APPLICATION OF EUCLIDEAN ALGORITHM TO SET THE CIPHER

ỨNG DỤNG CỦA THUẬT TOÁN EUCLID ĐỂ ĐẶT MẬT MÃ

Nguyễn Văn Bình, Nguyễn Hữu Thành, Phạm Mẫn Minh,
Ngô Thị Thu Ba, Võ Thị Thanh Giang
Trường Đại học Sư phạm - Đại học Đà Nẵng

ABSTRACT: *Arithmetic is one of the oldest fields of mathematics. However, today arithmetic still has very topical applications such as applications in information security. In this paper, we apply the Euclid algorithm and continued fractions to extend the results of [2] and [3] in setting encryption for some specific situations.*

Keyword: *Euclidean algorithm, continued fraction, cryptography.*

TÓM TẮT: *Số học là một trong những lĩnh vực cổ xưa nhất của toán học. Tuy nhiên, ngày nay số học vẫn có những ứng dụng rất thời sự như ứng dụng trong viêc bảo mật thông tin. Trong bài báo này, chúng tôi ứng dụng thuật toán Euclid và liên phân số để mở rộng các kết quả của [2] và [3] trong việc đặt mật mã cho một số tình huống cụ thể.*

Từ khóa: *Thuật toán Euclid, liên phân số, mật mã.*

1. GIỚI THIỆU

Được xem là một trong những thuật toán cổ xưa nhất mà nhân loại biết đến, thuật toán Euclid lần đầu tiên xuất hiện một cách tường minh trong cuốn "Euclid's Elements" vào khoảng năm 300 trước Công nguyên. Ban đầu, Euclid tiếp cận bài toán này dưới góc độ hình học, cụ thể là việc tìm ra một ước số chung cho độ dài của hai đoạn thẳng. Thuật toán của ông giải quyết vấn đề một cách khéo léo thông qua việc lặp đi lặp lại phép trừ đoạn dài hơn cho đoạn ngắn hơn. Tuy nhiên, có lẽ thuật toán này không hoàn toàn là "phát minh" của Euclid, mà rất có thể đã được biết đến từ trước đó khoảng hai thế kỷ. Thậm chí, người ta còn ghi nhận sự hiểu biết về thuật toán này bởi Eudoxus of Cnidus (khoảng năm 375 trước Công nguyên) và Aristotle (khoảng năm 330 trước Công nguyên).

Thuật toán Euclid và liên phân số là hai khái niệm và cũng là hai công cụ quan trọng trong nghiên cứu về số học (xem [1],[4]). Trong toán học, thì số học là một trong những lĩnh vực cổ xưa nhất. Tuy nhiên, cho tới ngày nay lĩnh vực này vẫn tồn tại nhiều bài toán và giả thuyết chưa có lời giải. Hơn nữa, số học không chỉ là lĩnh vực lí thuyết thuần tuý trong toán học mà cùng với sự phát triển của khoa học và công nghệ, số học vẫn có nhiều ứng dụng rất thời sự, đặc biệt là trong lĩnh vực bảo mật thông tin. Trong các tài liệu tham khảo [2] và [3], các tác giả đã giới thiệu một số kỹ thuật đặt mật mã. Bài báo này, chúng tôi sử dụng thuật toán Euclid và liên phân số để mở rộng các kết quả trong các tài liệu đó để đặt một số mật mã cụ thể.

2. MỘT SỐ KIẾN THỨC CHUẨN BỊ

Trong mục này, chúng tôi sẽ nhắc lại một số khái niệm và kết quả để chuẩn bị cho việc trình bày các kết quả chính ở mục sau.

2.1. Thuật toán Euclid

2.1.1. Thuật toán chia

Cho $a \in \mathbb{Z}, b \in \mathbb{Z}_{>0}$. Khi đó tồn tại duy nhất cặp số nguyên (q, r) sao cho $a = bq + r, 0 \leq r < b$. Khi đó, q được gọi là thương số trong phép chia a cho b và r được gọi là phần dư của phép chia đó.

Nội dung thuật toán Euclid:

