УДК 519.61
doi: 10.26583/bit.2024.2.04

Юрий Л. Зачёсов[1], Игорь М. Ядыкин[2]
[1]Независимый эксперт
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
*[1]e-mail: y_zaches@mail.ru, https://orcid.org/*0000-0002-5724-7640
[2]e-mail: IMYadykin@mephi.ru, https://orcid.org/0000-0003-3952-5288

АЛГОРИТМ ПОЛУЧЕНИЯ ИНВАРИАНТОВ

Аннотация. Для защиты информации часто используются две криптографических парадигмы: хэш-функции и алгоритмы, стойкость которых основана на сложности задачи факторизации. При этом хэш-функции обеспечивают стойкость разовых ключей, а алгоритмы, требующие для своего дешифрования решения задачи факторизации, долговременные ключи. Лучшие алгоритмы, решающие задачу факторизации, это субэкспоненциальные алгоритмы, которые для своего выполнения требуют много ресурсов. С 1994 г. часто обсуждается квантовый алгоритм Питера Шора, который также требует для решения большие ресурсы из-за сложностей связанных с новой техникой. Известно, что наиболее стойкий модуль факторизации состоит из двух множителей $N = pq$. Поэтому актуален любой подход, позволяющий снизить объём ресурсов для решения задач такого рода. В статье описан и, по возможности, строго доказан алгоритм получения инвариантных систем многочленов, взаимно-однозначно соответствующих элементам приведённой системы вычетов (ПСВ). Алгебраические структуры, получаемые на выходе алгоритма, в случае удачного решения с их помощью задачи выбора, приводят к полиномиальному методу факторизации. Алгоритм развивает некоторые идеи, связанные с решением задачи «короткой экспоненты», Д. Копперсмита и других авторов. Излагаемый материал относится к первой подзадаче динамической системы (ДС), которая состоит в том, что исходная задача включается в семейство подзадач разного размера, и они решаются одна за другой в правильном порядке. Для получения систем инвариантных уравнений применяется аппарат полиномиальных сравнений и LLL-алгоритм. Доказывается, что с помощью алгоритма всегда можно получать необходимое число многочленов. Предполагается, что алгоритм будет выполняться несколько раз с различными небольшими простыми числами R, в качестве управляющих входных параметров. Выполнение алгоритма позволит подготовить возмущающие входные данные для подзадачи выбора, описание которой выходит за рамки статьи. Подзадача выбора наведёт соответствие между элементом множества множеств многочленов и элементом ПСВ, который фактически является остатком s от деления простого числа на управляющий параметр R в формуле замены переменных $p = 2R(x + y) + s$. Без наличия инвариантных многочленов взаимно-однозначно связанных с ПСВ такая подзадача была бы в принципе невозможна. Набрав достаточное количество пар $\{R, s\}$, применив аппарат китайской теоремы об остатках, найдём множители числа, состоящего из двух множителей. В статье предлагается описание первого этапа ДС, который заменит алгоритм факторизации, зависящий от разрядности составного числа, на новый алгоритм, который будет иметь другие входные данные, меньшей, чем составное число разрядности.

Ключевые слова: алгебраические инварианты, алгоритм факторизации, короткая экспонента, сравнения, китайская теорема об остатках, динамическая система.
Для цитирования: ЗАЧЁСОВ, Юрий Л.; ЯДЫКИН, Игорь М. АЛГОРИТМ ПОЛУЧЕНИЯ ИНВАРИАНТОВ. Безопасность информационных технологий, [S.l.], т. 31, № 2, с. 65–80, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1634. DOI: http://dx.doi.org/10.26583/bit.2024.2.04.

Yurii L. Zachesov[1], Igor M. Yadykin[2]
[1]Independent expert, Russia

[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
*[1]e-mail: y_zaches@mail.ru, https://orcid.org/*0000-0002-5724-7640
[2]e-mail: IMYadykin@mephi.ru, https://orcid.org/0000-0003-3952-5288

Algorithm obtaining invariants

Abstract. For protect information are often used two cryptographic paradigms: a cache functions and algorithms are based on the factorization problem. A cache function ensures the durability of one-time keys and algorithms support long-keys. The best exponential factorization algorithms, including known in 1994 Peter Shor's quantum algorithm, require a lot of resources to perform them. It is known that the most stable factorization model consists of two primes $N = pq$. Any approach to reduce the amount of resources to solve these problems is relevant. The article describes and, if possible, strictly proves the algorithm for obtaining invariant systems of polynomials corresponding to the elements of the reduced deduction system. Invariants algebraic structures, obtained at the output of the algorithm, in the case of solving with their help the selection problem, lead to a polynomial factorization method. The method develops some Coppersmit's and other authors ideas. This is the first subtask of a dynamic system which is that the original subtask is included in a family of subtasks of different size and they are solved one after the other in the correct order. To obtain a system of invariant equations, the polynomial comparison apparatus and the LLL-algorithm are used. It is proved that with the help of the algorithm you can always get the required number of polynomials. It is assumed that the algorithm will be executed several times with different small prime numbers R as control input parameters. The execution of the algorithm will allow you to prepare perturbing input data for submitting a selection, the description of which is beyond the scope of the article. The selection subtask will make a correspondence between the element of the set of polynomials sets and the reduced deduction system. The element of the reduced deduction system s is the remainder of dividing a prime by the parameter algorithm R of the variable replacement formula $p = 2R(x + y) + s$. Without the presence of invariant polynomials, mutually unambiguously related to the reduced deduction system, that problem would have been impossible in principle. Having typed a sufficient number of pairs $\{R, s\}$, using the Chinese-style theorem on residues, find the factors of a number consisting of two factors. The reader is offered a description of the first stage of the dynamic system that will replace a factorization algorithm, depending on the bit depth of the composite number, with the new algorithm, that will have other input data less than the composite bit number size.
Keywords: algebraic invariants, factorization algorithm, short exhibitor, comparisons, the Chinese residue theorem, dynamic system.
For citation: ZACHESOV, Yurii L.; YADYKIN, Igor M. Algorithm obtaining invariants. IT Security (Russia), [S.l.], v. 31, no. 2, p. 65–80, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1634. DOI: http://dx.doi.org/10.26583/bit.2024.2.04.

Введение

Хотя теория чисел и является одним из древнейших разделов математики, именно задача разложения чисел на простые множители стимулировала в последние десятилетия ее развитие. В течение ряда последних лет принципиально новых идей в задаче факторизации не появляется. Все последние исследования сосредоточены в рамках «классической» концепции метода «прообразов»: уравнение, требующее решения, «вкладывается» в больший математический объект. При этом удается построить линейную систему уравнений, множество неизвестных которой содержит и искомые параметры. «Борьба» ведется вокруг вопросов эффективности реализации алгоритмов на конкретной вычислительной базе, разработки новых вычислительных устройств [1]. Все чаще и чаще теоретические исследования переходят в плоскость практической реализации ранее разработанных алгоритмов.

Трудоемкость известных методов факторизации зависит от разрядности составного числа. Лучшим переборным субэкспоненциальным алгоритмом просеивания является

метод, который называется решетом числового поля (NFS – Number Field Sieve). Два последних рекорда установлены в 2009 г. с помощью этого метода факторизация 768-битового числа была выполнена с трудоёмкостью ~1.4 10^{20} операций[1] и в 2019 г. тем же методом – факторизация 795-битового числа была выполнена с трудоёмкостью 4000 ядро-лет. В настоящее время публикации на эту тему отсутствуют.

Существует много алгоритмов [2], которые используют математические принципы, основанные на трудности разложения больших чисел на их простые множители. Алгоритм RSA (Rivest-Shamir-Adleman) [3] один из самых популярных и широко используемых алгоритмов шифрования и цифровой подписи. Алгоритм Rabin Cryptosystem [4] разработан на основе работы Майкла Рабина, имеет несколько преимуществ перед RSA, но тот же тип безопасности. Алгоритм шифрования EIGamal основан на сложности дискретного логарифмирования, однако его безопасность также может быть связана с трудностью факторизации чисел в его конкретной реализации. Алгоритм Blum-Blum-Shub (BBS) [5] использует псевдослучайные последовательности, генерируемые на основе операций в кольце вычетов по модулю составного числа, которое является произведением двух больших простых чисел. Его безопасность также основана на сложности факторизации. Алгоритм Goldwasser-Micali Cryptosystem отличается тем, что обеспечивает прямую защиту от атаки подбором по алгоритму, основанному на факторизации, что делает его более устойчивым к атакам. Стойкость всех этих алгоритмов держится на том, что в настоящее время решение задачи факторизации либо требует большого количества ресурсов: временных; аппаратных и других, либо для некоторых входных данных вообще не имеет решения.

