Компьютерная Математика

УДК 519.615

В.Ю. СЕМЕНОВ

МЕТОД ИЗВЛЕЧЕНИЯ КВАДРАТНЫХ КОРНЕЙ В КОЛЬЦАХ ПОЛИНОМОВ С ПОМОЩЬЮ РЕШЕНИЯ СИСТЕМ НЕЛИНЕЙНЫХ УРАВНЕНИЙ

Предложен метод извлечения квадратных корней из полиномов в контексте актуальной задачи факторизации целых чисел. Метод основан на предложенном подходе для нахождения всех корней систем нелинейных алгебраических уравнений, который использует критерий Кравчика в качестве средства для проверки существования решения системы уравнений на заданном многомерном интервале поиска корней.. Приводятся результаты моделирования предложенного метода, свидетельствующие о его применимости к решению поставленной задачи.

Введение. Задача факторизации больших чисел имеет важное прикладное значение для задач криптографии, таких, например, как алгоритм RSA. Среди известных методов решения этой задачи, общий метод решета числового поля (ОМРЧП, англ. – GNFS) является наиболее быстрым на данный момент из известных методов факторизации больших чисел [1]. К основным этапам этого метода относятся: факторизация нечетных натуральных чисел по методу Ферма; нахождение подмножества множества целых чисел, произведение которых является квадратом; составление факторной базы; нахождение квадратного корня по модулю числа, подвергаемого разложению.

Нахождение квадратных корней из больших целых чисел по целочисленному модулю является наиболее алгоритмически сложной частью метода ОМРЧП. Известно большое количество подходов к решению данной задачи (см., например, [2, 3]).

Известно, что задача нахождения квадратного корня в кольце $\mathbb{Z}_N$ целых чисел по модулю N эквивалентна нахождению квадратного корня из полинома над соответствующим кольцом полиномов [4]. В свою очередь, как будет показано далее, задача нахождения квадратного корня из полинома сводится к решению систем нелинейных (квадратичных) уравнений относительно коэффициентов искомого полинома. Поэтому в данной работе мы предлагаем метод из

полиномов, основанный на предложенном ранее автором методе решения систем нелинейных алгебраических уравнений. Также приводятся результаты моделирования предложенного метода, свидетельствующие о его применимости к решению поставленной задачи.

Предварительные сведения. Пусть перед нами стоит задача факторизации натурального числа N. Для его факторизации алгоритм ОМРЧП требует выбор неприводимого полинома $f(x)$ степени d с целочисленными коэффициентами:

$$f(x)=\sum_{k=1}^{d+1} f_k x^{d+1-k}\ ,\ \ 0\le f_k<N,\ k=2,...,d+1,\ f_1=1.$$

При этом предполагается, что полином $f(x)$ имеет корень m в кольце $\mathbb{Z}_N$, т. е. $f(m)=0\ (\mathrm{mod}\ N)$, а выбор порядка d полинома $f(x)$ может быть осуществлен по приблизительной формуле $d\approx\log_m n$.

Пусть $B(x)$ – исходный полином, из которого извлекается квадратный корень:

$$B(x)=\sum_{k=1}^{d} b_k x^{d-k}\ . \qquad (1)$$

Тогда задача вычисления квадратного корня состоит в нахождении коэффициентов полинома $A(x)$ на основе уравнения

$$\mathrm{mod}(A^2(x),\ f(x))=B(x), \qquad (2)$$

где

$$A(x)=\sum_{k=1}^{d} a_k x^{d-k}. \qquad (3)$$

Подставляя (1) и (3) в (2), мы получим, что нахождение коэффициентов $(a_1,a_2,...,a_d)$ приводит к системе квадратично-полиномиальных уравнений. Так, например, в случае $d=3$ после выполнения деления $A^2(x)$ на $f(x)$ и приведения подобных слагаемых, уравнение (2) сводится к следующей системе уравнений относительно (a_1,a_2,a_3):

$$\begin{cases}(2a_1a_3+a_2^2-(a_1^2f_3)/\ f_1-(\ f_2(2a_1a_2-(a_1^2f_2)/\ f_1))/\ f_1)=b_1,\\ (2a_2a_3-(a_1{}^2f_4)/\ f_1-(\ f_3(2a_1a_2-(a_1^2f_2)/\ f_1))/\ f_1)x=b_2,\\ a_3^2-(\ f_4(2a_1a_2-(a_1^2f_2)/\ f_1))/\ f_1=b_3.\end{cases} \qquad (4)$$

К решению системы (4) может быть применен метод решения систем нелинейных алгебраических уравнений, предложенный автором в работе [5]. Структура предложенного метода показана на рис. 1. Используемые нами тесты отсутствия корней и единственности корня основаны на критерии Кравчика и разложении функций системы в ряд Тейлора [5]. Уточнение корня производилось с помощью стандартного итерационного метода Ньютона.