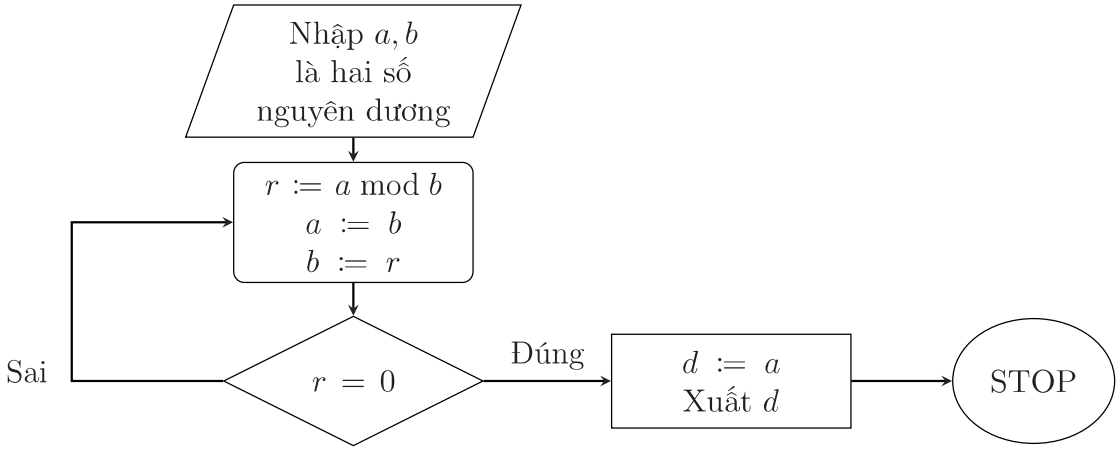
Cho $r_0 := a \in \mathbb{Z}$, $r_1 := b \in \mathbb{Z}_{>0}$ ta áp dụng liên tiếp thuật toán chia:
$r_j = r_{j+1}q_{j+1} + r_{j+2}$ với $q_{j+1}, r_{j+1} \in \mathbb{Z}$ mà $0 \leq r_{j+2} < r_{j+1}$ với $j = 0, 1, ...$ và nhận được dãy giảm ngặt các số tự nhiên $r_1 > r_2 > ...$ đến khi lần đầu tiên nhận được phần dư $r_n = 0$ $(2 \leq n \in \mathbb{Z})$.
Khi đó thuật toán khẳng định rằng ƯSCLN$(a, b) = r_{n-1}$ (phần dư khác 0 cuối cùng của phép chia).

Ví dụ 2.1

Muốn tìm ƯSCLN của hai số 867 và 697 thì các bước thuật toán sẽ như sau:

STT của j	r_j	r_{j+1}	q_{j+1}	$r_{j+2} = r_j \bmod r_{j+1}$	ƯSCLN của (a, b)
0	867	697	1	170	
1	697	170	4	17	
2	170	17	10	0	
3	17	0			**17**

Thuật toán được diễn tả ở dạng biểu đồ sau:



Hình 1: Thuật toán Euclid để tìm ước số chung lớn nhất của hai số nguyên dương a và b.

2.2. Liên phân số

2.2.1. Liên phân số hữu hạn

Định nghĩa 1. Liên phân số hữu hạn cấp n là biểu thức có dạng:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Trong đó $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{Z}_{>0}, a_1, a_2, \ldots, a_n$, được gọi là các *thương hụt* hay đơn giản là các *thương*. Số nguyên a_i được gọi là thương hụt thứ i, $i = 1, 2, \ldots, n$.

Kí hiệu liên phân số hữu hạn là $[a_0 \colon a_1, \ldots, a_n]$.

2.2.2. Liên phân số vô hạn

Định nghĩa 2. Liên phân số vô hạn là biểu thức có dạng:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cdots}}}}$$

Trong đó $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{Z}_{>0}, a_1, a_2, \ldots, a_{n,\ldots}$, được gọi là các thương hụt hay đơn giản là các thương. Số nguyên a_i được gọi là thương hụt thứ $i, i = 1, 2, \ldots, n, \ldots$.

Kí hiệu liên phân số vô hạn là $[a_0 \colon a_1, \ldots, a_n, \ldots]$.

Định nghĩa 3. Một liên phân số vô hạn $[a_0 \colon a_1, \ldots, a_n, \ldots]$ được gọi là tuần hoàn nếu tồn tại các số $N, k \in \mathbb{N}$ sao cho $a_n = a_{n+k}$ với mọi $n \geq N \in \mathbb{N}$.

Kí hiệu

$[a_0 \colon a_1, a_2, ..., a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k-1}}.]$

2.2.3 Biểu diễn số hữu tỉ thành liên phân số

Ta biết được mọi số hữu tỉ đều biểu diễn được dưới dạng $\frac{a}{b}$ với $a, b \in \mathbb{Z}, b \neq 0$, nên phân số có thể chuyển thành một liên phân số khi thực hiện các bước sau:

Bước 1: Chia lấy phần nguyên

Chia a cho b để lấy phần nguyên q_0 và phần dư $r_0 : q_0 = \left\lfloor \frac{a}{b} \right\rfloor, r_0 = a - q_0 b$.

Khi đó: $\frac{a}{b} = q_0 + \frac{r_0}{b}$.

Bước 2: Nghịch đảo phần phân số $\frac{r_0}{b}$.