С 1996 г. известен метод факторизации с облегчающими условиями. Так называемый метод «короткой экспоненты», основанный на идеях Д. Копперсмита и других авторов [6–10], применяется для поиска небольших корней уравнений, левая часть которых является многочленом. Имеет полиномиальную трудоёмкость, зависящую от разрядности модуля факторизации и структуры ключевой информации. Копперсмит также показал, что модуль, состоящий из двух простых множителей, может быть факторизован за полиномиальное время, если известна половина битов одного из множителей [11].

Не теряя общности, приведем формальное описание, сопутствующее «методу Копперсмита» для сравнения с двумя переменными.

Для фиксированного полинома $P(x,y) \in \mathbb{Z}[x,y]$ и ограничений $X, Y, W \in \mathbb{N}$ найти все целые решения сравнения $P(x,y) \equiv 0 (\mathrm{mod}\, W)$, которые удовлетворяют неравенствам $|x| < X$ и $|y| < Y$. В общем случае это трудно решаемая задача. Метод Копперсмита хорошо работает, если $X, Y \ll W$.

Сначала выбирается целое число $h \geq 2$ и рассматривается множество L многочленов $\mathrm{g}(x,y) \in \mathbb{Z}[x,y]$ удовлетворяющих условию $\forall\, x,y \in \mathbb{Z}\,[F(x,y) \equiv 0 (\mathrm{mod}\, W) \Rightarrow \mathrm{g}(x,y) \equiv 0 (\mathrm{mod}\, W^h)]$. Можно говорить, что из элементов L формируется решётка, состоящая из коэффициентов многочленов, так как $\mathrm{g}_1, \mathrm{g}_2 \in L \Rightarrow \mathrm{g}_1 - \mathrm{g}_2 \in L$.

Затем, находится многочлен $\mathrm{g}(x,y) \in L$ удовлетворяющий условию $\forall\, x,y \in \mathbb{Z}, |x| < X, |y| < Y, [\mathrm{g}(x,y) \equiv 0 (\mathrm{mod}\, W^h) \Rightarrow \mathrm{g}(x,y) = 0]$.

Предположим, что два независимых многочлена найдены, тогда решение исходного сравнения сводится к решению системы из двух уравнений с целыми или рациональными коэффициентами, например, методом результантов.

[1]Информационное сообщение о рекордных факторизациях различных модулей RSA. URL: http://www.crypto-world.com/FactorRecords.htm (дата обращения: 10.04.2024).

Для некоторых методов заполнения последние уравнения в решётке L имеют коэффициенты с небольшим значением. Надо построить решётку L и найти такие элементы для коэффициентов многочленов в ней. Для выполнения этого существует много алгоритмов, например, широко используется LLL-алгоритм [12]. Большинство других алгоритмов разработано для Евклидовых векторных пространств $\mathbb{R}^n$ со стандартными нормами. В случае их использования нужно преобразовывать целочисленную решётку.

Один из возможных алгоритмов преобразования коэффициентов многочлена $P(x,y) = \sum_{i,j} a_{ij} x^i y^j$ и параметров X и Y в вектор решётки определяется следующей формулой $\mathcal{V}(F;X,Y) = (a_{00}, a_{10}X, \dots, a_{i_w j_w} X^{i_w} Y^{j_w})$. Между ненулевыми мономами многочлена и элементами вектора устанавливается взаимно-однозначное соответствие.

Обычно алгоритм применяется в случае ослабленных ключей, а для получения многочлена из модуля, состоящего из двух простых множителей, используется техника $N = (P + x)(Q + y)$, которая даёт только многочлен второй степени с максимальным мономом xy.

Метод Д. Копперсмита был модифицирован в [13, 14] с целью расширения границ его применения. Модификация заключалась в том, что, в отличие от метода Д. Копперсмита, который использовал коэффициенты одного многочлена для заполнения одной входной LLL-матрицы, вырабатывались несколько многочленов $P(x,y)$, из которых только один по условию задачи приводил к результату. Благодаря такому приёму, в отличие от метода Д. Копперсмита, в котором правая часть уравнения $\mathrm{g}(x,y) = 0$ всегда равна нулю, на последнем этапе модифицированного метода допускалось, чтобы правая часть уравнения была небольшим числом. Далее задача решалась перебором этого числа. Новый подход обеспечивал получение многочленов $P(x,y)$, любой степени, а не только второй, как у Д. Копперсмита. Причём, каждый многочлен взаимно-однозначно связан с элементом приведённой системы вычетов (ПСВ). Первоначально модифицированный метод использовался для решения задачи «короткая экспонента».

Исследования показали, что трудоёмкость модифицированного метода**,** в случае решения систем уравнений зависит от алгебраических свойств уравнений, появляющихся на его последнем шаге, а именно от диапазона возможных значений правой части этих уравнений ($\sim 10^{75}$ при модуле N размером в 512 битов) или значений свободных членов многочленов.

Полученные результаты привели к выводу возможности замены методов факторизации, зависящих от разрядности составного числа, на новый метод, который будет иметь другие входные данные, меньшей, чем составное число разрядности. Алгоритм получения алгебраических инвариантов это первая подзадача динамической системы (ДС) – множество элементов, для которого задана функциональная зависимость между временем и положением в пространстве каждого элемента системы. Данная математическая абстракция позволяет изучать и описывать эволюцию системы во времени. Состояние ДС в любой момент времени описывается множеством вещественных чисел (или векторов), соответствующих определённой точке в пространстве состояний. Эволюция ДС определяется детерминированной функцией, то есть через заданный интервал времени система примет конкретное состояние, зависящее от текущего состояния. Пространство системы – совокупность всех допустимых состояний ДС. Таким образом, ДС характеризуется своим начальным состоянием и законом, по которому система переходит из начального состояния в приведённое состояние и наоборот. Начальное состояние как раз и характеризуется алгебраическими инвариантами.

В основе построения алгебраических инвариантов лежит модифицированный метод «короткой экспоненты», который отличается от своего предка лишь тем, что вместо последнего этапа – решения систем уравнений вида $g(x,y)=0$, из множества тех же функций $g(x,y)$, строятся функции с одной переменной $f(x)$, собственно они и являются алгебраическими инвариантами, вынесенными в заголовок статьи. Возможный способ использования инвариантов состоит в том, что путём выбора из множества алгебраических инвариантов «подходящего» определяется «правильный», однозначно с ним связанный, остаток. Затем повторяем процедуру алгоритма для других входных параметров, меняя небольшое простое число, набираем необходимое количество остатков, составляем новые сравнения и решаем их с помощью аппарата китайской теоремы об остатках.

В силу субэкспоненциальности метода NFS можно говорить, что для своего выполнения он требует применения суперкомпьютера. В статье развиваются методы, которые будут выполняться быстро, с конечной целью – создание полиномиального алгоритма факторизации не требующего для своего выполнения больших вычислительных ресурсов. Далее следует описание математического аппарата алгоритма, лежащего в основе построения алгебраических инвариантов.

1. Способ построения многочлена $P(x,y)$ левой части сравнения

Дано большое целое число $N=pq$, (1)

у которого неизвестные: p–наименьший простой делитель, q–большое простое число. Будем предполагать, что

$$a_1 < \frac{q}{p} < a_2, \tag{2}$$

где $1 \le a_1 < a_2$, a_1, a_2 – рациональные числа.

Из (1) имеем оценки $\sqrt{\frac{N}{a_2}} < p < \sqrt{\frac{N}{a_1}}$. Найдём однозначно нечётные числа

$$2h+1 \in \{\left\lceil\sqrt{\frac{N}{a_2}}\right\rceil, \left\lfloor\sqrt{\frac{N}{a_2}}\right\rfloor + 1\},\ 2h+1+2X \in \{\left\lfloor\sqrt{\frac{N}{a_1}}\right\rfloor - 1, \left\lfloor\sqrt{\frac{N}{a_1}}\right\rfloor\}.$$

Тогда неравенства (2) равносильны неравенствам

$$2h+1 \le p \le 2h+1+2X. \tag{3}$$

Пусть a, k – натуральные числа, r – целое неотрицательное число. При $r \ge 1$ числа $b_1, \dots, b_r$ – целые, $b_r \ne 0$; число $b_0 = 0$, если среди чисел a, $b_1, \dots, b_r$ чётное число нечётных чисел, иначе $b_0 = 1$. При $r = 0$ a – нечётное, $b_0 = 1$. При таком выборе параметров $a, k, r, b_0, \dots, b_r$ при некотором целом z верно равенство

$$aq^k = \sum_{i=0}^{r} b_i p^i + 2z \tag{4}$$

и так как (1), то

$$aN^k = \sum_{i=0}^{r} b_i p^{i+k} + 2z\,p^k, \tag{5}$$

где переменное значение функции $z = z(p) = \frac{1}{2}\left(aN^k p^{-k} - \sum_{i=0}^{r} b_i p^i\right)$ и её производная $z'(p) = \frac{1}{2}(-aN^k k p^{-k-1} - \sum_{i=0}^{r} b_i i p^{i-1})$.

