КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

M. Semotiuk

THE PRECISE METHOD FOR FACTORING COMPOSITE NUMBERS

We propose a method of factoring composite numbers on the basis of digit by digit makes it lyayuschy finite number of steps (iterations) equal to log2 N / 2 to find the factors due to number-theoretic concepts of number systems. The method allows reshat Diophantine equations, as well as get an accurate test for primality.
Key words: factorization, number theoretic transform, number systems, convolution.

Запропоновано метод факторизації складних чисел, що дозволяє за скінчене число ітерацій, рівному log2N/2, знайти співмножники, вирішувати діофантові рівняння, перевіряти простоту чисел.
Ключові слова: факторизація, теоретико-числове перетворення, системи числення, згортка.

Предложен метод факторизации составных чисел, позволяющий за конечное число итераций, равное log2N/2, найти сомножители, решать диофантовы уравнения, проверять простоту чисел.
Ключевые слова: факторизация, теоретико-числовое преобразование, системы счисления, свертка.

УДК 521(075)

М.В. СЕМОТЮК

О ТОЧНОМ МЕТОДЕ ФАКТОРИЗАЦИИ СОСТАВНЫХ ЧИСЕЛ

Введение. Отыскание простых множителей натурального числа называют для краткости «факторизацией». Факторизация больших чисел – чрезвычайно трудоемкая задача, даже с помощью электронных вычислительных машин.

Пусть составное число равно

$$C = a*b\ . \qquad (1)$$

Полагая, что $a = x + y$, $b = x - y$, имеем

$$C = x^2 - y^2.$$

П. Ферма – один из создателей теории чисел в своих вычислениях пользовался, несомненно, этим свойством. Приём, основанный на этом свойстве, называют «факторизацией по разности квадратов» и требует подбора квадратов чисел x и y.

Как приём факторизации также можно использовать известный алгоритм Эвклида для отыскания наибольшего общего делителя двух чисел. Однако он тоже требует подбора подходящего числа.

Возникает вопрос – можно ли сразу, по виду числа C, определить такое вспомогательное число точно, без использования процедур подбора. Постараемся ответить на этот вопрос положительно. Для этой цели рассмотрим понятие числового множества как структура.

Общая часть. Под структурой или решеткой [1 – 4] понимают частично упорядоченное множество, где каждое двухэлементное подмножество имеет точные верхнюю и нижнюю грани (необходимо единственные). Отметим, что если это подмножество имеет только одну из точных граней, то его называют полуструктурой (верхней или нижней

в зависимости от того, какая из точных граней существует). При этом структура может быть получена из полуструктур, например, путем пересечения, вычитания нижней полуструктуры из верхней полуструктуры, либо каким-нибудь иным путем.

В качестве верхней и нижней грани такого множества, именуемой структурой и обозначаемой в дальнейшем $\mathbf{S}$, наиболее часто используют выражения вида

$$\sup\ \mathbf{S} = \sup\{a,b\} = \max(a+b),$$
$$\inf\ \mathbf{S} = \inf\{a,b\} = \min(a\cdot b).$$

Хотя эти выражения ограничивают мощность несущего множества, но, так или иначе, они связаны с операциями, заданными той или иной алгеброй. Желательно иметь одно «универсальное» несущее множество, на котором возможно было бы задать не одну единственную, следуя принципу замкнутости, алгебру, а некоторое их множество. Эта цель достигается, если точные грани структуры задать следующим образом [5]:

$$\begin{aligned}\sup\ \mathbf{S} &= \sup\{a,b\} = \max[(a*b)\bmod M] = M-1,\\ \inf\ \mathbf{S} &= \inf\{a,b\} = \min[\operatorname{int}_p(a*b)] = 0,\end{aligned} \tag{2}$$

где $*$ – знак произвольной алгебраической операции, результат которой ограничен сверху операцией по модулю M, а саму операцию по модулю будем рассматривать как некоторую функцию, зависящую от M; $\operatorname{int}_p(\,)$ – функция, определяемая как целая часть по отношению к числу p.

$$\operatorname{int}_p(x) = \operatorname{int}_1\left(\frac{x}{p}\right). \tag{3}$$

Если $p=1,$ то эта функция принимает традиционные представления, в другом случае она отмечает тот факт, что целая часть существует не только при делении целых чисел, но и дробных и т. п.

