Державна служба України з надзвичайних ситуацій
Національна академія педагогічних наук України
Департамент освіти і науки Львівської обласної державної адміністрації
Львівський державний університет безпеки життєдіяльності
Інститут педагогічної освіти і освіти дорослих НАПН України
Інститут інформаційних технологій та засобів навчання НАПН України
Інститут професійно-технічної освіти НАПН України

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В СУЧАСНІЙ ОСВІТІ: ДОСВІД, ПРОБЛЕМИ, ПЕРСПЕКТИВИ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Випуск 5

Львів-2017

УДК 512.8

М. Ф. Стасюк, *канд. фіз.-мат. наук,*
Львівський державний університет безпеки життєдіяльності, м. Львів

ДЕЯКІ ПІДХОДИ ДО ПРОБЛЕМИ ФАКТОРИЗАЦІЇ

У запропонованих матеріалах викладені два підходи до розв'язання задачі факторизації, тобто до задачі про розклад великого непростого цілого числа на множники. Перший – це По-метод або метод Монте Карло, другий – факторизація Ферма. Ці методи використовують різноманітні конструкції алгебри і теорії чисел. Задача факторизації є важливою задачею криптології. Знаходження таємного ключа для системи RSA є еквівалентною задачею до задачі факторизації чисел, що є добутком двох простих.

Ключові слова: факторизація, відображення, ітерація, факторна база, лишок за модулем, B -числа.

In the proposed materials there have been outlined two approaches to the solution of the factorization problem, i.e. to the problem of the decomposition of a large non-complex integer into multipliers. The first one is the Po Method or the Monte Carlo Method; the second one is Fermat's factorization Method. These methods use various constructions of algebra and number theory. The problem of factoring is an important task of cryptology. Specifically, finding a secret key for the RSA system is equivalent to the problem of the factorization of numbers, which is the product of two prime numbers.

Key words: factorization, reflection, iteration, factor base, deduction modulo, B-numbers.

В предложенных материалах изложены два подхода к решению задачи факторизации, то есть к задаче о разложении большого непростого целого числа на множители. Первый – По-метод или метод Монте-Карло, второй – факторизация Ферма. Эти методы используют различные конструкции алгебры и теории чисел. Задача факторизации является важной задачей криптологии. Нахождение секретного ключа для системы RSA эквивалентна задаче факторизации чисел, которые суть произведение двух простых.

Ключевые слова: факторизация, отображение, итерация, факторная база, вычет по модулю, B-числа.

Факторизація натурального числа, тобто задача пошуку всіх його простих дільників належить до найважливіших задач криптології.

На сьогоднішній день задача факторизації є важкою. Найефективніший з відомих алгоритмів потребує часу

$$\exp\left\{c\sqrt{\ln n \ln\ln n}\right\},$$

причому в найкращому випадку $c = 1$.

На межі сучасних можливостей є факторизація чисел із 150 десятковими цифрами. Розклад на множники чисел, які мають 200 десяткових знаків, на думку експертів, залишається справою майбутнього[1].

В цьому повідомленні розглянуто два підходи до розв'язання задачі факторизації, які використовують тільки найпростіші поняття алгебри і теорії чисел. Ці підходи є відомими, проте вони адаптовані до засвоєння зацікавленими особами, які не мають ґрунтовної математичної підготовки. Всі викладки супроводжуються доступними прикладами.

1. Ро-метод (метод Монте-Карло)

Цей метод полягає в знаходженні дільника цілого числа n шляхом використання ітерацій деякого многочлена $f(x)$. Для застосування цього методу потрібно:

- вибрати кільце $\mathbb{Z}/n\mathbb{Z}$;
- вибрати незвідний многочлен $f(x)$, який здійснює відображення

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{f(x)} \mathbb{Z}/n\mathbb{Z};$$

- вибрати деяке конкретне значення x_0 (1, або 2, або випадкове ціле число) і послідовно обрахувати ітерації:

$$x_1 = f(x_0); \quad x_2 = f(x_1), \quad \ldots, \quad x_{i+1} = f(x_i), \quad 0,1,2,3,\ldots;$$

– порівняти різні x_i з метою знайти два різні класи лишків за модулем n, проте однакові за модулем деякого дільника n;
– як тільки такі класи знайдені, то знайти власний дільник a числа n, як $\text{НСД}(x_j - x_k, n)$.