Простое наблюдение показывает, что произведение двух нечётных чисел нечётно, произведение двух чётных чисел чётно и произведение нечётного и чётного чисел чётно. Сумма нечётных чисел чётна, сумма чётных чисел чётна и сумма чётного и нечётного числа нечётна. Эти аксиомы арифметики и то, что q и p априори нечётные простые числа, используется при составлении формулы (4).

Во время экспериментов параметры $a,\ b_1, \dots, b_r$ выбираются случайным равновероятным способом. Все равновероятные случайные величины брались из положительного целочисленного диапазона от 0 до k, где k – небольшое натуральное число. За счёт $a,\ b_1, \dots, b_r, k$, даже при одном и том же модуле факторизации получаются различные сравнения, однозначно соответствующие ПСВ, о которой скажем чуть позже.

Указав интервалы знакопостоянства производной $z'(p)$ на отрезке $[2h+1, 2h+1+2X]$, найдём целые границы для z такие, что $z_0 \le z \le z_1$. В частности, если $b_0, \dots, b_r$ – неотрицательные числа, то с расширением интервала возможных значений $z(p)$:

$$z_0 = \lfloor z(2h+1+2X) \rfloor \le z \le \lceil z(2h+1) \rceil = z_1. \quad (6)$$

Пусть $2 = \pi_0 < \pi_1 < \dots < \pi_m$ – произвольные маленькие простые числа. Положим

$$R = \prod_{i=\varsigma}^{m} \pi_i, \text{ где } 1 \le \varsigma \le m \quad (7)$$

и целочисленную замену переменных

$$p = 2R(\overline{x} + \overline{x}_0) + \overline{s}, \quad (8)$$

где $\overline{s} = 2\overline{c} + 1$ (при $\overline{c} \in \{1,2\}, \overline{s} \in \{3,5\}$, максимальное значение $\overline{c}$ – число различных уравнений (9)), НОД$(\overline{s}, R)$=1, элементы ПСВ $\overline{s} \in \{1, \dots, R-1\}$, $\overline{t} \in \{1, \dots, R-1\}$, переменные $z = R(\overline{y} + \overline{y}_0) + \overline{t}$, $\overline{x}_0 = x_0(\overline{s}) = \left\lceil \frac{h-\overline{c}}{R} \right\rceil$, $\overline{y}_0 = \left\lceil \frac{z_0-\overline{t}}{R} \right\rceil$. Если $\overline{x}, \overline{s}, \overline{t}$–значения, соответствующие целым $\overline{x_0}$, $\overline{y_0}$, тогда $0 \le \overline{x} \le \left\lceil \frac{h+X-\overline{c}}{R} \right\rceil - \left\lceil \frac{h-\overline{c}}{R} \right\rceil = A_1 = A_1(\overline{s})$, $0 \le \overline{y} \le \left\lceil \frac{z_1-\overline{t}}{R} \right\rceil - \left\lceil \frac{z_0-\overline{t}}{R} \right\rceil = A_2 = A_2(\overline{s})$. При большом значении X числа A_1, A_2 тоже велики.

Таким образом, формула (8) замены переменной служит для введения связи между неизвестным простым множителем p, выбранным небольшим простым числом R и остатком от их деления $\overline{s}$. Понятно, что при такой замене остатки $\overline{s}$ образуют систему вычетов, связанную с выбранным простым числом R, и только один элемент этой системы будет соответствовать «подходящему» значению p. Поэтому переменные в этой формуле обозначены сверху черточками. Задавая различные параметры $a,\ k,\ r,\ b_0, \dots, b_r$ и R будем получать множество многочленов, в которых одно значение переменных $\overline{x}$, $\overline{x}_0$, $\overline{y}$, $\overline{y}_0$ и $\overline{s}$ соответствует «подходящему» значению p, а все остальные относятся к случаю, когда хотя бы одно из чисел $\overline{x}_0$, $\overline{y}_0$ рациональное.

После замены переменных равенство (5) равносильно равенствам:

$$\sum_{i=0}^{r} b_i \left(2R\overline{x} + 2R\overline{x}_0 + \overline{s}\right)^{i+k} + 2\left(R\overline{y} + R\overline{y}_0 + \overline{t}\right)\left(2R\overline{x} + 2R\overline{x}_0 + \overline{s}\right)^k - aN^k = 0,$$

$$\sum_{i=0}^{r} b_i \left(\sum_{j=1}^{i+k} C_{i+k}^{j} (2R)^j (2R\overline{x}_0 + \overline{s})^{i+k-j} \overline{x}^j + (2R\overline{x}_0 + \overline{s})^{i+k} \right) +$$

$$+\left(2R\overline{y} + 2R\overline{y}_0 + 2\overline{t}\right)\left(\sum_{j=1}^{k} C_k^j (2R)^j (2R\overline{x}_0 + \overline{s})^{k-j} \overline{x}^j + (2R\overline{x}_0 + \overline{s})^k \right) - aN^k = 0. \quad (9)$$

Выберем теперь произвольное значение $s \in \{1, \dots, R-1\}$, $s = 2c + 1$, НОД(s, R)=1, вычислим $x_0 = x_0(s) = \left\lceil \frac{h-c}{R} \right\rceil$, выберем некоторое $t \in \{0,1, \dots, R-1\}$ и положим $y_0 = \left\lceil \frac{z_0-t}{R} \right\rceil$, $2Rx_0 + s \ge 2R\frac{h-c}{R} + s = 2h + 1$.

Потребуем выполнения равенства (9), в котором убраны все чёрточки над переменными (т.е. переменные принимают значения, которые соответствуют «подходящему» значению p), и запишем это равенство в следующем виде:

$$2R\sum_{i=1}^{r+k}\alpha_i x^i + 2Ry\sum_{i=0}^{k}\beta_i x^i - \mathrm{g} = 0, \quad (10)$$

где $\mathrm{g} = aN^k - \sum_{i=0}^{r} b_i(2Rx_0+s)^{i+k} - 2Ry_0(2Rx_0+s)^k - 2t(2Rx_0+s)^k$,

$\alpha_i = \sum_{i=\max(0,j-k)}^{r} b_i C_{i+k}^{j}(2R)^{j-1}(2Rx_0+s)^{i+k-j} + \mathrm{Ind}(1\le j\le k)(2Ry_0 + 2t)C_k^j(2R)^{j-1}(2Rx_0+s)^{k-j}$, $\beta_i = C_k^j(2R)^j(2Rx_0+s)^{k-j}$.

Заметим, что $\alpha_{r+k} = b_r(2R)^{r+k-1} \neq 0$, $\beta_i \geq C_k^j(2R)^j(2h+1)^{k-j}$ для j=1,…,k. Разделив (10) на 2R, получим равенство

$$\sum_{j=1}^{r+k}\alpha_j x^j + y\sum_{j=0}^{k}\beta_j x^j - \overline{\mathrm{g}} = 0, \quad (11)$$

где $\overline{\mathrm{g}} = \frac{\overline{n}-t(2Rx_0+s)^k}{R} - y_0(2Rx_0+s)^k$, $\overline{n} = \frac{aN^k-\sum_{i=0}^{r} b_i(2Rx_0+s)^{i+k}}{2}$ – целые числа. Этот факт можно использовать для проверки правильности построения многочлена.

Отсюда t находится однозначно. Действительно, так как $\mathrm{НОД}(R, 2Rx_0+s) = 1$, то существует единственное число $f \in \{1,\dots,R-1\}$ такое, что $f(2Rx_0+s)^k \equiv 1 (\mathrm{mod}\, R)$ ([15], с. 47). Следовательно, $\overline{n} \equiv t(2Rx_0+s)^k (\mathrm{mod}\, R)$, $f\overline{n} \equiv t (\mathrm{mod}\, R)$ и так как $t \in \{1,\dots,R-1\}$, то $t = \mathrm{ост}(f\overline{n},\ R)$.

Опробуя $n_0 = \prod_{i=0}^{m}(\pi_i - 1)$ возможных значений s (из (8)) и находя при каждом таком s единственное t, получим n_0 равенств (11), одно из которых (при s=$\overline{s}$, t=$\overline{t}$) имеет в качестве корня неизвестное простое число p из (1).

