УДК 511:003.26.09

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 3, pp. 270-279

ВЫБОР ЭФФЕКТИВНОГО БАЗОВОГО ОСНОВАНИЯ МОДУЛЯ ПРИ МНОГОКРАТНОМ ПРОРЕЖИВАНИИ ПРОБНЫХ ЗНАЧЕНИЙ В МЕТОДЕ ФАКТОРИЗАЦИИ ФЕРМА С НЕРАВНОМЕРНЫМ ШАГОМ

Е.В. Максименко

Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт»,
ул. Верхнеключевая, 4, Киев, 03056, Украина; e-mail: iszzi@i.ua

Рассмотрена задача поиска базового основания модуля (*bb*) при многократном прореживании пробных значений в методе Ферма с неравномерным шагом. Для достижения максимального коэффициента ускорения при известном ограничении на объем памяти ЭВМ, используемой для хранения допустимых пробных значений *x*, сформулирована математическая постановка такой задачи и предложен способ ее решения на основании установленного соотношения для минимальных значений коэффициентов ускорения. Показано, что последовательность приращений пробных *x* периодически повторяется и сумма элементов такой периодической части может быть значительно меньшим чем *bb*, либо, если *bb* делится на 4 без остатка, меньшим чем *bb*/2. Обсуждаются вопросы решения задачи поиска эффективного *bb* в случае фиксированного *N*, когда значение *N*mod*bb* может меняться при изменении *bb*.

Ключевые слова: факторизация, метод Ферма, прореживание, ускорение.

Введение

В информационно-телекоммуникационных системах для целей криптографической защиты информации применяется RSA алгоритм, что вызывает интерес к его криптоанализу. В работе [1] показано, что известные примеры компрометации RSA алгоритма не являются эффективней задачи факторизации. Поэтому на современном этапе актуальным является решение задачи факторизации. Основные используемые методы решения задачи факторизации представлены в работах [2-4]. В работе [5] для решения задачи факторизации чисел предложен подход, связанный с прореживанием пробных значений с неравномерным шагом при использовании базового и множества других оснований модуля. Там же были приведены примеры выбора разных вариантов базового основания модуля и на основании численных экспериментов установлено, что время решения задачи факторизации методом прореживания существенно зависит от выбора базового основания, что требует специального исследования.

Постановка задачи

Пусть задано составное нечетное число $N = pq$, которое следует разложить на множители, где p и q некоторые нечетные числа, не обязательно являющиеся простыми. Согласно исходному варианту метода Ферма для определения p и q решают уравнение

$$X^2 = N + Y^2, \qquad (1)$$

где X и Y – целые положительные числа.

Если в (1) неизвестную X представить в виде $X = \left(\left[\sqrt{N}\right]+1\right)+x = x_0 + x$, то решение уравнения (1) получают перебором пробных значений $x = 0,1,2,\ldots,$ до тех пор, пока остаток $X^2 - N$ не окажется полным квадратом целого числа.

Назовем допустимыми те пробные значения x по модулю некоторого основания b, при которых разность $(X^2 - N) \bmod b$ является квадратичным остатком по модулю b, и недопустимыми остальные. Исключение недопустимых пробных значений x будем называть их прореживанием. Как показано в работе [5], при решении задачи факторизации целесообразно использовать множество различных оснований модуля, но при этом особая роль отводится базовому основанию модуля (в дальнейшем bb), которое играет роль первичного просеивания до дальнейшего анализа на допустимость значений x при других основаниях модуля.

В работе [5] на основании численных экспериментов при согласованных условиях для ряда вариантов факторизуемых чисел было определено время расчета при разных значениях базового основания модуля. Оказалось, что по сравнению с базовым основанием $bb = 277200$ в случае $bb = 25200$ $(25200 = 277200/11)$ время расчета увеличилось в $1.74 \div 1.78$ раза (в среднем в 1.77 раза). Для обеспечения сравнимости результатов суммарное число простых чисел в дополнительных основаниях модулей увеличилось на единицу за счет замены основания $b_{12} = 109$ на $b'_{12} = 1199 = 109 \cdot 11$. При использовании значения основания модуля $bb = 3600$ $(3600 = 27720/11/7)$ время расчета увеличилось в $3.06 \div 3.17$ раза (в среднем в 3.11 раза).

