ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS
Հատոր Том Volume 101 2001 № 2

МАТЕМАТИКА

УДК 511

С. Л. Амбарян

Обобщение метода Ферма разложения на простые множители

(Представлено академиком Н. У. Аракеляном 18/XИ 2000)

Разложение на множители больших чисел является одной из труднейших вычислительных проблем теории чисел, для которой верхняя оценка количества шагов вычисления для числа n равна $0(n)^{1/4+\varepsilon}$, где $\varepsilon > 0$. Вопрос о вычислительной сложности разложения на множители в настоящее время не решен [1, 2]. Разработка новых методов криптографии, в частности, метода открытого распространения ключей Диффи-Хеллмана [3] и криптосистемы с открытым ключом RSA (R. Rivest, A. Shamir, L. Adleman) [4], дала новый толчок развитию четырех направлений теории чисел и компьютерной арифметики:

разработка алгоритмов разложения на множители [1, 2, 5];

разработка алгоритмов нахождения больших простых чисел [1, 5];

разработка эффективных алгоритмов умножения и деления [5, б];

разработка высокоскоростной арифметики многократной точности [5].

В настоящей работе рассматривается задача построения алгоритма разложения на множители, основанного на обобщении идеи, предложенной Пьером де Ферма.

Метод Ферма основан на представлении числа N в виде разности двух квадратов [5, 7-9]. Пусть требуется разложить на множители нечетное составное число $N;$ тогда если требуемое разложение имеет вид $N = p \cdot q,\ 1 < p < q,$ то полагая $x = (p+q)/2,\ y = (q-p)/2,$ задача сводится к представлению N в виде

$$N = x^2 - y^2\,,\quad 0 < y < x < N. \tag{1}$$

Как известно, метод Ферма обобщен Лежандром [5]. Метод Лежандра основан на поиске чисел x и $y,$ таких, что

$$y^2 \equiv x^2 (mod\ N)\,,\quad 0 < y < x < N\,,\ x + y \neq N\,. \tag{1a}$$

Из $(1a)$ следует, что нод $(N, x-y)$ и нод $(N, x+y)$ − делители числа N.

Предложенный Ферма метод проверки правых крайних цифр обобщен Д. Х. Лемером и его сотрудниками с привлечением других модулей (*метод просеивания)* [5].

В данной работе метод Ферма обобщен для произвольного количества k последних цифр полного квадрата, т. е. для сравнения

$$r \equiv x^2 (mod \;\; 10^k), \quad k = 1, 2, 3 \cdots$$

Как будет видно из дальнейшего изложения, это обобщение, с одной стороны, приводит к интересным результатам, а с другой стороны, что не менее важно, квадратичные вычеты всех натуральных чисел по степеням десяти будут представлены в виде простых математических формул (будем называть их структурными представлениями).

Аналогично сказанному для удобства рассмотрим вначале случаи малых k. В случае $k = 2$, как легко видеть, число является полным квадратом, если две его последние цифры определяют число, принадлежащее следующему множеству:

$$A = \{00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41,\\ 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96\}.$$

Элементы множества A разобьем на подмножества *(классы)* так, чтобы элементы одного и того же класса образовали арифметическую прогрессию с разностью $d_2 = 20$ либо заканчивались на 0 или 5 (этот класс назовем *нулевым классом):* $k_0 = (00{,}25) = (0{,}25)$; $k_1 = (1, 21, 41, 61, 81)$; $k_2 = (4, 24, 44, 64, 84)$; $k_3 = (9, 29, 49, 69, 89)$; $k_4 = (16, 36, 56, 76, 96)$.

При $k = 1$ имеем $k_0 - (0, 5)$; $k_1 = (1)$; $k_2 = (4)$; $k_3 = (9)$; $k_4 = (6)$;

при $k = 3$ и $d_3 = 40$ имеем

$$k_0 = (0,\ 25, 100, 225, 400, 500, 600, 625, 900);$$
$$k_1 = (1,\ 41,\ 81, \ldots,\ 921,\ 961);$$
$$k_2 = (4,\ 44,\ 84, \ldots,\ 924,\ 964);$$
$$k_3 = (9,\ 49,\ 89, \ldots,\ 929,\ 969);$$
$$k_4 = (16,\ 56,\ 96, \ldots,\ 936,\ 976);$$
$$k_5 = (36,\ 76, 116, \ldots,\ 956,\ 996);$$
$$k_6 = (64, 104, 144, \ldots,\ 984,\ 24) \text{ и т. д.}$$

Теперь перейдем к рассмотрению случаев произвольных k.