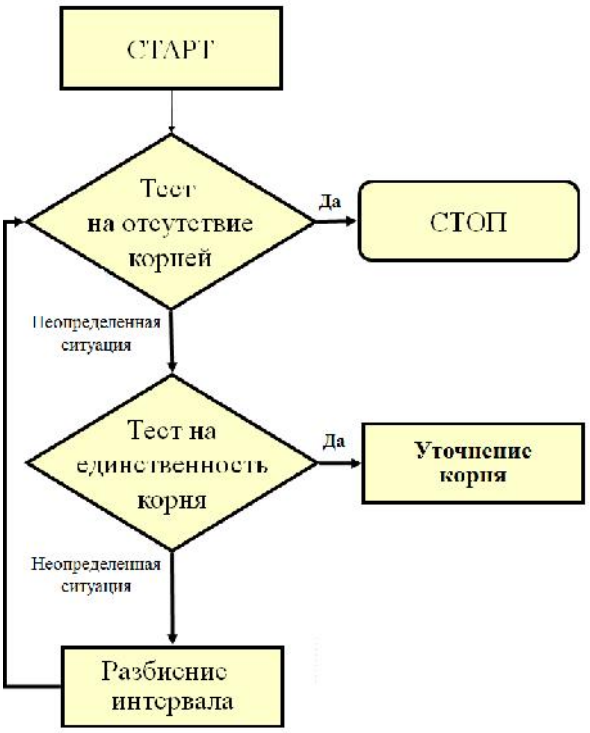

РИС. 1. Блок-схема метода нахождения всех корней системы уравнений, предложенная в работе [5]

Экспериментальные результаты. Следуя работе [4], рассматриваем случай, при котором

$$f(x) = x^3 + 15x^2 + 29x + 8,$$

т. е. в данном случае $(f_1, f_2, f_3, f_4) = (1,15,29,8)$.

Тогда система (4) принимает вид:

$$\begin{cases} 196a_1^2 - 30a_1a_2 + 2a_3a_1 + a_2^2 - b_1 = 0, \\ 427a_1^2 - 58a_2a_1 + 2a_2a_3 - b_2 = 0, \\ 120a_1^2 - 16a_2a_1 + a_3^2 - b_3 = 0. \end{cases} \tag{5}$$

Вначале рассмотрим пример, при котором значения параметров составляют $(b_1, b_2, b_3) = (18808, 41720, 11929)$.

Решение системы уравнений (5) на интервале $D = [-50,50] \times [-50,50] \times [-50,50]$ с помощью алгоритма [5] позволило найти все 8 корней данной системы $\mathbf{x}_k, k = 1,...,8$, которые приведены в таблице. Как видно, найденные значения корней симметричны относительно точки $(0,0,0)$. Общее количество

разбиений интервала D составило 13635. График проекции рекурсивного разбиения на плоскость (b_1, b_2), выполненный алгоритмом, на рис. 2. Корни $\mathbf{x}_k, k = 1,...,8$ обозначены на данном графике знаком “+”.

ТАБЛИЦА. Решения системы (5) при значениях параметров $b_1 = 18808$, $b_2 = 41720$, $b_3 = 11929$

$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	$\mathbf{x}_5$	$\mathbf{x}_6$	$\mathbf{x}_7$	$\mathbf{x}_8$
– 13.337	– 11.559	– 12	– 10.222	10.222	12	11.559	13.337
– 47.614	– 24.307	– 28	– 4.693	4.693	28	24.307	47.614
– 27.277	– 19.748	5	12.529	– 12.529	– 5	19.748	25.277