Khi đó: $\frac{b}{r_0} = \frac{1}{\frac{r_0}{b}}$.

Bước 3: Lặp lại quá trình đến khi $r_n = 0$.

Ví dụ: Hãy biểu diễn số hữu tỉ $\frac{867}{697}$ thành liên phân số.

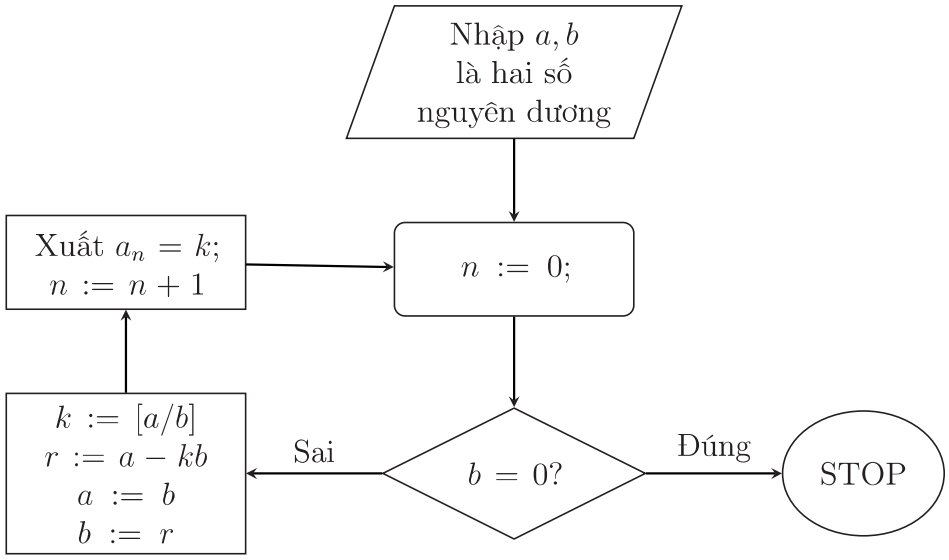
$$\frac{867}{697} = 1 + \frac{10}{41} = 1 + \frac{1}{\frac{41}{10}} = 1 + \frac{1}{4 + \frac{1}{10}}.$$

Vậy $\frac{867}{697} = 1 + \cfrac{1}{4 + \cfrac{1}{10}}$ hay $\frac{867}{697} = [1 : 4, 10]$.

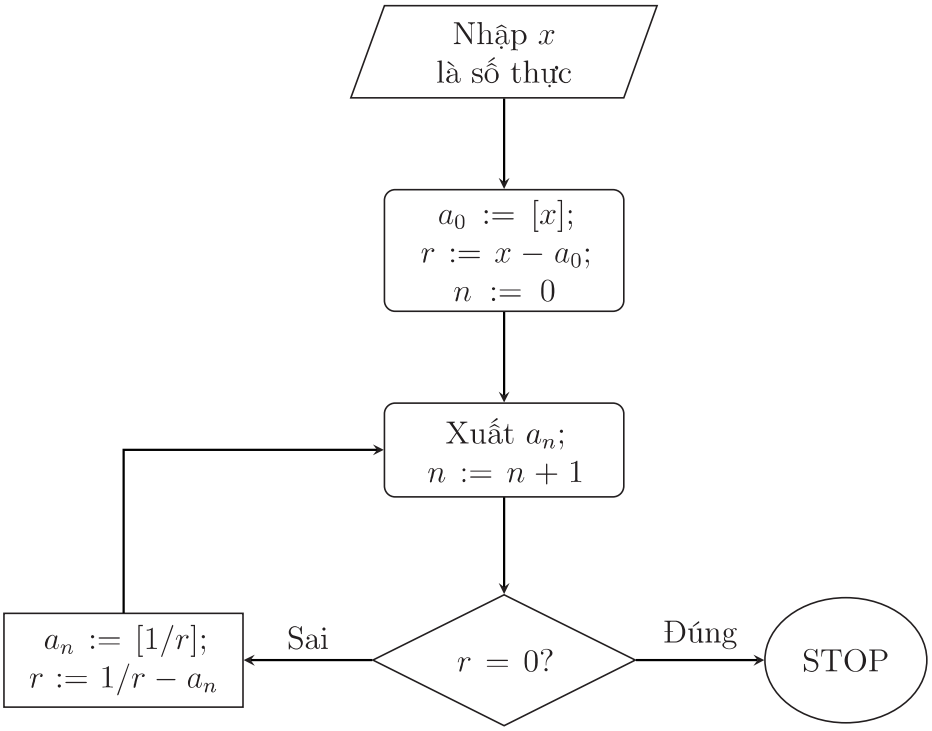
Đọc kĩ ta thấy được nhiều điểm tương đồng giữa phương pháp tìm liên phân số và thuật toán Euclid.

