УДК 004.056 /002:006.354

МЕТОДЫ СОПОСТАВИТЕЛЬНОГО АНАЛИЗА И ФОРМАНТНЫХ УРАВНЕНИЙ ТЕОРИИ ЧИСЕЛ В ЗАДАЧАХ КРИПТОГРАФИИ

А.А. Балабанов, А.Ф. Агафонов

Технический университет Молдовы

В статье дается краткий анализ современных методов теории чисел, используемых для решения задач криптографии и предлагается один из вариантов решения задачи факторизации на основе сопоставительного анализа и формантных уравнений.

Ключевые слова: *криптография, генераторы криптоклю-чей, теория чисел, сравнительный анализ, сопоставительный анализ, формантные уравнения.*

METHODS OF NUMBER THEORY, ANALYSIS OF THE COLLATION AND FORMANT EQUATIONS IN PROBLEMS OF CRYPTOGRAPHY

A.A. Balabanov, A.F. Agafonov

The article provides a brief analysis of the current methods of the theory of numbers used for the problems of cryptography and offers a solution to the factorization problem on the basis of analysis of the collation and formant equations.

Keywords: *cryptography, generators crypto key, number theory, analysis of the collation and comparative analysis, benchmarking, formant equation.*

ВВЕДЕНИЕ

Одной из причин, благодаря которой отдельные вопросы, интересовавшие специалистов по теории чисел превратились в новое направление, названное «вычислительной теорией чисел», явился быстрый рост мощности и сложности компьютеров. Вычислительные машины и электронные средства связи проникли практически во все сферы человеческой деятельности. Немыслима без них и современная криптография. Шифрование и дешифрование текстов можно представить как процессы обработки блоковых или потоковых данных в целых числах с помощью ЭВМ, а способы выполнения этих операций — как некоторые функции, определенные на множестве целых чисел. Все это делает естественным появление в криптографии методов теории чисел.

В элементарной теории чисел накоплено огромное множество четко сформулированных, поставленных и решенных теоретико-численных задач, впоследствии выросших в теоремы, методы и приемы рассуждений, ставшими классическими теориями. Так, в теорию чисел входят теории сравнений, диофантовых уравнений, непрерывных дробей, диофантовых приближений, трансцендентных чисел, сопоставительный и формантный анализ и др.

1. О СОПОСТАВИТЕЛЬНОМ АНАЛИЗЕ И ЗАДАЧАХ ТЕОРИИ ЧИСЕЛ

Под *сравнением* [7] в теории чисел понимают *соотношение* между двумя целыми числами a и b, означающее, что разность $(a–b)$ этих чисел делится на заданное целое число m, называемое *модулем сравнения*, что записывается как $a = b \pmod m$. Например, $2 = 8 \pmod 3$, т.к. (2–8)делится на 3 (и равно –2); $5 = 8 \pmod 3$, т.к. (5–8)делится на 3 (и равно –1); Из этих двух сравнений следует третье $2 = 5 \pmod 3$ и тоже равно $(–1)$[1].

Сопоставительный анализ [1] представлен двумя условно понимаемыми разделами, а именно, *сопоставительными уравнениями* и *формантным анализом*, с элементами теории вычетов. В сопоставительном анализе вместо числовых и алгебраических величин и действий над ними рассматриваются (сопоставляются) имманентные им математические аналоги. В сопоставительных уравнениях – это кратности числа (алгебраического выражения) по простому основанию (простому числу), а в формантном анализе – это

[1] Однако из сравнения явно не видно, чему равно частное (ядро) от деления разности чисел на модуль!

форманта числа или алгебраического выражения, например, уравнения.

Сопоставительный анализ в целочисленной математике рассматривает алгебраиче-ские выражения (многочлены) с точки зрения их *соответствия отношениям равенства их кратностей*, как это имеет место при сравнении обычных целых чисел (т.е. разложимость чисел на простые множители). Основанием для кратностей в сопоставительном анализе берутся *только простые числа*, в отличие от общего сопоставительного анализа, где в качестве оснований допускаются и составные числа. Рассмотрим, для примера, нахождение сопоставительного уравнения для следующего диофантового уравнения