Следовательно, для метода Ферма с прореживанием пробных значений базовое основания модуля bb является существенно влияющим параметром, и способам выбора эффективного bb посвящено настоящее исследование.

Характеристики, определяющие эффективность основания модуля

Пусть $KN(b,N)$ - число допустимых значений x для основания b, для которых остаток $\left(x^2 - N\right) \bmod b$ является квадратичным остатком по модулю b, $MK(b)$ – множество чисел k от 1 до b-1, для которых НОД$(k,b) = 1$, а n_{MK} – число элементов множества $MK(b)$. Пусть также как и в [5]:

$|r(b)|_{\min}$ – минимальное число элементов множества допустимых x среди всех значений $N \bmod b$, не имеющих общих делителей с b: $|r|_{\min} = \min\limits_{k \in MK(b)} (KN(b,k))$,

$|r(b)|_{\max}$ – максимальное такое число элементов: $|r|_{\max} = \max\limits_{k \in MK(b)} (KN(b,k))$,

$r(b)_{cp}$ – среднее значение числа элементов: $|r|_{cp} = \sum\limits_{k \in MK(b)} KN(b,k) / n_{MK}$.

Определим коэффициенты ускорения:

$z_{\min}(b) = b / |r(b)|_{\max}$ – коэффициент минимального ускорения,

$z_{\max}(b) = b / |r(b)|_{\min}$ – коэффициент максимального ускорения,

$z_{cp}(b) = b / |r(b)|_{cp}$ – усредненное значение коэффициента ускорения.

В работах [6, 7] для коэффициента $z_{cp}(b)$ экспериментально установлено:

1. $z_{\min}(2^4) = z_{cp}(2^4) = z_{\max}(2^4) = 4$,

2. $z_{cp}(2^k) < 6$ при $k > 4$,

3. $z_{cp}(cb) = z_{cp}(c) \cdot z_{cp}(b)$, если c и b взаимно простые,

4. $z_{cp}(b) = 2$, если b простое число.

Свойства 2 и 4 не выполняются для $z_{\min}(b)$, а выполнение (или невыполнение) свойства 3 требует обоснования. На основании численных экспериментов в работе [6] определено, что для случая простых b $z_{\min}(b) = 2b/(b+1)$. В работе [5] на основании такого равенства получена оценка для $z_{\min}(b)$, когда b является произведением двух простых чисел. Коэффициент $z_{\min}(b)$ определяет условия максимально сложного варианта для метода многократного прореживания, который для случая метода факторизации Ферма будет при тех $N \bmod b$, при которых коэффициент ускорения будет минимальным. Поэтому при выборе b важно иметь оценку для $z_{\min}(b)$.

Исходя из соотношения $z_{\min}(b) = 2b/(b+1)$, для случая простых b можно предположить, что увеличения $z_{\min}(bb)$ можно добиться за счет умножении исходного основания bb на простые числа, которые еще не являются его множителями. Элементарные вычисления показывают, что число таких простых множителей не может быть большим, поскольку очень быстро растет их произведение и, как следствие, требуемая оперативная память компьютера для хранения допустимых x. Поэтому при выборе базового основания модуля целесообразно использовать и степени простых чисел. В табл. 1 приведены результаты численного определения $z_{\min}(b)$ для степеней $m = 1,2,3$ простых чисел $p < 24$, а также числа $4 = 2^2$.

Таблица 1.

