

SỐ HỌC

THUẬT TOÁN EUCLID MỞ RỘNG – GIẢI PHƯƠNG TRÌNH DIOPHANTINE

Tác giả: Phan Thành Hưng (PTNK, ĐHQG TP. HCM)

I. Giới thiệu

Cho bài toán sau:

“Tìm nghiệm nguyên x, y biết:

$$ax + by = c \quad (1)$$

với a, b, c là số nguyên.”

II. Thuật toán

Thông thường, ta có một số cách giải nhanh. Nếu tập giá trị của x, y nhỏ thì ta có thể thử hết mọi giá trị của x hoặc y trong miền cho trước và tìm ra nghiệm. Tuy nhiên, ta cần một cách làm tổng quát hơn.

1. Thuật toán ngây thơ

Ta biến đổi:

$$\begin{aligned} ax + by &= c \\ \Rightarrow y &= \frac{c - ax}{b} \end{aligned}$$

Do đó, ta chỉ cần duyệt qua từng giá trị nguyên của x và nếu y là số nguyên thì ta nhận được nghiệm cần tìm. Ta có thể sử dụng tính năng table để giải quyết.

Phân tích độ hiệu quả: Nếu miền giá trị của x từ L tới R thì số vòng lặp cần duyệt qua là $R - L + 1$. Nếu giá trị này rất lớn thì rõ ràng thuật toán này không hiệu quả.

2. Thuật toán tối ưu

Ta có thể chứng minh được phương trình (1) có nghiệm khi và chỉ khi c chia hết cho $\gcd(a, b)$.

Tham khảo chứng minh:

- <https://www.math.ualberta.ca/~dam/Math324/1dequations.pdf>
- <https://principlesofcryptophy.com/number-theory-primer-the-diophantine-equation-ax-by-c/>

Với $g = \gcd(a, b)$, ta giải phương trình sau:

$$ax' + by' = g \quad (2)$$

Nếu tìm được nghiệm của phương trình trên, có thể đưa về phương trình (1) bằng cách nhân cả hai vế với $\frac{c}{g}$.

$$ax' \cdot \frac{c}{g} + by' \cdot \frac{c}{g} = g \cdot \frac{c}{g}$$

$$\Leftrightarrow ax + by = c$$

Ta có hai cách để giải phương trình (2), đều sử dụng [thuật toán Euclid mở rộng](#).

Thuật toán 1:

Thay vì giải trực tiếp phương trình (2), ta đưa về bài toán khác là giải:

$$(b) \cdot x_1 + (a \bmod b) \cdot y_1 = g$$

Nếu tìm được nghiệm x_1, y_1 , ta có thể biến đổi để khôi phục lại được nghiệm x', y' của phương trình (2) như sau:

$$bx_1 + \left(a - b \cdot \left\lfloor \frac{a}{b} \right\rfloor\right) y_1 = bx_1 + ay_1 - b \left\lfloor \frac{a}{b} \right\rfloor y_1 = a(y_1) + b \left(x_1 - y_1 \left\lfloor \frac{a}{b} \right\rfloor\right) = g$$

Do đó, $x' = y_1, y' = x_1 - y_1 \left\lfloor \frac{a}{b} \right\rfloor$.

Nhận thấy $\gcd(a, b) = \gcd(b, a \bmod b)$, nếu ta liên tục thực hiện việc đưa về các bài toán con, cho tới khi $a = g, b = 0$ thì lúc này ta được trường hợp cơ sở:

$$gx' + 0y' = g$$

$\Rightarrow$ Tại trường hợp cơ sở, $x' = 1, y' = 0$ để thỏa mãn phương trình trên, từ đó ta truy ngược lên các phương trình ta đã đi qua và khôi phục lại các nghiệm gốc, từ đó giải được phương trình (2).

Thuật toán 2:

Dựa trên cùng ý tưởng với **thuật toán 1**, nhưng cách xử lý lại khác.

Đặt $a = a_0x_0 + b_0y_0$, $b = a_0x_1 + b_0y_1$

Với a_0, b_0 là a, b ban đầu và x_0, y_0, x_1, y_1 là các hệ số.

Dễ thấy, tại trường hợp cơ sở, $x_0 = 1, y_0 = 0, x_1 = 0, y_1 = 1$.

Lúc này, ta sẽ gán a, b lần lượt thành b và $a \bmod b$.

