

计算机算法设计与实践 第10周作业

181002222 连月菡

计算机算法设计与实践 第10周作业

[题目描述](#)

[解答思路](#)

[伪代码](#)

[C++代码](#)

[运行结果](#)

题目描述

假设 n 是一个素数, 令 x 为 $1 \leq x \leq n - 1$ 的整数, 如果存在一个整数 y , $1 \leq y \leq n - 1$, 使得 $x \equiv y^2 \pmod n$, 则称 y 是 x 模 n 的平方根, 例如, 9 就是3 模13 的平方根。

设计一个拉斯维加斯型概率算法, 求整数 x 模 n 的平方根。

解答思路

拉斯维加斯型 (Las Vegas) 概率算法对同一个输入实例反复多次运行算法, 直到运行成功, 获得问题的解, 如果运行失败, 则在相同的输入实例上再次运行算法。

在这道题中, 对于输入实例 n, x , 由于 x 为 $1 \leq x \leq n - 1$, $1 \leq y \leq n - 1$, 所以运行次数设置为 n 次, 每次求出 $y^2 \pmod n$ 的值, 与 x 进行比较, 如果相等则停止尝试, 输出答案, 进行 n 次后仍没有结果, 则输出无解。

伪代码

```
1  input n, x //输入素数n, x (1<=x, x<=n-1)
2  srand(x) //生成随机数种子
3  for i=1:n //进行n次尝试
4      y= rand() % (n - 1)+ 1 //生成随机数y, 且1<= y<= n - 1
5      if x=y^2 mod n //得到解
6          ok=1
7          break//标志改为1, 表示成功, 结束循环
8  end for
9  if !ok //没有找到解
10     output 无解
```

C++代码

```
1  #include<iostream>
2  using namespace std;
3
4  int main()
5  {
6      int n, x, y;
```

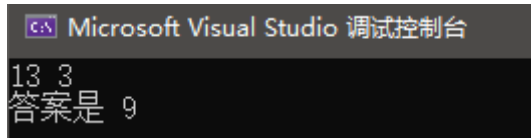
```

7   bool ok = 0;
8   cin >> n >> x; //输入素数n, x (1<=x, x<=n-1)
9   srand(x); //生成种子
10  for (int i = 1; i <= n; ++i)
11  {
12      y = rand() % (n - 1) + 1; //1<=y, y<=n-1
13      if (y * y % n == x) //得到解
14      {
15          ok = 1; //标志改为1,表示成功,结束循环
16          cout << "答案是 " << y << endl;
17          break;
18      }
19  }
20  if (!ok) cout << "无解" << endl;
21  return 0;
22  }

```

运行结果

输入 13,3 由于 $9 \times 9 \% 13 = 3$, 因此答案为9



```

Microsoft Visual Studio 调试控制台
13 3
答案是 9

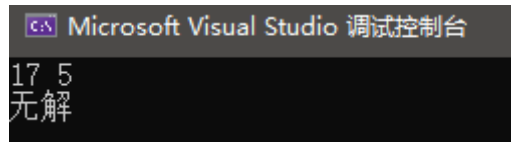
```

输入17,5, 经过遍历验证,确实没有满足的答案,利用拉斯维加斯算法,得到的答案也是无解

```

1   y = i; //修改上面的 第12行代码 即可使用蛮力法验证结果是否正确
2   // y = rand() % (n - 1) + 1; //1<=y, y<=n-1

```



```

Microsoft Visual Studio 调试控制台
17 5
无解

```