Значения коэффициентов ускорения

Z	$Z_{\min}$			$Z_{\max}$			Z_{cp}		
m	1	2	3	1	2	3	1	2	3
$p=3$	1.5	3	3	3	4.5	6.75	2	3.6	4.154
$p=4$	2	4	4	2	4	8	2	4	5.333
$p=5$	1.667	2.5	2.5	2.5	3.571	4.032	2	2.941	3.086
$p=7$	1.75	2.333	2.333	2.333	3.0625	3.236	2	2.649	2.711
$p=11$	1.833	2.2	2.2	2.2	2.630	2.683	2	2.396	2.418
$p=13$	1.857	2.167	2.167	2.167	2.522	2.558	2	2.331	2.346
$p=17$	1.889	2.125	2.125	2.125	2.388	2.407	2	2.249	2.257

Как следует из данных табл. 1, для простых $p > 2$

$$z_{\min}\left(p^m\right) = \begin{cases} 2p/(p+1), m=1 \\ 2p/(p-1), m>1 \end{cases}. \qquad (2)$$

А в случае составного числа $p = 4$ при $m > 1$ $z_{\min}\left(4^m\right) = 4$.

Поскольку для произвольного bb существует $k = N \bmod bb$, для которого $|r|_{\max} = KN(b,k)$, то задача построения эффективного bb, гарантирующего заданное ускорение независимо от $N \bmod bb$, сводится к задаче построения наименьшего bb, обеспечивающего заданное минимальное ускорение. Для решения такой задачи определим общую структуру bb.

Общая структура bb и оценка значения $z_{\min}(bb)$

Согласно основной теореме арифметики произвольное целое число можно единственным способом представить в виде произведения простых чисел (с учетом перестановки множителей и их знаков). Поэтому общая структура базового основания модуля может быть записана в виде

$$bb = \prod_{k=1}^{n(bb)} p_k^{m_k}, \tag{3}$$

где $n(bb)$ – количество простых чисел – множителей bb, p_k $(k = 1 \div n)$ – простые числа – множители bb, m_k $(k = 1 \div n)$ – показатели степеней c_k. При этом, согласно данным табл. 1, имеет смысл использовать степени простых чисел не больше второй, а для числа 2 – четвертой. Если для произведения взаимно простых чисел $p1$ и $p2$ верно соотношение

$$z_{\min}(p1 \cdot p2) \geq z_{\min}(p1) \cdot z_{\min}(p2), \tag{4}$$

то для $z_{\min}(bb)$ будет достоверной оценка

$$z_{\min}(bb) \geq \prod_{k=1}^{n(bb)} z_{\min}(p_k^{m_k}). \tag{5}$$

Покажем, что соотношение (4) справедливо для произвольных взаимно простых чисел $p1$ и $p2$. Для этого первоначально докажем, что существует N такое, что количество чисел y в диапазоне от 0 до $p1 \cdot p2 - 1$, для которых $(y^2 - N) \bmod p1$ и $(y^2 - N) \bmod p2$ одновременно являются квадратичными остатками, равно произведению $z_{\min}(p1) \cdot z_{\min}(p2)$.

Действительно, для произвольных $p1$ и $p2$ существуют $z_{\min}(p1)$ и $z_{\min}(p2)$. Тогда существуют числа $k1\,(0 < k1 < p1)$ и $k2\,(0 < k2 < p2)$ такие, что $|r(p1)|_{\max} = KN(p1, k1)$ и $|r(p2)|_{\max} = KN(p2, k2)$.

Очевидно, что если для некоторого $x1\,(0 < x1 < p1)$ $(x^2 - k1) \bmod p1$ является квадратичным остатком по модулю $p1$, то таким же квадратичным остатком по модулю $p1$ будут числа $x_i = x1 + p1 \cdot i$ для $i \geq 0$.

Пусть $MPK(p1, p2, t)$ – множество чисел $\{(t + p1 \cdot i) \bmod p2\}_{i=0}^{p2-1}$. Множество $MPK(p1, p2, t)$ содержит все числа от 0 до $p2 - 1$. Если бы это было не так, то нашлись два равных значения $(t + p1 \cdot i1) \bmod p2 = (t + p1 \cdot i2) \bmod p2$, где $i1 < i2$. Следовательно, разность $(t + p1 \cdot i2) - (t + p1 \cdot i1) = p1 \cdot (i2 - i1)$ делилась бы на $p2$. Но $i2 - i1 < p2$, откуда следовало бы, что $p1$ и $p2$ имеют общий делитель больший единицы, т.е. не являются взаимно простыми.