Nghĩa là:

$$a = b = a_0x_1 + b_0y_1$$

$$\begin{aligned} b = a - b \left\lfloor \frac{a}{b} \right\rfloor &= a_0x_0 + b_0y_0 - (a_0x_1 + b_0y_1) \cdot \left\lfloor \frac{a}{b} \right\rfloor \\ &= a_0x_0 + b_0y_0 - a_0x_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor - b_0y_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor \\ &= a_0 \left(x_0 - x_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor \right) + b_0 \left(y_0 - y_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor \right) \end{aligned}$$

$$\Rightarrow (x_0, y_0) := (x_1, y_1) \text{ và } (x_1, y_1) := \left(x_0 - x_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor, y_0 - y_1 \cdot \left\lfloor \frac{a}{b} \right\rfloor \right).$$

Ta liên tục biến đổi như vậy cho tới khi $a = g, b = 0$.

Vì $a = a_0x_0 + b_0y_0 = g$ nên (x_0, y_0) chính là một nghiệm (x', y') của phương trình **(2)**.

Việc cần làm tiếp theo:

Sau khi tìm được nghiệm x', y' thỏa mãn, ta nhân cả hai nghiệm đó với $\frac{c}{g}$ để tìm ra nghiệm x, y của phương trình **(1)**.

[*] Tìm tất cả các nghiệm

Biến đổi phương trình **(2)**:

$$\begin{aligned} ax' + by' &= g \\ \Leftrightarrow ax' + \frac{ab}{g} + by' - \frac{ab}{g} &= g \\ \Leftrightarrow a \left(x' + \frac{b}{g} \right) + b \left(y' - \frac{a}{g} \right) &= g \end{aligned}$$

Do vậy, nếu ta tìm được một nghiệm (x'_0, y'_0) bất kì thì tất cả các nghiệm của phương trình **(2)** có thể tìm được dưới dạng:

$$x' = x'_0 + \frac{b}{g} \cdot t$$

$$y' = y'_0 - \frac{a}{g} \cdot t$$

Với $t \in \mathbb{Z}$. Từ đó, có thể xác định tất cả nghiệm dựa vào công thức tổng quát trên.

Cài đặt:

Có thể thấy, **thuật toán 1** được chia thành 2 giai đoạn. Tại giai đoạn 1, ta sẽ liên tục duyệt tới khi $a = g, b = 0$. Giai đoạn 2 truy ngược lại và khôi phục lại nghiệm. Còn đối với **thuật toán 2**, ta duyệt một lần duy nhất và tìm ra nghiệm luôn. Do vậy, đối với máy Casio fx-580VN X, ta sẽ ưu tiên cài đặt **thuật toán 2** vì nó nhanh và gọn.

Và sau đây là cài đặt mẫu của **thuật toán 2**:

$$M = 0xyABCD + \text{Int}\left(\frac{C}{D}\right) : z = A : A = x - MA : x = z : z = B : B = y - MB : y = z : z = D : D = C - MD : C = z$$

- Giá trị ban đầu: $x = 1; y = 0; A = 0; B = 1; C = \text{hệ số } a; D = \text{hệ số } b$

- Cách dùng: nhập các dữ liệu vào theo đề bài, sau đó lặp đa câu lệnh cho tới khi gặp “**Lỗi phép tính**” (**Math ERROR**) thì dừng. Nghiệm x', y' lần lượt nằm trong biến x và y .

Phân tích độ hiệu quả: Số vòng lặp duyệt qua đã được chứng minh là khoảng $\log \min(a, b)$ (bạn có thể tham khảo [tại đây](#)). Do vậy, thuật toán này rất hiệu quả.

Đối với dòng máy Casio fx-880BTG, ta có thể cài đặt thuật toán 1 bằng tính năng *spreadsheet*. Phần cài đặt trên dòng máy đó được coi như là bài tập vui vẻ dành cho người đọc. Hướng dẫn cài đặt sẽ được mình chia sẻ sau.

TÓM TẮT THUẬT TOÁN:

$$M = 0xyABCD + \text{Int}\left(\frac{C}{D}\right) : z = A : A = x - MA : x = z : z = B : B = y - MB : y = z : z = D : D = C - MD : C = z$$

- Giá trị ban đầu: $x = 1; y = 0; A = 0; B = 1; C = \text{hệ số } a; D = \text{hệ số } b$

- Cách dùng: nhập các dữ liệu vào theo đề bài, sau đó lặp đa câu lệnh cho tới khi gặp “**Lỗi phép tính**” (**Math ERROR**) thì dừng. Nghiệm x', y' lần lượt nằm trong biến x và y .

Chú ý: Sau khi thu được nghiệm x', y' của phương trình, ta nhân cả x', y' cho $\frac{c}{g}$ để tìm ra nghiệm gốc. Nghiệm gốc của phương trình là $x = x' \cdot \left(\frac{c}{g}\right); y = y' \cdot \left(\frac{c}{g}\right)$.