Из последнего определения следует, что структура, заданная выражениями (2), получена из двух полуструктур, верхняя грань одной из которых задана модулем M, а нижняя – модулем M_1. Такую структуру, задаваемую выражениями (2), в дальнейшем будем называть машинной структурой, понимая под этим термином не технический термин, а математический. Из последних выражений следует, что, с одной стороны, такое определение структуры достаточно полно согласуется с теми числовыми множествами, которые задаются разрядной сеткой ЭВМ. С другой стороны, существует достаточно основательно разработанная математическая теория вычетов, которая и составляет фундаментальную базу теоретико-числовых подходов в математике. Основными аксиоматическими положениями этой теории являются алгебры вычетов по одному и тому же самому модулю, такие как кольцо вычетов, группа вычетов, поле вычетов, поле Галуа, а также пространства, оболочки, вычетов, либо над полем вычетов, или групповые алгебры вычетов и их конструкции.

Однако остается не выясненным вопрос, чем придется поступиться и с какими трудностями придется сталкиваться при использовании на практике определенных таким образом машинных структур. Для этого рассмотрим следующий случай.

Пусть кольцо вычетов по единственному модулю задано алгеброй вида

$$Z_m =< \mathbf{S}, +, \cdot, \mathbf{0}, \mathbf{1} >, \tag{4}$$

где Z_m – здесь и далее кольцо вычетов по единственному модулю M; $\mathbf{S}$ – несущее множество, представляющее собой структуру, заданную выражениями (3, 4), в которых $p=1$; $+,*$ – основные операции кольца; $\mathbf{0},\mathbf{1}$ – нейтральные элементы операций сложения и умножения соответственно.

При этом формально считается, что $\mathbf{0}\neq\mathbf{1}$, т. е. нейтральные элементы операции сложения и умножения различны. Но, на практике, это условие не всегда может быть выполнимо, например, дополнительный код в ЭВМ, а в других случаях является даже необходимым условием, например, булева алгебра. Если положить, что $\mathbf{0}=\mathbf{1}$, т. е. нейтральные элементы операций сложения и умножения совпадают и равны единице, то возникает двойственность. Действительно, пусть

$$a + a' = \mathbf{1},$$

где a' – обратный элемент a по отношению к операции сложения (дополнение до 1).

Тогда для кольца (4) $a + a' = M + 1$. Далее, используя правила де Моргана, имеем

$$(a' * b')' = M + 1 - (M + 1 - a)(M + 1 - b) =$$
$$= M + 1 - M^2 - 2M - 1 + Ma + a + Mb + b - ab.$$

Окончательно, для кольца вычетов по модулю M в соответствии с верхней гранью структуры (3) получаем

$$(a' * b')' \overset{Z_m}{=\!=} a + b - ab, \tag{5}$$

где $\overset{Z_m}{=\!=}$ означает тот факт, что вычисления выполняются в кольце вычетов Z_m и как в левой части равенства, так и в правой, ограничены сверху величиной модуля M и принадлежат множеству $\mathbf{S}$.

Полученное выражение известно в литературе как звездное произведение [6]. Таким образом, установлено, что операции кольца вычетов Z_m (сложение и умножение), заданные на структуре, могут быть двойственны, т. е. могут быть определены двумя различными путями, либо, при одних и тех же условиях, возможно получение двух различных результатов одной и той же операции. В заключение заметим, что результаты вычислений в алгебрах вычетов и обычных алгебрах могут не совпадать, если не будут приняты соответствующие меры их коррекции.

