P11961 [GESP202503lv3] 原根判断

2025 年 3 月 29 日 薛周峻

首先分析题意，不难发现题目条件一 $1 < g < p$ 在数据范围中已满足，故考虑条件二、三（以下简称 $\mathbf{Q}_i(i \in \mathbb{N}*)$）。

首先因为指数项较大，故采用快速幂（Quick Power）.

注意到 $\mathbf{Q}_2$ 和费马小定理等价，得

$$g^{p-1} \equiv 1(\bmod\ p \in \mathbb{P}, g \in \mathbb{N}^*) \Leftrightarrow g \bmod p \neq 1$$

又注意到

$$\mathbf{Q}_3 : \forall\ 1 \leq i < p-1, g^i \bmod p \neq 1$$

$$\Downarrow$$

$$\text{只要}\mathbf{Q}_3' : \exists\ 1 \leq i < p-1, g^i \bmod p = 1，\ \mathbf{Q}_3\text{就不成立}$$

故只要我们找到一个不符条件三得 i，就可以排除。如果程序运行到此处，那么所有不满足条件二的

$$g^{p-1} \bmod p \neq 1$$

就被排除了。注意到

$$a^{pq} = (a^p)^q \equiv 1^q \equiv 1(\ \bmod\ P \in \mathbb{P}\ )$$

与条件二进行对比

$$g^m \equiv 1$$

$$g^{mn} \equiv 1$$

$$g^{p-1} \equiv 1$$

$$(\ \bmod\ p \in \mathbb{P}, g, m, n \in \mathbb{N}^*)$$

这说明，当 $p-1 = mn$ 时，若关于 $g^{mn} \equiv 1, \exists n \Rightarrow g^m \equiv 1$，则 $\mathbf{Q}_3$ 不成立。即 $p-1$ 如果有一个因数 f 使得 $g^f \equiv 1$，则条件三不成立。

综上所述，程序设计思路如下：

（1）输入 T，若干个 a、p；

（2）检查 $g \bmod p \neq 1$ 与 $p-1$ 不存在因子 i 使得 $g^i \equiv 1$ 或 $g^{\frac{p-1}{i}} \equiv 1(\ \bmod\ p \in \mathbb{P}\ )$ 并使用快速幂，输出每组答案。

总程序如下：

```cpp
#include <bits/stdc++.h>
#define ull unsigned long long
using namespace std;
ull T, g, p;

inline ull qpm(ull a,ull b) { //快速幂 模p
```

```
7         int res=1;
8         while(b) {
9                 if(b&1) res=res*a%p;
10                b>>=1, a=a*a%p;
11        }
12        return res;
13}
14
15void find_ys(vector<ull>* v) { //找因数
16        for (ull i = 2; i*i <= p-1; ++i)
17        if ((p-1)%i==0) {
18                v->push_back(i);
19                v->push_back((p-1)/i);
20        }
21}
22
23bool check() {
24        vector<ull> v; //因数
25        find_ys(&v);
26        if (g%p==1) return 0; //g^{p-1}\mod p=1
27        for (ull j = 0; j < v.size(); ++j) {
28                ull i = v[j];
29                if (qpm(g, i)==1) return 0;
30                //只要p-1有一个因数关于p的模是1, 就不成立
31        }
32        return 1;
33}
34
35int main() {
36        cin >> T;
37        while (T--) {
38                cin >> g >> p;
39                printf(check()?"Yes\n":"No\n");
40        }
41        return 0;
42}
```