УДК 512.8

СКІНЧЕНІ ЛАНЦЮГОВІ ДРОБИ ТА ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

М.М. Стасюк, Р.М. Таційй, О.Ю. Пазен

Львівський державний університет безпеки життєдіяльності, Львів
e-mail: marta_stasiuk@yahoo.com

Ланцюгові дроби мають різноманітні застосування у фізиці, астрономії, геометрії, теорії чисел, криптографії.

Нехай $\frac{a}{b}$ – раціональне число з додатним знаменником, тобто a,b – цілі числа. Застосуємо до чисел a і b алгоритм Евкліда, який найчастіше використовують для знаходження НСД (a,b). Маємо:

$$\begin{aligned}
&a = bq_1 + r_2, \quad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},\\
&b = r_2q_2 + r_3, \quad \frac{b}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}},\\
&r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},\\
&r_{n-1} = r_nq_n, \quad \frac{r_{n-1}}{r_n} = q_n.
\end{aligned} \tag{1}$$

Тоді

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots \; \ddots + \cfrac{1}{q_n}}} \tag{2}$$

Числа $q_1, q_2, ..., q_n$ називаються неповними частками послідовних поділів у алгоритмі Евкліда, а вираз (2) – ланцюговим дробом і позначається

$$\frac{a}{b}=[q_1,q_2,...,q_n] \tag{3}$$

Дроби $\delta_1=q_1,\quad \delta_2=q_1+\frac{1}{q_2},\quad \delta_3=q_1+\frac{1}{q_2+\frac{1}{q_3}},\quad ...,$ називаються підхідними дробами. Для підхідних дробів $\delta_s=\frac{P_s}{Q_s},\quad s=2,3,...,n,$ справджується рекурентна формула [1]

$$\frac{P_s}{Q_s}=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}},\quad P_0=1,\quad Q_0=0,\quad P_1=q_1,\quad Q_1=1. \tag{4}$$

Ланцюгові дроби можна ефективно використовувати при розв'язанні конгруенцій

$$ax\equiv b(\mathrm{mod}\,m). \tag{5}$$

За умови, що $a,b,m-$цілі, НСД$(a,m)=1$, розв'язок (5) –єдиний і подається у вигляді[1]

$$x\equiv(-1)^{n-1}P_{n-1}b(\mathrm{mod}\,m), \tag{6}$$

де $\frac{m}{a}=[q_1,q_2,...,q_n]$, а $\delta_{n-1}=\frac{P_{n-1}}{Q_{n-1}}$.

Запропонована в 1977 році система RSA є однією з найпопулярніших криптосистем з відкритим ключем. Генерування ключів (відкритого і таємного) в цій системі здійснюється[2] наступним чином: а) вибирають два досить великі прості числа p і q та обчислюють їх добуток $n=p\cdot q.$ Для числа n обчислюють функцію Ейлера $\varphi(n)=\varphi(p)\cdot\varphi(q)=(p-1)(q-1);$ б) випадковим чином вибирають елемент $e\in Z^*_{\varphi(n)}$, який не перевищує $\varphi(n)$ і взаємно простий з $\varphi(n);$ в) знаходять інверсію елемента e за $\mathrm{mod}\,\varphi(n),$тобто розв'язують конгруенцію

$$e\cdot d\equiv 1(\mathrm{mod}\,\varphi(n)), \tag{7}$$

яка через сформульовані вимоги, має єдиний розв'язок.

Описані дії визначають відкритий ключ $e, n = p \cdot q$ і таємний ключ d.

Таємний ключ d, як розв'язок конгруенції (7), можна шукати за формулою (6), де $\frac{\varphi(n)}{e} = [q_1, q_2, ..., q_k]$, тобто використовуючи скінчені ланцюгові дроби.

Приклад. Нехай $p = 41, \quad q = 53, \quad e = 1297$. Знайдемо таємний ключ d.

Переконаємось, що НСД $(e, \varphi(n)) = (1297, 2080) = 1$ й одночасно знайдемо ланцюговий дріб $\frac{2080}{1297}$. Застосувавши алгоритм Евкліда до чисел 2080 і 1297, прийдемо до такого ланцюгового дробу

$$\frac{2080}{1997} = [1,1,1,1,1,10,4,1,4].$$

Для знаходження таємного ключа d розв'яжемо конгруенцію

$$1297 \cdot d \equiv 1(2080).$$

Розв'язок цієї конгруенції знайдемо за формулою (6). Для цього складемо таблицю чисельників підхідних дробів, використовуючи рекурентну формулу (4):

Таблиця 1

Чисельники підхідних дробів

q_s		1	1	1	1	1	10	4	1
P_s	1	1	2	3	5	8	85	348	433

Тоді за формулою (6) маємо:

$$d \equiv (-1)^8 433 (\mathrm{mod}\, 2080) \equiv 433 (\mathrm{mod}\, 2080).$$

Отже таємний ключ $d = 433$. Зауважимо, що приклад – ілюстративний, бо реально в криптосистемі *RSA* використовують дуже великі прості числа.

Література

1. И. М. Виноградов Основы теории чисел / И. М. Виноградов. – Москва.:Наука, 1965. – 172с.

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