КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

M. Semotyuk

AN ANALYTICAL METHOD FOR FACTORING COMPOSITE NUMBERS

Difficulties factoring composite numbers reduced to the fact, that in the ring of integers there is only one equation that represents is a product of the numbers. The use of residue rings modulo allows you to get the second equation. This significantly reduces the computational cost.
Key words: factorization, the residue ring modulo, the inverse elements.

Труднощі факторизації чисел зводяться до того, що в кільці цілих чисел існує одне рівняння, що представляє їх добуток. Використання кілець залишків по модулю дозволяє отримати друге рівняння.
Ключові слова: факторизація, кільце залишків по модулю, зворотні елементи.

Трудности факторизации чисел сводятся к тому, что в кольце целых чисел существует одно уравнение, представляющее их произведение. Применение колец вычетов по модулю позволяет получить второе уравнение.
Ключевые слова: факторизация, кольцо вычетов по модулю, обратные элементы.

УДК 512(075)

М.В. СЕМОТЮК

ОБ АНАЛИТИЧЕСКОМ 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 [1]. В работе [2] показано, что существует точный метод факторизации составных чисел, основанный на решении системы логических уравнений. Однако применение этого метода на практике сталкивается с трудностями решения этой системы уравнений на современных ЭВМ в силу использования большого количества весьма мелких логических операций. Однако, как и алгоритм Шора [3], он эффективен для факторизации чисел на квантовом компьютере.

Основная часть. Все трудности факторизации составных чисел исходят из того, что в кольце целых чисел Z существует всего лишь одно уравнение, представляющее факторизуемое число, вида

$$C = a \cdot b, \qquad (1)$$

где a и b – числа, из которых состоит это число. Однако в кольце вычетов Z_m можно получить второе уравнение. Тогда, согласно определению, в кольце вычетов Z_m [4] существуют обратные элементы по отношению операции сложения такие, что

$$a + a' \overset{Z_m}{=} 0, \quad b + b' \overset{Z_m}{=} 0,$$

m – модуль этого кольца вычетов Z_m, которые определяются как

$$a + a' = m, \quad b + b' = m, \qquad (2)$$

или

$$a' = m - a, \quad b' = m - b, \qquad (3)$$

где a', b' – обратные элементы (дополнения до m) чисел a и b этого же кольца. Тогда

$$a \cdot b' = a \cdot (m - b) = m \cdot a - a \cdot b,$$

откуда

$$-a \cdot b = a \cdot b' - m \cdot a.$$

Однако

$$C' = m^2 - C,$$

где C' – обратный элемент в кольце вычетов Z_m по отношению к C, где модуль кольца равен m^2.

Тогда в кольце вычетов Z_m можно записать

$$C' \overset{Z_m}{\equiv} a \cdot b' - m \cdot a. \tag{4}$$

Таким образом, получено второе уравнение (3), которое вместе с (1) составляет следующую систему уравнений:

$$\begin{cases} C = a \cdot b, \\ C' = a \cdot b' - m \cdot a. \end{cases} \tag{5}$$

Очевидно, что решение этой системы возможно если

$$m > a \cdot b', \tag{6}$$

что разделяет второе уравнение системы (4) на две части. Тогда

$$a \cdot b' = (C') \bmod m. \tag{7}$$

Используя алгоритм Эвклида, легко находим решение. Или еще проще

$$-m \cdot a = C' - (C') \bmod m,$$

что равносильно

$$-a = \text{int}\,(C'/m),$$

откуда

$$a = m - \text{int}\,(C'/m). \tag{8}$$

Пример. Пусть $a = 5$, $b = 7$, $C = 35$, $m = 8$, $C' = 64 - 35 = 29$.
Тогда $a = 8 - \text{int}\,(29/8) = 5$.

Круг факторизуемых чисел для данного способа можно расширить, если положить, что $b = m + b'$. Тогда

$$C = a \cdot b = a \cdot (m + b') = m \cdot a + a \cdot b',$$

а с учетом (5) имеем

$$a = \text{int}\,(C/m). \tag{9}$$

Пример. Пусть $a = 3$, $b = 17$, $C = 51$, $m = 16$. Тогда $a = \text{int}\,(51/16) = 3$.
Данные два выражения (7) и (8) совместно с известной теоремой Ферма [5], основанной на представлении числа разность квадратов

$$C = x^2 - y^2, \tag{10}$$

где $x = (a+b)/2$, $y = (a - b)/2$, позволяют эффективно факторизовать составные числа на ЭВМ за приемлемое время, ибо выражение (10) эффективно, когда числа a и b близки по величине, при этом выражения (8) и (9) эффективны, если числа a и b существенно различаются.