Множество чисел, определяемых k последними цифрами полных квадратов, обозначим через $\tilde{A}_k$, а его мощность – через A_k; $k = 1, 2, 3, \cdots$.

Определим вектор L_k, $k = 1, 2, 3, \cdots$, состоящий из шести компонент

$$L_k = (a_k, b_k, d_k, |k_0|, A_k^*, A_k)\,, \qquad (2)$$

где a_k количество ненулевых классов;

$b_k = 5^{k-1}$ количество элементов в каждом ненулевом классе;

$d_k = 2^k \cdot 5$ разность между соседними элементами ненулевых классов;

$|k_0|$ – мощность *нулевого класса;*

$A_k^* = a_k \cdot b_k$ – мощность *регулярного множества* $\tilde{A}_k^*$ (без *нулевого класса);*

$A_k = A_k^* + |k_0|$ – мощность множества $\tilde{A}_k$.

Ниже приводятся рекуррентные соотношения между элементами $a_k;\ k = 1, 2, 3, \cdots$, а также явное выражение a_k через k:

$$\begin{aligned} &a_1 = a_2 = 4; \quad a_k = a_{k-2} + 2^{k-2}, \quad k = 3, 4, 5, \cdots \\ &a_k = (2^k - (-1)^k)/3 + 3; \quad k = 1, 2, 3, \cdots \end{aligned} \tag{3}$$

Формула (3) позволяет найти мощность *регулярного множества* $\tilde{A}_k^*$ для любого k.

В данной постановке задачи представляют интерес те квадраты, которые заканчиваются на 0, 025, 225 и 625 (других окончаний длиной в три цифры в нулевом классе не существует), эти множества обозначим через $E_k(0), E_k(025), E_k(225)$ *и* $E_k(625)$, а их мощности – соответственно через $e_k(0)$, $e_k(025)$, $e_k(225)$ $e_k(625)$ при $k \geq 3$.

Нетрудно убедиться, что

$$e_k(0) = A_{k-2}, \quad e_k(025) = 10^{k-3}, \quad e_k(225) = 10^{k-3}; \quad k = 3, 4, 5, \cdots$$

Через c_k обозначим следующее число:

$$c_k = e_k(025) + e_k(225) + e_k(625); \quad k = 3, 4, 5, \cdots$$

Ниже приводятся рекуррентные соотношения между элементами $c_k;\ k = 3, 4, 5, \cdots$, а также явное выражение c_k через k

$$\begin{aligned} &c_3 = 3; \quad c_4 = 22; \quad c_k = 2 \cdot 10^{k-3}, \quad k = 5, 6, \cdots \\ &c_k = 2^{k-5}((5^{k-1} - (-1)^{k-1})/3 + 3 + (-1)^{k-1}; \quad k = 3, 4, 5, \cdots \end{aligned} \tag{4}$$

Формула (4) позволяет найти мощность множества $r \equiv 0 (mod\ 5)$ (кроме $E_k(0)$) для любого k.

Ниже приводятся рекуррентные соотношения между элементами $A_k;\ k = 1, 2, 3, \cdots$, а также явное выражение A_k через k:

$$A_1 = 6, \quad A_2 = 22; \quad A_k = A_{k-2} + u_k; \quad u_k = a_k \cdot b_k + c_k; \ k = 3, 4, 5, \ldots$$

$$u_k = ((2^k - (-1)^k)/3 + 3) \cdot 5^{k-1} + 2^{k-5}((5^{k-1} - (-1)^{k-1})/3 + 3 + (-1)^{k-1}); \ k = 3, 4, 5, \ldots$$

$$A_k = A_1 + 1/36((5^2(10^{k-1} - 1) + 5^3(5^{k-1} - 1) + 11(2^{k-1} - 1)); \ k = 1, 3, 5, \ldots \tag{5.1}$$

$$A_k = A_2 + 1/18((5^3(10^{k-2} - 1) + 2 \cdot 5^3(5^{k-2} - 1) + 7(2^{k-2} - 1)); \ k = 2, 4, 6, \ldots \tag{5.2}$$

Формулы (5.1) и (5.2) позволяют найти мощность множества $\tilde{A}_k$ для любого k.