Пусть $|r(p2)|_{\max} = \max_{k \in MK(p2)} (KN(p2, k)) = KN(p2, k2)$, где $0 \leq k2 \leq p2$. Поскольку множество $MPK(p1, p2, t)$ содержит все числа от 0 до $p2 - 1$, то среди элементов множества $\{t + p1 \cdot i\}_{i=0}^{p2-1}$ будет ровно $KN(p2, k2)$ значений $\{t_j = t + p1 \cdot i_j\}_{j=0}^{KN(p2,k2)}$, для которых $(t_j^2 - k2) \bmod p2$ будут квадратичными остатками по модулю $p2$. Так как это

верно для произвольного t в пределах от 0 до $p1-1$, то верно и для всех x, для которых $(x^2-k1)\bmod p1$ является квадратичным остатком.

Согласно китайской теореме об остатках существует единственное значение N такое, что $N \bmod p1 = k1 \bmod p1$, $N \bmod p2 = k2 \bmod p2$ и $0 < N < p1 \cdot p2$. Поэтому для произвольного $x1\,(0 < x1 < p1)$, для которого $(x^2-k1)\bmod p1$ является квадратичным остатком по модулю $p1$, существует $KN(p2,k2)$ чисел $\{x_j = x1 + p1 \cdot i_j\}_{j=0}^{KN(p2,k2)}$, для которых $(x_j^2-N)\bmod p1$ является квадратичным остатком по модулю $p1$, а $(x_j^2-N)\bmod p2$ – квадратичным остатком по модулю $p2$. А с учетом того, что при разных значениях $x1$ ($x1_1$ и $x1_2$) множества $MPK(p1,p2,x1_1)$ и $MPK(p1,p2,x1_2)$ не пересекаются, то суммарное количество чисел в диапазоне от 0 до $p1 \cdot p2 - 1$, для которых $(y^2-N)\bmod p1$ и $(y^2-N)\bmod p2$ одновременно являются квадратичными остатками, равно произведению $z_{\min}(p1) \cdot z_{\min}(p2)$, что и требовалось доказать.

Пусть теперь для взаимно простого с $p1$ и $p2$ числа $N\,(0 < N < p1 \cdot p2)$ $|r(p1 \cdot p2)|_{\max} = \max\limits_{k \in MK(p1 \cdot p2)} (KN(p1 \cdot p2,k)) = KN(p1 \cdot p2,N)$. Покажем, что для каждого $x\,(0 < x < p1 \cdot p2)$, для которого $(x^2-N)\bmod(p1 \cdot p2)$ является квадратичным остатком по модулю $p1 \cdot p2$, выполнены условия:

- $(x^2-N)\bmod p1$ является квадратичным остатком по модулю $p1$,
- $(x^2-N)\bmod p2$ является квадратичным остатком по модулю $p2$.

Поскольку $(x^2-N)\bmod(p1 \cdot p2)$ является квадратичным остатком по модулю $p1 \cdot p2$, то существует $y\,(0 < y < p1 \cdot p2)$, что $(x^2-N)\bmod(p1 \cdot p2) = y^2 \bmod(p1 \cdot p2)$.

Тогда $y^2 = c \cdot p1 \cdot p2 + r0$, где c – некоторое натуральное число или 0, а $r0 = y^2 \bmod(p1 \cdot p2)$. Если $r0$ представить в виде $r0 = c1\,p1 + r1$, где $c1$ – некоторое натуральное число или 0, а $r0$ – натуральное число, то $r1 = r0 \bmod p1$. Следовательно, $y^2 \bmod p1 = (c \cdot p1 \cdot p2 + c1 \cdot p1 + r0) \bmod p1 = r0$, а для x значение $(x^2-N)\bmod p1$ является квадратичным остатком по модулю $p1$.

Аналогично доказывается, что $(x^2-N)\bmod p2$ является квадратичным остатком по модулю $p2$.

