THUẬT TOÁN EUCLID (Euclidean algorithm)

Một thuật toán tìm ước chung lớn nhất của hai số nguyên. Thuật toán này được viết trong cuốn Cơ sở của Euclid (khoảng 300 năm trước công nguyên).

Thuật toán được mô tả như sau. Cho trước hai số nguyên dương $a > b$. Chia a cho b, ta được $a = qb + b_1$, với thương q và số dư b_1, $0 \leq b_1 < b$. Nếu b_1 khác 0, ta lấy b chia cho b_1, được $b = q_1 b_1 + b_2$. Cứ tiếp tục như vậy, ta được

$$\begin{aligned} a &= qb + b_1 \\ b &= q_1 b_1 + b_2 \\ b_1 &= q_2 b_2 + b_3 \\ &\dots \end{aligned}$$

cho đến khi số dư $b_{k+1} = 0$. Khi đó số b_k chính là ước chung lớn nhất của a và b.

Ví dụ, ta muốn tìm ước chung lớn nhất của $a = 60$ và $b = 36$. Thực hiện các phép chia liên tiếp, ta được

$$\begin{aligned} 60 &= 1 \times 36 + 24 \\ 36 &= 1 \times 24 + 12 \\ 24 &= 2 \times 12. \end{aligned}$$

Ước chung lớn nhất của 60 là 36 là 12.

Việc tìm ước chung lớn nhất của hai số nguyên là một bước quan trọng trong một số thuật toán phân tích số nguyên. Thuật toán Euclid là một thuật toán hữu hiệu để tìm ước chung lớn nhất. Người ta cũng có thể chứng minh được rằng với hai số $a > b$ như trên, thuật toán Euclid sẽ kết thúc sau không quá $\left\lfloor \dfrac{\ln a}{\ln((1+\sqrt{5})/2)} \right\rfloor$ bước.

Thuật toán Euclid cũng được mở rộng lên cho một đối tượng khác như trên các số nguyên Gauss hay trên các đa thức một biến.

NGUYỄN DUY TÂN

Tài liệu tham khảo

1. D. S. Dummit and R. M. Foote, *Abstract Algebra* (3rd ed.), John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.
2. T. Koshy, *Elementary Number Theory with Applications* (2nd ed.), Academic Press, USA, 2007.
3. W. J. LeVeque, *Topics in Number Theory* Vol. I, II, reprint of the 1956 original, with separate errata list for this edition by the author, Dover Publications, Inc., Mineola, New York, 2002.
4. K. H. Rosen, *Elementary Number Theory and its Applications* (6th ed.), Addison-Wesley Publishing Company, Massatchusetts, 2011.