Теперь можно сформулировать следующие предельные теоремы.

Теорема 1. *Отношение мощности регулярного множества* $\tilde{A}_k^*$ *к* 10^k *при стремлении* k *к бесконечности есть постоянное число, равное* $1/15 = 0.06(6)$.

Теорема 2. *Отношение мощности множества* $r \equiv 0(mod\ 5)$ *(кроме* $E_k(0)$*)* *к* 10^k *при стремлении* k *к бесконечности есть постоянное число, равное* $1/480$.

Теорема 3. *Отношение мощности множества* $\tilde{A}_k$ *к* 10^k *при стремлении* k *к бесконечности есть постоянное число, равное* $5/72 = 0.0694(4)$.

Ниже приводятся рекуррентные соотношения между элементами a_k; $k = 3, 4, 5, \cdots$, а также явное выражение a_k через k:

$$a_5 = a_6 = 1; \quad a_k = a_{k-2} + 2 \cdot 5^{k-7}; \quad k = 5, 6, 7 \cdots$$
$$a_k = (5^{k-5} - 5^{\delta(k)})/12 + 1; \quad k = 5, 6, 7, \cdots \quad \text{где} \quad \delta(k) = (1 + (-1)^k)/2. \tag{7}$$

Формула (7) позволяет найти мощности множеств $E_k(0625)$ и $E_k(5625)$, т. е. $E_k(6\,25)$ для любого k.

Теперь сформулируем задачу нахождения минимальных элементов (наименьший неотрицательный вычет − первый элемент арифметической прогрессии) ненулевых классов. Дадим следующее определение.

Определение 1. *Всякий минимальный элемент* r *одного из ненулевых классов, содержащихся в* $\tilde{A}_k^*$, $k \geq 1$, *который входит в представление минимальных элементов других ненулевых классов в виде*

$$S(r) = d \cdot n + r, \quad d \in D = \{d_k;\ k \geq 3\}; \quad n = 1, 2, 3, \cdots$$

называется порождающим числом $\tilde{A}_k^*$.

Справедлива следующая обобщенная лемма.

Лемма 1. *При неограниченном возрастании длины окончания квадрата* k, *числа*

$$\begin{aligned}
&1 \text{ и } 9, \text{ с разностью } d = d_3 = 40;\\
&4 \text{ и } 36, \text{ с разностью } d = d_5 = 160;\\
&16 \text{ и } 144, \text{ с разностью } d = d_7 = 640;\\
&64 \text{ и } 576, \text{ с разностью } d = d_9 = 2560;\\
&256 \text{ и } 2304, \text{ с разностью } d = d_{11} = 10240
\end{aligned}$$

являются порождающими числами $\tilde{A}_k^*$.

Полученная закономерность дает возможность сформулировать следующую основную теорему в этом направлении.

Теорема 4. *При неограниченном возрастании длины окончания квадрата* k*числа*

$$1 \cdot 4^m (mod\ d_k) \text{ и } 9 \cdot 4^m (mod\ d_k),$$

и только они с разностью $d = d_{2m+3} = 4^{m+1} \cdot 10$; $m = 0, 1, 2, \cdots$ *являются порождающими числами* $\tilde{A}_k^*$.

Теперь сформулируем задачу нахождения минимальных элементов $E_k(625)$. Дадим следующее определение.

Определение 2. *Всякий минимальный элемент r, содержащийся в $E_k(625)$ $k \geq 3$, который входит в представление других минимальных элементов, в виде*

$$S(r) = d \cdot n + r, \ \textit{с разностью} \ d = 2^{\delta} \cdot 5^k; \quad k \geq 3; \quad \delta = \{0, 3\}; \quad n = 1, 2, 3, \cdots$$

называется порождающим числом $E_k(625)$.

Справедлива следующая лемма.

Лемма 2. *При неограниченном возрастании длины окончания квадрата kчисла*

$$39 \ \textit{и} \ 351, \ \textit{с разностью} \ d = 5^4;$$

$$r_1 = 14.39(mod\ 50) \ \textit{и} \ r_2 = 1.76(mod\ 125), \ \textit{с разностью} \ d = 2^3 \cdot 5^3$$

являются порождающими числами $E_k(625)$.

Исследования потвердили, что имеет место следующая теорема.

