Thuật toán Miller-Rabin là một thuật toán xác định tính nguyên tố của một số nguyên dương n. Nó là một thuật toán xác suất, có nghĩa là kết quả của nó có thể không chính xác với xác suất rất nhỏ, nhưng trong hầu hết các trường hợp, kết quả sẽ là chính xác.

Thuật toán Miller-Rabin hoạt động dựa trên một định lý trong lý thuyết số, gọi là Định lý Fermat nhỏ. Định lý này nói rằng nếu p là một số nguyên tố và a là một số nguyên không chia hết cho p, thì a^(p-1) ≡ 1 (mod p).

Thuật toán Miller-Rabin sử dụng phương pháp kiểm tra xem một số nguyên dương n có phải là số nguyên tố hay không bằng cách chọn ngẫu nhiên một số a trong khoảng [1, n-1] và kiểm tra xem a có thỏa mãn định lý Fermat nhỏ không. Nếu a không thỏa mãn định lý Fermat nhỏ, thì n không phải là số nguyên tố. Ngược lại, nếu a thỏa mãn định lý Fermat nhỏ, thì thuật toán sẽ tiếp tục kiểm tra với một số a khác. Thực hiện quá trình này tối đa k lần, với k là một số nguyên dương được chọn trước đó. Nếu trong số k lần kiểm tra, tất cả đều cho kết quả là a không phải là số nguyên tố, thì thuật toán sẽ kết luận n không phải là số nguyên tố. Trong trường hợp khác, thuật toán sẽ kết luận rằng n có xác suất rất cao là số nguyên tố.

Thuật toán Miller-Rabin được coi là một trong những thuật toán kiểm tra số nguyên tố nhanh nhất hiện nay và được sử dụng rộng rãi trong các ứng dụng liên quan đến lý thuyết số, mật mã học và khoá công khai.

Giải thuật miller-rabin

Input: số nguyên n cần kiểm tra tính nguyên tố, số lần kiểm tra k

1. Nếu n <= 1 hoặc n == 4, trả về False.

2. Nếu n <= 3, trả về True.

3. Tính các giá trị r và s sao cho n-1 = 2^r \* s, với s là số lẻ.

4. Duyệt qua k lần kiểm tra sau:

4.1. Chọn số nguyên tố ngẫu nhiên a trong khoảng [2, n-2].

4.2. Tính x = a^s mod n.

4.3. Nếu x == 1 hoặc x == n-1, ta chuyển sang kiểm tra lần kiểm tra kế tiếp.

4.4. Với mỗi j từ 1 đến r-1, tính x = x^2 mod n.

Nếu x == n-1, ta chuyển sang kiểm tra lần kiểm tra kế tiếp.

4.5. Nếu không tìm được j nào sao cho x == n-1, trả về False.

5. Trả về True.