Розклад числа на прості множники

Означення. ***Розкладом*** натурального числа n ***на прості множники*** (***факторизацією*** числа) називається представлення його у вигляді $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$, де p_i – взаємно прості числа, $k_i \geq 1$.

Задача перевірки числа на простоту є простішою за задачу факторизації. Тому перед розкладанням числа на прості множники слід перевірити число на простоту.

Означення. ***Розбиттям*** числа називається задача представлення натурального числа n у вигляді $n = a * b$, де a, b – натуральні числа, більші за 1 (не обов'язково прості).

Метод Ферма [2, стор. 255-256]

Нехай n – складене число, яке не є степенем простого числа. Метод Ферма намагається знати такі натуральні x та y, що $n = x^2 - y^2$. Після чого дільниками числа n будуть $a = x - y$ та $b = x + y$: $n = a * b = (x - y)(x + y)$.

Якщо припустити що $n = a * b$, то в якості x та y (таких що $n = x^2 - y^2$) можна обрати

$$x = \frac{a+b}{2},\ y = \frac{a-b}{2}$$

Приклад. Виберемо $n = 143 = 11 * 13$.
Тоді $x = (13 + 11) / 2 = 12$, $y = (13 - 11) / 2 = 1$.
Перевірка: $x^2 - y^2 = 12^2 - 1^1 = 143 = n$.

Теорема. Якщо $n = x^2 - y^2$, то $\sqrt{n} < x < (n + 1) / 2$.

Доведення. З рівності $n = x^2 - y^2$ випливає, що $n < x^2$, тобто $\sqrt{n} < x$.

Оскільки $a = n / b$, то $x = \frac{(n/b)+b}{2}$. Максимальне значення x досягається при мінімальному b, тобто при $b = 1$. Звідси x = $\frac{(n/b)+b}{2} < \frac{n+1}{2}$.

Отже для пошуку представлення $n = x^2 - y^2$ слід перебрати всі можливі значення x із проміжку $[\sqrt{n},\ (n + 1) / 2]$, перевіряючи при цьому чи є вираз $x^2 - n$ повним квадратом.

Приклад. Розкласти на множники $n = 391$ методом Ферма. $\sqrt{n} = 19$.
$20^2 - 391 = 9 = 3^2$. Маємо рівність: $391 = 20^2 - 3^2$.
Звідси $391 = (20 - 3)(20 + 3) = 17 * 23$.

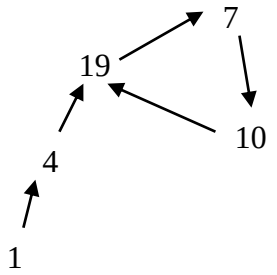
Алгоритм Полард - ро факторизації числа [2, стор.261-263]

У 1974 році Джон Полард запропонував алгоритм знаходження нетривіального дільника натурального числа n. Пр цьому алгоритм використовує лише операції додавання, множення та віднімання модулярної арифметики.

Ідея алгоритма Полард – ро полягає в ітеративному обчисленні деякої наперед заданої поліноміальної функції f з цілими коефіцієнтами. Побудуємо послідовність x_i наступним чином: x_0 оберемо довільним із Z_n, а $x_{i+1} = f(x_i) \bmod n$, $i \geq 0$. Оскільки x_i можуть приймати лише скінченний набір значень (цілі числа від 0 до n), то існують такі цілі n_1 та n_2 ($n_1 < n_2$), що $x_{n_1} = x_{n_2}$. Враховуючи поліноміальність f, для кожного натурального k маємо: $x_{n_1+k} = x_{n_2+k}$, тобто починаючи з індекса $i = n_1$ послідовність $\{x_i \bmod n\}$ буде періодичною.

Приклад. Нехай $n = 21$, $x_0 = 1$, $x_{i+1} = x_i^2 + 3 \bmod 21$.
Тоді послідовність x_i має вигляд: 1, 4, 19, 7, 10, 19, 7, 10, ...
Таким чином $x_3 = x_6$, період послідовності дорівнює 3.