$$F_5(X^2+5Y)=5k+(1, 4). \qquad (1)$$

Кратность по основанию p левой части уравнения $K_p[X^4+10Y^3]$ есть кратность суммы (X^4+10Y^3), кратность правой части — тоже кратность суммы $(3X+3Y^5)$. Понятно, что если уравнение (1) имеет целочисленное решение, то имеет место и равенство кратностей обеих частей уравнения (по любому основанию), что записывается следующим образом:

$$[4K_p(X);K_p(10)+3K_p(Y)]= \\ =[K_p(3)+K_p(X);K_p(3)+K_p(Y)]. \qquad (2)$$

Это выражение называется *сопоставительным уравнением* по основанию p исходного алгебраического уравнения (1). В частности, если за основание принято число p=3, то сопоставительное уравнение (2) будет иметь следующий вид:

$$[4K_3(X);K_3(10)+3K_3(Y)]= \\ =[K_3(3)+K_3(X);K_3(3)+5K_3(Y)]$$

или, с учетом известных кратностей целых чисел по основанию 3 (коэффициенты уравнения (2)) $K_3(10)=0$, $K_3(3)=1$, получим

$$[4K_3(X);0+3K_3(Y)]=[1+K_3(X);1+5K_3(Y)].$$

Ключевым понятием *формантного анализа* является форманта $F_p(M)$ по основанию p некоторого числа, неизвестного x, алгебраического выражения или многочлена M, под которой понимается его (их) *линейное представление в виде трехчленной (трехмерной)*[2] *математической конструкции*: $F_p(M)=pk+q$, где p есть база (основание) форманты, k — ядро или целая часть от деления M на основание p и q — неотрицательный целый остаток.

[2] Мы можем говорить и о мерности конструкции, по аналогии с n-мерным пространством, в котором рассматривается состояние некоторой динамической системы, описываемой дифференциальным уравнением n-го порядка.

Приведем пример обозначения форманты математического выражения, а именно, бинома $M=X^2+5Y$. Его форманта выглядит так: $F_p(X^2+5Y)$, что читается: *форманта по основанию p алгебраического двучлена вида* (X^2+5Y).

Если p = 5, то форманта приведенного выше бинома будет иметь такой вид:

$$F_5(X^2+5Y)=5k+(1, 4).$$

Математический смысл форманты, в данном случае, означает следующее: *если* X^2 *не делится на* 5, *то при любых целых X и Y, остаток от деления этого двучлена на* 5 *будет равным или* 1, *или* 4.

Неотрицательный остаток (он может быть и ноль) называется *формантной скобкой* (или просто скобка), содержащей одно или более чисел. Количество чисел в скобке определяет *размерность форманты*.

В структуре форманты присутствует так называемое *ядро* (k) форманты, т.е. целая часть от деления данного числа или алгебраического выражения на базу p.

Таким образом, форманта полностью определяется тремя величинами p, k и q. *Любое число единственным образом определяется формантой по заданному основанию*.

Существуют несколько типов формант. Подробнее см. [1].

2. О ДИОФАНТОВЫХ УРАВНЕНИЯХ

Под *диофантовыми уравнениями* понимают алгебраические уравнения или их системы с целыми коэффициентами, где число неизвестных превосходит количество уравнений, для которых разыскиваются целые или рациональные решения. Например, уравнение $x^2=Ny^2+l$ всегда имеет решение в натуральных числах x и y; в действительности оно имеет бесконечное множество таких решений.

Непрерывная дробь (цепная дробь) является одним из важнейших способов изображения чисел. К непрерывной дроби, изображающей некоторое (не целое) число a, приходят, записывая это число в виде:

$$a=a_0+\frac{1}{a_1},$$

где a_0 — целое число и $0 \le \frac{1}{a_1} \le 1$; далее, записывая a_1 в таком же виде, т.е. $a_1=a_1+\frac{1}{a_2}$, и продолжая этот процесс для a_2 и т.д., получают непрерывную дробь: $a=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2}...}$. Например, $\sqrt{5}=2+\cfrac{1}{4+\cfrac{1}{4+...}...}$.

Диофантовы приближения — это раздел теории чисел, изучающий приближения действительных чисел рациональными, а также вопросы, связанные с решением в целых числах линейных и нелинейных неравенств с действительными коэффициентами [7, 9].

