МАТЕРІАЛИ ДРУКУЮТЬСЯ УКРАЇНСЬКОЮ, АНГЛІЙСЬКОЮ, ПОЛЬСЬКОЮ ТА РОСІЙСЬКОЮ МОВАМИ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

XII Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів

До 70-річчя заснування університету

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Частина 2

Львів – 2017

РЕДАКЦІЙНА КОЛЕГІЯ:

УДК 512.8

СКІНЧЕНІ ЛАНЦЮГОВІ ДРОБИ ТА ЇХ ЗАСТОСУВАННЯ

Хомич І.
Стасюк М.Ф., канд. фіз.-мат. наук.
Львівський державний університет безпеки життєдіяльності

Ланцюгові дроби мають різноманітні застосування у фізиці, астрономії, геометрії, теорії чисел. В криптології ланцюгові дроби використовуються для генерування таємного ключа в RSA системі з відкритим ключем.

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:

$$a = bq_1 + r_2, \quad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = r_2 q_2 + r_3, \quad \frac{b}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}}, \tag{1}$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n, \quad \frac{r_{n-1}}{r_n} = q_n.$$

Тоді

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

Числа $q_1, q_2, \ldots, q_n$ називаються *неповними остачами* послідовних поділів у алгоритмі Евкліда, а вираз (2) – *ланцюговим дробом* і позначається

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

Дроби

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \quad \ldots,$$

називаються *підхідними дробами*. Для підхідних дробів $\delta_s = \frac{P_s}{Q_s}$, $s = 2, 3, \ldots, n$, справджується рекурентна формула [1]

$$\frac{P_s}{Q_s} = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}, \quad P_0 = 1, \quad Q_0 = 0, \quad P_1 = q_1, \quad Q_1 = 1. \qquad (4)$$

Застосування. Для знаходження таємного ключа d в *RSA* системі з відкритим ключем потрібно розв'язати конгруенцію [1]

$$ed \equiv 1 \pmod{\varphi(pq)}.$$

Розв'язок такої конгруенції, яку можна записати, в загальному випадку, у вигляді $ax \equiv b \pmod{m}$, за умови, що a, b, m – цілі, НСД$(a, m) = 1$ – єдиний і подається у вигляді [1]

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m}, \qquad (5)$$

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

Приклад. Знайти інверсію числа 1710 за модулем 1997, тобто розв'язати конгруенцію $1710x \equiv 1 \pmod{1997}$.

Використовуючи (1), запишемо ланцюговий дріб для дробу $\frac{1997}{1710}$ у вигляді (3). Складемо таблицю чисельників підхідних дробів, використовуючи рекурентну формулу (4):

q_s		1	5	1	22	1	11
P_s	1	1	6	7	160	167	

Тоді за формулою (5) маємо:

$$x \equiv (-1)^5 \, 167 \pmod{1997} \equiv -167 \pmod{1997} \equiv 1830 \pmod{1997}.$$

Отже інверсія числа 1710 за модулем 1997 дорівнює 1830.

Література:

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