Dễ thấy sự trùng nhau giữa liên phân số $[1 : 4, 10]$ và cột q_{j+1} của ***Ví dụ 2.1*** trong thuật toán Euclid cho hai số 867 và 697.

2.2.4 Sơ đồ khối biểu diễn thuật toán Euclid thành liên phân số



Hình 2: Thuật toán Euclid tìm liên phân số của số hữu tỉ $\frac{a}{b}$.



Hình 3: Thuật toán Euclid tìm liên phân số của số thực x.

3. ĐẶT VẤN ĐỀ

Bài toán xấp xỉ số hữu tỉ được đặt ra như sau: Cho hai số nguyên dương R, S, hãy tìm hai số nguyên dương p, q sao

cho thỏa mãn các điều kiện sau:

(i) $0 < p, q < L$ (L là một số nguyên dương cho trước);

(ii) $\left|\frac{p}{q} - \frac{R}{S}\right| < \frac{1}{S}$ (tức là hai phân số $\frac{p}{q}$ và $\frac{R}{S}$ gần bằng nhau).

Vấn đề đặt ra đối với bài toán xấp xỉ số hữu tỉ là phân số xấp xỉ $\frac{p}{q}$ của phân số $\frac{R}{S}$ nếu tồn tại thì phải là duy nhất. Bổ đề sau đây được P. Wang [3] chứng minh trong trường hợp $L = \sqrt{\frac{S}{2}}$.

Bổ đề 3. Cho trước hai số nguyên dương R, S. Khi đó, nếu tồn tại hai số nguyên dương p, q thỏa mãn các điều kiện (i) và (ii) trong trường hợp $L = \sqrt{\frac{S}{2}}$ thì hai số đó là duy nhất.

Chứng minh. Thật vậy, giả sử tồn tại 2 lời giải (p_1, q_1) và (p_2, q_2) thỏa mãn (i) và (ii).

Ta có:

$$\begin{aligned} &\left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right| \le \left|\frac{p_1}{q_1} - \frac{R}{S}\right| \\ &+ \left|\frac{p_2}{q_2} - \frac{R}{S}\right| \le \frac{1}{S} + \frac{1}{S} = \frac{2}{S} \\ \Rightarrow\ &\left|\frac{p_1q_2 - p_2q_1}{q_1q_2}\right| \le \frac{2}{S} \\ \Rightarrow\ &|p_1q_2 - p_2q_1| \le \frac{2q_1q_2}{S} < \frac{2L^2}{S}. \end{aligned}$$

Xét trường hợp $L = \sqrt{\frac{S}{2}}$, ta có $|p_1q_2 - p_2q_1| < 1$.

Lại có $|p_1q_2 - p_2q_1| \in \mathbb{N}$ nên ta suy ra $p_1q_2 - p_2q_1 = 0$ hay $\frac{p_1}{q_1} = \frac{p_2}{q_2}$

Suy ra (p_1, q_1) là duy nhất. □

4. ỨNG DỤNG XẤP XỈ SỐ HỮU TỈ ĐỂ ĐẶT MẬT MÃ

Đối với bài toán mở đầu của Nguyễn Hùng Sơn [2], một bài đố nhỏ mang tính thực tế, được chúng tôi mở rộng và thay đổi như sau:

Cho một dãy số gồm $2n$ chữ số $\underbrace{\overline{abcdef\ldots}}_{2n \text{ chữ số}}$ với $n \in \mathbb{Z}_{>0}$. Ta dùng một chiếc máy tính xách tay đơn giản (gồm 4 phép tính$+, -, \times, \div$ và 10 chữ số) để tính tỉ số n chữ số đầu chia cho n chữ số sau. Ta nhận được kết quả gần đúng là một số thập phân x gồm ít nhất $2n$ chữ số và ghi nhớ lại trên một tờ giấy.

Làm thế nào để tìm lại được dãy số trong thời gian ngắn nhất nếu chỉ có chiếc máy tính xách tay đơn giản và dãy số là gì?

Đối với bài toán này thì có thể kiểm tra bằng cách kiểm tra tất cả các phân số dạng n chữ số đầu chia cho n chữ số sau cho đến khi tìm được phân số có giá trị như yêu cầu. Tuy nhiên phương pháp này không hiệu quả và mất nhiều thời gian và phương pháp hiệu quả hơn chính là khai triển số thập phân x thành dạng liên phân số $x = [a_0 : a_1, a_2, \ldots]$ và biến nó trở thành phân số.