П р и м е ч а н и е: дальше в практических случаях будем полагать m=1 (из (7)) и ставить в соответствие набору уравнений разные простые числа π_i (отличные от двойки). В этом случае число равенств будет $n_0 = \pi_i - 1$.

Пусть w – натуральное число. При $r \geq 2$ из равенства (11) следует сравнение степени r+k:

$$P(x,y) = x^{r+k} + \sum_{i=0}^{r+k-1}\gamma_i x^i + y\sum_{i=0}^{k}\delta_i x^i \equiv 0 (\mathrm{mod}\, M), \quad (12)$$

где $M = (2R)^{r+k-1}b_r w - 1$ новое значение модуля сравнения, $\gamma_0 \equiv (-\overline{\mathrm{g}}w)(\mathrm{mod}\, M)$, $\gamma_i \equiv \alpha_i w (\mathrm{mod}\, M)$; для i=1,…,r+k–1, $\delta_i \equiv \beta_i w (\mathrm{mod}\, M)$, для i=1,…,k, $w = \left\lfloor \frac{M_0}{2R}\cdot W_0 \right\rfloor$, $M_0 = 1 + (4^{-(\frac{2}{3}-\frac{1}{T+1})*(T-1)} * \sqrt{\tau} * \alpha^{\frac{\tau-1}{4}} * (\mathrm{A}_1 * \mathrm{A}_2)^{(\frac{T-1}{3})})^{\frac{\tau}{\sigma}}$, $T, \tau, \alpha, \sigma, W_0$ – параметры алгоритма.

При $r \in \{0,1\}$ из (12) следует сравнение степени k+1:

$$P(x,y) = y\sum_{i=0}^{k}\delta_i x^i + \sum_{i=0}^{k+r}\gamma_i x^i \equiv 0 (\mathrm{mod}\, M), \quad (13)$$

где $M = (2R)^k w - 1$, $\gamma_0 \equiv (-\overline{\mathrm{g}}w)(\mathrm{mod}\, M)$, $\delta_i \equiv \beta_i w (\mathrm{mod}\, M)$ для i=1,…,k, $\delta_k = 1$, $\gamma_i \equiv \alpha_i w (\mathrm{mod}\, M)$ для i=1,…,k+r. Параметр w позволяет выбирать сколь угодно большие значения M. При этом каждое, построенное таким образом сравнение, соответствует строго одному элементу ПСВ.

Сравнения (12 (13)) имеют решение, которые можно найти среди всех целых решений $x \in [0, A_1]$, $y \in [0, A_2]$, если выбраны подходящие значения переменных $\overline{s}, \overline{t}$.

П р и м е ч а н и е: в ряде работ предлагалось задачу факторизации (1) сводить к решению квадратичного сравнения $xy + ax + by + c \equiv 0 (\mathrm{mod}\, M)$. Достигалось это за счёт опробования младших или старших бит в двоичном представлении множителя p [16].

Здесь предлагается вместо опробования бит в p использовать представление (8). Этот способ более экономичный, чем опробование бит в p. Кроме того мы рассматриваем сравнения (12 (13)) не только второй степени [7, 11] и по любому значению модуля.

2. Получение инвариантных функций с одной переменной

Пусть натуральное число $T-1 \geq \overline{k} = k + \max(r, 1)$, тогда можно по сравнению (12 (13)) при условии $0 \leq x \leq A_1$, $0 \leq y \leq A_2$ построить $\tau = \frac{T(T+1)}{2}$ целочисленных многочленов $Q_i(x, y)$ степени не выше $T-1$ по каждой переменной таких, что

$$Q_i(\overline{x}, \overline{y}) = j_i M^{\psi}, \tag{14}$$

где $i=1,\ldots,\tau$ при некотором j_i и целом неотрицательном параметре ψ, если выбраны «подходящие» $\overline{s}, \overline{t}$ уравнение превращается в тождество.

Из (11) имеем:

$$y = \varphi(x) = \frac{\overline{\mathrm{g}} - \sum_{j=1}^{r+k} \alpha_j x^j}{\sum_{j=0}^{k} \beta_j x^j}. \tag{15}$$

Следовательно, если выбраны «подходящие» значения $\overline{s}, \overline{t}$, то $Q_i(\overline{x}, \varphi(\overline{x})) = j_i M^{\psi}$, $i=1,\ldots,\tau$.

Таким образом, достаточно при каждом из n_0 значений s найти целые решения из $[0, A_1]$ $(A_1 = A_1(s))$ одного из уравнений или каким-то образом оценить системы уравнений (14) на предмет возможного наличия у них больших простых корней.

$$F_i(x) = Q_i(x, \varphi(x)) = \frac{f_i(x)}{g_i(x)} = j_i M^{\psi} \tag{16}$$

при $j_i \in \{min_i, \ldots, max_i\}$ (всего $H_i = max_i - min_i + 1$ уравнений (16)), где $min_i = \left\lceil M^{-\psi} \min\limits_{0 \leq x \leq A_1} F_i(x) \right\rceil$, $max_i = [M^{-\psi} \max\limits_{0 \leq x \leq A_1} F_i(x)]$, $i=1,\ldots,\tau$.

Так как $Q_i(x, y) = \sum_{\mu=0}^{T-1} \sum_{\vartheta=0}^{\mu} q_{i\mu\vartheta} x^{\vartheta} y^{\mu-\vartheta}$ и $\sum_{j=0}^{k} \beta_j x^j > 0$ при $x \geq 0$, то уравнение (16) равносильно уравнению

$$f_i(x) = \sum_{\mu=0}^{T-1} \sum_{\vartheta=0}^{\mu} q_{i\mu\vartheta} x^{\vartheta} \left(\overline{\mathrm{g}} - \sum_{j=1}^{r+k} \alpha_j x^j \right)^{\mu-\vartheta} \left(\sum_{j=0}^{k} \beta_j x^j \right)^{T-1-(\mu-\vartheta)} =$$
$$= \sum_{\mu=0}^{T-1} \sum_{\vartheta=0}^{\mu} q_{i\mu\vartheta} \sum_{t=0}^{d} L_{t,\mu\vartheta} x^t = j \left(\sum_{t=0}^{k} \beta_i x^t \right)^{T-1} M^{\psi}, \tag{17}$$

где $L_{d(\mu,\vartheta),\mu\vartheta} = (-\alpha_{r+k})^{\mu-\vartheta} \beta_k^{T-1-(\mu-\vartheta)} \neq 0$,

$d(\mu, \vartheta) = \vartheta + (r+k)(\mu-\vartheta) + k\big(T-1-(\mu-\vartheta)\big) = k(T-1) + \mu r - \vartheta(r-1)$,

$L_{\vartheta,\mu\vartheta} = \overline{\mathrm{g}}^{\mu-\vartheta} \beta_k^{T-1-(\mu-\vartheta)}$, $L_{t,\mu\vartheta} = 0$, если $t \notin [\vartheta, d(\mu, \vartheta)]$.

Степень целочисленного многочлена $f_i(x)$ не превосходит $d = \max\limits_{0 \leq \mu \leq T-1} \max\limits_{0 \leq \vartheta \leq \mu} d(\mu, \vartheta)$.

Если $r \geq 1$, то $d = \max\limits_{0 \leq \mu \leq T-1} (k(T-1) + \mu r) = (T-1)(k+r)$. Если $r = 0$, то $d = \max\limits_{0 \leq \mu \leq T-1} \max\limits_{0 \leq \vartheta \leq \mu} (k(T-1) + \vartheta) = \max\limits_{0 \leq \mu \leq T-1} (k(T-1) + \mu) = (T-1)(k+1)$.

Таким образом, $d = (T-1)\overline{k}$. Отсюда следует, что при задании параметров алгоритма T, r и k необходимо соблюдать выполнение неравенств $r+k \leq T-1$, если $r=0$, то $k+1 \leq T-1$. Иначе в матрице, подаваемой на вход LLL-алгоритму, будет не хватать информационных столбцов.

Уравнения (16) разнятся оценками H_i. Среди всех $f_i(x)$, $i = 1, \ldots, \tau$, не равных тождественно константе, найдём то, для которого H_i минимально, а при равных значениях H_i выберем $f_i(x)$ с минимальной степенью.