Рассмотрим еще один частный случай звездного произведения

$$a' * b = (M - a) * b = M * b - a * b. \tag{6}$$

Очевидно, что такое составное число и есть подходящим числом для алгоритма Эвклида. Действительно пусть $C = a * b = 7 * 5 = 35$, $M = 10$. Тогда согласно (6) имеем $M * b - a * b = 10 * 5 - 7 * 5 = 15$, а числа 35 и 15 имеют общий множитель 5. С другой стороны

$$-C = -(a * b) = M^2 - (a * b), \tag{7}$$

представляет собой дополнение произведения $a * b$ до модуля M^2 и отличается в кольце вычетов по модулю M^2 от (7) на величину $M*b$, которую следует вычесть в выражении (7) для того чтобы получить верный результат. В машинной арифметике этот прием называют коррекцией умножения.

Далее полагая, что $M = p^N$ и $M^2 = p^{2N}$ имеем для кольца вычетов по модулю M два числа: $-C \overset{Z_m}{\equiv} p^k * b - (a * b)$, $C \overset{Z_m}{\equiv} (a * b)$.

Очевидно, величину $p^n * b$ вычислить невозможно, так как неизвестно b. Однако, полагая, что p – основание некоторой системы счисления, а модуль кольца равен p^N, имеем

$$\begin{gathered} -C \overset{Z_m}{\equiv} -(a * b) = a' * b, \\ C \overset{Z_m}{\equiv} (a * b), \\ M = p^N, \end{gathered} \tag{8}$$

где a' дополнение до модуля числа a.

Отсюда следует, что мы имеем точные младшие части двух разных чисел с разрядностью N, которые имеют общий множитель. Заметим, что к системе (8) применим алгоритм Эвклида, если вычисления выполнять в кольце вычетов Z_m. Однако в этом случае некоторого перебора вариантов не избежать. Покажем теперь, что существует точный метод факторизации составных чисел, не требующий перебора вариантов и сформулируем следующее утверждение.

Утверждение 1. Для любого составного числа C, которое представляет собой произведение вида $C = a * b$, где a и b простые числа больше 2, в силу единственности разложения его на простые множители, существует точный вычислительный метод его факторизации с конечными вычислительными затратами. Докажем это утверждение.

Для этой цели сначала рассмотрим следующую теорему, которая является фундаментальной теоремой обобщенных теоретико-числовых преобразований. Ее фундаментальный характер обусловлен тем, что с ее помощью доказывается весь комплекс теорем этих преобразований без исключения. Доказательство теоремы приведено в [5].

Пусть алгебра вида $Z_m = <\mathbf{S}, +, \cdot, \mathbf{0}, \mathbf{1}>$ где $(\mathbf{0} \neq \mathbf{1})$ и $\mathbf{S} \in \mathbf{Z}$ – структура (решетка) имеющая $\sup \mathbf{S} = \max[(a * b) \bmod M] = s^p - 1$ и $\inf \mathbf{S} = \min[\mathrm{int}_p (a * b)] = 0$, представляет собой кольцо вычетов Z_m с единицей, в котором своими аргументами задана степенная зависимость $y = s^x$.

Тогда для $\forall s \in \mathbf{S}, \forall p \in \mathbf{N}, \forall x = \overline{0,N}$ и $\forall p << N$ существует такое число M, равное $M = \sum_{m=0}^{N-1} s^m < \sup \mathbf{S}$, при котором в кольце вычетов Z_m имеет место следующее соотношение:

$$s^{(x) \bmod N} \overset{Z_m}{=\!=} (s^x) \bmod M, \tag{9}$$

где $\overset{Z_m}{=\!=}$ – обозначает «имеет место», равно или сравнимо в кольце вычетов Z_m в общем случае не всегда совпадающее с известным понятием «сравнение по модулю» в силу разных значений модуля в левой и правой частях выражения. В правой части целое выражение, ограниченное модулем M, а в левой части ограничен только показатель степени модулем N. Модуль M при этом есть функция от переменных s и N. $M = f(s, N)$.