Под *трансцендентным числом* понимают число, не удовлетворяющее никакому алгебраическому уравнению с целыми коэффициентами. Трансцендентными числами являются: число p=3,14159...; десятичный логарифм любого целого числа, не изображаемого единицей с нулями; число e =2,71828... и др.

Основоположниками вышеперечисленных теорий по праву считаются Евклид и Диофант, Ферма и Эйлер, Гаусс, Чебышев, Эрмит и др., чьи труды содержат остроумные и весьма эффективные алгоритмы решения диофантовых уравнений, выяснения разрешимости сравнений, построения больших по тем временам простых чисел, нахождения наилучших приближений и т.д.

3. О КРИПТОГРАФИИ

Теория простых чисел относится к одной из немногих областей чистой мате-матики, которая нашла непосредственное практическое приложение, а именно в криптографии. Процесс кодирования требует использования ключа к шифру и получателя шифровки необходимо снабдить этим ключом [5], что является самым слабым звеном в цепи обеспечения безопасности обмена сообщениями. Проблема ключа вращается вокруг того факта, что дешифровка с известным ключом должна производиться столь же легко, как и шифровка. Но смысл защиты сообщения заключается в том, чтобы дешифровка при отсутствии ключа была гораздо сложнее, чем шифровка: приготовить яичницу-болтунью несравненно легче, чем вернуть яичницу-болтунью в исходное состояние, восстановив и разделив белки и желтки.

В 1977 г. Р. Ривест, А. Шамир и Л. Адлеман — математики и компьютерные специалисты из Массачусеттского технологичес-кого института — выяснили, что простые числа являются идеальным базисом для процесса легкой шифровки и трудной дешифровки. Результаты, положенные в основу разработанного ими алгоритма, получившего название *RSA*, изложены, например, в [4, 6–9)].

Рассмотрим простой пример. Предположим, что выбирается и сообщается всем желающим составное число 589, позволяющее каждому посылать шифрованные послания. Если бы кому-нибудь удалось найти два простых множителя числа 589, то такой человек также смог бы дешифровывать адресованные другому человеку послания. Но сколь ни мало число 589, найти его простые множители вручную не так-то просто. Но на ПК в несколько секунд можно было бы обнаружить, что простые множители числа 589 равны 31 и 19 ($31 \cdot 19 = 589$), поэтому такой ключ не мог бы гарантировать безопасность переписки достаточно долго. Но если бы составное число содержало более сотни знаков, это сделало бы поиск простых множителей практически неразрешимой задачей. Даже если для разложения огромного составного числа на два простых множителя (ключей шифрования и дешифрования) использовать самые мощные компьютеры, которые только существуют в мире, то и тогда, чтобы найти эти множители, понадобилось бы несколько и даже сотни лет.

В настоящее время алгоритм RSA активно реализуется как в виде самостоятельных криптографических продуктов[3], так и в качестве встроенных средств в популярных приложениях[4].

Вместе с возникновением в криптографии новых понятий и методов расширился и круг криптографических приложений теории чисел. В дополнение к элементарной и аналитической теории чисел все более широко используется *алгебраическая теория чисел* и *арифметическая алгебраическая геометрия*: тесты на простоту с применением сумм Гаусса и Якоби, криптосистемы, основанные на квадратичных полях, решето числового поля, факторизация при помощи *эллиптических кривых*, криптосистемы, основанные на эллиптических и гиперэллиптических кривых и абелевых многообразиях.

Довольно успешно, несмотря на свою сложность, реализуются криптосистемы, основанные на эллиптических кривых. Название *«эллиптические кривые»* способно ввести в заблуждение, потому что они — не эллипсы и даже не кривые в обычном смысле слова. Речь идет об уравнениях общего вида $y^2=x^3+ax^2+bx+c$, где a, b, c — некоторые числа.

Свое название эллиптические кривые получили потому, что некоторые функции, тесно связанные с этими кривыми, потребовались для измерения длин эллипсов (а, следовательно, и длин планетных орбит). Уравнения такого вида называются кубическими. Проблема эллиптических кривых, как и проблема доказательства Великой теоремы Ферма, заключается в вопросе — имеют ли соответствующие им уравнения целочисленные решения, и если имеют, то сколько. Например, кубическое уравнение $y^2=x^3-2$, где $a=b=0$, $c=-2$, имеет только одно решение в целых числах, а именно: $y=5$; $x=3 \rightarrow 25=27-2$.

