УДК 511.13

МОДИФИКАЦИЯ СПОСОБА ФЕРМА ФАКТОРИЗАЦИИ ЧИСЕЛ И СВЯЗЬ МЕЖДУ ПРОСТЫМИ И ТРЕУГОЛЬНЫМИ ЧИСЛАМИ

Козаченко Е.С., инженер, Величко И.Г., к.ф.-м.н., доцент

Запорожский национальный университет

В работе предлагается способ поиска сомножителей нечетного числа, который во многих случаях является более эффективным, чем классический метод Ферма. Также предложен другой способ получения расчетных формул в алгоритмах факторизации, предложенных ранее в статьях соавторов. Доказано, что нечетное число n является простым или степенью простого числа тогда и только тогда, когда оно является делителем какого-нибудь треугольного числа с номером, меньшим чем $n-1$.

Ключевые слова: простое число, факторизация, сравнение, треугольные числа.

Козаченко Є.С., Величко І.Г. МОДИФІКАЦІЯ СПОСОБУ ФЕРМА ФАКТОРИЗАЦІЇ ЧИСЕЛ І ЗВ'ЯЗОК МІЖ ПРОСТИМИ І ТРИКУТНИМИ ЧИСЛАМИ / Запорізький національний університет,Україна

У роботі пропонується спосіб пошуку множників непарного числа, який в багатьох випадках є більш ефективним, ніж класичний метод Ферма. Також запропоновано інший спосіб отримання розрахункових формул в алгоритмах факторизації, запропонованих раніше в статтях співавторів. Доведено, що непарне число n є простим або ступенем простого числа тоді і тільки тоді, коли воно є дільником деякого трикутного числа з номером, меншим ніж $n-1$.

Ключові слова: просте число, факторизація, порівняння, трикутні числа.

Kozachenko E.S., Velichko I.G. THE MODIFICATION OF THE FERMAT THECHNIQUE OF THE FACTORIZATION OF THE NUMBERS AND THE RELATION BETWEEN THE PRIME NUMBERS AND THE TRIANGULAR NUMBER / Zaporizhzhya national university, Ukraine

The technique of the finding of the factors of the odd numbers is presented in the article. This technique is more efficient then the classical Fermat technique. The article also gives the technique of the derivation of the calculation formulae in the factorization algorithm, which was proposed by the authors before. It is proved that the odd number n is prime or the degree of the prime number when and only when this number is the divisor of some triangular number T_m, where $m < n-1$.

Key words: prime number, factorization, checking, triangular number.

ВВЕДЕНИЕ

В 2003 году сенсацией стало открытие Agraval M., Kayal N. и Saxena N. быстрого теста на простоту [1]. Однако их метод позволяет лишь проверять, является ли число простым или составным. А эффективное разложение числа на множители, что является важным, например, в задачах шифрования с открытым ключом, является открытой задачей [2].

Существующие методы являются, по сути, методами последовательных испытаний. Наиболее известными из них являются метод проверки простых делителей и метод Ферма.

В предлагаемой работе предлагается модификация метода Ферма, которая в некоторых случаях является более эффективной. Кроме того, более просто получены способы, основанные на нахождении минимального точного квадрата в заданной арифметической последовательности, и описанные в [3,4]. Указана связь между разложением числа на множители и треугольными числами.

1. МЕТОД ФЕРМА ФАКТОРИЗАЦИИ НЕЧЕТНЫХ ЧИСЕЛ

Пусть дано нечетное натуральное число n. Ставится задача о его факторизации (разложении на натуральные множители), то есть о представлении его в виде

$$n = m_1 m_2, \tag{1}$$

где m_1, m_2 - нечетные натуральные числа. Договоримся, что $m_1 \geq m_2$. Если n - простое число, то обязательно $m_1 = n, \quad m_2 = 1$. Если же n составное, то существуют другие значения m_1, m_2, при которых равенство (1) имеет место.
Будем искать множители в виде

$$m_1 = x + y, \quad m_2 = x - y. \tag{2}$$

Тогда $x = \frac{m_1 + m_2}{2}$, $y = \frac{m_1 - m_2}{2}$. В силу того, что m_1, m_2 - нечетные числа, получаем, что x, y - целые неотрицательные числа. Подставляя (2) в (1), получаем

$$n = x^2 - y^2 \tag{3}$$

Нам нужно найти такие целые неотрицательные значения x, y, при которых имеет равенство (3).