Полагая теперь, что главное значение числовой степенной последовательности находится на закрытом интервале $[0, p-1] = [0, N-1]$, а $\sup \mathbf{S} = M = \sum_{m=0}^{N-1} s^m$ – модуль кольца Z_m, определим формально следующее преобразование, заданное на структуре $\mathbf{S}$

$$X(k) \overset{Z_m}{=\!=} \sum_{i=0}^{N-1} x(i) s^{-(ki) \bmod N}, \tag{10}$$

$$x(i) \overset{Z_m}{=\!=} \frac{1}{N} \sum_{k=0}^{N-1} X(k) s^{(ki) \bmod N}, \tag{11}$$

$$M = \sum_{m=0}^{N-1} s^m,$$

где N – некоторое число из множества $\mathbf{N}$; $x(i)$, $X(k)$ – числовые последовательности, представляющие оригинал и изображение соответственно; s – некоторое число, в общем случае комплексное; i, k – номера (индексы) компонент последовательностей.

Выражение (10) представляет собой прямое преобразование, выражение (11) – обратное.

Это преобразование в работе названо обобщенным теоретико-числовым преобразованием или S-преобразованием (преобразование задано на структуре, решетке S). Обобщенный характер этого преобразования вытекает из того, что модуль кольца $M = \sum_{m=0}^{N-1} s^m$ не всегда простое число и разлагается на множители, которые в свою очередь могут быть модулями преобразования Ферма, Мерсена, Гаусса и т. д.

Покажем одно важное свойство этого преобразования. Для этой цели взве-

сим оригинал в выражении (10) последовательностью вида

$$w(i) = \{0, 1, 0,..., 0\}, \qquad (12)$$

вычислим S-преобразование и сузим верхнюю и нижнюю грани структуры следующим образом:

$$\{\text{int}(*)\} \bmod s.$$

Тогда будем иметь

$$X(k) \overset{Z_m}{=} \{\text{int}[\sum_{i=0}^{N-1} x(i)w(i)s^{-(ki)\bmod N}]\} \bmod S,$$

$$x(i) \overset{Z_m}{=} \frac{1}{N}\sum_{k=0}^{N-1} X(k)s^{(ki)\bmod N}, \qquad (13)$$

$$M = \sum_{m=0}^{N-1} s^m.$$

Проанализируем (13). Из выражения (11) следует, что

$$w(i) = 1 \text{ при } i = 1 \text{ и } w(i) = 0 \text{ если } i \neq 1.$$

Тогда $x(i)w(i) = x(1)$ если $i = 1$, и $x(i)w(i) = 0$ если $i \neq 1$.

И, следовательно, (13) можно переписать

$$X(k) \overset{Z_m}{=} \{\text{int}[\sum_{i=1} x(1)w(1)s^{-(k)\bmod N}]\} \bmod s,$$

$$x(i) \overset{Z_m}{=} \sum_{k=0}^{N-1} X(k)s^{(ki)\bmod N}, \text{ только для } i = 1, \qquad (14)$$

$$M = \sum_{m=0}^{N-1} s^m.$$

Теперь полагая в (14) $s = p$, где p – основание системы счисления, $i = 1$, $x(1) = A$, где A – число, принадлежащее множеству **N**, для которого

$$\sup \mathbf{N} = M = \sum_{m=0}^{N-1} p^m$$

(т. е. верхняя грань множества **N** совпадает с модулем кольца вычетов Z_m) и, учитывая, что $w(1) = 1$, получаем

$$X(k) \overset{Z_m}{=} \{\text{int}[A \cdot p^{-(k)\bmod N}]\} \bmod p,$$

$$A \overset{Z_m}{=} \sum_{k=0}^{N-1} X(k)s^{(ki)\bmod N}, \text{ только для } i = 1, \qquad (15)$$

$$M = \sup \mathbf{N} = \sum_{m=0}^{N-1} p^m.$$

Из выражений (15) следует, что представление чисел в какой-либо системе счисления является частным случаем обобщенного теоретико-числового преобразования, которое для краткости назовем **P**-преобразованием [7]. Отсюда можно сделать вывод, что позиционные системы счисления обладают всеми свойствами представлений в алгебраическом смысле этого слова. При этом, представ-