Пусть любыми методами из набора (см. [7, 8, 16] и приводимую в них литературу): методом «максимальный перпендикуляр» (ММП), методом «минимальный вектор» (ММВ), при произвольных коэффициентах уравнения (11) и произвольных параметрах a и $b_0, \ldots, b_r$, k, r, T, $\tau = \frac{T(T+1)}{2}$) построены функции – несократимые дроби:

$$F_i(x) = \frac{f_i(x)}{(2Rx+2Rx_0+s)^{\gamma_i}}, \qquad i=1,\ldots,\Omega, \tag{18}$$

где натуральный показатель $\gamma_i \geq 1$, $\overline{f}_i(x) = \sum_{t=0}^{d_i} C_{it}x^t$ – целочисленный многочлен степени $d_i \geq 0$, $C_{it} \neq 0$, параметр Ω определяет количество неконстантных и несократимых дробей (то есть $\overline{f}_i(x)$, $0 \leq d_i \leq d = \overline{k}(T-1)$, $C_{id_i} \neq 0$, не делится на $2Rx + 2Rx_0 + s$).

П р и м е ч а н и е: ММП, ММВ – альтернативные способы заполнения решётки перед LLL-алгоритмом в методе Д. Копперсмита. В [13] было экспериментально доказано, что ММП лучше в сравнении с ММВ без редукции и с редукцией.

Заменой переменной $z=2Rx+2Rx_0+s$ можно перейти от уравнения (18) к системе уравнений

$$\overline{F}_i(z) = \frac{\overline{f}_i(z)}{z^{\gamma_i}}. \tag{19}$$

Из эксперимента известно, что

$$\overline{F}_i(z) = \overline{j}_i M^{\psi} \tag{20}$$

при некотором целом $\overline{j}_i$.

Полагая $2h+1 \leq z \leq 2h+1+2X$, $x = \frac{z-2Rx_0-s}{2R} = \frac{z-s}{2R} - x_0$, $0 \leq x \leq \left[\frac{h-c+X}{R}\right] - \left[\frac{h-c}{R}\right]$ преобразуем функцию из системы (19) по следующему правилу

$$\overline{F}_i(x) = \frac{\overline{f}_i\left(\frac{z-2Rx_0-s}{2R}\right)}{z^{\gamma_i}} = z^{\gamma_i}\sum_{t=0}^{d_i} C_{it}\,(z-2Rx_0-s)^t(2R)^t,$$

$$(2R)^{d_i}z^{\gamma_i}\overline{F}_i(x) = \sum_{t=0}^{d_i} C_{it}\,(2R)^{d_i-t}\sum_{j=0}^{t} C_t^j(-2Rx_0-s)^{t-j}z^j = \sum_{j=0}^{d_i} z^j A_{ij},$$

где $A_{ij} = \sum_{j=0}^{t} C_t^j(-2Rx_0-s)^{t-j}(2R)^{d_i-t}\,C_{it}$.

Производная от функции $\overline{F}'_i(z) = 0$ при $2R\min(x) + 2Rx_0 + s \leq z \leq 2R\max(x) + 2Rx_0 + s$. Так как при $x = \overline{x}$, $x_0 = \overline{x}_0$, $s = \overline{s}$ имеем $z = p$ (неизвестный множитель модуля факторизации), то

$$\sum_{j=0}^{d_i} p^j A_{ij} = \overline{j_i}(2R)^{d_i}p^{\gamma_i}, \tag{21}$$

при некотором целом $\overline{j_i}$ значение функции $\overline{F}_i(x)$.

Тогда

$$\sum_{j=0}^{\gamma_i-1} p^{j-\gamma_i}A_{ij} \tag{22}$$

целое число, т.е. $\sum_{j=0}^{\gamma_i-1} p^{j-\gamma_i}A_{ij} = \vartheta_i$, $\vartheta_i \in \{min_i, \ldots, max_i\}$, где

$$min_i = \left\lceil \min_{2h+1\leq p\leq 2h+1+2X} \sum_{j=0}^{\gamma_i-1} p^{j-\gamma_i}A_{ij} \right\rceil, \tag{23}$$

$$max_i = \left\lfloor \max_{2h+1\leq p\leq 2h+1+2X} \sum_{j=0}^{\gamma_i-1} p^{j-\gamma_i}A_{ij} \right\rfloor.$$

И система уравнений (14) и уравнение с одной переменной (20), если выбраны «подходящие» значения $\bar{s}$, $\bar{t}$ имеют одинаковые решения, связанные линейным соотношением.

Рассмотрим целочисленную линейную комбинацию равенств (12):

$$\sum_{i=0}^{h} \alpha_i \sum_{j=0}^{d_i} p^j A_{ij} = \sum_{i=0}^{h} \overline{j_i}(2R)^{d_i}p^{\gamma_i}. \tag{24}$$

Тогда $\sum_{i=0}^{h} \alpha_i \sum_{j=0}^{d_i} p^j A_{ij}$ – целое число, то есть $\sum_{i=0}^{h} \alpha_i \sum_{j=0}^{d_i} p^j A_{ij} = \vartheta$, $\vartheta \in \{min, \ldots, max\}$,

где $min = \left\lceil \min_{2h+1\leq p\leq 2h+1+2X} \sum_{j=0}^{\gamma_i-1} p^{j-\gamma_i}\left(\sum_{j=0}^{h} \alpha_i A_{ij}\right) \right\rceil$,

$$max = \left[\max_{2h+1 \le p \le 2h+1+2X} \sum_{j=0}^{\gamma_i - 1} p^{j-\gamma_i} \left(\sum_{j=0}^{h} \alpha_i A_{ij} \right) \right].$$

П р и м е ч а н и е: алгебраические инварианты алгоритма сведѐния повторяются для одинаковых наборов параметров и различных значений исследуемого модуля факторизации, то есть значение коэффициентов функций для различных значений N меняется, а форма функций и их места в выходном списке сохраняются.

У ММВ и ММВР столбцы матрицы B_0 соответствуют используемым мономам, а число строк зависит от параметра τ (у ММВР число строк меньше чем у ММВ). У ММП строки соответствуют мономам, а число столбцов равно τ.

Взаимосвязь получаемых мономов в сравнениях (12 (13)) и параметров метода для различных методов получения входной LLL-матрицы показана в табл. 1–3.

По основной теореме интервальной арифметики [17], если для таких функций $f(x)$ определён результат $\boldsymbol{f}(\boldsymbol{x})$ подстановки вместо аргументов интервалов их изменения $\boldsymbol{x} \in \mathbb{IR}$ по правилам интервальной арифметики, тогда $\{f(x) | x \in \boldsymbol{x}\} \subseteq \boldsymbol{f}(\boldsymbol{x})$.

Таблица 1. Возможные значения и месторасположение мономов с ММВ

T	Размер матрицы	Количество коэффициентов в многочлене и их мономы	r	k	№ строки[2]	Количество элементов в строке до главной диагонали
3	6x6	5 (1,x,y,xy, x^2)	1	1	5	4
4	10x10	7 (1,x,y,xy, x^2,x^2y, x^3)	1	2	8	7
5	15x15	8 (1,x,y,xy, x^2,x^2y, x^3, x^4)	2	2	11	10
6	21x21	10 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5)	2	3	16	15
7	28x28	11 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5, x^6)	3	3	22	21
11	66x66	17 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^4y, x^5, x^5y, x^6, x^7, x^8, x^9, x^{10})	5	5	56	55

Таблица 2. Возможные значения и месторасположение мономов с ММВР

T	Размер матрицы	Количество коэффициентов в многочлене и их мономы	r	k	№ строки	Количество элементов в строке до главной диагонали
3	5x5	5 (1,x,y,xy, x^2)	1	1	5	4
4	7x7	7 (1,x,y,xy, x^2,x^2y, x^3)	1	2	7	6
5	8x8	8 (1,x,y,xy, x^2,x^2y, x^3, x^4)	2	2	8	7
6	10x10	10 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5)	2	3	10	9
7	11x11	11 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5, x^6)	3	3	11	10
11	17x17	17 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^4y, x^5, x^5y, x^6, x^7, x^8, x^9, x^{10})	5	5	17	16

[2]Во всех матрицах только одна многозначная строка, кроме главной диагонали.