В По-методі многочлен $f(x)$ повинен визначати відображення $\mathbb{Z}/n\mathbb{Z}$ в себе нерегулярним випадковим способом, тобто $f(x)$ повинен бути не лінійним і не визначати ізоморфне відображення.

Суть По-методу полягає в послідовному обчисленні $x_k = f(x_{k-1})$ і порівнянні x_k з раніше отриманим x_j до того часу, поки не знайдеться пара з $НСД(x_k - x_j) = r > 1$. Однак, з ростом k обчислення $НСД(x_k - x_j, n)$ для всіх $j < k$ стає трудомістким, тому покажемо, як потрібно діяти, щоб для кожного k обчислювати тільки один НСД.

Для цього застосуємо модифікацію По-методу. Ця модифікація полягає в тому, що при обчисленні x_k на кожному кроці, виконаємо наступне:

– подамо k у вигляді $(n+1)$ – розрядного числа в двійковій системі координат, тобто $2^n \le k \le 2^{n+1}$
– покладемо $j = 2^n - 1$;
– порівняємо x_k з x_j, тобто обчислимо $НСД(x_k - x_j, n)$;
– якщо в результаті отримаємо, що $НСД(x_k - x_j, n) = r \neq 1$, то зупиняємось;
– в іншому випадку перейдемо до $k+1$.

Ця модифікація скорочує кількість операцій і виявляє дільник r числа n, $1 < r < \sqrt{n}$ за $O(n \ln^3 n)$ двійкових операцій.

Приклад 1. Розкласти на множники число $n = 8051$.

Виберемо $f(x) = x^2 + 1$ і покладемо $x_0 = 1$. Обчислимо послідовно ітерації в $\mathbb{Z}/8051\mathbb{Z}$:

$$x_1 = f(x_0) = 2; \quad x_2 = f(x_1) = 5; \quad x_3 = f(x_2) = 26;$$
$$x_4 = f(x_3) = 677; \quad x_5 = f(x_4) = 7474; \quad x_6 = f(x_5) = 2839.$$

Враховуючи алгоритм модифікованого По-методу, обчислимо $\text{НСД}(x_k - x_j, 8051)$, аж поки не прийдемо до варіанту $\text{НСД}(x_k - x_j, 8051) = r \neq 1$.

Маємо

$$НСД(x_1 - x_0, 8051) = НСД(1, 8051) = 1; \quad НСД(x_2 - x_1, 8051) = НСД(3, 8051) = 1;$$
$$НСД(x_3 - x_1, 8051) = НСД(24, 8051) = 1; \quad НСД(x_4 - x_3, 8051) = НСД(651, 8051) = 1;$$
$$НСД(x_5 - x_3, 8051) = НСД(7448, 8051) = 1; \quad НСД(x_6 - x_3, 8051) = НСД(2813, 8051) = 97.$$

Отже, $8051 = 97 \cdot 83$.

2. Факторизація Ферма

Факторизація Ферма ґрунтується на наступному твердженні.

Твердження 1. Нехай n – натуральне число. Існує взаємно-однозначна відповідність між факторизацією $n = a \cdot b$, $a \ge b > 0$ і поданням числа n у вигляді $t^2 - s^2$, де s і t – невід'ємні цілі числа:

$$t=\frac{a+b}{2},\quad s=\frac{a-b}{2},\quad a=t+s,\quad b=t-s.$$

Дійсно, якщо $n=a\cdot b$, то $n=\left(\frac{a+b}{2}\right)^2-\left(\frac{a-b}{2}\right)^2=t^2-s^2$.

Навпаки, якщо $n=t^2-s^2$, то $n=(t+s)\cdot(t-s)$.