Доказать, что это уравнение имеет только одно решение в целых числах — трудная задача. Этот факт доказал П. Ферма.

Особый интерес кубические уравнения вызывают тем, что они занимают нишу между более простыми уравнениями, решения которых почти тривиальны, и более сложными, решить которые невозможно. Изменяя значения a, b и c в общем кубическом уравнении, можно получить бесконечное множество уравнений, каждое из которых обладает своими характерными особенностями, но все они уравнения и поддаются

[3] Например, в нашумевшей программе PGP (Pretty Good Privacy). http://www.gloffs.com/pgp.htm

[4] В браузерах Интернет от Microsoft и Netscape

анализу. Первыми изучали кубические уравнения древнегреческие математики, в том числе и Диофант, который посвятил им большие разделы своей «Арифметики». Существует множество простых на первый взгляд вопросов относительно кубических уравнений, являющихся до сих пор не решенными, в частности те, которые рассматривал еще Ферма, до сих пор остаются без ответа. В каком-то смысле вся математика восходит если не к Великой теореме Ферма, то к другим его идеям.

В качестве первого шага исследования можно не находить явного решения кубического уравнения, а поставить вопрос: сколько решений вообще может быть? Как правило, и на этот вопрос ответить очень сложно, однако математики придумали способ, как упростить эту задачу. Например, кубическое уравнение $x^3-x^2=y^2+y$, почти невозможно решить напрямую. Одно, тривиальное решение очевидно: $x=0$, $y=0$. Чуть больший интерес представляет собой решение $x=1$, $y=0$. Действительно, $1^3-1^2=0^2+0$. Возможно, существуют и другие решения, но если принять во внимание, что перебору подлежит бесконечное множество целых чисел, то станет ясно, что составление полного списка решений этого уравнения в целых числах — задача невозможная. Более простой задачей является поиск решений в конечном числовом пространстве — в так называемой *арифметике вычетов*.

4. ПРИМЕНЕНИЕ СОПОСТАВИТЕЛЬНОГО АНАЛИЗА ДЛЯ РЕШЕНИЯ ДИОФАНТОВЫХ УРАВНЕНИЙ ПРИМЕНИТЕЛЬНО К КРИПТОАЛГОРИТМАМ RSA. ПОСТАНОВКА ЗАДАЧИ

Рассмотрим большое составное число в виде произведения двух простых чисел $M=N_1N_2$ (или, как в системе *RSA*: $n = p \cdot q$). Далее будем исследовать, в качестве исходных, квадратичные диофантовы уравнения нулевого порядка в следующих трех видах (где M — факторизуемое число):

1 вид: $$X \cdot Y=M=N_1N_2; \qquad (3)$$

2 вид: $$X^2=Y^2+M \to X^2-Y^2=M=N_1N_2=(X+Y)(X-Y); \qquad (4)$$

3 вид: $$X^2-2X \cdot Y=M=N_1N_2. \qquad (5)$$

Во всех этих случаях нужно найти значения неизвестных X и Y. Задача облегчается уже тем, что изначально примерно известен порядок чисел N_1 и N_2. Например, большая практика работы с ключами RSA показывает, что N_1 и N_2 (полагая $N_1>N_2$) — числа одного порядка или отличаются на один, максимум на два порядка. Поскольку в сопоставительном анализе мы имеем дело с формантами, то от алгебраических уравнений (3), (4), (5) перейдем к формантным уравнениям следующих трех видов (соответственно, к трем вычислительным схемам), записанных в общем виде:

$$F_p(X) \cdot F_p(Y)=F_p(M); \qquad (6)$$
$$F_p(X^2) \cdot F_p(Y^2)=F_p(M); \qquad (7)$$
$$F_p(X^2) \cdot 2F_p(Y)=F_p(M). \qquad (8)$$

Какой схемой воспользоваться – определяет оператор.