Однако существует метод факторизации, не требующий применения выражения (8). Он исходит из следующих предпосылок. Перемножив формулы выражения (2) имеем

$$(a + a') \cdot (b + b') = m^2.$$

Далее с учетом выражений (3) полученная запись примет вид

$$a \cdot b + (m - a) \cdot b + a \cdot (m - b) + a' \cdot b' = m^2,$$
$$a \cdot b + m \cdot b - a \cdot b + m \cdot a - a \cdot b + a' \cdot b' = m^2,$$
$$m \cdot (a + b) - a \cdot b + a' \cdot b' = m^2, \quad (11)$$

а в кольце вычетов Z_m имеем разновидность известного звездного произведения [6]

$$a \cdot b \overset{Zm}{=} m \cdot (a + b) + a' \cdot b'. \quad (12)$$

Из выражений (11) находим

$$a + b = (m + a \cdot b - a' \cdot b')/m,$$

а вместе с (1) имеем систему уравнений

$$\begin{cases} a + b = (m^2 + a \cdot b - a' \cdot b)/m \\ a \cdot b = C \end{cases}. \quad (13)$$

Если же выбрать модуль m таким образом, что

$$m > a' \cdot b', \quad (14)$$

то из (12) в кольце Z_m следует соотношение

$$(a' \cdot b') \bmod m \overset{Zm}{=} (a \cdot b) \bmod m. \quad (15)$$

Тогда систему уравнений можно переписать

$$\begin{cases} a + b = (m^2 + a \cdot b - (a \cdot b) \bmod m)/m, \\ a \cdot b = C \end{cases}$$

или

$$\begin{cases} a + b = (m^2 + C - (C) \bmod m)/m, \\ a \cdot b = C. \end{cases} \quad (16)$$

Решение этой системы уравнений приводит к квадратному уравнению вида

$$a^2 - ka + C = 0.$$

Ее корни равны

$$a_{1,2} = \frac{\text{к} \pm \sqrt{\text{к}^2 - 4 * \text{C}}}{2}, \quad (17)$$

где

$$k = (\text{m}^2 + \text{C} - (\text{C}) \bmod \text{m})/\text{m}. \quad (18)$$

Здесь же заметим, что $k/2$ есть ни что иное, как переменная x из формулы Ферма (10)

$$x = k/2 = (\text{m}^2 + \text{C} - (\text{C}) \bmod \text{m})/2 \cdot \text{m}, \quad (19)$$

при этом переменная y этой же формулы равна

$$y = \frac{\sqrt{\kappa^2 - 4 \cdot C}}{2} = \frac{\sqrt{(m^2 + C - 0(C) \bmod m)/m - 4 \cdot C}}{2}. \qquad (20)$$

Пример. Пусть числа a и b равны 11 и 13 соответственно. Выберем модуль m = 16. Тогда

$$C = 11 \cdot 13 = 143, \; m^2 = 256, \quad k = (256 + 143 - (143) \bmod 16)/16 = 24$$

и $$a_{1,2} = \frac{24 \pm \sqrt{24^2 - 4 \cdot 143}}{2} = \frac{24 \pm 2}{2}, \; a = a_1 = 11, \; b = a_2 = 13.$$

Условие (14) может и не выполнятся. Тогда можно изменить представление (3)

$$a = m + a_1, \; b = m + b_1 \qquad (21)$$

и

$$C = a \cdot b = (m + a_1) \cdot (m + b_1) = m^2 + m \cdot (a_1 + b_1) + a_1 \cdot b_1,$$

откуда

$$m \cdot (a_1 + b_1) = C - m^2 - a_1 \cdot b_1,$$
$$a_1 + b_1 = (C - m^2 - a_1 \cdot b_1)/m$$

или

$$a + b = a_1 + b_1 + 2 \cdot m = (C - m^2 - a_1 \cdot b_1)/m + 2 \cdot m$$

и, окончательно, система уравнений с условием

$$m > a_1 \cdot b_1,$$

запишется

$$\begin{cases} a + b = (C - m^2 - (C) \bmod m)/m + 2 \cdot m, \\ a \cdot b = C \end{cases} \qquad (22)$$

и решить ее не составляет никаких трудностей.

Заметим, что кроме представлений по выражениям (3) и (21), существует еще два представления чисел a и b, одно из которых

$$a = m + a_1, \; b = m - b', \qquad (23)$$

тогда

$$C = a \cdot b = (m + a_1) \cdot (m - b') = m^2 + m \cdot (a_1 - b') - a_1 \cdot b' =$$
$$= m^2 + m \cdot a_1 - a_1 \cdot b - m \cdot b'. \qquad (24)$$

Из выражений (22) имеем

$$a_1 = a - m \;\text{ и }\; b' = m - b \qquad (25)$$

и подставляя эти значения в (23), получаем

$$C = m^2 + m \cdot a_1 - a_1 \cdot b' - m \cdot b' = m^2 + m \cdot (a - m) - a_1 \cdot b' - m \cdot (m - b) =$$
$$= m^2 - m^2 + m \cdot a - a_1 \; b' + m \cdot b - m^2.$$

Приводя подобные члены, имеем

$$C = m \cdot (a + b) - a_1 \cdot b' - m^2. \qquad (26)$$

Нетрудно заметить, что если в качестве модуля m выбрать число

$$m = (a + b)/2, \qquad (27)$$

то тогда частный случай выражения (26) при таком модуле представляет собой

не что иное, как формулу Ферма (10).