Якщо множники a і b – близькі, то $\frac{a-b}{2}$ – мале число і t – трохи більше за $\sqrt{n}$. Тоді для перевірки співвідношення $n=t^2-s^2$ можна випробовувати всі значення t, починаючи з $\left|\sqrt{n}\right|+1$ до того часу, поки не знайдемо таке його значення, для якого виконується рівність $t^2-n=s^2$, тобто різниця t^2 і n дає повний квадрат.

Приклад 2. Розкласти на множники число $n=92296873$.

Оскільки $\left|\sqrt{92296873}\right|=9607$, то випробовуємо значення $t=\left|\sqrt{92296873}\right|+1=9608$, $t=\left|\sqrt{92296873}\right|+2=9609,\ldots$, $t=\left|\sqrt{92296873}\right|+6=9613$. Легко переконатись, що останнє число $t=2613$ забезпечує повний квадрат $s^2=336^2$ в рівності $t^2-n=s^2$, а попередні t не забезпечують повного квадрата. Тому, число n, за твердженням 1, розкладається на множники

$$92296873=(9613+336)\cdot(9613-336)=9949\cdot 9277.$$

Факторні бази.

Ще одне узагальнення ідеї, що лежить в основі факторизації Ферма приводить до більш ефективного методу факторизації цілого n. А саме, якщо вдається отримати конгруенцію $t^2\equiv s^2\pmod n$ з $t\neq\pm s\pmod n$, то можна знайти множник числа n, як НСД$(t+s,n)$ (або НСД$(t-s,n)$). Дійсно, n ділить $t^2-s^2=(t+s)(t-s)$, проте не ділить ні $t+s$, ні $t-s$, то НСД$(t+s,n)$ має бути власним дільником a числа n, а $b=\frac{n}{a}$ ділить НСД$(t-s,n)$.

Виникає запитання, чи можливо при випадковому виборі різних b швидко отримати таке його значення, щоб найменший додатний лишок b^2 за модулем n був повним квадратом? Такий вибір досягається з допомогою методу факторних баз.

Надалі, *найменшим абсолютним лишком числа a за модулем n* називатимемо ціле число з інтервалу $\left(-\frac{n}{2},\frac{n}{2}\right)$, яке конгруентне числу a за модулем n.

Означення.

- *Факторною базою* називається множина $B=\{p_1,p_2,\ldots,p_h\}$, яка складається з різних простих чисел, окрім числа p_1, яке може дорівнювати -1.
- Скажемо, що квадрат числа b є B – число (для заданого числа n), якщо найменший абсолютний лишок $b^2\pmod n$ можна записати, як добуток чисел з множини B.

Приклад 3. Нехай $n=4633$ і факторна база B – це множина $\{-1,2,3\}$. Тоді квадрати чисел $67,68,69$ – це B – числа для заданого $n=4633$.

Дійсно,

$$67^2=4489\equiv -144\pmod{4633},\quad 67^2=-1\cdot 2^4\cdot 3^2,$$

$$68^2 = 4624 \equiv -9 \pmod{4633}, \quad 68^2 = -1 \cdot 3^2,$$
$$69^2 = 4761 \equiv 128 \pmod{4633}, \quad 69^2 = 2^7.$$

Нехай F_2^h – векторний простір над полем F_2, тобто $F_2^h = \{a_1, a_2, ..., a_h\}$, $a_i \in F_2$, $i = \overline{1,h}$. Тоді, якщо задане число n і задана факторна база B, то кожному B – числу $b^2 \pmod{n} = \prod_{j=1}^{h} p_j^{\alpha_j}$ поставимо у відповідність вектор $\vec{\varepsilon} \in F_2^h$ наступним чином: $b^2 \to \vec{\varepsilon} = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_h)$, де

$$\varepsilon_j = \begin{cases} 0, & якщо \quad j - парне \\ 1, & якщо \quad j - непарне \end{cases}, \quad j = \overline{1,h}.$$