4.1. Định lí tổng quát với mật mã là dãy $2n$ chữ số, dãy $(n+m)$ chữ số

Định lí 4. Cho R, S, p, q là các số tự nhiên có n chữ số sao cho các phân số $\frac{R}{S}$ và $\frac{p}{q}$ khi đổi sang số thập phân thì giống nhau ít nhất đến chữ số thứ $2n$. Khi đó, $\frac{R}{S} = \frac{p}{q}$.

Chứng minh. Ta có:

$$\left|\frac{p}{q}-\frac{R}{S}\right| = 0,\underbrace{000000\ldots}_{2n \text{ chữ số } 0}\alpha_1... = 0,$$

$\alpha_1 \ldots 10^{-2n} < 10^{-2n}$. (với $\alpha_1 = 1, 2, \ldots, 9$)

$$\Rightarrow \left|\frac{p}{q}-\frac{R}{S}\right| < 10^{-2n}$$

$\Leftrightarrow |pS - Rq| < qS \cdot 10^{-2n} < 10^{2n}$

$10^{-2n} = 1$ (do q, S có n chữ số) .

$\Rightarrow 0 \leq |pS - Rq| < 1.$

Vì $pS - Rq \in \mathbb{N} \Rightarrow pS - Rq = 0 \Rightarrow pS = Rq \Rightarrow \dfrac{R}{S} = \dfrac{p}{q}.$ □

Đối với một dãy số gồm $n+m$ chữ số $\underbrace{\overline{abcdef...}}_{n+m \text{ chữ số}}$ với $n, m \in \mathbb{Z}_{>0}$. Thỏa mãn bài toán mở rộng ban đầu và tính tỉ số n chữ số đầu chia cho m chữ số sau. Ta nhận được kết quả gần đúng là một số thập phân x gồm ít nhất $n+m$ chữ số (với $m \leq n$) hoặc ít nhất $2m$ chữ số.

Định lí 5 với số thập phân có ít nhất $n+m$ chữ số (với $m \leq n$) và Định lí 6 với số thập phân có ít nhất $2m$ chữ số được chứng minh như sau:

Định lí 5. Cho R, p là các số tự nhiên có n chữ số và S, q là các số tự nhiên có m chữ số sao cho các phân số $\dfrac{R}{S}$ và $\dfrac{p}{q}$ khi đổi sang số thập phân thì giống nhau ít nhất đến chữ số thứ $(n+m)$ (với $m \leq n$). Khi đó, $\dfrac{R}{S} = \dfrac{p}{q}$.

Chứng minh. Ta có:

$$\left|\frac{p}{q}-\frac{R}{S}\right| = 0,\underbrace{000000\ldots}_{n+m \text{ chữ số } 0}\alpha_1... = 0,$$

$\alpha_1 \ldots 10^{-(m+n)} < 10^{-(m+n)}$.
(với $\alpha_1 = 1, 2, \ldots, 9$)

$$\Rightarrow \left|\frac{p}{q}-\frac{R}{S}\right| < 10^{-(m+n)}$$

$\Leftrightarrow |pS - Rq| < qS \cdot 10^{-(m+n)} < 10^{m}$

$\cdot 10^{m} \cdot 10^{-(m+n)} = 10^{m-n}$

(do q, S có m chữ số).

Theo giả thiết $m \leq n$, nên

$$\begin{aligned} &10^{m-n} \leq 1 \\ &\Leftrightarrow |pS - Rq| < 1 \\ &\Rightarrow 0 \leq |pS - Rq| < 1. \end{aligned}$$

Vì $pS - Rq \in \mathbb{N} \Rightarrow pS - Rq = 0 \Rightarrow pS = Rq \Rightarrow \dfrac{R}{S} = \dfrac{p}{q}.$ □

Định lí 6. Cho R, p là các số tự nhiên có n chữ số và S, q là các số tự nhiên có m chữ số sao cho các phân số $\dfrac{R}{S}$ và $\dfrac{p}{q}$ khi đổi sang số thập phân thì giống nhau ít nhất đến chữ số thứ $2m$. Khi đó, $\dfrac{R}{S} = \dfrac{p}{q}$.

Chứng minh. Ta có:

$$\left|\frac{p}{q}-\frac{R}{S}\right| = 0,\underbrace{000000\ldots}_{2m \text{ chữ số } 0}\alpha_1... = 0,$$

$\alpha_1 \ldots 10^{-2m} < 10^{-2m}$. (với $\alpha_1 = 1, 2, \ldots, 9$)

$$\Rightarrow \left|\frac{p}{q}-\frac{R}{S}\right| < 10^{-2m}$$

$\Leftrightarrow |pS - Rq| < qS \cdot 10^{-2n} < 10^{2m}$

$10^{-2m} = 1$ (do q, S có m chữ số) .