Решение задачи факторизации M, очевидно, будет получено, после того, как мы найдем значения X и Y, что очевидно при решении обычного алгебраического уравнения. В сопоставительном же анализе, во многих случаях, *достаточно найти только форманты неизвестных по какому-либо основанию*, *что*, как будет показано, *намного проще*. Поставим задачу: *разработать методику нахождения собственных формант*[5] *неизвестных* X и Y. Действительно, предположим, например, для уравнения (4) и формантной схемы (7), что уже найдены собственные форманты по некоторому большóму основанию p:

$$X=pn+(X_0);\ Y=pm+(Y_0);$$
Тогда $$X+Y=p(n+m)+(X0+Y0)=N_1$$
$$X-Y=p(n-m)+(X_0-Y_0)=N_2.$$

Если $p>N_1$, то указанные форманты (суммы и разности) по основанию p являются *предельными*[6], поэтому находим сразу искомые числа:

$$N_1=(X_0+Y_0);\ N_2=(X_0-Y_0)$$

Можно показать, что, в случае использования схемы (8) для уравнения (5), необходимо обеспечить $p>M$, что, конечно же, намного сложнее, поэтому предпочтение следует отдавать первым двум схемам. Поясним процедуру нахождения собственных формант неизвестных на простом примере.

Пример. Пользуясь изложенным подходом, найдем разложение числа **1643** в виде последовательности этапов решения диофантового уравнения 2-го порядка с помощью методов формантного анализа.

1. Составление формантного уравнения по основанию p=13

Поскольку любое составное число можно представить согласно (4) и (7), как

$$F_{13}^{np}(X^2)=13m+(1\ 4\ 9) \qquad (4,б)$$

то легко убедиться, что X — четное, а Y — нечетное. Действительно, $X^2+1-Y^2=1644$, на основании чего

[5] Собственной (единственной), если скобка содержит только одно число [1].

[6] Предельной по основанию p, если при основаниях больших величина остатка не меняется.

можно записать следующее сопоставительное уравнение по основанию 2:

$$K_2(X^2+1), 2K_2(Y)=K_2(1644)=2,$$

которое будет разрешимо, если X — четное, а Y — нечетное. Если же (4,б) переписать в виде[7]: $X^2=Y^2-1+1644$ и записать для него также сопоставительное уравнение по основанию 2 [1]

$$2K_2(X)=K_2[(Y^2-1), 2]2\geq 2,$$

то оно будет разрешимо, если $2K_2(X)\geq 2$, т.е. если X делится на 2, на 4 и больше.

Из сопоставительного анализа и теории степенных вычетов известно, что форманта квадрата числа по основанию p может быть записана как $F_p(X^2)=pm+q$, где $q={}_2V_p$ — *квадратичный вычет(ы) основания p*. Кроме того, согласно (4) свободным членом является факторизуемое число, т.е.

$$X^2=Y^2+1643, \qquad (9)$$

Из уравнения (9) видно, что $Y<X$ и формально можно записать формантное уравнение, где $C(N)$ и $q(N)$ — соответственно целая часть и остаток от деления числа N=1643 на основание форманты p=13. Получаем

$$\underbrace{13m+{}_2V_{13}}_{F_{13}(X^2)}=\underbrace{13k+{}_2V_{13}}_{F_{13}(Y^2)}+\underbrace{C(N)+q(N)}_{N}\rightarrow$$

$$\rightarrow F_{13}(X^2)=F_{13}(Y^2)+N\rightarrow$$

$$\rightarrow 13m+(1\ 4\ 9\ 10\ 11\ 12)=$$
$$=13k+(1\ 4\ 9\ 10\ 11\ 12)+13\cdot 126+(5). \qquad (10)$$

2. Переход к скобочному уравнению

(опускаем целые части)

$$(1\ 4\ 9\ 10\ 11\ 12)=(1\ 4\ 9\ 10\ 11\ 12)+(5)$$

Работаем с правой скобкой, т.е. с выражением для Y^2+N. Выполняем действие сложения для остатков в правой части

$$(1\ 4\ 9\ 10\ 11\ 12)+5=(6\ 9\ 14\ 15\ 16\ 17).$$

Все остатки больше основания p=13, уменьшаем на величину p. Имеем

$$(6\ 9\ 14{-}13\ 15{-}13\ 16{-}13\ 17{-}13)=(6\ 9\ 1\ 2\ 3\ 4).$$

Полученную скобку сравниваем с левой скобкой форманты для X^2 и находим равные остатки (выделены жирным шрифтом)

$$(\mathbf{1}\ \mathbf{4}\ \mathbf{9}\ 10\ 11\ 12)=(6\ \mathbf{9}\ \mathbf{1}\ 2\ 3\ \mathbf{4})$$