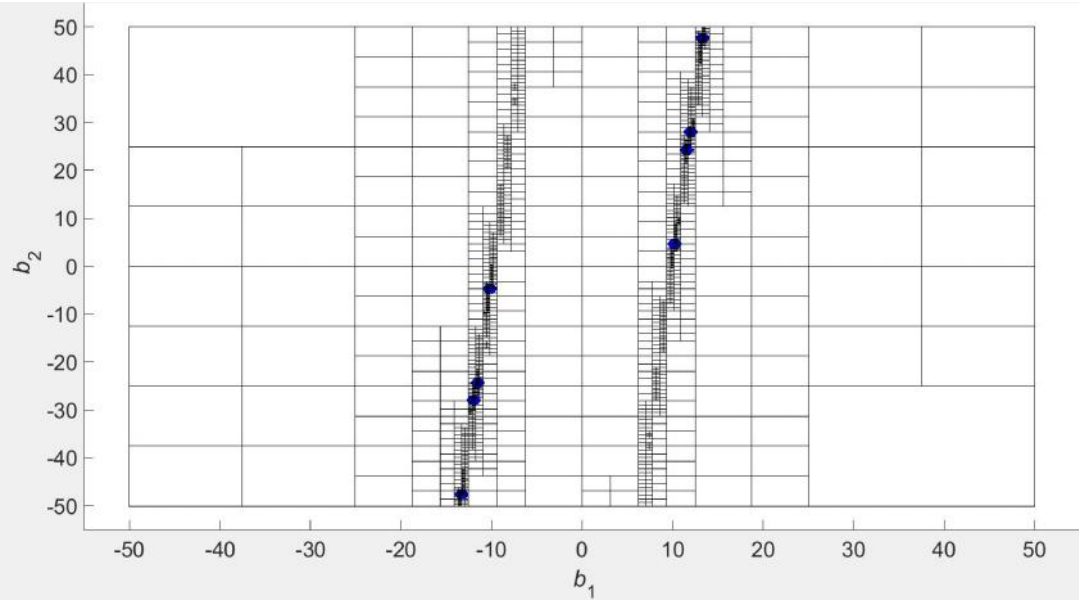

РИС. 2. График проекции рекурсивного разбиения на плоскость (b_1, b_2), выполненный для решения системы (5)

Теперь учтем интересующее нас обстоятельство, – целочисленные решения системы (5). Это означает, что в процессе решения системы (5) мы будем исключать интервалы, которые не могут содержать целочисленное решение. В этом случае общее количество разбиений интервала D составило 8953 (т. е. на 52 % меньше), в результате чего были найдены два искомых целочисленных решения: $\mathbf{x}_1 = (-12, -28, 5)$, $\mathbf{x}_2 = (12, 28, -5)$. График проекции рекурсивного разбиения на плоскость (b_1, b_2), выполненный алгоритмом, показан на рис. 3. Корни обозначены на данном графике знаком “+”.

Теперь рассмотрим случай, в котором $b_1 = 22455983949710645412$, $b_1 = 54100105785512562427$, $b_3 = 22939402657683071224$.

