Ганна Куленкова,
студентка ІІ курсу факультету
фізики, математики та інформатики
Уманського державного педагогічного
університету імені Павла Тичини
Інна Поліщук,
студентка ІІ курсу факультету
фізики, математики та інформатики
Уманського державного педагогічного
університету імені Павла Тичини

СПОСОБИ РОЗКЛАДУ НА ПРОСТІ МНОЖНИКИ ВЕЛИКИХ НАТУРАЛЬНИХ ЧИСЕЛ СПЕЦІАЛЬНОГО ВИГЛЯДУ

При розв'язувані типових задач на розклад простих множників можна застосовувати кілька різних способів. Одним із досі повністю недосліджених способів є факторизація. Факторизацією цілого числа називається його розклад на добуток простих співмножників. Такий розклад, згідно основної теореми арифметики, завжди існує та є єдиним (з точністю до порядку слідування множників). Більшість існуючих методів факторизації є достатньо трудомісткими [1], тому потребують значних обчислювальних ресурсів для чисел великої довжини. Крім того, питання про існування алгоритму на комп'ютері для виконання факторизації є однією з важливих відкритих проблем сучасної теорії чисел.

В історії розвитку методів факторизації важливу роль відіграли числа спеціальної форми, на яких використовувалися ті чи інші алгоритми перевірки простоти та факторизації. Метою нашої статті є опис простих способів та алгоритмів факторизації для великих цілих чисел спеціальної форми.

Метод елементарних перетворень. Серед чисел спеціальної форми в першу чергу потрібно виділити числа вигляду $a^n \pm b^n$. З курсу елементарної математики розклад чисел такого вигляду є відомим:

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right), \; n \in N$$

Якщо n – непарне, то:

$$a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots - ab^{n-2} + b^{n-1}\right), \; n = 2k-1, \; k \in N$$

Приклад 1. Записати розклад на прості множники числа $5^{12} - 2^{12}$.

Розв'язання.

$$5^{12} - 2^{12} = \left(\left(5^6\right)^2 - \left(2^6\right)^2\right) = \left(5^6 - 2^6\right)\cdot\left(5^6 + 2^6\right) = \left(\left(5^3\right)^2 - \left(2^3\right)^2\right)\cdot\left(\left(5^2\right)^3 + \left(2^2\right)^3\right) =$$

$$= \left(125^2 - 8^2\right)\cdot\left(25^3 + 8^3\right) = (125-8)\cdot(125+8)\cdot(25+4)\cdot\left(25^2 - 25\cdot 4 + 4^2\right) =$$

$$= 117 \cdot 133 \cdot 29 \cdot 541.$$

Далі, залишилось розкласти кожен співмножник на прості множники: $29 = 29$

$$117 = 9 \cdot 13 = 3^2 \cdot 13$$

$$133 = 7 \cdot 19$$

$$541 = 541$$

Отже, $5^{12} - 2^{12} = 3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 541$.

Метод Ферма. Нехай $n = p \cdot q$ – відоме ціле число, що є добутком двох невідомих простих чисел p та q, яке потрібно знайти. Більшість сучасних методів факторизації [2] засновано на ідеї, започаткованій ще П'єром Ферма, що полягає у пошуку пар натуральних чисел *A* та *B* таких, що виконується співвідношення:

$$n = A^2 - B^2.$$

Алгоритм Ферма може бути описаний наступним способом:

1. Виділимо цілу частину від квадратного кореня із n:

$$m = \lfloor \sqrt{n} \rfloor.$$

2. Для $x = 1,2,\ldots$ будемо обчислювати значення

$$q(x) = (m + x)^2 - n,$$

до тих пір, поки чергове значення $q(x)$ не виявиться рівним повному квадрату.

3. Нехай $q(x)$ є повним квадратом, наприклад, числа B: $q(x) = B^2$.

Визначимо $A = m + x$, звідки з рівності $A^2 - n = B^2$ знайдемо $n = A^2 - B^2 = (A + B) \cdot (A - B)$, та шукані дільники p та q обчислюються, як $p = A + B$, $q = A - B$.

Приклад 2. Записати розклад на прості множники числа $n = 19691$.

Розв'язання.

Обчислимо $m = \lfloor \sqrt{n} \rfloor = 140$. Представимо процедуру обчислення дільників n у вигляді таблиці:

x	*y*	$\sqrt{y}$
1	190	13,78
2	473	21,75
3	758	27,53
4	1045	32,33
5	1334	36,52
6	1625	40,31
7	1918	43,79
8	2213	47,04
9	2510	50,10
10	2809	53

Із останнього стовпця одержимо: $(140+10)^2 - n = 53^2$, звідки $n = 150^2 - 53^2 = 203 \cdot 97$. Отже, $19691 = 203 \cdot 97$.