ляющим пространством, в котором описывается любое число из множества **N**, является пространство, построенное над кольцом вычетов Z_m. $X(k)$ – суть цифры в разрядах системы счисления с основанием p, в которой представляется это число и которые теперь можно определить в любом интересующем нас порядке. Отсюда следует главный вывод о таком представлении − значение цифры в любом разряде любой системы счисления не зависит от значения цифры в других разрядах этого представления. Например, число 37 и нас интересует значение цифры во втором разряде этого числа, представленного двоичной системой счисления. Его двоичный код 100101. Выполним преобразование для индекса $k = 2$.

$$X(2) \overset{Zm}{=} \{\mathrm{int}[37 * 2^{-(2)\mathrm{mod}N}]\} \mathrm{mod} 2 = 1.$$

Для $k = 3$, $X(3) \overset{Zm}{=} \{\mathrm{int}[37 * 2^{-(3)\mathrm{mod}N}]\} \mathrm{mod} 2 = 0$ и т. д. Таким образом, существует возможность создать «теорию» одного разряда.

Далее, теоретико-числовое преобразование является изоморфным преобразованием и для него существует ряд теорем, в том числе и теорема о свертке изображения.

Поэлементное произведение двух последовательностей-оригиналов в кольце вычетов Z_m приводит к свертке их изображений:

$$x(i) \cdot y(i) \xrightarrow{Z_m} X(k) * Y(k), \qquad (16)$$

где * – (здесь и далее) обозначение свертки, как оператора; $\xrightarrow{Z_m}$ – обозначение означающее « приводит» в кольце вычетов Z_m к такой-то зависимости.

Действие этой теоремы распространяется и на частные случаи этого преобразования. Оно имеет место и в нашем случае. Действительно, если в (16) $X(k)$ и $Y(k)$ – суть цифры некоторой системы счисления ($X(k) = a_k$, $Y(k) = b_k$), а размерность преобразования увечим до $2N$, чтобы получить апериодическую свертку, имеем в матричной записи

$$\begin{bmatrix} a_0 & 0 & 0 & 0 & 0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & 0 & 0 & 0 & 0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 & 0 \\ a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \\ S_7 \end{bmatrix} = \begin{bmatrix} a_0 * b_0 \\ a_0 * b_1 + a_1 * b_0 \\ a_0 * b_2 + a_1 * b_1 + a_2 * b_0 \\ a_0 * b_3 + a_1 * b_2 + a_2 * b_1 + a_3 * b_0 \\ a_1 * b_3 + a_2 * b_2 + a_3 * b_1 \\ a_2 * b_3 + a_3 * b_2 \\ a_3 * b_3 \\ 0 \end{bmatrix}, \qquad (17)$$

где S_k – коэффициенты свертки, а для примера $N = 3$.

Очевидно также, что коэффициенты свертки S_k не совпадают с цифрами C_k в разрядах представления числа C в той или иной системе счисления, по-

скольку значения этих коэффициенты превышают основание системы счисления, т. е. $S_k > p$.

Однако значения C_k можно вычислить, осуществив сначала обратное, а затем прямое **P**-преобразование в соответствии с выражениями (15).

$$c(k) \overset{Zm}{=\!=} \{\mathrm{int}[(\sum_{k=0}^{N-1} X(k) p^{(ki) \bmod N}) \cdot p^{-(k) \bmod N}]\} \bmod p,$$