Таблица 3. Возможные значения и месторасположение мономов с ММП

T	Размер матрицы	Количество коэффициентов в многочлене и их мономы	r	k	Номер столбца[3] с наибольшими элементами
3	6x6	5 (1,x,y,xy, x^2)	1	1	5
4	10x10	7 (1,x,y,xy, x^2,x^2y, x^3)	1	2	8
5	15x15	8 (1,x,y,xy, x^2,x^2y, x^3, x^4)	2	2	11
6	21x21	10 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5)	2	3	16
7	28x28	11 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^5, x^6)	3	3	22
11	66x66	17 (1,x,y,xy, x^2,x^2y, x^3, x^3y, x^4, x^4y, x^5, x^5y, x^6, x^7, x^8, x^9, x^{10})	5	5	56

3. Оценка числа константных многочленов

Функцию $\overline{f}_i(x)$ представим так:

$$\overline{f}_i(x) = \sum_{t=0}^{d} x^t \sum_{\mu=0}^{T-1} \sum_{v=0}^{\mu} q_{i,\mu v} L_{t,\mu v} = \sum_{t=0}^{d} x^t (\mathbf{L}_t, \mathbf{q}_i), \qquad (25)$$

где $\mathbf{q}_i = \left(q_{i,00}, q_{i,10}, q_{i,11}, \dots, q_{i,T-1,0}, \dots, q_{i,T-1,T-1}\right)$,
$\mathbf{L}_t = \left(L_{t,00}, L_{t,10}, L_{t,11}, \dots, L_{t,T-1,0}, \dots, L_{t,T-1,T-1}\right)$ – τ-мерные векторы. Все числа $L_{t,\mu v}$ не зависят от $\mathbf{q}_i$ и могут быть вычислены до построения многочленов $Q_i(x, y)$ из уравнения (14).

Векторы $\mathbf{q}_1, \dots, \mathbf{q}_{\boldsymbol{\tau}}$ – линейно независимы, так как они получены применением LLL-алгоритма к τ линейно независимым τ-мерным векторам [11].

Вектор $\mathbf{L}_d$ ненулевой, так как из (25) следует при $r \geq 1$ неравенство $\mathbf{L}_{d,T-1,0} = (-\alpha_{r+k})^{T-1} \neq 0$, а при $r = 1$ неравенство $\mathbf{L}_{d,T-1,T-1} = \beta_k^{T-1} \neq 0$.

Исследуем, когда из уравнения (25) нельзя найти *x*. Это происходит в том случае, когда верно тождество

$$\sum_{t=0}^{d} x^t (\mathbf{L}_t, \mathbf{q}_i) = \theta\left(\sum_{t=0}^{k} \beta_t x^t\right)^{T-1} \qquad (26)$$

при некотором действительном числе θ. В этом случае уравнение (25) вырождается в равенство $\theta = j$.

Пусть $\sum_{t=0}^{k} (\beta_t x^t)^{T-1} = \sum_{t=0}^{k(T-1)} C_t x^t$. Тождество (26) верно тогда и только тогда, когда

$$(\mathbf{L}_t, \mathbf{q}_i) = \theta C_t,\ t = 0,1, \dots, k(T-1),\ (\mathbf{L}_t, \mathbf{q}_i) = 0,\ t = k(T-1)+1, \dots, d. \qquad (27)$$

Равенства (27) можно рассматривать как систему линейных уравнений с неизвестными $q_{i,00}, \dots, q_{i,T-1,T-1}$.

Исследуем случай θ=0. В этом случае равенства (27) могут выполняться, только если ранг d матрицы $L = \begin{pmatrix} L_0 \\ L_1 \\ \vdots \\ L_d \end{pmatrix}$ меньше τ ([18], п. 6.20, с. 44); $\overline{d} \geq 1$, так как L_d – ненулевой вектор. При этом количество различных векторов $\mathbf{q}_i$, удовлетворяющих (27) и ортогональных ко всем векторам $\mathbf{L}_i$, не превосходит $\tau - \overline{d}$ ([18], п. 6.15, с. 44). Действительно $\mathbf{L}_i$ принадлежат подпространству $L_{\overline{d}}$ размерности $\overline{d}$, а размерность $L_{\overline{d}}^{\perp}$ – ортогонального дополнения к $L_{\overline{d}}$ равна $\tau - \overline{d}$ ([18], п. 5.22, п. 5.23, п. 5.39, с. 37–38).

[3]Во всех матрицах выше побочной диагонали нули, при увеличении *T* чаще один столбец, указанный в колонке 6 таблицы 4, остается многозначным, все остальные нулевые

Если бы количество линейно независимых и ортогональных ко всем $\mathbf{L}_1, \dots, \mathbf{L}_d$ векторов $\mathbf{q}_i$ было больше $\tau - \overline{d}$, то размерность пространства $L_{\overline{d}}^{\perp}$ была бы больше $\tau - \overline{d}$.

Заметим, что $\overline{d} < \tau$, если d+1< τ, что равносильно неравенству $\overline{k} < 1 + \frac{T}{2}$.

При решении сравнения (12 (13)) строится матрица, в τ столбцах которой расставляются коэффициенты степеней $\lambda_1, \dots, \lambda_\tau$ многочлена $P(x, y)$, стоящего в левой части сравнения.

Пусть $\mu = \max(\lambda_1, \dots, \lambda_\tau) > 0$, $\sigma = \sum_{t=1}^{\tau} \lambda_i$.

Теорема 1. Ранг $\overline{d} \le \tau - \left\lceil \frac{\sigma}{\mu} \right\rceil$.

Доказательство. При применении ММВ для решения сравнения (12 (13)) многочлены $Q_i(x, y)$ таковы, что

$$H_t = \min_{\substack{0 \le x \le A \\ 0 \le y \le B}} \left| Q_{v(t)}(x, y) \right| \le \sqrt{\tau} \left(\alpha^{\frac{\tau(\tau-1)}{4}} (AB)^{\frac{(T-1)\tau}{3}} \right)^{\frac{1}{(\tau - t + 1)}} N^{\frac{\mu}{(\tau - t + 1)} - \sigma},$$

где $\sigma = \min\limits_{i \in \{1, \dots, \tau\}} (\mu_i + \lambda_i)$, $\mu = \sum_{i=1}^{\tau} \mu_i$, $v(1), \dots, v(\tau)$ – перестановка чисел $1, \dots, \tau$ такая, что $\left\| q_{v(1)} \right\| \le \dots \le \left\| q_{v(\tau)} \right\|$ ($\|\bullet\|$ – евклидова норма), $\alpha = \left(\delta - \frac{1}{4} \right)^{-1}$, $\delta \in \left(\frac{1}{4}, 1 \right)$ – параметр LLL-алгоритма.

Отсюда следует, что при $t \in \left\{ 1, \dots, \left\lceil \frac{\sigma}{\mu} \right\rceil \right\}$ величина $\max\limits_{\substack{0 \le x \le A \\ 0 \le y \le B}} \left| Q_{v(t)}(x, y) \right|$ стремится к 0 при $N \to \infty$ (то есть при $w \to \infty$).

Предположим, что в ММВ при некотором $i \in \left\{ 1, \dots, \left\lceil \frac{\sigma}{\mu} \right\rceil \right\}$ и при некотором максимальном $t_0 \in \{0,1, \dots, d\}$ величина $\left(\mathbf{L}_{t_0}, \mathbf{q}_{v(i)} \right) \ne 0$. Так как $\mathbf{L}_{t_0}$, $\mathbf{q}_{v(i)}$ – целочисленные векторы, то $\left(\mathbf{L}_{t_0}, \mathbf{q}_{v(i)} \right) \ge 1$. Используя «чебышевскую» оценку из [13], получим неравенства:

$$\max_{0 \le x \le A} \left| \overline{f}_{v(i)} \right| \ge \left(\mathbf{L}_{t_0}, \mathbf{q}_{v(i)} \right) \left(\frac{A}{4} \right)^{t_0} \ge \left(\frac{A}{4} \right)^{t_0},$$

$$\max_{0 \le x \le A} \left| \frac{\overline{f}_{v(i)}}{\left(\sum_{t=0}^{k} \beta_t x^t \right)^{T-1}} \right| = \max_{0 \le x \le A} \left| Q_{v(t)}(x, \varphi(x)) \right| \ge \frac{\left(\frac{A}{4} \right)^{t_0}}{\left(\sum_{t=0}^{k} \beta_t x^t \right)^{T-1}},$$

$$\max_{\substack{0 \le x \le A \\ 0 \le y \le B}} \left| Q_{v(t)}(x, y) \right| \ge \frac{\left(\frac{A}{4} \right)^{t_0}}{\left(\sum_{t=0}^{k} \beta_t x^t \right)^{T-1}}.$$

Последнее неравенство невозможно при большом значении w.

