1. Định nghĩa

* Trong số học môđun, một số g được gọi là một phần tử nguyên thủy modulo n nếu mọi số nguyên tố với n đều đồng dư với một lũy thừa của g modulo n. Về mặt toán học, g là một phần tử nguyên thủy modulo n khi và chỉ khi với bất kỳ số nguyên a nào sao cho gcd (a, n) = 1, tồn tại một số nguyên k sao cho: , k khi đó được gọi là chỉ số hoặc logarit rời rạc của a với cơ số g modulo n. g còn được gọi là phần tử sinh của nhóm nhân các số nguyên modulo n.
* Đặc biệt, đối với trường hợp n là một số nguyên tố, các lũy thừa của phần tử nguyên thủy chạy qua tất cả các số từ 1 đến n − 1.
* Điều kiện tồn tại phần tử nguyên thủy modulo n là: n = 1,2,4 hoặc n là lũy thừa của 1 số nguyên tố ( hoặc n là 2 lần lũy thừa của số nguyên tố (

với số nguyên tố và lũy thừa .

* Gọi g là một phần tử nguyên thủy modulo n. Theo định lý Euler, số k nhỏ nhất mà (mod n) bằng 𝟇(n). Điều ngược lại cũng đúng, số lượng phần tử nguyên thủy modulo n bằng .

1. Thuật toán tìm kiếm phần tử nguyên thủy

* Với bất kỳ số nào là số nguyên tố với n, theo định lý Euler, ta có . Để kiểm tra xem g có phải là phần tử nguyên thủy hay không, chỉ cần kiểm tra rằng với mọi d nhỏ hơn 𝟇(n) thì .
* Từ định lý Lagrange, ta có chỉ số của 1 trong bất kỳ số nào modulo n phải là ước của 𝟇(n). Do đó, nó đủ để xác minh cho tất cả các ước số thích hợp d | 𝟇(n) rằng
* Phân tích 𝟇(n) = …. Cần phải chứng minh rằng trong thuật toán trước, chỉ cần xem xét các giá trị của d có dạng Thật vậy, hãy cho d là bất kỳ ước số nào của 𝟇(n). Khi đó, tồn tại j mà d |, nghĩa là d.k = . Nếu , ta có: , nghĩa là trong số các số có dạng sẽ có ít nhất một số sao cho các điều kiện không được thỏa mãn.

Chúng ta có một thuật toán hoàn chỉnh để tìm phần tử nguyên thủy:

1. Đầu tiên, tìm 𝟇(n) và phân tích dưới dạng thừa số nguyên tố.
2. Sau đó lặp qua tất cả các số g ∈ [1, n], và đối với mỗi số, để kiểm tra xem nó có phải là phần tử nguyên thủy hay không, chúng ta thực hiện như sau: Tính (mod n). Nếu tất cả các giá trị tính được khác 1, thì g là một phần tử nguyên thủy.

Ví dụ : n = 7, 𝟇(7) = 6 = 2.3.

g = 2: mod 7 = 1

g = 3: mod 7 = 6, 2

g = 4: mod 7 = 1

g = 5: mod 7 = 6,

g = 6:

Ta thấy 3 và 5 là phần tử nguyên thủy modulo 7.