The Quadratic Sieve Factoring Algorithm

Vũ Cao Cường
Nguyễn Thanh Hoàng

Đại học Bách khoa Hà Nội

Ngày 8 tháng 1 năm 2016

Overview

Phát biểu bài toán

Bài toán phân tích thừa số nguyên tố

- Phân tích thừa số là bài toán phân tích một hợp số ra thành tích của những số nguyên bé hơn.
- Nếu những số nguyên này là số nguyên tố thì đó là bài toán phân tích thừa số nguyên tố.
- Chưa có thuật toán hiệu quả nếu hợp số là số lớn.

Các thuật toán phân tích thừa số nguyên tố

Với giá trị của số N cần phân tích:

- Nhỏ hơn 2^{16}: Tìm các số nguyên tố n chia hết dựa trên kiểm thử.
- Nhỏ hơn 2^{70}: Richard Brent's modification of Pollard's rho algorithm.
- Nhỏ hơn 10^{50}: Lenstra elliptic curve factorization
- Nhỏ hơn 10^{100}: Quadratic Sieve
- Lớn hơn 10^{100}: General Number Field Sieve

Ứng dụng

Bài toán RSA

- Bài toán Phân tích ra thừa số nguyên tố các số nguyên lớn là vấn đề toán học của độ an toàn hệ thống RSA.
- Nếu kẻ tấn công tìm được 2 số nguyên tố p và q sao cho: $n = pq$, kẻ tấn công sẽ tìm ra số mũ bí mật d từ khóa công khai và có thể giải mã theo đúng quy trình của thuật toán.

Định lí Fermat

Định lí Fermat

- Cho một số nguyên n, Định lí Fermat tìm số nguyên x và y thoả mãn: $n = x^2 - y^2$ hay $n = (x + y)(x - y)$
- Tính $p = gcd(x + y, n)$ và $q = gcd(x - y, n)$
- $n = pq$ là cách phân tích số nguyên n ra thừa số.

Thuật toán Quadratic Sieve

How it Works

- Fermat's method hoạt động tốt với trường hợp nhân tử có giá trị gần $\sqrt{N}$.
- Hạn chế của sử dụng Fermat's method: Độ phức tạp tính toán là lớn đối với số nguyên lớn ($O(N^{1/3})$).

Thuật toán Quadratic Sieve

How it Works

- Xét
$$Q(x) = (x + \lceil \sqrt{n} \rceil)^2 - n = X^2$$
- Tính toán $Q(x_1), Q(x_2), \ldots, Q(x_k)$ với $Q(x_i)$ khi phân tích ra các số nguyên tố thì chỉ chứa các số nguyên tố trong vector cơ sở.
- Chọn một tập con r phần tử $Q(x_{i1}), Q(x_{i2}), \ldots, Q(x_{ir})$ sao cho
$$Q(x_{i1})Q(x_{i2}) \ldots Q(x_{ir}) = y^2$$
bằng phương pháp khử Gauss.

Thuật toán Quadratic Sieve

How it Works

- Từ r phần tử $Q(x_{i1}), Q(x_{i2}), \ldots, Q(x_{ir})$, ta có

$$Q(x_{i1})Q(x_{i2})\ldots Q(x_{ir}) = Y^2$$

  trong đó $X^2 - Y^2 = n$
- Từ X và Y, tính p và q theo Fermat's method.

Thuật toán Quadratic Sieve

How it Works

- Với $k = B + 10$, với B là số lượng số nguyên tố trong vector cơ sở, xác suất để tìm được tập con r phần tử thỏa mãn $Q(x_{i1})Q(x_{i2})\dots Q(x_{ir}) = y^2$ là $\frac{1023}{1024}$

The End