или учесть влияние переносов традиционным способом с учетом возможностей **P**-преобразования о независимости образования цифр в разрядах системы счисления следующим образом:

$$c_0 = (S_0) \bmod p,$$
$$c_1 = (S_1 + \mathrm{int}_{p^1} S_0) \bmod p,$$
$$c_2 = (S_2 + \mathrm{int}_{p^2} S_0 + \mathrm{int}_{p^2} S_1) \bmod p,$$
$$c_3 = (S_3 + \mathrm{int}_{p^3} S_0 + \mathrm{int}_{p^3} S_1 + \mathrm{int}_{p^3} S_2) \bmod p,$$
$$c_4 = (S_4 + \mathrm{int}_{p^4} S_0 + \mathrm{int}_{p^4} S_1 + \mathrm{int}_{p^4} S_2 + \mathrm{int}_{p^4} S_3) \bmod p,$$
$$c_5 = (S_5 + \mathrm{int}_{p^5} S_0 + \mathrm{int}_{p^5} S_1 + \mathrm{int}_{p^5} S_2 + \mathrm{int}_{p^5} S_3 + \mathrm{int}_{p^5} S_4) \bmod p,$$
$$c_6 = (S_6 + \mathrm{int}_{p^6} S_0 + \mathrm{int}_{p^6} S_1 + \mathrm{int}_{p^6} S_2 + \mathrm{int}_{p^6} S_3 + \mathrm{int}_{p^6} S_4 + \mathrm{int}_{p^6} S_5) \bmod p,$$
$$c_7 = (S_7 + \mathrm{int}_{p^7} S_0 + \mathrm{int}_{p^7} S_1 + \mathrm{int}_{p^7} S_2 + \mathrm{int}_{p^7} + \mathrm{int}_{p^7} S_4 + \mathrm{int}_{p^7} S_5 + \mathrm{int}_{p^7} S_6) \bmod p,$$

где $\mathrm{int}_{p^k} S_l$ – перенос в k-й разряд от l-го коэффициента свертки.

Поскольку из (8) мы имеем только N точных разрядов этих чисел, то размерность свертки можно сократить до N

$$\begin{bmatrix} a_0 & 0 & 0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_2 & a_1 & a_0 & 0 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} a_0 * b_0 \\ a_0 * b_1 + a_1 * b_0 \\ a_0 * b_2 + a_1 * b_1 + a_2 * b_0 \\ a_0 * b_3 + a_1 * b_2 + a_2 * b_1 + a_3 * b_0 \end{bmatrix}$$

$$c_0 = (S_0) \bmod p, \qquad (18)$$
$$c_1 = (S_1 + \mathrm{int}_{p^1} S_0) \bmod p,$$
$$c_2 = (S_2 + \mathrm{int}_{p^2} S_0 + \mathrm{int}_{p^2} S_1) \bmod p,$$
$$c_3 = (S_3 + \mathrm{int}_{p^3} S_0 + \mathrm{int}_{p^3} S_1 + \mathrm{int}_{p^3} S_2) \bmod p.$$

Запишем выражения (18) для первого числа из (8) через дополнение a' числа a

$$a' = M - a.$$

Тогда

$$\begin{bmatrix} a'_0 & 0 & 0 & 0 \\ a'_1 & a'_0 & 0 & 0 \\ a'_2 & a'_1 & a'_0 & 0 \\ a'_3 & a'_2 & a'_1 & a'_0 \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{bmatrix} = \begin{bmatrix} a'_0 \cdot b_0 \\ a'_0 \cdot b_1 + a'_1 \cdot b_0 \\ a'_0 \cdot b_2 + a'_1 \cdot b_1 + a'_2 \cdot b_0 \\ a'_0 \cdot b_3 + a'_1 \cdot b_2 + a'_2 \cdot b_1 + a'_3 \cdot b_0 \end{bmatrix},$$

$$c'_0 = (S'_0) \bmod p,$$

$$c'_1 = (S'_1 + \text{int}_{p^1} S'_0) \bmod p,$$

$$c'_2 = (S'_2 + \text{int}_{p^2} S'_0 + \text{int}_{p^2} S'_1) \bmod p,$$

$$c'_3 = (S'_3 + \text{int}_{p^3} S'_0 + \text{int}_{p^3} S'_1 + \text{int}_{p^3} S'_2) \bmod p,$$

где c'_i, S'_i – суть цифры соответствующих дополнений чисел *c* и *S*.