Таким образом, если w достаточно велико, то $\left(\mathbf{L}_t, \mathbf{q}_{v(i)} \right) = 0$ для $t \in \{0,1, \dots, d\}$, $i \in \left\{ 1, \dots, \left\lceil \frac{\sigma}{\mu} \right\rceil \right\}$. Отсюда следует, что $\overline{d} \le \tau - \left\lceil \frac{\sigma}{\mu} \right\rceil$ ■

П р и м е ч а н и е: Строго доказать теорему 1 для ММП не удалось, но в [11] доказано, что $j_i \le \overline{H}_i$, причём для случая ММП с «чебышевской» матрицей верна оценке ([11], формула (18)):

$$\overline{H}_\tau \le c (AB)^{\frac{T-3}{3}} \sqrt{\tau} \alpha^{\frac{\tau-1}{4}} N^{-\frac{\sigma}{\tau}}, \text{ где } c = 4^{-\left(\frac{2}{3} - \frac{1}{T+1} \right)(T-1)}.$$

На практике при применении ММП для решения сравнения (12 (13)) при достаточно большом w и при $d + 1 \ge \tau$ (что равносильно неравенству $\overline{k} \ge 1 + \frac{T}{2}$) получались равенства $\overline{d} = \tau - \left\lceil \frac{\sigma}{\mu} \right\rceil$, $\left(\mathbf{L}_t, \mathbf{q}_{v(i)} \right) = 0$ для $t = 1, \dots, \tau$ только при $i = \tau$,

$\tau-1,\dots,\tau-\left\lceil\frac{\sigma}{\mu}\right\rceil$. Следовательно, в этом случае векторы $\mathbf{q}_\tau,\mathbf{q}_{\tau-1},\dots,\mathbf{q}_{\tau-\left\lceil\frac{\sigma}{\mu}\right\rceil+1}$ образуют фундаментальную систему решений системы (27) при $\theta=0$. При этом оказывалось, что система (27) выполняется при $\theta=1$, $i=\tau-\left\lceil\frac{\sigma}{\mu}\right\rceil$.

Теорема 2. Если имеется $\tau-\overline{d}$ векторов $\{r_1,\dots,r_{\tau-\overline{d}}\in\mathbf{q}_1,\dots,\mathbf{q}_\tau\}$, удовлетворяющих (27) при $\theta=0$, то существует не более одного вектора $\mathbf{q}_i$, удовлетворяющего (27) при некотором $\theta=1$.

Доказательство. Ранг расширенной матрицы $\begin{pmatrix}\mathbf{L}_0 & C_0\\ \mathbf{L}_1 & \vdots\\ \vdots & C_{k(T-1)}\\ \mathbf{L}_d & 0\end{pmatrix}$ системы (27) равен $\overline{d}$, так как из (25) имеем равенства $L_{t,00}=C_t$ для $t=1,\dots,k(T-1)$, $L_{t,00}=0$ для $t=k(T-1),\dots,d$, то есть первый и последний столбцы в расширенной матрице совпадают. По теореме Кронекера-Капелле система (27) имеет решение при любом $\theta\neq0$. Если $\overline{d}=1$, то не более одного вектора $\mathbf{q}_i$ удовлетворяет (27) при $\theta\neq0$ ($\mathbf{r}_1,\dots,\mathbf{r}_{\tau-\overline{d}}$ это $\tau-1$ векторов $\mathbf{q}_i$).

Пусть $\overline{d}>2$ и (27) выполняются при некотором $\mathbf{q}_i$ и $\theta=\theta_1\neq0$, а также при некотором $\mathbf{q}_j\neq\mathbf{q}_i$ и $\theta=\theta_2\neq0$ (θ_1может равняться θ_2); $\mathbf{q}_j,\mathbf{q}_i\notin\{\mathbf{r}_1,\dots,\mathbf{r}_{\tau-\overline{d}}\}$. Тогда $(\mathbf{L}_t,\theta_2\mathbf{q}_i)-(\mathbf{L}_t,\theta_1\mathbf{q}_j)=0$, $(\mathbf{L}_t,\theta_2\mathbf{q}_i-\theta_1\mathbf{q}_j)=0$ для $t=0,1,\dots,d$.

Следовательно, $\theta_2\mathbf{q}_i-\theta_1\mathbf{q}_j=\sum_{t=0}^{\tau-\overline{d}}u_tr_t$ при некоторых $u_1,\dots,u_{\tau-\overline{d}}$ ([18], п. 6.15, с. 44). Но тогда $\mathbf{q}_j,\mathbf{q}_i,\mathbf{r}_1,\dots,\mathbf{r}_{\tau-\overline{d}}$ – линейно зависимые векторы, а это не так ■

Рассмотрим ещё один случай, когда уравнение (25) имеет на $[0,A]$ A+1 целых корней. Это происходит, когда

$$\sum_{t=0}^{d}x^t(\mathbf{L}_t,\mathbf{q}_i)=g(x)\left(\sum_{t=0}^{k}\beta_t\,x^t\right)^{T-1},\qquad(28)$$

где $g(x)$ – целочисленный многочлен (не константа). (То, что $g(x)$ целочисленный следует из [13]).

В этом случае уравнение (25) равносильно уравнению $g(x)=j$, которое верно при каждом $x\in\{0,1,\dots,A\}$. Вопрос о возможности равенства (28) остаётся открытым.

Доказано, что константных $\overline{f}_i(x)$ будет не более $\tau-\overline{d}$, то есть в алгоритме всегда будет получаться какое-то множество содержательных функций для дальнейшего анализа.

При k=1, $r\in\{0,1\}$, $\overline{k}=2$ имеем d=2(T-1), $T\geq3$, d=2(T-1)<$\frac{T(T-1)}{2}=\tau$, $\overline{d}\leq d$, $\tau-\overline{d}\geq\tau-d=\frac{T(T-1)}{2}-2(T-1)$.

На практике при любых w получалось всегда не более $\frac{T(T-1)}{2}-2(T-1)$ константных $\overline{f}_i(x)$, а при достаточно большом w, как правило, константных $\overline{f}_i(x)$ было равно $\frac{T(T-1)}{2}-2(T-1)$ [11]. Это говорит в пользу равенства $\overline{d}=d$.

Можно ожидать, что при $d\geq\tau$ величина $\overline{d}$ будет равна τ. В этом случае все $\overline{f}_i(x)$ – не константы.

Исследуем возможность неравенства $d\geq\tau$, тогда должны выполняться неравенства $T-1\geq\overline{k}>\frac{T(T+1)}{2(T-1)}$. Отсюда следует, что $2(T-1)^2\geq T(T+1)$, $T^2-5T+2\geq0$, $T\geq5$.

Заметим, что $\overline{k} \neq \frac{T(T+1)}{2(T-1)}$, так как $\frac{T(T+1)}{2(T-1)}$ – не целое число. Возможные значения для $\overline{k}$ приведены в табл. 4.

Таблица 4. Возможные значения для $\overline{k}$

T	$\overline{k} = k + \max(r, 1)$	τ
5	4	15
6	5	21
7	5, 6	28
8	6, 7	36
9	6, 7, 8	45
10	7, 8, 9	55
11	7, 8, 9, 10, 11	66

Заключение

Теоремы 1 и 2 служат обоснованием того, что в результате работы алгоритма всегда будем получать инвариантные многочлены, ранжированные оценками. Эксперименты показали, что места многочленов в списке выходных параметров зависят от входных управляющих параметров алгоритма *T,r,k*. Места многочленов инвариантны по отношению к входным возмущающим параметрам алгоритма, одним из которых является *N*. То есть для одного и того же *N*, при определённых параметрах, на выходе алгоритма всегда будут получаться многочлены определённой структуры на одних и тех же местах выходных списков. Выходной параметр алгоритма – множество множеств дробно-рациональных функций с одной переменной $f: \mathbb{R} \to \mathbb{R}$. Размер выходного множества зависит от параметра алгоритма R (простое число). Чем больше R, тем больше размер выходного множества. Среди множеств рациональных функций только одна система, по ним построенная, даёт решением искомое простое число. Число элементов множества и альтернативных множеств зависит от управляющих параметров. Сами множества, из которых будет выполняться выбор, представлены элементами трёх видов: константы; многочлены $f(x) = \sum_i a_i x^i$ с рациональными коэффициентами и рациональные функции $f(x) = \sum_{i,j} \frac{a_i x^i}{x^j}$. Понятно, что константы не могут служить данными анализа. Экспериментально определено, что многочлены, получаемые в результате работы алгоритма $f(x) = \sum_i a_i x^i$ имеют корни в положительной полуплоскости. Рациональные функции $f(x) = \sum_{i,j} \frac{a_i x^i}{x^j}$ имеют точки разрыва и корни, как при положительном, так и при отрицательном значении аргумента. Непрерывные функции с положительными корнями являются предпочтительными для дальнейших исследований. Главное, что предлагаемый алгоритм, масштабируемый и позволяет, изменяя входные управляющие параметры, получать нужное для дальнейшего анализа число выходных функций (например, многочленов).

Инвариантные многочленные рациональные функции, стоящие в левой части уравнения (20), можно геометрически интерпретировать параболами, кубическими параболами, линиями и т.п. По корням кривых линий можно строить метрические пространства, путём получения верхних и нижних границ диапазонов их возможных значений.