Метод розкладу Ейлера. Це техніка факторизації числа шляхом його запису у вигляді суми двох квадратів різними шляхами. Метод факторизації Ейлера більш ефективний, ніж метод Ферма для чисел, дільники яких не близькі і, суттєво ефективніше, ніж пробне ділення, якщо можна знайти представлення чисел у вигляді суми двох квадратів достатньо швидко. Великим недоліком цього методу є факт, що його не можна застосувати для розкладу цілих чисел з простим дільником виду *4k+3*, що входить в розклад на прості множники з непарним степенем, оскільки такі числа не можуть бути представлені у вигляді суми двох квадратів. Навіть непарні складені числа вигляду *4k+1* часто являються добутком двох простих вигляду *4k+3* (наприклад, 3053 = 43*71) і не можуть бути розкладені методом Ейлера.

Тепер перейдемо до суті цього методу. Тотожність Брахмагупти-Фібоначчі стверджує, що добуток двох сум двох квадратів є сумою двох квадратів: $(a^2+b^2)\cdot(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$

$$= (ac+bd)^2 + (ad-bc)^2,$$

яку легко перевірити, розкривши дужки правої та лівої частин рівності. Метод Ейлера опирається на цю теорему, але може розглядуватися як зворотний підхід, якщо дано (або можна знайти) $n = a^2 + b^2 = c^2 + d^2$, ми шукаємо розклад *n* на добуток двох квадратів.

Спочатку ми виводимо, що

$$a^2 - c^2 = d^2 - b^2$$

та розкладаємо обидві частини на множники

$$(a+c)(a-c) = (d+b)(d-b) \quad (1)$$

Тепер нехай $k = НСД(a-c, d-b)$, а $h = НСД(a+c, d+b)$, так, що існують деякі числа l, m, l', m', для яких

- $(a-c) = kl$,
- $(d-b) = km$, $НСД(l,m) = 1$
- $(a+c) = hm'$,
- $(d+b) = hl'$, $НСД(l',m') = 1$.

Після підстановки в (1) одержимо $klhm' = kmhl'$.

Після скорочення спільних множників одержимо $lm' = l'm$

Тепер, використовуючи факт, що (l,m) та (l',m') взаємно прості, маємо

- $l = l'$
- $m = m'$

Таким чином,

- $(a-c)=kl$,
- $(d-b)=km$,
- $(a+c)=hm$,
- $(d+b)=hl$.

Тепер, ми бачимо, що $m=НСД(a+c,d-b)$, а $l=НСД(a-c,d+b)$. Після застосування згаданої тотожності Брахмагупти-Фібоначчі, одержимо наступний розклад числа $n=\left(\left(\frac{k}{2}\right)^2+\left(\frac{h}{2}\right)^2\right)(l^2+m^2)$.

Приклад 3. Дано $488881=684^2+145^2=665^2+216^2$. Розкладіть це число на прості множники.

Розв'язання.

Із формул вище складемо таблицю:

$a=684$	(A) $a-c=19$	$k=НСД(A,C)=1$
$b=145$	(B) $a+c=1349$	$h=НСД(B,D)=19$
$c=665$	(C) $d-b=71$	$l=19$
$d=216$	(D) $d+b=361$	$m=71$

$$488881=\left(\left(\frac{k}{2}\right)^2+\left(\frac{h}{2}\right)^2\right)(l^2+m^2)=\left(\left(\frac{1}{2}\right)^2+\left(\frac{19}{2}\right)^2\right)(19^2+71^2)=$$

$$=\left(\frac{1^2+19^2}{4}\right)(19^2+71^2)=\frac{362}{2}\cdot\frac{5402}{2}=181\cdot 2701=181\cdot 37\cdot 73.$$

Отже,

Дослідивши проблему факторизації можна сказати, що факторизація бере початок ще з молодших класів в закладах середньої освіти, коли розглядають завдання розкладання чисел на прості множники. Робиться це просто поділом даного числа на прості послідовні числа. Якщо число велике, цей алгоритм працюватиме довго, навіть на комп'ютері. З іншого боку, ми запропонували «швидкі» способи, що дозволяють для чисел спеціального вигляду виконати розклад на прості множники.

Список використаних джерел

1. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие. Казань: Казан. ун. 2011. 190 с.
2. Тимошенко Л., Івасьєв С., Вербик К. Удосконалений метод Ферма факторизації чисел. *Проблеми становлення інформаційної економіки в Україні*: матеріали Всеукр. наук.-практ. конф. (Львів, 23–25 жовтня 2014 р.). Л.: Ліга-Прес, 2014. С. 280–283.