Приклад 4. У факторній базі $B = \{-1, 2, 3\}$ для $n = 4633$ B – числам $67^2, 68^2, 69^2$ відповідають вектори :

$$67^2 \to (1,0,0); \quad 68^2 \to (1,0,0); \quad 69^2 \to (0,1,0).$$

Припустимо, що ми маємо множину B – чисел $b_i^2 \pmod{n} \to \vec{\varepsilon}_i = (\varepsilon_{i1}, \varepsilon_{i2}, ..., \varepsilon_{ih})$ таких, що

$$\sum_{i=1}^{h} \vec{\varepsilon}_i = \vec{0}. \tag{1}$$

Тоді справджується рівність

$$\prod_i b_i^2 \pmod{n} = \prod_{j=1}^{h} p_j^{\sum \alpha_{ij}}$$

і показник кожного p_j в правій частині останньої рівності – парне число і отже є квадратом числа $\prod_{j=1}^{h} p_j^{\gamma_j}$, де $\gamma_j = \frac{1}{2} \sum_i \alpha_{ij}$. Отже, ми приходимо до конгруенції

$$b = \prod_i b_i \equiv \prod_{j=1}^{h} p_j^{\gamma_j} \pmod{n} = c, \tag{2}$$

в якій ліва і права частини отримані різними шляхами.

Якщо виявиться, що $b \equiv \pm c \pmod{n}$, то шукатимемо нову сукупність B – чисел, для яких сума відповідних векторів дорівнює 0. Виявляється, що при випадковому виборі b_i і непростому n слід очікувати, що $b \equiv \pm c \pmod{n}$ не більше, як у 50% випадках [2]. Якщо ж ми повторимо описану процедуру k разів, то ймовірність невдачі не перевищить $\frac{1}{2^k}$.

Приклад 5. Розкладемо на множники число $n = 1829$, вибравши за b_i числа $\left|\sqrt{1829}k\right|, \left|\sqrt{1829}k\right| + 1, ...$ $k = 1,2,3,4$ такі, що $b_i^2 \pmod{n}$ дорівнюють добутку простих чисел, які менші за 20.

Такими b_i є числа: $42, 43, 61, 74, 85, 86$. Знайдемо b_i^2:

$$42^2 \equiv -65 \pmod{1829} = -1 \cdot 5 \cdot 13 \to (1, \ 0, \ 0, \ 1, \ 0, \ 0, \ 1),$$
$$43^2 \equiv 20 \pmod{1829} = 2^2 \cdot 5 \to (0, \ 0, \ 0, \ 1, \ 0, \ 0, \ 0),$$

$$61^2 \equiv 63 \pmod{1829} = 3^2 \cdot 7 \to (0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0),$$
$$74^2 \equiv -11 \pmod{1829} = -1 \cdot 11 \to (1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0),$$
$$85^2 \equiv -91 \pmod{1829} = -1 \cdot 7 \cdot 13 \to (1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1),$$
$$86^2 \equiv -80 \pmod{1829} = -1 \cdot 2^4 \cdot 5 \to (1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0).$$

Отже, для $b_i^2 \pmod{1829}$ вказані відображення в F_2^7, а за факторну базу потрібно вибрати множину $B = \{-1,2,3,5,7,11,13\}$. Знайдемо вектори (1), тобто ті вектори, які є образами $b_i^2 \pmod{1829}$ і в сумі дають $\vec{0}$-вектор. Легко бачити, що це образи квадратів $43^2 \pmod{1829}, 61^2 \pmod{1829}, 85^2 \pmod{1829}$.

Використавши формулу (2), прийдемо до конгруенції

$$(42 \cdot 43 \cdot 61 \cdot 85)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2 \pmod{1829},$$

яка еквівалентна наступній $1459^2 \equiv 901^2 \pmod{1829}$. Таким чином, дільником a числа $n = 1829$ є НСД$(1459 + 901, 1829) = 59$ і остаточно отримуємо $1829 = 59 \cdot 31$.

Зауважимо, що знаходження таємного ключа для системи RSA є еквівалентною задачею до задачі факторизації чисел, що є добутком двох простих.

Список літератури:

1. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998. – 246 с.

2. Коблиц Н. Курс теории чисел и криптография / Коблиц Н. – М. : Научное издательство ТВП, 2001. – 254с.