Послідовність x_i можна відобразити у вигляді кола з хвостом: коло відповідає періодичній частині, а хвіст – доперіодичній. Картинка нагадує грецьку літеру ρ, тому метод який застосовується в алгоритмі називається ρ – евристикою. Послідовність із попереднього прикладу можна зобразити так:



Ідея алгоритму полягає в обчисленні для кожного $i > 0$ значення $d = НСД(x_{2i} - x_i, n)$. Якщо на деякому кроці $d > 1$, то це і є нетривіальний дільник числа n.

Побудуємо послідовність елементів x_i наступним чином:

$$x_0 = 2,\ x_{i+1} = f(x_i) = (x_i^2 + 1) \bmod n,\ i > 0$$

Алгоритм

Вхід: натуральне число n, параметр $t \geq 1$.
Вихід: нетривіальний дільник d числа n.
1. $a = 2$, $b = 2$;
2. for $i \leftarrow 1$ to t do
   2.1. Обчислити $a \leftarrow (a^2 + 1) \bmod n$; $b \leftarrow (b^2 + 1) \bmod n$; $b \leftarrow (b^2 + 1) \bmod n$;
   2.2. Обчислити $d \leftarrow НСД(a - b, n)$;
   2.3. if $1 < d < n$ return (d); // знайдено нетривіальний дільник
3. return (False); // дільника не знайдено

Вважаємо, що функція f(x) = (x^2 + 1) mod n генерує випадкові числа. Тоді для знаходження дільника числа n необхідно виконати не більш ніж O($\sqrt{n}$) операцій модулярного множення.

Якщо алгоритм Поларда – ро не знаходить дільника за t ітерацій, то замість функції f(x) = (x^2 + 1) mod n можна використовувати f(x) = (x^2 + c) mod n, для деякого цілого c, c ≠ 0, -2.

Приклад. Нехай n = 19939.

Послідовність x_i: 2, 5, 26, 677, 19672, 11473, 12391, 6582, 15217, 5483, 15217, 5483, 15217, ...

a	b	d
2	2	1
5	26	1
26	19672	1
677	12391	1
19672	15217	1
11473	15217	1
12391	15217	157

Знайдено розклад 19939 = 157 * 127.

Нехай n = 143. Послідовність x_i: 2, 5, 26, 105, 15, ...

a	b	d
2	2	1
5	26	НСД(21, 143) = 1
26	15	НСД(11, 143) = 11

Знайдено розклад 143 = 11 * 13.

Ймовірносний квадратичний алгоритм факторизації числа

Твердження. Нехай x та y – цілі числа, $x^2 \equiv y^2$ (mod n) та $x \neq \pm y$ (mod n). Тоді $x^2 - y^2$ ділиться на n, при чому жоден із виразів $x + y$ та $x - y$ не ділиться на n. Число d = НСД($x^2 - y^2$, n) є нетривіальним дільником n.

Теорема. Якщо n – непарне складене число, яке не є степенем простого числа, то завжди існують такі x та y, що $x^2 \equiv y^2$ (mod n), при чому $x \neq \pm y$ (mod n).

Доведення. Нехай $n = n_1 * n_2$ – добуток взаємно простих чисел. Оберемо таке y, що НСД(y, n) = 1. Далі розв’яжемо систему рівнянь:

$$\begin{cases} x \equiv y \,(\mathrm{mod}\, n_1) \\ x \equiv -y \,(\mathrm{mod}\, n_2) \end{cases}$$

Розв'язком системи будуть такі x та y за модулем n = НСК(n_1, n_2), що $x^2 \equiv y^2$ (mod n). Якщо при цьому припустити, що $x \equiv -y$ (mod n), то з другого рівняння системи маємо: $y \equiv -y$ (mod n_2), або 2 * y = 0 (mod n_2). Оскільки було обрано НСД(y, n_2) = 1, то з останньої рівності випливає що n_2 ділиться на 2, тобто є парним. Це суперечить умові теореми про непарність n.

Приклад. Виберемо n_1 = 11, n_2 = 13 – взаємно прості числа. Тоді n = 11 * 13 = 143. Покладемо y = 5, НСД(5, 143) = 1. Складемо систему порівнянь:

$$\begin{cases} x \equiv 5 \,(\mathrm{mod}\, 11) \\ x \equiv -5 \,(\mathrm{mod}\, 13) \end{cases} \text{ або } \begin{cases} x \equiv 5 \,(\mathrm{mod}\ 11) \\ x \equiv 8 \,(\mathrm{mod}\ 13) \end{cases}$$

Розв'язком системи буде x ≡ 60 (mod 143).

