KIỂM TRA TÍNH NGUYÊN TỐ CỦA MỘT SỐ BẤT KỲ

3. GIỚI THIỆU LÝ THUYẾT SỐ

7. Kiểm tra tính nguyên tố

- Cách kiểm tra một số lớn có phải là số nguyên tố hay không ta dựa vào 2 tính chất sau:
- ***Tính chất 1***: Nếu p là số nguyên tố và a là một số nguyên dương nhỏ hơn p thì $a^2 \bmod p = 1$ khi và chỉ khi $a \bmod p = 1$ hoặc $a \bmod p = p - 1$.

3. GIỚI THIỆU LÝ THUYẾT SỐ

7. Kiểm tra tính nguyên tố

- ***Tính chất 2***: Nếu p là số nguyên tố lớn hơn 2 thì ta có thể phân tích $p - 1 = 2^k \times q$, với k > 0 và q là số lẻ. Gọi a là một số nguyên bất kỳ, với 1 < a < p – 1. Khi đó, một trong hai điều kiện sau đây được thỏa mãn:

  1. $a^q \equiv 1 (mod\ p)$
  2. Một trong các số $a^q, a^{2.q}, a^{4.q}, \dots, a^{2^{(k-1)}.q}$ đồng dư với $1 \bmod p$

3. GIỚI THIỆU LÝ THUYẾT SỐ

7. Kiểm tra tính nguyên tố

- Thuật toán Miller-Rabin: là thuật toán kiểm tra tính nguyên tố của một số nguyên p. Đây là phương pháp kiểm tra số nguyên tố theo thuật toán xác suất.

```
TEST(p)
    Tìm k, q với k> 0, q lẻ thỏa mãn p = 2^k q + 1
    Chọn số ngẫu nhiên a trong khoảng [2, p - 1]
    If a^q mod p = 1 Then
        return "p có thể là số nguyên tố";
    For j= 0 to k-1 do
        If a^(2^j*q) mod p = 1 Then
            return "p có thể là số nguyên tố";
    return "p không phải là số nguyên tố";
```

3. GIỚI THIỆU LÝ THUYẾT SỐ

7. Kiểm tra tính nguyên tố

- ***Ví dụ 1***: Kiểm tra số $p = 29$. Ta có, $p - 1 = 28 = 2^2 * 7 = 2^k * q$
- Nếu chọn a = 10.

  Ta tính $a^q \ mod \ p = 10^7 mod \ 29 = 17$. Giá trị này không trùng với *1* và *28* nên ta tiếp tục tính $(10^7)^2 mod \ 29 = 28$. Thủ tục kiểm tra sẽ trả về "có thể là số nguyên tố".
- Nếu chọn a = 2.

  Ta tính $a^q \ mod \ p = 2^7 mod \ 29 = 12$. Giá trị này không trùng với *1* và *28* nên ta tiếp tục tính $(2^7)^2 mod \ 29 = 28$. Thủ tục kiểm tra cũng sẽ trả về "có thể là số nguyên tố".
- Tiếp tục thử a = 2 ÷ 28 đều nhận được kết quả như trên. Vì vậy, có thể chắc chắn rằng 29 là số nguyên tố.