$\Rightarrow 0 \leq |pS - Rq| < 1.$

Vì $pS - Rq \in \mathbb{N} \Rightarrow pS - Rq = 0 \Rightarrow pS = Rq \Rightarrow \dfrac{R}{S} = \dfrac{p}{q}$. □

Một số trường hợp riêng của bài toán tổng quát

4.2. Đặt mật mã là dãy số có bốn chữ số

Ví dụ 4.2.1 Bạn An vì muốn mượn điện thoại của mẹ để chơi game nên đã xin phép nhưng mẹ muốn đố An nếu mở được mật khẩu điện thoại với gợi ý mẹ đưa ra là dãy số $x = 0.32432$ và mật khẩu là số có bốn chữ số thì sẽ được chơi game thỏa thích. Hãy giúp An mở được mật khẩu điện thoại (x thỏa Định lí 4 với n=2).

Giải.

Giả sử dãy số cần tìm là $\overline{abcd} \Rightarrow \dfrac{\overline{ab}}{\overline{cd}} \approx x$.

Sau dấu phẩy 5 chữ số thập phân $x = 0.32432$.

Áp dụng thuật toán hình 3, ta có:

$a_0 = 0$	$r_0 = 0.32432$	$x_0 = 0$
$a_1 = 3$	$r_1 = 0.24324$	$x_1 = \dfrac{1}{3}$
$a_2 = 11$	$r_2 = 0.99414$	$x_2 = \dfrac{1}{3 + \dfrac{1}{11}} = \dfrac{11}{34}$
$a_3 = 1$	$r_3 = 0.00589$	$x_3 = \dfrac{1}{3 + \dfrac{1}{11 + \dfrac{1}{1}}} = \dfrac{12}{37}$

⇒ Hiện 2 dãy số để thử là: 1134 và 1237.

⇒ Đã tìm được $\boxed{1237}$.

4.3. Đặt mật mã là dãy số có năm chữ số

Trường hợp 1: Hai chữ số trên ba chữ số

Ví dụ 7. Bình vì đi học muộn nên đã đánh rơi vé xe với độ dài là số có năm chữ số, đám bạn của Bình đã nhặt được và muốn đánh đố Bình nói rằng "chúng tôi lấy hai chữ số đầu chia cho ba chữ số sau thì nhận được xấp xỉ $x = 0.1037463$, nếu tìm được số đó thì sẽ trả lại vé xe". Hãy giúp Bình tìm được số đó (x thỏa Định lí 6 với n=2 và m=3).

Giải. Giả sử dãy số cần tìm là $\overline{abcde} \Rightarrow \dfrac{\overline{ab}}{\overline{cde}} \approx x$.

Sau dấu phẩy 7 chữ số thập phân $x = 0.1037463$.

Áp dụng thuật toán hình 3, ta có:

$a_0 = 0$	$r_0 = 0.1037463$	$x_0 = 0$
$a_1 = 9$	$r_1 = 0.6388979$	$x_1 = \dfrac{1}{9}$

$a_2 = 1$	$r_2 = 0.5651953$	$x_2 = \dfrac{1}{9+\dfrac{1}{1}} = \dfrac{1}{10}$
$a_3 = 1$	$r_3 = 0.7692999$	$x_3 = \dfrac{1}{9+\dfrac{1}{1+\dfrac{1}{1}}} = \dfrac{2}{19}$
$a_4 = 1$	$r_4 = 0.2998831$	$x_4 = \dfrac{1}{9+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1}}}} = \dfrac{3}{19}$
$a_5 = 3$	$r_5 = 0.3346327$	$x_5 = \dfrac{1}{9+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{3}}}}} = \dfrac{11}{106}$
$a_6 = 2$	$r_6 = 0.9883511$	$x_6 = \dfrac{1}{9+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{3+\dfrac{1}{2}}}}}} = \dfrac{25}{241}$
$a_7 = 1$	$r_7 = 0.0117861$	$x_7 = \dfrac{1}{9+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{3+\dfrac{1}{2+\dfrac{1}{1}}}}}}} = \dfrac{36}{347}$

$\Rightarrow$ Hiện 3 dãy số để thử là: 11106; 25241 và 36347

$\Rightarrow$ Đã tìm được $\boxed{36347}$.

Trường hợp 2: **Ba chữ số trên hai chữ số**

Ví dụ 8. Tương tự Ví dụ 7 với $x = 9.638888$ nhưng thay đổi ba chữ số trên hai chữ số. (x thỏa Định lí 5 với n=3 và m=2)

Giải.

Giả sử dãy số cần tìm là $\overline{abcde}$ $\Rightarrow$ $\dfrac{\overline{abc}}{\overline{de}} \approx x$.

Sau dấu phẩy 6 chữ số thập phân $x = 9.638888$.