и равные остатки сохраняем: 1 4 9. Записываем *промежуточную форманту* для X^2

$$F_{13}^{np}(X^2)=13m+(1\ 4\ 9). \qquad (11)$$

Ищем теперь форманту для Y^2. Сначала находим т.н. *дифферент d*

$$d=p-q(N)=13-5=8$$

и в скобке (11) для $F_{13}^{np}(X^2)$ каждый остаток, меньше, чем p=13, увеличиваем на величину дифферента d=8, а больший, чем $q(N)$=5 — уменьшаем на $q(N)$=5. Тогда имеем для скобки остатков:

$$(1\ 4\ 9)_{13}^{X^2}=(1+d\ \ 4+d\ \ 9-q(N))_{13}^{Y^2},$$

что дает $(1\ 4\ 9)_{13}\rightarrow(9\ 12\ 4)_{13}$.

Теперь можно записать *окончательную форманту* для Y^2

$$F_{13}(Y^2)=13k+(9\ 12\ 4). \qquad (12)$$

Окончательная форманта для X^2 получается из полученной форманты (12) для $F_{13}(Y^2)$ путем добавления $q(N)$ *к каждому члену остатка*

$$F_{13}(X^2)=F(Y^2)_{13}+q(N)=13k+(9\ 12\ 4)+5\rightarrow$$
$$F_{13}(X^2)=13k+(14\ 17\ 9). \qquad (13)$$

Все остатки больше p=13 уменьшаем на 13:

$$(14-13=1\ \ 17-13=4\ \ 9)$$

Окончательно для $F_{13}(X^2)$ имеем, ср. с ф. (11):

$$F_{13}(X^2)=13+(1\ 4\ 9);\ F_{13}(Y^2)=13k+(9\ 12\ 4). \qquad (14)$$

3. Расширение формант. Переход к составной форманте

Общий алгоритм. Вводится коэффициент расширения основания p = 13, т. е. шаг s, больше 1 или кратный любому числу, в частности самому основанию, если оно простое число, например, как в нашем примере, s=13

[7] Кратность суммы Кр[A+B] равна наименьшей кратности из кратностей слагаемых; при равенстве кратностей слагаемых кратность суммы больше или равна кратности слагаемых (в случае четности – т.е. кратности по основанию 2; кратность суммы всегда не меньше кратностей слагаемых) [1]
Кр[A + B] = min(Кр[A]; Кр[B]), если Кр[A] ≠ Кр[B),
Кр[A + B] ≥Кр[A] , при Кр[A] = Кр[B]), если p > 2,
Кр[A + B] >Кр[A] , при Кр[A] = Кр[B]), если p = 2.

ПРИМЕЧАНИЕ: Коэффициент расширения м.б. любым числом, кратным основанию, самим основанием или одним из его сомножителей. Например, если основание p=13 то шаг s м.б. только кратен 13. Если же основание p=12 и нужно перейти к основанию 20, то это расширение можно сделать за несколько проходов: от 12 к 16 или до 18, далее к 20. Шаг s м.б. равен s=2, 3, 4, 6 или 12 (т.е. равным любому из делителей основания p=12 (кроме s=8, т.к. 8 не является делителем числа 12), [1].

В качестве методического примера новое основание выберем, увеличив прежнее вдвое, т.е. $p_н$=2 · 13=26. Число остатков в скобке увеличится тоже в 2 раза и будет состоять из всех старых остатков плюс такое же число новых. Каждый новый добавляемый остаток равен старому, увеличенному на 13. Тогда получим для составной форманты $F_{26}(X^2)$ с учетом остатков исходной форманты (3), следующие выражения-переходы:

$$F_{13}(X^2)=13m+(1, 4, 9) \rightarrow F_{26}(X^2),$$
$$F_{26}(X^2)=26m+(1, 4, 9, 1+13, 4+13, 9+13) \rightarrow$$
$$F_{26}(X^2)=26m+(1, 4, 9,14, 17, 22).$$