Теорема 5. *При неограниченном возрастании длины окончания квадрата kчисла*

$$39 \ \textit{и} \ 351, \ \textit{с разностью} \ d = 5^4;$$

$$r_1 \equiv 14.39(mod\ 50) \ \textit{и} \ r_2 \equiv 1.76(mod\ 125), \ \textit{с разностью} \ d = 2^3 \cdot 5^3,$$

и только они являются порождающими числами $E_k(625)$.

Следствие 1. *Минимальные элементы $E_k(0625)$ определяются формулами*

$$S_1(r) \equiv (625n + 39) mod\ 5^{k-4}; \ n \in \{0, 3, 5, 8(mod\ 10) \& 14.39(mod\ 50)\}.$$

$$S_2(r) \equiv (1000n + r_1) mod\ 5^{k-4}; \quad n = 1, 2, 3, \cdots$$

Следствие 2. *Минимальные элементы $E_k(5625)$ определяются формулами*

$$S_1(r) \equiv (625n + 351) mod\ 5^{k-4}; \ n \in \{0, 2, 5, 7(mod\ 10) \& 1.76(mod\ 125)\}.$$

$$S_2(r) \equiv (1000n + r_2) mod\ 5^{k-4}; \quad n = 1, 2, 3, \cdots$$

Замечание: $S_1(r) \cap S_2(r) \neq \emptyset$.

Таким образом, согласно полученным результатам, для чисел натурального ряда структура окончаний их квадратов известна и поэтому, в частности, для (2), при $k \geq 3$, $10^{k-1} < N < 10^k$, из равенства $N = x^2 - y^2$ и $x \neq (N + 1)/2$ следует

$N = n_N d_k + r_N$, где $r_N -$ остаток от деления N на d_k,

$x^2 \equiv (n_x d_k + r_x)\ mod\ 10^k$, $x^2 = 10^k x_0 + n_x d_k + r_x$,

где $r_x -$ минимальный элемент строки числа x;

$y^2 = (n_y d_k + r_y) mod\ 10^k$, $y^2 = 10^k y_0 + n_y d_k + r_y$,

где $r_y -$ минимальный элемент строки числа y;

$x^2 \equiv \big((n_N + n_y) d_k + r_N + r_y\ \big)\ mod\ 10^k$,

при $x_0 = y_0$; $r_N = r_x - r_y$; $n_N = n_x - n_y$ не исключены и другие случаи,

например, $r_N = d_k + r_x - r_y$; и/или $x_0 = y_0 + 1$; $n_N = (n_x + 5^{k-1} - 1) - n_y$.

Рассмотрим сравнения

$$x^2 \equiv \left((n_N + n_y)d_k + r_N + r_y\right) mod\ 10^k; \quad (8)$$

$$y^2 \equiv \left(n_y d_k + r_y\right) mod\ 10^k. \quad (9)$$

В этих выражениях единственное неизвестное $-n_y$. Так как $n_N + n_y \leq 5^k - 1$, то задача нахождения сомножителей $N = p \cdot q$, $1 < \text{p} < q$, в общем случае, сводится к перебору по n_y в промежутке $0 \leq n_y \leq 5^k - n_N - 1$.

Таким образом, при $0 \leq n_y < C$ или $5^k - n_N - C < n_y \leq 5^k - n_N - 1$, где C – предел перебора на базе современной технологии, число $N = p \cdot q$ криптосистемы с открытыми ключами RSA раскрываемо независимо от его величины.

Согласно теории сравнения второй степени по составному модулю исследованы и решены сравнения вида [8]

$$x^2 \equiv a(mod\ 2^k), (a, 2) = 1 \text{ и } x^2 = a(mod\ 5^k), \ (a, 5) = 1,$$

которые совместно дают решения сравнения вида

$$x^2 \equiv a(mod\ 10^k), (a, 10) = 1; \quad k = 1, 2, \cdots, 8.$$

Пусть

$x = f_i(n_y)$ – некоторое решение сравнения $x^2 \equiv ((n_N + n_y)d_k + r_N + r_y)\ mod\ 10^k$

и $y = g_j(n_y)$ – некоторое решение сравнения$y^2 \equiv \left(n_y d_k + r_y\right) mod\ 10^k$.