Суть метода Ферма состоит в следующем: Перепишем соотношение (3) в виде

$$x^2 = n + y^2 \tag{4}$$

Далее в выражение $n + y^2$ по очереди подставляем $y = 0, 1, 2...$, пока не получим точный квадрат. Если это происходит только при $y = \frac{n-1}{2}$, то число n является простым. Если же точный квадрат получается раньше, то по найденному y по формуле (4) определяют число x и записывают исходное разложение в виде (3). Заметим, что число y равно полуразности двух делителей числа n. То есть этот метод эффективен, если число n имеет делители, близкие к $\sqrt{n}$.

Пример:

$n = 187$;

$y = 1, x^2 = 187 + 1 = 188$;

$y = 2, x^2 = 187 + 4 = 191$;

$y = 3, x^2 = 187 + 9 = 196 = 14^2$;

$n = (x + y)(x - y) = (14 - 3)(14 + 3) = 17 \cdot 11 = 187$

Искомое разложение достигнуто на 3-м шаге.

2. МОДИФИКАЦИЯ МЕТОДА ФЕРМА ФАКТОРИЗАЦИИ НЕЧЕТНЫХ ЧИСЕЛ

В данной работе предлагается модификация метода Ферма, которая в некоторых случаях оказывается эффективнее.

Из анализа соотношения (4) делаем вывод, что $x \geq \sqrt{n}$. Поэтому представим x в виде

$$x = z + k, \tag{5}$$

где $z = \left[\sqrt{n}\right]$ (квадратные скобки означают целую часть числа).

Подставляя (5) в (3), раскрывая скобки и приводя подобные, получим соотношение

$$n = z^2 + 2kz + k^2 - y^2,$$

которое перепишем в виде

$$y^2 = k(k + 2z) - t \tag{6}$$

где

$$t = n - z^2 = n - \left[\sqrt{n}\right]^2 \geq 0. \tag{7}$$

Утверждение. Если $t \equiv 0,3 \pmod 4$, то k -четное, а если $t \equiv 1,2 \pmod 4$, то k -нечетное.

Доказательство.

Замечание. Из нечетности n и соотношения (7) следует, что числа t и z имеют разную четность.

В равенстве (6) перейдем к сравнению по модулю (4). Получим, что

$$k(k + 2z) - t \equiv 0,1 \pmod 4 \tag{8}$$

Последовательно рассмотрим случаи, когда $t \equiv 0,1,2,3 \pmod 4$

Пусть $t \equiv 0 \pmod 4$. Если $k = 2d + 1$, то $k(k + 2z) - t \equiv 1 + 2z \pmod 4$. Равенство (8) получается только в том случае, если z -четное, а это противоречит сформулированному выше замечанию. Значит если $t \equiv 0 \pmod 4$, то k - четное число.

Пусть $t \equiv 1 \pmod 4$. Если $k = 2d$, то $k(k + 2z) - t \equiv 3 \pmod 4$. Значит, если $t \equiv 1 \pmod 4$, то k - нечетное число.

Пусть $t \equiv 2 \pmod 4$. Если $k = 2d$, то $k(k + 2z) - t \equiv 2 \pmod 4$. Но это противоречит (8). Значит, если $t \equiv 2 \pmod 4$, то k - нечетное число.

Пусть $t \equiv 3 \pmod 4$. Если $k = 2d + 1$, то $k(k + 2z) - t \equiv 2 + 2z \pmod 4$. Равенство (8) получается только в том случае, если z - нечетное, а это противоречит сформулированному выше замечанию. Значит, если $t \equiv 3 \pmod 4$, то k - четное число.

Утверждение доказано.

Использование доказанного утверждения позволяет сократить количество проб в два раза.

Теперь сформулируем предложенный способ факторизации.

1. По заданному нечетному числу n находим числа $z=\left[\sqrt{n}\right]$ и $t=n-z^2$.
2. В выражение $k(k+2z)-t$ по очереди подставляем $k=0,2,4...$, если $t\equiv 0,3(\mathrm{mod}\,4)$, или $k=1,3,5...$ если $t\equiv 1,2(\mathrm{mod}\,4)$, пока оно не станет точным квадратом.
3. По найденному значению k находим x по формуле (5), y - по формуле (6) и записываем искомое разложение числа: $n=(x+y)(x-y)$.
4. В случае, если число n является простым, точный квадрат получается только при $k=\frac{n-1}{2}-\left[\sqrt{n}\right]$. Если найденное $k<\frac{n-1}{2}-\left[\sqrt{n}\right]$, то число является составным.