Далее проверяем полученную новую скобку остатков на делимость на 2, потом на 4 и, наконец, на 8, т.е. удваиваем делители до $2p_i$<13. Из получаемых остатков формант отбрасываем те остатки (выделены жирным), делящиеся на указанные делители. Получим

$$F_{26}(X^2)=26m+(1, 9, 17) \qquad (15)$$

Теперь вычислим расширенную составную форманту для (14) $F_{26}(Y^2)$. Имеем:

$$F_{26}(Y^2)=13k+(\mathbf{9}, \mathbf{12}, \mathbf{4}) \rightarrow (\mathbf{9}, \mathbf{12}, \mathbf{4}, 9+13, 12+13, 4+13) \rightarrow$$
$$\rightarrow F_{26}(Y^2)=26k+(\mathbf{9}, 12, 4, 22, \mathbf{25}, 17),$$

что после отсева кратных остатков дает

$$F_{26}(Y^2)=26k+(9, \mathbf{25}, \mathbf{17}). \qquad (16)$$

Тогда формантное уравнение (15) тоже изменится

$$F_{26}(X^2)=26m+(1, 9, 17)=F_{26}(Y^2)+N=26k+(9, 25, 17).$$

Поскольку Y есть нечетная форманта[8], и остатки должны совпадать с левой частью уравнения, т.е. с (15), где нет остатка 25, получим для форманты Y^2 (16)

$$F_{26}(X^2)=26m+(9, 17)=F_{26}(Y^2)=26k+(9, 17). \qquad (17)$$

Из уравнения (17) перебором k находим Y.

Рассмотрим теперь первое возможное уравнение (17): Y^2=26k+9. k=0 дает Y^2=9, откуда Y=3. Подставим это значение в уравнение для $X^2=Y^2+1643$, что не дает полного квадрата: $1652 \neq X^2$. Значит Y=3 не является сомножителем числа N=1643.

Продолжаем далее перебор уравнений. k=1 дает Y^2=26+9=35. Что, к сожалению, тоже не является квадратом числа; k=2 дает 61 — тоже нет квадрата, k=3 дает 87, k=4 нет... но, наконец, k=20 дает Y^2=529, откуда $Y^2=\sqrt{529}=23$.

Проверяем: $X=\sqrt{1643+Y^2}=\sqrt{1643+529}$ и... решения в целых числах нет!?

Рассмотрим теперь второе возможное уравнение (17): Y^2=26k+17. k=0, нет квадрата, k=1 дает 42 — нет квадрата... k=4 дает 26 · 4+17=121 откуда Y=11 — нечетное! Тогда, согласно (1), можем найти X и убедиться в справедливости найденного решения. Действительно:

$$X=\sqrt{1643+Y^2}=\sqrt{1643+121}=\sqrt{1764}=42 \text{ (четное!)},$$

$\sqrt{42^2}=\sqrt{11^2}+1643$ или 1643=422–112=1764–121=1643!!!

Тогда $N1=X+Y$; $N2=X-Y$, откуда $N1$=42+11=53; $N2$=42–11=31 → N=31 · 53=1643 Ч.т.д.

Так обстоят дела с модельным примером. Число 1643 факторизовано! В случае же факторизации большого составного числа (например, N в системе RSA), не зная, естественно, заранее значения для Y^2 мы первоначально «имеем в уме» только тот математический факт, вытекающий из свойств исходного уравнения, что Y^2 меньше 1643 и при этом есть проверка $Y^2=X^2-1643$. Поэтому на основании такой оценки величины Y^2 мы должны расширить форманту $F_p(Y^2)$ до основания p>1643, или возможно ближе подойти к этому числу, что можно выполнить за несколько шагов. Например, взяв коэффициент расширения, равным 36-кратному шагу по 26, т.е. s=36 и перейти от базы p=26 сначала к основанию (базе) 26 · 36=936. В результате мы получим длинную скобку, из которой должны исключить все четные числа и все нечетные, делящиеся на 3.