Из доказанного следует, что в случаях N, когда максимальным будет количество значений $x\,(0 < x < p1 \cdot p2)$, для которых $(x^2-N)\bmod(p1 \cdot p2)$ является квадратичным остатком по модулю $p1 \cdot p2$, такое количество не превосходит числа тех $x\,(0 < x < p1 \cdot p2)$, для которых $(x^2-N)\bmod p1$ является квадратичным остатком по модулю $p1$, а $(x^2-N)\bmod p2$ – квадратичным остатком по модулю $p2$. Следовательно, $|r(p1 \cdot p2)|_{\max} \le |r(p1)|_{\max} \cdot |r(p2)|_{\max}$, а

$$z_{\min}(p1 \cdot p2) = \frac{p1 \cdot p2}{|r(p1 \cdot p2)|_{\max}} \ge z_{\min}(p1) \cdot z_{\min}(p2) = \frac{p1}{|r(p1)|_{\max}} \cdot \frac{p2}{|r(p2)|_{\max}},$$

что доказывает справедливость оценок (4).

Для оценки соотношения между $z_{\min}(p1 \cdot p2)$ и $z_{\min}(p1) \cdot z_{\min}(p2)$ были проведены ряд численных экспериментов и некоторые из их результатов приведены в табл. 2.

Таблица 2.

Сравнительные данные о коэффициентах ускорения

№ п/п	bb	p	2	3	5	7	11	13	$\prod z_{\min}$	$z_{\min}(bb)$
1	3600	m	4	2	2				30	30
		$z_{\min}(p^m)$	4	3	5/2					
2	25200	m	4	2	2	1			52.5	52.5
		$z_{\min}(p^m)$	4	3	5/2	7/4				
3	277200	m	4	2	2	1	1		96.25	96.25
		$z_{\min}(p^m)$	4	3	5/2	7/4	11/6			
4	3603600	m	4	2	2	1	1	1	178.75	178.75
		$z_{\min}(p^m)$	4	3	5/2	7/4	11/6	13/7		

В табл. 2 символом p обозначены простые числа, символом m – показатели их степеней, а $\prod z_{\min}$ – это произведение $z_{\min}(p^m)$.

В данных табл. 2 значение $z_{\min}(bb)$ в соотношении (5) в точности равно $\prod_{k=1}^{n(bb)} z_{\min}(c_k^{m_k})$. Поэтому для оценки эффективности базового основания модуля вместо $z_{\min}(bb)$ допустимо использовать произведение $\prod_{k=1}^{n(bb)} z_{\min}(c_k^{m_k})$.

Значение $z_{\min}(bb)$ позволяет определить размер оперативной памяти, необходимой для хранения максимально возможного количества допустимых x, равного $|r(b)|_{\max} = bb / z_{\min}(bb)$. Такие данные для вариантов bb, представленных в табл. 2, приведены в табл. 3. Следует отметить, что bb увеличивается значительно быстрее, чем коэффициент ускорения. Следовательно, быстро растет объем данных о допустимых x, что является ограничением и что следует учитывать при выборе bb.

Таблица 3.

Данные о количестве допустимых x для вариантов bb, представленных в табл. 2

Вариант bb	bb	$z_{\min}(bb)$	$\lvert r(b)\rvert_{\max} = bb / z_{\min}(bb)$
1	3600	30	120
2	25200	52.5	480
3	277200	96.25	2880
4	3603600	178.75	20160

Математическая постановка задачи выбора эффективного bb

Базовое основание модуля будем считать эффективным, если оно позволяет обеспечить максимальное ускорение при заданном ограничении на объем требуемой оперативной памяти ЭВМ для хранения информации о допустимых пробных значениях x для произвольных $N \bmod bb$, полагая при этом выполнение равенства в соотношении (5).

Согласно определению эффективности для bb можно сформулировать следующую задачу нелинейного программирования:

$$\prod_{k=1}^{n(bb)} z_{\min}(c_k^{m_k}) \to \max, \tag{6}$$

$$bb / \prod_{k=1}^{n(bb)} z_{\min}(c_k^{m_k}) \le S, \tag{7}$$

где S – некоторое заданное значение.