Має місце рівність $60^2 \equiv 5^2$ (mod 143) , при чому 60 ≠ ±5 (mod 143).

Тоді дільником числа n буде d = НСД(60 – 5, 143) = 11.

Формально ймовірносний квадратичний алгоритм факторизації будується на наступній ідеї:

Нехай $F = \{p_0, p_1, p_2, \ldots, p_t\}$ – множникова основа, p_i – різні прості числа, при чому дозволяється обрати p_0 = -1. Побудуємо множину порівнянь

$$x_i^2 \equiv z_i \,,$$

таку що значення z_i є повністю факторизованими у множині F :

$$z_i = \prod_{j=0}^{t} p_j^{e_{ij}} \,,$$

та добуток деякої підмножини значень z_i є повним квадратом:

$$z = \prod_{i=1}^{k} z_i^{f_i} = y^2, y \in \mathrm{Z}, f_i \in \{0, 1\}$$

Якщо множина порівнянь із вказаними властивостями побудована, то поклавши $x = \prod_{i=1}^{k} z_i^{f_i}$ і перевіривши виконання нерівності $x \neq \pm y$ (mod n), отри маємо $x^2 \equiv y^2$ (mod n). Число d = НСД($x^2 - y^2$, n) є нетривіальним дільником n.

Приклад. Знайти дільник числа n = 143.

Обираємо випадково число $x \in$ [2, 142], обчислюємо x^2 (mod 143) та розкладаємо результат на множники:

1. $z_1 = 19^2$ (mod 143) = 75 = 3 * 5^2.
2. $z_2 = 77^2$ (mod 143) = 66 = 2 * 3 * 11.
3. $z_3 = 29^2$ (mod 143) = 126 = 2 * 3^2 * 7.
4. $z_4 = 54^2$ (mod 143) = 56 = 2^3 * 7.

Можна помітити, що добуток z_3 та z_4 є повним квадратом:

$$z = z_3 * z_4 = 2^4 * 3^2 * 7^2 = (2^2 * 3 * 7)^2 = 84^2$$

Маємо рівність:

$$z_3 * z_4 = 29^2 * 54^2 \equiv 84^2 \pmod{143}$$

або враховуючи що $29 * 54 \pmod{143} \equiv 136$, маємо:

$$136^2 = 84^2 \pmod{143}, \text{ при чому } 136 \neq \pm 84 \pmod{143}$$

Дільником числа $n = 143$ буде $d = НСД(136 - 84, 143) = НСД(52, 143) = 13$.

Квадратичний алгоритм факторизації [2, стор. 293-301]

Серед усіх існуючих алгоритмів факторизації найшвидшим є квадратичний. Він ефективно застосовується для чисел, кількість цифр яких менша за 100 та які не мають малих простих дільників. Еврістичний аналіз, проведений Померансом [1] у 1981 році показав, що число N може бути розкладено на множники за час $e^{(1+o(1))\sqrt{\ln N \ln\ln N}}$.

Нехай n – число, яке факторизується, $m = \sqrt{n}$. Розглянемо многочлен

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

Квадратичний алгоритм обирає $a_i = x + m$ ($x = 0, \pm1, \pm2, \ldots$), обчислює значення $b_i = (x + m)^2 - n$ та перевіряє, чи факторизується b_i у множниковій основі $F = \{p_0, p_1, p_2, \ldots, p_t\}$.

Помітимо, що $a_i^2 = (x + m)^2 - n \equiv (x + m)^2 \pmod{n} \equiv b_i \pmod{n}$.

Алгоритм

Вхід: натуральне число n, яке не є степенм простого числа.

Вихід: нетривіальний дільник d числа n.

1. Обрати множникову основу $F = \{p_0, p_1, p_2, \ldots, p_t\}$, де $p_0 = -1$, p_i – i - те просте число p, для якого n є квадратичним лишком за модулем p.

2. Обчислити $m = [\sqrt{n}]$.