Пример:

1) $n=187$;

$z=\left[\sqrt{187}\right]=13, t=187-13^2=187-169=18\equiv 2(\mathrm{mod}\,4)$;

Нужно брать нечетные значения k.

$k=1,\quad 1\cdot(1+2\cdot 13)-18=9=3^2,\quad y=3,\quad x=z+k=13+1=14$;

$n=(x+y)(x-y)=(14-3)(14+3)=17\cdot 11=187$

Искомое разложение достигнуто на 1-м шаге

2) $n=12871$,

$z=\left[\sqrt{12871}\right]=113,\quad t=n-z^2=102\equiv 2(\mathrm{mod}\,4)$

Нужно брать нечетные значения k.

$k=1,\quad 1(1+2\cdot 113)-102=123\neq y^2$;

$k=3,\quad 3(3+2\cdot 113)-102=585\neq y^2$;

…

$k=23,\quad 23(23+2\cdot 113)-102=5625=75^2$;

$y=75,\quad x=z+k=113+23=136$;

$n=12871=(x+y)(x-y)=211\cdot 61$;

Разложение достигнуто на 12 пробе.

3. ФАКТОРИЗАЦИЯ ЧИСЕЛ, НЕ ЯВЛЯЮЩИХСЯ СТЕПЕНЯМИ ПРОСТЫХ

Покажем, как можно другим способом получить результаты, описанные в статьях [3,4]. Будем искать разложение нечетного натурального числа n в виде

$$n=\frac{ab}{c},\ a,b,c\in N \tag{9}$$

Ясно, что если $c=1$, то получается разложение (1). Так как мы ввели дополнительный параметр c, то на числа a и b можно наложить дополнительное условие.

Если мы потребуем, чтобы числа a и b были последовательными натуральными числами, то, после перехода к другим переменным, получим

$$n=\frac{x(x+1)}{y}. \tag{10}$$

Равенство (10) перепишем в виде

$$x^2+x-ny=0$$

Выразим отсюда переменную x:

$$x=\frac{-1+\sqrt{1+4ny}}{2}.$$

Так как по условию x является натуральным, то перед знаком радикала взят «плюс», и, кроме того, подкоренное выражение должно быть точным квадратом. Подкоренное выражение $1+4ny$ является нечетным и при делении на 4 дает остаток 1. Следовательно, при делении на 8 оно будет давать остаток 1 или 5.

Известно, что все квадраты натуральных чисел при делении на 8 дают остаток 1 [Бух]. Следовательно, необходимо потребовать, чтобы выражение $4ny$ делилось на 8. Это будет в том и только в том случае, если y -четное число. То есть можно положить, что $y = 2z$.

Отсюда следует следующий способ факторизации нечетного числа n:

1. В выражение $1+8nz$ по очереди подставляем $z = 1,2,...,$ пока оно не станет точным квадратом.

2. Если найденное $z = \frac{n-1}{2}$, то число n является простым или степенью простого числа.

3. Если найденное $z < \frac{n-1}{2}$, то находим x по формуле

$$x = \frac{-1+\sqrt{1+8nz}}{2}$$

и представляем число в виде: $n = \frac{x(x+1)}{z}$.

4. Сократив числитель и знаменатель этой дроби на z, получаем искомое разложение в виде (1). На практике сократить эту дробь можно, представив z в виде $z = НОД(x,z)\cdot НОД(x+1,z)$. Наибольший общий делитель можно найти, например, используя алгоритм Евклида [5].

Таким образом, задача разложения нечетного числа n сводится к поиску минимального точного квадрата в последовательности $t_n = 1+8nz$.

Если мы потребуем, чтобы числа a и b отличались на два, то, после перехода к другим переменным, получим

$$n = \frac{x(x+2)}{y}. \qquad (11)$$

Равенство (11) перепишем в виде

$$x^2 + 2x - ny = 0$$

Выразим отсюда переменную x:

$$x = \sqrt{1+n\cdot y} - 1.$$

Так как по условию x является натуральным, то перед знаком радикала взят «плюс», и, кроме того, подкоренное выражение должно быть точным квадратом.