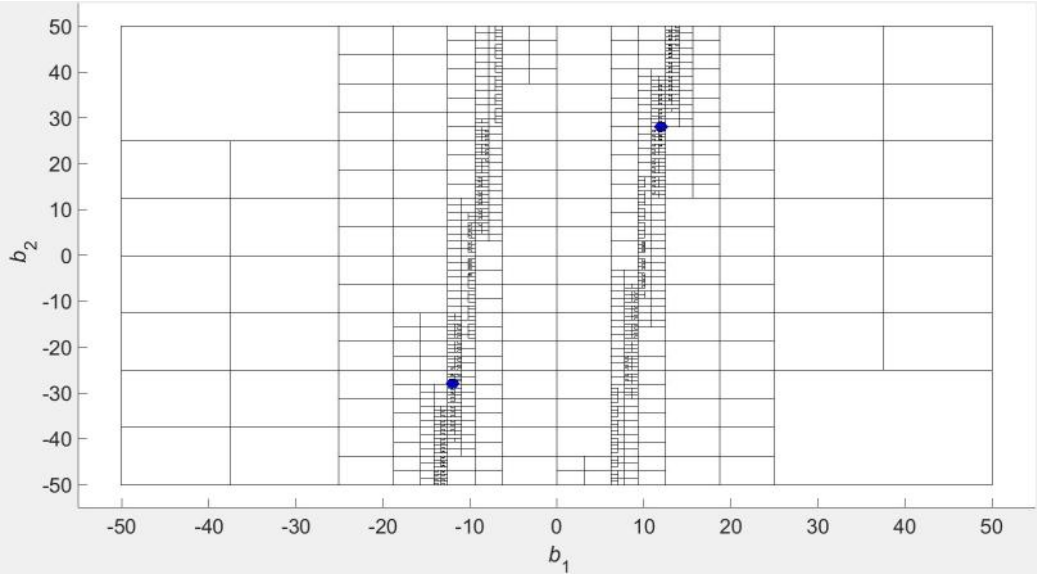

РИС. 3. График проекции рекурсивного разбиения на плоскость (b_1, b_2), выполненный для решения системы (5) с учетом целочисленности корней

Поиск корней системы (5) производился на интервале $D = [-5\times10^9, 5\times10^9]\times$ $\times[-5\times10^9, 5\times10^9]\times[-5\times10^9, 5\times10^9]$. При применении алгоритма [5] к решению соответствующей системы (5) за 12995 рекурсивных разбиений были найдены все 8 ее решений, из которых целочисленным является только два: $\mathbf{x}_1 = (599923511, 3686043120, 3889976768)$ и $\mathbf{x}_2 = (-599923511, -3686043120, -3889976768)$. Таким образом, искомым ответом является полином

$$A(x) = 599923511x^2 + 3686043120x + 3889976768.$$

Выводы. Предложен метод извлечения квадратных корней из полиномов в контексте задачи факторизации целых чисел. Метод основан на предложенном подходе к решению систем нелинейных алгебраических уравнений с помощью критерия Кравчика. Приводятся результаты моделирования предложенного метода, свидетельствующие о его применимости к решению поставленной задачи. Метод также может быть применен к нахождению корней произвольной степени в кольцах полиномов.

В.Ю. Семенов

МЕТОД ОБЧИСЛЕННЯ КВАДРАТНИХ КОРЕНІВ У КІЛЬЦЯХ ПОЛИНОМІВ
ЗА ДОПОМОГОЮ РОЗВ'ЯЗАННЯ СИСТЕМ НЕЛІНІЙНИХ РІВНЯНЬ

Запропоновано метод обчислення квадратних коренів з поліномів у контексті актуальної задачі факторизації цілих чисел. Метод засновано на запропонованому підході до розв'язання систем нелінійних алгебраїчних рівнянь на основі використання критерія Кравчіка як засіб перевірки єдиності кореня системи рівнянь на заданому багатовимірному інтервалі. Наведено результати моделювання запропонованого методу, що свідчать можливість його застосування до вирішення поставленої задачі.

V. *Semenov*

METHOD FOR CALCULATION OF SQUARE ROOTS IN POLYNOMIAL
RINGS BASED ON THE SOLUTION OF SYSTEMS OF NONLINEAR EQUATIONS

A method for calculation of square roots of polynomials in the context of integer numbers' factorization. The method is based on the proposed approach to solving systems of nonlinear algebraic equations, which use Krawczyk criterion as a test for the uniqueness of a root on the given interval. The results of modelling the method show its applicability to solve the problem under consideration.

Список литературы

1. Lenstra A.K., Lenstra H.W. The development of the number field sieve. *Lecture Notes in Mathematics*. Vol. 1554, Berlin, Springer-Verlag, 1993.
2. Montgomery P.L. Square roots of products of algebraic numbers. *Proceedings of Symposia in Applied Mathematics, Mathematics of Computation 1943-1993.* 1993. P. 567 – 571.
3. Couveignes *J.M.* Computing a square root for the number field sieve. *Lecture Notes in Mathematics*, Vol. 1554, Berlin, Springer-Verlag, 1993. P. 95 – 102.
4. Briggs M. An Introduction to the General Number Field Sieve. *Master's Thesis, Virginia Polytechnic Institute and State University*. 1998. P. 1 – 84.
5. Семенов В.Ю. Метод нахождения всех корней системы нелинейных алгебраических уравнений, основанный на операторе Кравчика. *Кибернетика и системный анализ.* 2015. № 5. С. 169 – 175.

Получено 12.03.2019

Об авторе:

Семенов Василий Юрьевич,
кандидат физико-математических наук,
докторант Института кибернетики имени В.М. Глушкова НАН Украины.
E-mail: vasyl.delta@gmail.com