Áp dụng thuật toán hình 3, ta có:

$a_0 = 9$	$r_0 = 0.638888$	$x_0 = 9$
$a_1 = 1$	$r_1 = 0.565219$	$x_1 = 9 + \frac{1}{1} = 10$
$a_2 = 1$	$r_2 = 0.769225$	$x_2 = 9 + \frac{1}{1 + \frac{1}{1}} = \frac{19}{2}$
$a_3 = 1$	$r_3 = 0.300009$	$x_3 = 9 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{29}{3}$
$a_4 = 3$	$r_4 = 0.333233$	$x_4 = 9 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}} = \frac{106}{11}$
$a_5 = 3$	$r_5 = 0.000903$	$x_5 = 9 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{3}}}}} = \frac{347}{36}$

$\Rightarrow$ Hiện 2 dãy số để thử là: 10611 và 34736.

$\Rightarrow$ Đã tìm được $\boxed{34736}$.

4.4. Đặt mật mã là dãy số có sáu chữ số

Ví dụ 9. Ngân hàng gửi mật khẩu thẻ tín dụng với số có sáu chữ số cho một cô tỷ phú, cô sợ lọt vào tay kẻ gian nên lấy ba chữ số đầu chia cho ba chữ số sau và nhận được kết quả là số thập phân xấp xỉ $x = 0.9429928$ và ghi vào sổ ghi chú. Sau đó cô bị quên, để rút tiền thì cô phải tìm ra mật khẩu hãy giúp cô ấy tìm ra mật khẩu (x thỏa Định lí 4 với n=3).

Giải.

Giả sử dãy số cần tìm là $\overline{abcdef}$ $\Rightarrow$ $\frac{\overline{abc}}{\overline{def}} \approx x$.

Sau dấu phẩy 7 chữ số thập phân $x = 0.9429928$.

Áp dụng thuật toán hình 3, ta có:

$a_0 = 0$	$r_0 = 0.9429928$	$x_0 = 0$
$a_1 = 1$	$r_1 = 0.0604534$	$x_1 = \frac{1}{1}$
$a_2 = 16$	$r_2 = 0.5416668$	$x_2 = \frac{1}{1 + \frac{1}{16}} = \frac{16}{17}$

$a_3 = 1$	$r_3 = 0.8461533$	$x_3 = \dfrac{1}{1+\dfrac{1}{16+\dfrac{1}{1}}} = \dfrac{17}{18}$
$a_4 = 1$	$r_4 = 0.1818189$	$x_4 = \dfrac{1}{1+\dfrac{1}{16+\dfrac{1}{1+\dfrac{1}{1}}}} = \dfrac{33}{35}$
$a_5 = 5$	$r_5 = 0.4999782$	$x_5 = \dfrac{1}{1+\dfrac{1}{16+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{5}}}}} = \dfrac{182}{139}$
$a_6 = 2$	$r_6 = 0.000087$	$x_6 = \dfrac{1}{1+\dfrac{1}{16+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{5+\dfrac{1}{2}}}}}} = \dfrac{397}{421}$

$\Rightarrow$ Hiện 2 dãy số để thử là: 182139 và 397421

$\Rightarrow$ Đã tìm được $\boxed{397421}$.

4.5. Đặt mật mã là dãy số có bảy chữ số

Trường hợp 1: Ba chữ số trên bốn chữ số

Ví dụ 10. Bạn Trung đi mua nước uống với mệnh giá 5 000 đ cho 1 chai nước nhưng cầm nhầm tờ tiền kỷ niệm mà mẹ tặng để thanh toán. Một lúc sau chợt nhận ra thì Trung gặp lại cô chủ quán để đổi lại tờ tiền ấy nhưng nó đã lẫn lộn vào trong xấp tiền 5 000 của cô chủ quán và chỉ có cô biết tờ nào, cô chủ quán đam mê toán học và biết rằng Trung cũng thích toán cho nên cô đã cho Trung dữ kiện tờ tiền giấy có 7 chữ số, $x = 0.026932340$ (cô lấy 3 chữ số đầu chia cho 4 chữ số sau). Nếu Trung tìm được dãy số seri của tờ tiền thì cô tặng lại tờ 5 000 đ kỉ niệm đó cho Trung. Hãy giúp Trung tìm lại số seri của tờ tiền đó. (x thỏa Định lí 6 với n=3 và m=4)

Giải.

Giả sử dãy số cần tìm là $\overline{abcdefg} \Rightarrow \dfrac{\overline{abc}}{\overline{defg}} \approx x$.

Sau dấu phẩy 9 chữ số thập phân $x = 0.026932340$.