Таким образом, задача сводится к отысканию положительного целочисленного решения следующих уравнений:

$$f_i^2(n_y) - g_j^2(n_y) - N = 0; \quad i, j \in \{1, 2, \cdots, 8\}.$$

Алгоритм разложения для $\tilde{A}_k^*$

Шаг 1. Вычислить k из условия $10^{k-1} < N < 10^k$.

Шаг 2. Представить N в виде $N = n_N \cdot d_k + r_N$, $0 < r_N < d_k$.

Шаг 3. Найти минимальные элементы r_x и r_y такие, чтобы

$$r_N = r_x - r_y \text{ (либо } r_N = d_k + r_x - r_y).$$

Шаг 4. Решить сравнение (8).

Шаг 5. Пусть $x = f_i(n_y)$ – некоторое решение сравнения (8).

Шаг б. Решить сравнение (9).

Шаг 7. Пусть $y = g_i(n_y)$ – некоторое решение сравнения (9).

Шаг 8. Найти целочисленное решение уравнений

$$f_i^2(n_y) - g_j^2(n_y) - N = 0; \quad i,j \in \{1,2,\cdots,8\}.$$

Шаг 9. Если $n_y \in Z_+$, то $N - составное,$ иначе $N - простое.$

Объединение представлений (2), (6), $E(0)$ и $E(25)$ для окончательного уточнения алгоритма разложения на множители и проектирования специального процессора для этой цели находится в стадии разработки.

В заключение выражаю глубокую признательность И. Д. Заславскому за полезные обсуждения и предложения.

Ереванский научно-исследовательский
институт математических машин

Ս. Լ. Համբարյան

Պարզ արտադրիչների վերլուծման Ֆերմայի մեթոդի ընդհանրացումը

Դիցուք պահանջվում է վերլուծել արտադրիչների $n = \mathrm{p} \cdot q,\ 1 < p < q$ կենտ թիվը: Այդ դեպքում տեղադրելով.

$$x = (p+q)/2 \qquad և \qquad y = (p-q)/2,$$

n թիվը կներկայացվի երկու բնական թվերի քառակուսների տարբերության տեսքով.

$$x^2 = y^2 + n, \qquad 0 < y < x < n: \tag{1}$$

Ֆերմայի մեթոդը կայանում է երանում, որ փնտրվում են x-ի և y-ի այնպիսի արժեքներ, որոնք բավարարում են (1) հավասարմանը, այսինքն՝ նրա աջ մասը պետք է լինի լրիվ քառակուսի:

Լրիվ քառակուսու վերջին երկու նիշերը կարող են լինել՝ $00, 25, al, a4, a9$, կամ $b6$, որտեղ a-ն զույգ, իսկ b-ն կենտ նիշ է:

Այս աշխատանքում Ֆերմայի մեթոդը ընդհանրացվում է լրիվ քառակուսու վերջին ցանկացած k քանակով նիշերի րնդգրկմամբ՝ հաշվի առնելով n թվի բոլոր նիշերը.

$$10^{m-1} < n < 10^m, \qquad r \equiv x^2 (mod 10^k); \quad m \le k = 1,2,3\cdots$$

Աշխատանքում ապացուցված են մի քանի սահմանային թեորեմներ քառակուսային մնացքների վերաբերյալ:

Քառակուսային մնացքները ներկայացվում են պարզ մաթեմատիկական բանաձևերի օգնությամբ, որը հնարավորություն է տալիս էապես կրճատել արտադրիչների վերլուծման ալգորիթմի գործողությունների քանակը (հատարկման ծավալը):

Литература

1. Кибернетический сборник. Новая серия. Вып. 23. М.: Мир, 1986.
2. *Pollard J.* - Proc. Cambridge Philos. Soc. 1974. V. 76.
3. *Diffie W., Hellman. M. B.* - IEEE Trans.Informat. Theory, 1976. V. IT-22. Nov.
4. *Rivest R. L, Shamir A., Adleman. L.* - CACM. 1978. V. 21, № 2. Feb.
5. *Кнут. Д.* Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М: Мир, 1977.
6. *Schdnhage A., StrassenV.* - Computing, Archiv fur elektronisches Rech- nen. № 7. 1971.
7. *Арнольд. И. В.* Теория чисел. М. Учпедгиз. 1939.
8. *Виноградов. И. М.* Основы теории чисел. М.-Л.: Гос. изд-во техн.- теоретич. лит., 1952.
9. *Трост. Э.* Простые числа. М.: Гос. изд-во физ.-мат. лит., 1959.