3. Знаходження $t + 1$ пари (a_i, b_i).

   Значення x перебираються у послідовності $0, \pm1, \pm2, \ldots$.

   Покласти $i \leftarrow 1$. Поки $i \leq t + 1$ робити:

   3.1. Обчислити $b = q(x) = (x + m)^2 - n$ та перевірити, чи розкладається b у множниковій основі F. Якщо ні, обрати наступне x та повторити цей крок.

   3.2. Нехай $b = \prod_{j=1}^{t} p_j^{e_{ij}}$. Покласти $a_i = x + m$, $b_i = b$, $v_i = (v_{i1}, v_{i2}, \ldots, v_{it})$, де $v_{ij} = e_{ij} \bmod 2$, $1 \leq j \leq t$.

   3.3. $i \leftarrow i + 1$.

4. Знайти підмножину $T \subseteq \{1, 2, \ldots, t + 1\}$ таку що $\sum_{i \in T} v_i = 0$.

5. Обчислити $x = \prod_{i \in T} a_i \bmod n$.

6. Для кожного j, $1 \leq j \leq t$, обчислити $l_j = (\sum_{i \in T} e_{ij}) / 2$.

7. Обчислити $y = \prod_{j=1}^{t} p_j^{l_j} \bmod n$.

8. Якщо $x \equiv \pm y \pmod n$, знайти іншу підмножину $T \subseteq \{1, 2, \ldots, t + 1\}$ таку що $\sum_{i \in T} v_i = 0$ та перейти до кроку 5.
9. Обчислити дільник $d = НСД(x - y, n)$.

Приклад. Розкласти на множники $n = 24961$.
1. Побудуємо множникову основу: $F = \{-1, 2, 3, 5, 13, 23\}$
2. $m = [\sqrt{24961}\,] = 157$.
3. Побудуємо наступну таблицю:

i	x	q(x)	факторизація q(x)	a_i	v_i
1	0	-312	$-2^3 * 3 * 13$	157	(1, 1, 1, 0, 1, 0)
2	1	3	3	158	(0, 0, 1, 0, 0, 0)
3	-1	-625	-5^4	156	(1, 0, 0, 0, 0, 0)
4	2	320	$2^6 * 5$	159	(0, 0, 0, 1, 0, 0)
5	-2	-936	$-2^3 * 3^2 * 13$	155	(1, 1, 0, 0, 1, 0)
6	4	960	$2^6 * 3 * 5$	161	(0, 0, 1 ,1, 0, 0)
7	-6	-2160	$-2^4 * 3^3 * 5$	151	(1, 0, 1, 1, 0, 0)

4. Виберемо T = {1, 2, 5}, оскільки $v_1 + v_2 + v_5 = 0$.
5. Обчислимо x = $(a_1 a_2 a_5) \pmod n = 936 = 2^6 * 3^4 * 13^2$.
6. $l_1 = 1$, $l_2 = 3$, $l_3 = 2$, $l_4 = 0$, $l_5 = 1$, $l_6 = 0$.
7. $y = -2^3 * 3^2 * 13 \pmod n = 24025$.
8. Оскільки $936 \equiv -24025 \pmod n$, необхідно шукати іншу множину T.
9. Виберемо T = {3, 6, 7}, оскільки $v_3 + v_6 + v_7 = 0$.
10. Обчислимо x = $(a_3 a_6 a_7) \bmod n = 23405 = 2^{10} * 3^4 * 5^6$.
11. $l_1 = 1$, $l_2 = 5$, $l_3 = 2$, $l_4 = 3$, $l_5 = 0$, $l_6 = 0$.
12. $y = -2^5 * 3^2 * 5^3 \pmod n = 13922$.
13. $23405 \neq \pm 13922 \pmod n$.
$d = НСД(x - y, n) = НСД(9483, 24961) = 109$ – дільник.
Відповідь: 109 – дільник 24961.

Література

1. Pomerance C. Analysis and comparison of some integer factorization algorithms. In Computational Methods in Number Theory, vol.154, H.Lenstra and R.Tijdeman, Eds. Amsterdam Mathematics Center 1982, pp. 89 – 139.

2. Крэндалл Р., Померанс К. Простые числа. Криптографические и вычислительные аспекты.