Таким образом, задача разложения нечетного числа n сводится к поиску минимального точного квадрата в последовательности $t_n = 1+ny$. Тем самым другим способом получены результаты, описанные в работе [3,4].

4. СВЯЗЬ МЕЖДУ РАЗЛОЖЕНИЕМ ЧИСЛА НА МНОЖИТЕЛИ И ТРЕУГОЛЬНЫМИ ЧИСЛАМИ

При заданном натуральном x переменная y определяется однозначно. Нужно так подобрать x, что бы y тоже было натуральным числом. Равенство (10) будет выполняться, например, при $x = y = n-1$.

Утверждение. Если равенство (10) выполняется при натуральных значениях x и y, меньших чем $n-1$, то число n будет составным.

Доказательство. Так как число $\frac{x(x+1)}{y}$ является целым, то y можно представить в виде произведения натуральных чисел $y = y_1 \cdot y_2$ так, что бы числа $m_1 = \frac{x}{y_1}$ и $m_2 = \frac{x+1}{y_2}$ были целыми. Так как числа x и $x+1$ являются взаимно-простыми, то взаимно-простыми будут и числа m_1 и m_2.

Если $y_1 = x$, то $n = m_2 = \frac{x+1}{y_2} < \frac{(n-1)+1}{y_2} = \frac{n}{y_2} \le n$. Получаем противоречие.

Если $y_2 = x+1$, то $n = m_1 = \frac{x}{y} < \frac{(n-1)}{y_1} \le n-1 < n$. Получили противоречие. Так как мы показали, что $y_1 \neq x$ и $y_2 \neq x+1$, то $m_1 > 1$, $m_2 > 1$ и значит, число $n = m_1 m_2$ является составным.

Утверждение доказано.

Из проведенного доказательства видно, что в полученном таким способом разложении вида (1) множители m_1 и m_2 являются взаимно-простыми. То есть нечетные числа, которые являются простыми или степенями простых чисел, разложить таким способом нельзя. То, что таким образом можно разложить все остальные числа, следует из результатов работы [3]. Заметим, что этот вопрос эквивалентен вопросу о существовании чисел вида $x(x+1)$, кратных n при $x < n-1$.

Напомним, что число s называется треугольным, если оно имеет вид $T_r = \frac{r(r+1)}{2}$ при некотором натуральном r [5]. Таким образом, из результатов работы [3] следует

Утверждение. Нечетное число n является простым или степенью простого числа тогда и только тогда, когда оно является делителем какого-нибудь треугольного числа с номером, меньшим чем $n-1$.

Пример Последовательность треугольных чисел имеет вид

1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, ….

Число 7 является простым, и первый элемент этой последовательности, делящий число 7 – это число $21 = T_{7-1} = T_6$.

Число 9 является степенью простого числа, и первый элемент этой последовательности, делящий число 9 – это число $36 = T_{9-1} = T_8$.

Число 15 не является простым или степенью простого числа. Первый элемент этой последовательности, делящий число 15 – это число $15 = T_5$, причем $5 < 15 - 1 = 14$.

ВЫВОДЫ

Данная работа посвящена решению задачи о разложении нечетного составного числа на сомножители. Предложена модификация известного метода Ферма, которая в некоторых случаях оказывается более эффективной.

Кроме того, предложен более простой подход к получениям расчетных формул в методах факторизации, связанных с нахождением точных квадратов в последовательностях. Установлена связь между структурой числа и треугольными числами, кратными этому числу.

ЛИТЕРАТУРА

1. Agraval M., Kayal N., Saxena N. Primes is in P. Preprint, 6 August 2002.
2. Коблиц Н. Курс теории чисел и криптографии. - М.: Научное издательство «ТВП», 2001.- 270 с.
3. Козаченко Е.С., Величко И.Г. Способ разложения на множители нечетных чисел, не являющихся примарными // Вісник Запорізького національного університету. Фіз.-мат. науки. Біологічні науки. – 2005.- №1.- С. 21-24.
4. Козаченко Е.С., Величко И.Г. Новый метод факторизации чисел// Вісник Запорізького національного університету. Фіз.-мат. науки. – 2006.- №1.- С. 70-73.
5. Бухштаб А.А. Теория чисел. - М.:Просвещение, 1966. – 384с.