Теперь найдем разность между вторым и первым числом выражения (8)

$$\begin{bmatrix} a_0 - a'_0 & 0 & 0 & 0 \\ a_1 - a'_1 & a_0 - a' & 0 & 0 \\ a_2 - a'_2 & a_1 - a'_1 & a_0 - a'_0 & 0 \\ a_3 - a'_3 & a_2 - a'_2 & a_1 - a'_1 & a_0 - a'_0 \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} S_0 - S'_0 \\ S_1 - S'_1 \\ S_2 - S'_2 \\ S_3 - S'_3 \end{bmatrix} = \begin{bmatrix} (a_0 - a'_0) \cdot b_0 \\ (a_0 - a'_0)_0 \cdot b_1 + (a_1 - a'_1) \cdot b_0 \\ (a_0 - a'_0) \cdot b_2 + (a_1 - a'_1) \cdot b_1 + (a_2 - a'_2) \cdot b_0 \\ (a_0 - a'_0)_0 \cdot b_3 + (a_1 - a'_1)_1 \cdot b_2 + (a_2 - a'_2) \cdot b_1 + (a_3 - a'_3) \cdot b_0 \end{bmatrix},$$

$$\begin{aligned} c_0 - c'_0 &= [S_0 - S'_0] \bmod p, \\ c_1 - c'_1 &= [S_1 - S'_1 + \text{int}_{p^1} (S_0 - S'_0)] \bmod p, \\ c_2 - c'_2 &= [S_2 - S'_2 + \text{int}_{p^2} (S_0 - S'_0) + \text{int}_{p^2} (S_1 - S'_1)] \bmod p, \\ c_3 - c'_3 &= [S_3 - S'_3 + \text{int}_{p^3} (S_0 - S'_0) + \text{int}_{p^3} (S_1 - S'_1) + \text{int}_{p^3} (S_2 - S_2)] \bmod p. \end{aligned} \quad (19)$$

Полагая, что p = 2 (т. е. система счисления двоичная) можно записать логические выражения для (19) следующим образом с учетом возможного переполнения:

$$\begin{bmatrix} S_0 - S'_0 \\ S_1 - S'_1 \\ S_2 - S'_2 \\ S_3 - S'_3 \\ S_4 - S'_4 \end{bmatrix} = \begin{bmatrix} (a_0 \oplus a'_0) \& b_0 \\ (a_0 \oplus a'_0) \& b_1 \oplus (a_1 \oplus a'_1) \& b_0 \\ (a_0 \oplus a'_0) \& b_2 \oplus (a_1 \oplus a'_1) \& b_1 \oplus (a_2 \oplus a'_2) \& b_0 \\ (a'_0 \oplus a_0) \& b_3 \oplus (a_1 \oplus a'_1) \& b_2 \oplus (a_2 \oplus a'_2) \& b_1 \oplus (a_3 \oplus a'_3) \& b_0 \\ (a_1 \oplus a'_1) \& b_3 \oplus (a_2 \oplus a'_2) \& b_2 \oplus (a_3 \oplus a'_3) \& b_1 \end{bmatrix}.$$

В правой части полученного равенства выражение $a_i \oplus a'_i$ в силу свойств двоичного дополнительного кода, для всех $i \neq 0$ равно 1, а при i = 0 равно 0. Тогда имеем