При решении задачи (6)-(7) целесообразно учесть некоторые соотношения и оценки для отношения $c_k^{m_k} / z_{\min}(c_k^{m_k})$, являющегося составной частью $bb / \prod_{k=1}^{n(bb)} z_{\min}(c_k^{m_k})$.

Для произвольного простого числа $p > 2$ определим значение отношения $c_k^{m_k} / z_{\min}(c_k^{m_k})$ для $m_k = 1$ и $m_k = 2$, являющегося множителем для левой части неравенства (7):

$$\begin{cases} p / z_{\min}(p) = p / (2p / (p+1)) = (p+1)/2 \\ p^2 / z_{\min}(p^2) = p^2 / (2p / (p-1)) = p(p-1)/2 \end{cases}.$$

Если при этом $p1 > p2 > 2$, то

$$\begin{cases} p1 / z_{\min}(p1) = (p1+1)/2 > (p2+1)/2 = p2 / z_{\min}(p2), \\ p1^2 / z_{\min}(p1^2) = p1(p1-1)/2 > p2(p2-1)/2 = p2^2 / z_{\min}(p2^2). \end{cases} \tag{8}$$

Следовательно, отношение $c_k^{m_k} / z_{\min}(c_k^{m_k})$ будет тем меньшим, чем меньшим будет простое число c_k.

Кроме того, при $p1 > p2 > 2$, для $t1 = p1^2 \cdot p2$ и $t2 = p1 \cdot p2^2$

$$\begin{aligned} t1 / z_{\min}(t1) - t2 / z_{\min}(t2) &= p1(p1-1)/2 \cdot (p2+1)/2 - (p1+1)/2 \cdot p2(p2-1)/2 = \\ &= (p1^2 p2 + p1^2 - p1p2 - p1) - (p2^2 p1 + p2^2 - p1p2 - p2) = \\ &= (p1 - p2)(p1p2 - p1 - p2 - 1) > (p1 - p2)(2p1 - p1 - p2 - 1) = \\ &= (p1 - p2)(p1 - p2 - 1) > 0. \end{aligned} \tag{9}$$

Согласно соотношению (9) $p1^2 \cdot p2 / z_{\min}(p1^2 \cdot p2) < p1 \cdot p2^2 / z_{\min}(p1 \cdot p2^2)$, если $p1 > p2 > 2$. Следовательно, в решении задачи (6)-(7) показатели степени простых чисел не могут увеличиваться при росте значения простого числа в произведении (3).

Из соотношений (8) и (9) следует, что если индекс k для простых чисел c_k в формуле (3) означает порядковый номер простого числа, причем (как исключение) $c_1 = 4$, то в результате решения задачи (6)-(7) получится bb следующего вида:

$$bb = \prod_{k=1}^{n(bb)} c_k \cdot \prod_{k=1}^{n2(bb)} c_k, \tag{10}$$

где $n2(bb)$ – некоторое число, не превышающее $n(bb)$.

Исходя из структуры bb, представленной формулой (10), решение задачи (6)-(7) будет состоять в переборе вариантов значений $n(bb)$ и $n2(bb)$ и выборе лучшего из них.

Рассмотрим пример задачи (6)-(7).

Пусть располагаемый объем оперативной памяти ЭВМ для хранения информации о допустимых значениях x ограничен 10^6 числами. Необходимо определить bb, обеспечивающее максимальное значение минимального ускорения, при котором количество допустимых x $|r(bb)|_{\max}$ не превышает 10^6.

Результаты расчетов для разных вариантов bb в зависимости от $n(bb)$ и $n2(bb)$, величины $z_{\min}(bb)$ и $|r(bb)|_{\max}$ представлены в табл. 4 для случая $|r(bb)|_{\max} \le 10^6$.

Таблица 4.