Модельно рассмотрим дальнейшую процедуру. Для этого найдем квадратичные вычеты нового основания ${}_2V_{936}$ и уменьшим скобку остатков, исключив указанные числа (исключить все четные числа и все нечетные, делящиеся на 3)

${}_2V_{936}$ =(**1** 4 9 16 25 36 40 **49** 52 64 81 88 100 108 **121** 144 153 160 **169** 172 196 208 217 220 225 244 256 **289** 313 324 328 337 352 360 **361** 364 376 400 412 432 **433** 441 468 472 **481** 484 504 508 520 **529** 556 568 576 585 **601** 612 625 628 640 **649** 664 **673** 676 688 712 724 729 745 784 792 **793** 796 820 828 832 **841** 844 880 900 **913**)

$$F_{26}(Y^2)=26k+(9, 17) \rightarrow$$
$$\rightarrow F_{936}(Y^2)=936m+(5, 17, 25, 121, 169 \ldots, 217, 289, 337, 361, \rightarrow$$
$$\rightarrow 433, 441, 481, 529, \ldots, 601, 625, 649, 673, 793, 841, 913, \ldots).$$

[8] Форманта массива нечетных чисел

Подобный же «фокус» следует проделать и с формантой для X^2. Затем решить новое формантное уравнение, и найти новые (с меньшими по длине скобками) форманты для X^2 и Y^2. Получим новую форманту для Y^2 по основанию 936, с длинной скобкой

$$F_{936}(Y^2)=936k+(..121...), \qquad (18)$$

содержащую в скобке остатков всех «кандидатов на «должность» Y^2 и X^2. Проанализировав далее все числа-остатки в скобке «на полный квадрат», (аналогично уравнению (17)), убедимся, что таковым окажется единственное число, удовлетворяющее исходному уравнению $X^2=Y^2+1643$, а именно: 121 (по аналогии с рассмотренным модельным примером, хотя в нем исследовалось не большое число!). В результате получим уравнение (18), аналогичное (17), откуда теперь можно будет найти Y:

$$F_{1872}(Y^2)=1872k+(9, 17, ..., 121...) \rightarrow$$

Очевидно, при k=0 и остатке 121 это уравнение имеет решение Y=11, которое приводит к решению исходной задачи факторизации, удовлетворяющеми диофантовому уравнению (1).

ЗАКЛЮЧЕНИЕ

Предлагаемый авторами алгоритм строится на основе исследования свойств диофантовых уравнений (по аналогии с подходами в алгоритмах Ферма), но с использованием методов сопоставительного анализа. Существенным моментом здесь являются новые, нетрадиционные для теории чисел способы и подходы к решению классической задачи факторизации, а также разрешимости/неразрешимости исходного диофантового уравнения.

Программная реализация описанного алгоритма заключается в программиро-вании всех описанных шагов, важнейшими из которых является *фильтрация ложных формант* (уменьшение длины скобочных уравнений за счет просеивания кратных остатков и решения частных уравнений методом перебора).

Литература

1. **Агафонов А.Ф.** Научные труды 1960-2010 / научн. ред. Балабанов А.А., Кишинев, ТУМ, 2012.
2. **Балабанов А.А., Агафонов А.А, Шегева С.** Об одном методе экспериментальной оценки операционной емкости вероятностных алгоритмов и степени достоверности заключения о простоте числа: // Информационные технологии-2004 BiT+», 3-9 мая 2004, Кишинев.
3. **Балабанов А.А., Агафонов А.Ф., Рыку В.А.** Алгоритм быстрой генерации ключей в криптографической системе RSA, http://www.vntr.ru/ftpgetfile.php?id=323.
4. **Балабанов А.А., Агафонов А.Ф, Кожухарь И.** Возможности создания новых и модернизированных алгоритмов для системы RSA, http://www.vntr.ru/ftpgetfile.php?id=451
5. **Баричев С.** Криптография без секретов. М., 2001.
6. Введение в криптографию / Под общ. ред. В.В. Ященко. М., 2000.
7. **Виноградов И.М.** Основы теории чисел. М.: Наука, 1972.
8. **Сингх С.** Великая теорема Ферма. 2000.
9. **Шафаревич И.Р., Боревич З.И.** Теория чисел. М., 1985.

Балабанов Анатолий Александрович,
д.т.н., профессор кафедры автоматики и информационных технологий Технического университета Молдовы

Агафонов Анатолий Федорович,
с.н.с., инженер-математик кафедры автоматики и информационных технологий Технического университета Молдовы

➲ МД-2004, Респ. Молдова, г. Кишинев, бульвар Штефан чел Маре, д. 168, e-mail: bbalsoft@gmail.com