Действительно, заменив переменные в соответствии с (25), (27) имеем

$$C = m \cdot (a + b) - a_1 \cdot b' - m^2 = m \cdot (a + b) - (a - m) \cdot (m - b) - m^2,$$

$$C = ((a + b)/2) \cdot (a + b) - (a - (a + b)/2)) \cdot ((a + b)/2) - b) - ((a + b)/2)^2.$$

Выполнив указанные в последнем выражении операции и приводя подобные члены, получим известную формулу Ферма (10)

$$C = ((a + b)/2)^2 - ((a - b)/2)^2.$$

Далее, если член $a_1 \cdot b'$ в выражении (25) удовлетворяет условию

$$a_1 \cdot b' < m, \tag{28}$$

то из выражения (26) следует

$$a + b = (C + m^2 + (C') \bmod m)/m,$$

где $a_1 \cdot b' = (C') \bmod m$.

Окончательно, система уравнений с условием $a_1 \cdot b' < m$ запишется как

$$\begin{cases} a + b = (C + m^2 + (C') \bmod m)/m, \\ a \cdot b = C. \end{cases} \tag{29}$$

Впрочем, представление чисел a и b, в котором

$$a = m - a_1, \; b = m + b',$$

не имеет смысла рассматривать, так как b' должно быть отрицательным числом. Следовательно, оно сводится к представлению (3) и системе уравнений (16).

Заметим, что всегда существует модуль m такой, что, по крайней мере, условие (28) всегда выполняется, так как из представления (22) следует, что выполняется следующее соотношение:

$$a > m > b. \tag{30}$$

Действительно, полагая $m = a - 1$ и учитывая, что $b' = m - b$, (т. е. b' меньше m) имеем по выражению (28) $1 \cdot b' < m$, что и требовалось доказать.

Заметим, что в указанном методе факторизации с применением колец вычетов Z_m возможно применение двух модулей m_1 и m_2 таких, что

$$m_1 > a, \; m_2 > b \;\text{ и }\; a > b, \tag{31}$$

что обычно имеет место на практике.

Тогда модуль кольца вычетов равен $m_1 \cdot m_2$ и

$$C = a \cdot b = (m_1 - a') \cdot (m_2 - b') = m_1 \cdot m_2 - m_2 \cdot a' - m_1 \cdot b' + a' \cdot b'.$$

Заменив a' на $m_1 - a$ и b' на $m_2 - b$ имеем

$$C = m_1 \cdot m_2 - m_2 \cdot a' - m_1 \cdot b' + a' \cdot b' = m_1 \cdot m_2 - m_2 \cdot (m_1 - a) - m_1 \cdot (m_2 - b) + a' \cdot b'$$

или

$$C = m_1 \cdot m_2 - m_1 \cdot m_2 + m_2 \cdot a - m_1 \cdot m_2 + m_1 \cdot b + a' \cdot b' =$$

$$= - m_1 \cdot m_2 + m_2 \cdot a + m_1 \cdot b + a' \cdot b',$$

откуда

$$m_2 \cdot a + m_1 \cdot b = C + m_1 \cdot m_2 - a' \cdot b'.$$

Полагая, что $a' \cdot b' = (C) \bmod m_2$ имеем уравнение

$$m_2 \cdot a + m_1 \cdot b = C + m_1 \cdot m_2 - (C) \bmod m_2 . \quad (32)$$

Вместе с (1) получаем следующую систему уравнений:

$$\begin{cases} m_2 \cdot a + m_1 \cdot b = C + m_1 \cdot m_2 - (C) \bmod m_2 , \\ a \cdot b = C. \end{cases} \quad (33)$$

Решить данную систему не представляет никаких трудностей, так как в конечном счете это обыкновенное квадратное уравнение.

Выводы. Таким образом, изложенное выше показывает, что применение кольца вычетов по простому модулю позволяет создать аналитический метод факторизации составных чисел. Он сводит процедуру факторизации к решению системы алгебраических уравнений второго порядка. Решением этой системы, в свою очередь, является обыкновенное квадратное уравнение. Это достигается путем грубого выбора соответствующего модуля кольца вычетов, что в конечном счете существенно сокращает вычислительные затраты на факторизацию в целом.

1. *Бойко А.А., Зиятдинов Д.Б., Ишмухаметов Ш.Т.* Об одном подходе к проблеме факторизации натуральных чисел. – М.: Изв. вузов. матем., 2001. – № 4. – С. 15 – 22.
2. *Семотюк М.В.* О существовании точного метода факторизации составных чисел // УСиМ. – 2011. – № 6. – С. 46 – 52.
3. *Shor P.* Polynomial –Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Jour. Comp. – 1997. – Vol. 26, N 5. – P. 1484 – 1509.
4. *Семотюк М.В.* Заметки по машинной алгебре/монография. – Киев: Сталь, 2012. – 250 с.
5. *Коблиц Н.* Курс теории чисел и криптографии. – М.: Научное издательство ТВП, 2001. – 254 с.
6. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1979. – 624 с.

Получено 12.09.2013