Результаты расчетов для примера задачи (6)-(7)

$n2$	bb, $z_{\min}(bb)$ $\lvert r(bb)\rvert_{\max}$	n				
		4	5	6	7	8
0	bb	420	4620	60060	1021020	19399380
	z	8.75	16.0417	29.7917	56.2731	106.919
	r	48	288	2016	18144	181440
1	bb	1680	18480	240240	4084080	77597520
	z	17.5	32.0833	59.5833	112.5463	213.838
	r	96	576	4032	36288	362880
2	bb	5040	55440	720720	12252240	232792560
	z	35	64.1667	119.167	225.0926	427.6759
	r	144	864	6048	54432	544320
3	bb	25200	277200	3603600	61261200	
	z	52.5	96.25	178.75	337.6389	
	r	480	2880	20160	181440	
4	bb	176400	1940400	25225200	*428828400*	
	z	70	128.33333	238.33333	*450.18519*	
	r	2520	15120	105840	*952560*	
5	bb		21344400	277477200		
	z		154	286		
	r		138600	970200		

Полученное решение задачи (6)-(7) выделено в табл. 4 курсивом, где $bb = 428828400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$.

Как следует из данных табл. 3 и 4, быстрый рост bb сопровождается относительно медленным ростом $z_{\min}(bb)$ и, следовательно, быстрым ростом требуемой памяти ЭВМ для хранения информации о допустимых x. Поэтому представляют интерес способы сокращения объема требуемой памяти ЭВМ без потери информации о допустимых x либо увеличения коэффициента ускорения без увеличения объема требуемой памяти ЭВМ. Эти вопросы рассматриваются ниже.

Сокращение объема требуемой памяти ЭВМ для эффективного bb

Согласно формуле (10), определяющей структуру эффективного базового основания модуля, bb всегда нацело делится на 4. Поэтому в случае допустимого $x < bb/2$, допустимыми окажутся также значения: $bb/2 - x$, $bb/2 + x$, $bb - x$. Действительно,

$$(bb/2-x)^2 \bmod bb = (bb^2/4 - bb\cdot x + x^2) \bmod bb = (bb(b/4-x)+x^2) \bmod bb = x^2 \bmod bb,$$

$$(bb/2+x)^2 \bmod bb = (bb^2/4 + bb\cdot x + x^2) \bmod bb = (bb(b/4+x)+x^2) \bmod bb = x^2 \bmod bb,$$

$$(bb-x)^2 \bmod bb = (bb^2 - 2bb\cdot x + x^2) \bmod bb = (bb(b-2x)+x^2) \bmod bb = x^2 \bmod bb.$$

Следовательно, если определить некоторое начальное допустимое значение x и приращения для определения следующих допустимых x, то последовательность приращений будет повторяться через $KN(bb,N)/2$ значений, где сумма приращений равна $bb/2$. Поэтому в памяти ЭВМ достаточно хранить данные только о приращениях для допустимых x, сумма которых равна $bb/2$.

В дальнейшем для периодической последовательности приращений, сумма периодической части элементов которой равна некоторому числу P, будем говорить, что такая последовательность обладает периодом длины P вне зависимости от числа элементов ее периодической части. При этом для произвольного bb независимо от N длина периода $P = bb$. В случае же, когда bb делится без остатка на 4, $P = bb/2$.

Следует отметить, что при незначительном усложнении программного кода можно сократить объем хранимой информации еще в два раза, если воспользоваться условием, что вместе с x допустимым является $bb/2 - x$.

Дальнейшее сокращение объема требуемой памяти ЭВМ возможно для отдельных случаев чисел N, когда длина периода P может быть меньшей чем $bb/2$, что требует более глубокого анализа структуры N и bb.

Выводы

Проведенные исследования показали, что задачу выбора эффективного базового основания модуля следует рассматривать в двух постановках:

1. как задачу поиска bb такого, что независимо от $N \bmod bb$ будет выполнено ограничение на максимально возможный объем памяти ЭВМ, необходимой для хранения информации о допустимых x, и тогда математическая постановка задачи сводится к задаче динамического программирования (6)-(7), которую, с учетом полученного общего вида bb (формула (10)), можно решить перебором небольшого числа вариантов;
2. как задачу поиска эффективного bb для разложения на множители известного N, когда при изменении bb может меняться $N \bmod bb$. Тогда общая постановка задачи поиска базового основания модуля, обеспечивающего максимальное ускорение при выполнении ограничений на объем требуемой памяти ЭВМ формально может соответствовать задаче (6)-(7). Но при этом не будут выполняться соотношения (4), (8), (9), а ее решение возможно на основе перебора вариантов показателей степеней простых чисел, которые могут превышать значение 2.