$a_0 = 0$	$r_0 = 0.026932340$	$x_0 = 0$
$a_1 = 37$	$r_1 = 0.130082272$	$x_1 = \dfrac{1}{37}$
$a_2 = 7$	$r_2 = 0.687442605$	$x_2 = \dfrac{1}{37 + \dfrac{1}{7}} = \dfrac{7}{260}$
$a_3 = 1$	$r_3 = 0.454666895$	$x_3 = \dfrac{1}{37 + \dfrac{1}{7 + \dfrac{1}{1}}} = \dfrac{8}{297}$
$a_4 = 2$	$r_4 = 0.199412385$	$x_4 = \dfrac{1}{37 + \dfrac{1}{7 + \dfrac{1}{1 + \dfrac{1}{2}}}} = \dfrac{23}{854}$
$a_5 = 5$	$r_5 = 0.014733663$	$x_5 = \dfrac{1}{37 + \dfrac{1}{7 + \dfrac{1}{1 + \dfrac{1}{2 + \dfrac{1}{5}}}}} = \dfrac{123}{4567}$

Đã tìm được: $\boxed{1234567}$.

Trường hợp 2: Bốn chữ số trên ba chữ số

Ví dụ 11. Tương tự Ví dụ 10 với $x = 37.1300813$ nhưng thay đổi bốn chữ số trên ba chữ số. (x thỏa Định lí 5 với n=4 và m=3).

Giải.

Giả sử dãy số cần tìm là $\overline{abcdefg} \Rightarrow \dfrac{\overline{abcd}}{\overline{efg}} \approx x$.

Sau dấu phẩy 8 chữ số thập phân $x = 37.13008130$.

Áp dụng thuật toán hình 3, ta có:

$a_0 = 37$	$r_0 = 0.13008130$	$x_0 = 37$
$a_1 = 7$	$r_1 = 0.68750004$	$x_1 = 37 + \dfrac{1}{7} = \dfrac{260}{7}$
$a_2 = 1$	$r_2 = 0.45454536$	$x_2 = 37 + \dfrac{1}{7 + \dfrac{1}{2}} = \dfrac{297}{8}$
$a_3 = 2$	$r_3 = 0.20000045$	$x_3 = 37 + \dfrac{1}{7 + \dfrac{1}{1 + \dfrac{1}{2}}} = \dfrac{854}{23}$

$a_4 = 4$	$r_4 = 0.99998875$	$x_4 = 37 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{4}}}} = \frac{3713}{100}$
$a_5 = 1$	$r_5 = 0.00001125$	$x_5 = 37 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \frac{1}{1}}}}} = \frac{4567}{123}$

$\Rightarrow$ Hiện 2 dãy số để thử là: 3713100 và 4567123.

Đã tìm được: $\boxed{4567123}$.

5. KẾT LUẬN

Trong bài báo này, chúng tôi đã trình bày việc mở rộng ứng dụng của thuật toán Euclid và liên phân số để xây dựng, phân tích và khôi phục các dạng mật mã trong những tình huống cụ thể, dựa trên ý tưởng ban đầu trong [2] và [3]. Các định lý được tổng quát hóa nhằm bao quát nhiều trường hợp với số lượng chữ số khác nhau, từ đó xây dựng quy trình logic giúp giải các bài toán khôi phục mật mã một cách nhanh chóng và hiệu quả. Cách tiếp cận này không chỉ góp phần làm rõ mối liên hệ giữa lý thuyết số và ứng dụng thực tế mà còn tạo điều kiện để người học dễ dàng tiếp cận với tư duy thuật toán thông qua các ví dụ gần gũi, sinh động.

Vì vậy kết quả bài báo là khá hữu ích đối với các bạn sinh viên và học viên chuyên ngành toán- tin và các chuyên ngành khác cần sự ứng dụng của thuật toán trong thực tế.

TÀI LIỆU THAM KHẢO

[1] H. H. Khoái (2004), *Số Học*, Nhà xuất bản Giáo dục.

[2] N. H. Sơn (2019), *Thuật toán phục hồi số hữu tỉ*, Tạp chí Pi, Tập 3-Số 6.

[3] P. Wang, *P.adic reconstruction of rational numbers*, ACM Sigsam Bulletin, Vol.16 (2), pp. 2-3. DOI: 10.1145/1089292.1089293.

[4] Hardy G. H., Wright E. M. (1979), *An Introduction to the Theory of Numbers (5th ed.), Clarendon Press, Oxford.*

Liên hệ:

Nguyễn Văn Bình

Khoa Toán học, Trường Đại học Sư phạm - Đại học Đà Nẵng

Địa chỉ: 459 Tôn Đức Thắng, Hòa Khánh Nam, quận Liên Chiểu, TP. Đà Nẵng

Email: binhnguyen.281004@gmail.com

Ngày nhận bài: 01/4/2025

Ngày gửi phản biện: 06/4/2025

Ngày duyệt đăng: 19/5/2025