Идея Д. Копперсмита в том, чтобы построить полиномиальные уравнения, правая часть которых равна нулю. В модифицированном методе допускалось отличная от нуля правая часть уравнений. Свободный член в многочлене отвечает за движение кривой вдоль оси ординат. Поэтому, для всех инвариантных кривых линий результат доставляется только их вертикальным движением. Используя аппарат инвариантных функций можно не решать полиномиальные уравнения, как это делал Д. Копперсмит и другие авторы, а используя геометрию движения кривых выбирать из альтернативных множеств такие функции, которые первыми приведут к пересечению всех кривых в точке с координатой $(x = p, y = 0)$, где p – простое число. Описание таких методов выбора будет темой следующих исследований.

Полученные результаты предполагают в дальнейшем разработку полиномиального алгоритма факторизации, состоящего из нескольких этапов. Первый описан в данной статье. Эффективность многих современных средств защиты информации основана на том, что для их дешифрования требуются большие временные или вычислительные ресурсы, а часто и временные, и вычислительные одновремённо. У будущей динамической системы (ДС) время работы не будет сильно зависеть от размера входных данных, так как от него зависит время работы современных субэкспоненциальных алгоритмов факторизации. Также будущая ДС не будет требовать для своего выполнения разработки специальных вычислительных устройств, замечательно описанных в статье Питера Шора, которая стала ключевым вкладом в развитие квантовых алгоритмов и вызвала огромный интерес к возможностям квантовых компьютеров в области криптографии и защиты информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Peter Shor, Polynomial-Time Algorithms for Prime Factorization and Descrete Logarithms on Quantum Computer. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS ’94). DOI: 10.1109/SFCS.1994.365700, 1994.
2. Пучков А.Ю., Соколов А.М., Широков С.С., Прокимнов Н.Н., Алгоритм выявления угроз информационной безопасности в распределённых мультисервисных сетях органов государственного управления. Прикладная информатика. 2023, т. 18, № 2, с. 85–102. DOI: 10.37791/2687-0649-2023-18-2-85-102. – EDN: FUXPSC.
3. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2022. – 832 p. ISBN-13: 978-1-2924-3748-4.
4. Douglas R. Stinson, Maura B. Paterson. Cryptography: Theory and Practice, CRC Press, 2018. – 598 p. ISBN-13: 978-1-1381-9701-5.
5. Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography, Chapman and Hall/CRC, 2014. – 603 p. ISBN-13: 978-1-4665-7027-6.
6. Coppersmith, D. (1996). Finding a Small Root of a Univariate Modular Equation. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. Lecture Notes in Computer Science, v. 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_14.
7. Coppersmith D. Solving low degree polynomials. Asiacrypt 2003. URL: https://www.iacr.org/publications/dl/coppersmith03/dcasia.pdf (дата обращения: 10.04.2024).
8. Coron, JS. (2004). Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology – EUROCRYPT 2004. Lecture Notes in Computer Science, v. 3027. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-24676-3_29.
9. Herrmann, M., May, A. (2008). Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. In: Pieprzyk, J. (eds) Advances in Cryptology – ASIACRYPT 2008. Lecture Notes in Computer Science, v. 5350. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-89255-7_25.
10. Josef Pieprzyk (eds), Advances in Cryptology – ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 2008, Proceedings, Springer. – XIV, 572 p.
11. Coppersmith, D. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. J. Cryptology 10, p. 233–260 (1997). DOI: https://doi.org/10.1007/s001459900030.
12. Nguyen, P.Q., Stern, J. (2001). The Two Faces of Lattices in Cryptology. In: Silverman, J.H. (eds) Cryptography and Lattices. CaLC 2001. Lecture Notes in Computer Science, v. 2146. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-44670-2_12.
13. Зачёсов Ю.Л., Салихов Н.П. О методе решения полиномиального сравнения $P(x)\equiv 0 \pmod N$. Обозрение прикладной и промышленной математики. 2008, т. 15, № 5, с. 769–784. – EDN: KAXSIZ.
14. Зачёсов Ю.Л., Салихов Н.П. Экспериментальная программная оценка размера списка простых чисел, необходимых для отсева полиномиальных уравнений без целых корней. ISSN 2311-2263 (online), ISSN 2071-0410 (print). Прикладная дискретная математика. Приложение. Тезисы докладов VIII Сибирской научной школы-семинара с международным участием «Компьютерная безопасность и криптография» SIBECRYPT'09. Омск, ОмГТУ, 8–11 сентября 2009. DOI: http://journals.tsu.ru/pdm2/&journal_page=archive&id=1137&article_id=18523 (дата обращения: 10.04.2024).
15. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. – 415 с.

16. Coppersmith, D. (1996). Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. Lecture Notes in Computer Science, v. 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_16.
17. Шарый С.П. Конечномерный интервальный анализ. Институт вычислительных технологий СО РАН. Новосибирск: Издательство XYZ, 2013. – 606 с.
18. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. М.: Мир, 1984. – 318 с.

REFERENCES:

[1] Peter Shor, Polynomial-Time Algorithms for Prime Factorization and Descrete Logarithms on Quantum Computer, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS ’94). DOI: 10.1109/SFCS.1994.365700, 1994.
[2] Puchkov A.Y., Sokolov A.M., Shirokov S.S., Prokimnov N.N. Algorithm for identifying threats to information security in distributed multiservice networks of government bodies. Applied Informatics. 2023, v. 18, no 2, p. 85–102 DOI: 10.37791/2687-0649-2023-18-2-85-102 (in Russian). – EDN: FUXPSC.
[3] William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2022. – 832 p. ISBN-13: 978-1-2924-3748-4.
[4] Douglas R. Stinson, Maura B. Paterson. Cryptography: Theory and Practice, CRC Press, 2018. – 598 p. ISBN-13: 978-1-1381-9701-5.
[5] Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography, Chapman and Hall/CRC, 2014. – 603 p. ISBN -13: 978-1-4665-7027-6.
[6] Coppersmith, D. (1996). Finding a Small Root of a Univariate Modular Equation. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. Lecture Notes in Computer Science, v. 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_14.
[7] Coppersmith D. Solving low degree polynomials. Asiacrypt 2003. URL: https://www.iacr.org/publications/dl/coppersmith03/dcasia.pdf (accessed: 10.04.2024).
[8] Coron, JS. (2004). Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology – EUROCRYPT 2004. Lecture Notes in Computer Science, v. 3027. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-24676-3_29.
[9] Herrmann, M., May, A. (2008). Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. In: Pieprzyk, J. (eds) Advances in Cryptology –ASIACRYPT 2008. Lecture Notes in Computer Science, v. 5350. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-89255-7_25.
[10] Josef Pieprzyk (eds), Advances in Cryptology – ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 2008, Proceedings, Springer. – XIV, 572 p.
[11] Coppersmith, D. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. J. Cryptology 10, p. 233–260 (1997). DOI: https://doi.org/10.1007/s001459900030.
[12] Nguyen, P.Q., Stern, J. (2001). The Two Faces of Lattices in Cryptology. In: Silverman, J.H. (eds) Cryptography and Lattices. CaLC 2001. Lecture Notes in Computer Science, v. 2146. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-44670-2_12.
[13] Zachesov Y.L., Salikhov N.P. A method for solving of polynomial congru ence P(X) = 0 (MOD N). Reviews of applied industrial mathematic. 2008, v.15, no. 5, p. 769–784 (in Russian). – EDN: KAXSIZ.
[14] Zachesov Y.L., Salikhov N.P. Experimental program estimate the size of the list prime number, necessary for otseva polynomial equations without integer roots. ISSN 2311-2263 (online), ISSN 2071-0410 (print). Applied discrete mathematic. Application. Abstracts of reports VIII Siberian scientific seminar school with international participation "Computer security and cryptography" SIBECRYPT'09. Omsk, OGTU, 8–11 September 2009. DOI: http://journals.tsu.ru/pdm2/&journal_page=archive&id=1137&article_id=18523 (accessed: 10.04.2024) (in Russian).
[15] Aireland K., Rouzen M. Classical introduction to modern number theory. – M.: Mir, 1987. – 415 p. (in Russian).
[16] Coppersmith, D. (1996). Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. Lecture Notes in Computer Science, v. 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_16.
[17] Shary S.P. Konechnomerny interval analysis. Institute Computational Technologies CO PAH. Novosibirsk: Publishing house «XYZ», 2013. – 606 p. (in Russian).
[18] Voevodin V.V., Kuznetsov Y.A. Matrix and calculations. M.: Mir, 1984. – 318 p. (in Russian).

Поступила в редакцию – 10 апреля 2024 г. Окончательный вариант – 24 мая 2024 г.
Received – April 10, 2024. The final version – May 24, 2024.