Список литературы

1. Brown, Daniel R.L. Breaking RSA May Be As Difficult As Factoring [Электронный ресурс] / Daniel R.L. Brown // Cryptology ePrint Archive. – Report 2005/380. –. Режим доступа: http://eprint.iacr.org/2005/380
2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328с.
3. Song, Y. Yan Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) / Y. Yan Song. – Springer, 2009. – 372 pp.

4. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань: Казан. ун., 2011. – 190 с.
5. Винничук, С.Д. Многократное прореживание для ускорения метода факторизации ферма при неравномерных шагах для неизвестной / С.Д. Винничук, Е.В. Максименко // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – 2016. – № 64. – С. 13-24.
6. Винничук, С.Д. Алгоритм Ферма факторизации чисел вида N=pq методом прореживания / С.Д. Винничук, А.В. Жилин, В.Н. Мисько // Электронное моделирование. – 2014. – №2. – Т. 36. – С. 3-14.
7. Місько, В.М. Прискорення методу Ферма методом проріджування з використання декількох баз / В.М. Місько // Безпека інформації. – 2015. – №1. – Т. 21. – С. 64-68.

ВИБІР ЕФЕКТИВНОЇ БАЗОВОЇ ОСНОВИ МОДУЛЯ ПРИ БАГАТОРАЗОВОМУ ПРОРІДЖУВАННІ ПРОБНИХ ЗНАЧЕНЬ В МЕТОДІ ФАКТОРИЗАЦИИ ФЕРМА З НЕРІВНОМІРНИМ КРОКОМ

Є.В. Максименко

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут»
вул. Верхньоключова, 4, Київ, 03056, Україна; e-mail: iszzi@i.ua

Розглянуто задачу пошуку базової основи модуля (*bb*) при багаторазовому проріджуванні пробних значень в методі Ферма з нерівномірним кроком. Для досягнення максимального коефіцієнта прискорення при відомому обмеження на обсяг пам'яті ЕОМ, яка використовується для зберігання допустимих пробних значень *x*, сформульована математична постановка такого завдання і запропонований спосіб її вирішення на підставі встановленого співвідношення для мінімальних значень коефіцієнтів прискорення. Показано, що послідовність збільшень пробних *x* періодично повторюється і сума елементів такої періодичної частини може бути значно меншим за *bb*, або, якщо *bb* ділиться на 4 без залишку, меншим за *bb*/2. Обговорюються питання вирішення завдання пошуку ефективного *bb* в разі фіксованого *N*, коли значення *N*mod*bb* може змінюватися при зміні *bb*.
Ключові слова: факторизація, метод Ферма, проріджування, прискорення.

SELECTION OF EFFECTIVE BASIC BASIS OF MODULE WITH MULTIPLE THINNING TRIAL VALUE IN THE FACTORIZATION FERMAT'S METHOD WITH IRREGULAR PITCH

Ye. Maksymenko

Institute of Special Communication and Information Protection of National Technical University of Ukraine "Kyiv Polytechnic Institute",
4, Verhnyoklyuchova st., Kyiv, 03056, Ukraine; e-mail: iszzi@i.ua

The task of searching the basic module basis (*bb*) with repeated thinning test values in the Fermat's method with irregular pitch was considered. To achieve the maximum acceleration rate during a known restriction on the limited amount of computer memory used to store the valid test values of *x*, the mathematical formulation of this problem is formulated and proposed a way to solve it on the basis of the established relations for the minimum values of the acceleration coefficient. It is shown that the sequence of test increments of *x* periodically repeated and the sum of elements of the periodic part can be significantly smaller for *bb*, or if divided by 4 *bb* without a residue for less *bb/2*. The issues with the problem of search effective *bb* in the case of fixed *N*, when *N*mod*bb* value can change with *bb* are discussed.
Keywords: factorization, method of Fermat, thinning, acceleration.