$$\begin{bmatrix} S_0 - S'_0 \\ S_1 - S'_1 \\ S_2 - S'_2 \\ S_3 - S'_3 \\ S_4 - S'_4 \end{bmatrix} = \begin{bmatrix} 0\&b_0 \\ 0\&b_1 \oplus 1\&b_0 \\ 0\&b_2 \oplus 1\&b_1 \oplus 1\&b_0 \\ 0\&b_3 \oplus 1\&b_2 \oplus 1\&b_1 \oplus 1\&b_0 \\ 1\&b_3 \oplus 1\&b_2 \oplus 1\&b_1 \end{bmatrix} \text{ или } \begin{bmatrix} S_0 - S'_0 \\ S_1 - S'_1 \\ S_2 - S'_2 \\ S_3 - S'_3 \\ S_4 - S'_4 \end{bmatrix} = \begin{bmatrix} 0 \\ b_0 \\ b_1 \oplus b_0 \\ b_2 \oplus b_1 \oplus b_0 \\ b_3 \oplus b_2 \oplus b_1 \end{bmatrix}.$$

Заметим, что матричные записи выражений здесь и выше, если говорить языком машинной арифметики, только иллюстрируют процесс образования частичных произведений. Точные значения цифр разрядов определяются всегда с учетом переносов

$$\begin{cases} c_0 - c'_0 = [0] \bmod p, \\ c_1 - c'_1 = [b_0 \oplus \operatorname{int}_{p^1}(S_0 - S'_0)] \bmod p, \\ c_2 - c'_2 = [b_1 \oplus b_0 \oplus \operatorname{int}_{p^2}(S_0 - S'_0) \oplus \operatorname{int}_{p^2}(S_1 - S'_1)] \bmod p, \\ c_3 - c'_3 = [b_2 \oplus b_1 \oplus b_0 \oplus \operatorname{int}_{p^3}(S_0 - S'_0) \oplus \operatorname{int}_{p^3}(S_1 - S'_1) \oplus \operatorname{int}_{p^3}(S_2 - S'_2)] \bmod p, \\ c_3 - c'_3 = [b_3 \oplus b_2 \oplus b_1 \oplus \operatorname{int}_{p^3}(S_1 - S'_1) \oplus \operatorname{int}_{p^3}(S_2 - S'_2) \oplus \operatorname{int}_{p^3}(S_3 - S'_3)] \bmod p. \end{cases} \quad (20)$$

Полученная запись (20) представляет собой систему уравнений, в которой каждое уравнение содержит только цифры соответствующих разрядов одного и того же числа b и переносов в эти же разряды. Решение этой системы не имеет каких-либо трудностей, поскольку эти уравнения представляют собой так называемую «хвостовую» рекурсию. Так из второго уравнения легко определяется b_0, из третьего уравнения b_1 и т. д. Такой метод решения обычно называют методом цифра за цифрой из-за того, что на каждом этапе определяется одна только цифра числа b. Отсюда следует, что действительно существует точный метод факторизации, требующий для своей реализации всего лишь $\log 2\ N/2$ шагов вычислений, где N – разрядность числа C в двоичной системе счисления.

Выводы. Впервые в практике теории чисел доказано существование точного метода факторизации составных чисел. Сам метод относится к классу методов цифра за цифрой и имеет конечное число шагов (итераций) для своей реализации равное $\log 2\ N/2$. Его применение на практике позволит решать многие задачи факторизации составных чисел в криптографии, решать диофантовые уравнения, а также создать точные тесты определения простых чисел.

1. *Фрид Э.* Элементарное введение в абстрактную алгебру. – М.: Мир, 1979. – 230 с.
2. *Скорняков Л.А*. Элементы алгебры. – М.: Наука, 1966. – 240 с.
3. *Поспелов Д.А*. Логические методы анализа и синтеза схем. – М.: Энергия, 1974. – 366 с.
4. *Корн Г., Корн Т*. Справочник по математике. – М.: Наука, 1973. – 632 с.
5. *Семотюк М.В*. Обобщенное теоретико-числовое преобразование. – Киев, 1994. – 30 с. (Препр. / НАН Украины, Ин-т кибернетики им. В.М. Глушкова; 94–6).
6. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1979. – 624 с.
7. *Семотюк М.В.* Теоретико-числовые представления систем счисления // УСиМ. – 2004. – № 5. – С. 36 – 42.

Получено 11.10.2011