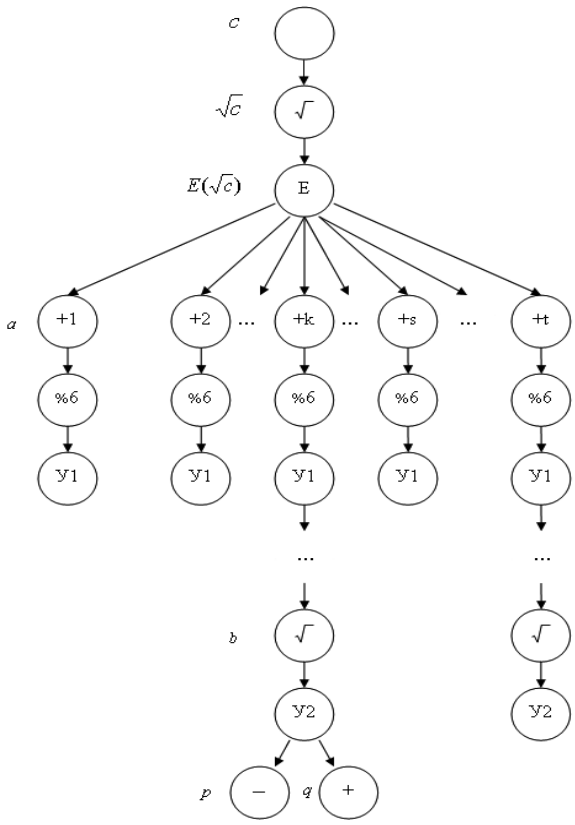

Рис. 1. Модель алгоритма факторизации в виде графа «операции – операнд»

Арифметические операции, записанные в вершинах графа, соответствуют арифметическим операциям языка программирования C.

У1 (условие 1) – равенство остатка от деления на 6 (остаток получен на предыдущем шаге операцией %6) в зависимости от того, каким числом является C: МСЧ или ПСЧ.

У2 (условие 2) – значение $\sqrt{a^2 - C}$ должно быть целым.

Очевидно, что в модели (рис. 1) существуют операции, между которыми нет пути, а значит, они могут выполняться параллельно.

Соответственно предложенный нами алгоритм может быть легко распараллелен, что дает возможность существенно увеличить его эффективность по мере подключения вычислительных мощностей при осуществлении факторизации.

Литература

1. Lehman, R.S. Factoring Large Integers // Math. Comp. 1974. – V. 28. – P. 637–646.

2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. – М. : МЦНМО, 2003.

3. Минаев, В.А., Хренов, В.П. Безопасность в сфере конфиденциальной информации и закон формирования простых чисел // Спецтехника и связь. – 2008. – № 3/ноябрь – декабрь. – С. 45–48.

4. Минаев, В.А., Хренов, В.П. Открытые закономерности образования простых чисел и некоторые прикладные аспекты открытия // Вестник Российского нового университета : сборник научных трудов – Управление, вычислительная техника и информатика. Выпуск 3. – М. : РосНОУ, 2008. – С. 49–59.

5. Хренов, В.П. Свидетельство № 2005613012 от 22 сентября 2005 г. : О регистрации программы «Линейный генератор простых чисел подряд».

6. Кнут, Д. Искусство программирования. Т. 2. Получисленные методы. – 3-е изд. – М. : Вильямс, 2007.

7. Коблиц, Н. Курс теории чисел и криптографии. – М. : Научное издательство ТВП, 2001.

8. Фомичев, В.М. Дискретная математика и криптология : курс лекций. – М. : Диалог-МИФИ, 2003.

9. Minaev, V.A., Khrenov, V.P., Zernov, V.A. Discovery of Natural Number Laws and Some Applied Aspects of Discovery : Recent Advanced in Management and Information Security / 1-st International Conference On Management of Technologies & Information Security, 21-st – 24-th January, 2010. – New Delhi, Shree Publishers & Distributors, 2010.

10. Алферов, А.П., Зубов, А.Ю., Кузьмин, А.С., Черемушкин, А.В. Основы криптографии. – М. : Гелиос АРВ, 2002.

11. Гергель, В.П. Теория и практика параллельных вычислений. – М. : Бином, Лаборатория знаний, Интернет-университет информационных технологий, 2007.