Report One

崔航

2023.09.30

摘要

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

目录

1 Mille-Rabin方法

1.1 费马小定理

当p为素数时，对于任意整数a，有$a^p \equiv a \pmod{p}$。即$a^{p-1} \equiv 1 \pmod{p}$。

1.1.1 算法描述

1. 选取一个整数a，使得$1 < a < n$。
2. 计算$a^{n-1} \pmod{n}$。
3. 若$a^{n-1} \not\equiv 1 \pmod{n}$，则$n$为合数；否则，$n$可能为素数。
4. 重复步骤1-3，k次后，若n为合数，则n为合数；否则，n可能为素数。

1.1.2 证明

1. 若n为素数，由费马小定理可知，$a^{n-1} \equiv 1 \pmod{n}$。
2. 若n为合数，由费马小定理可知，$a^{n-1} \equiv 1 \pmod{n}$。

1.2 算法实现

1.2.1 python实现

```
def miller_rabin(n, k):
    if n == 2:
        return True
    if n % 2 == 0:
        return False
    s = 0
    d = n - 1
    while d % 2 == 0:
        s += 1
        d //= 2
    for i in range(k):
        a = random.randint(2, n - 1)
        x = pow(a, d, n)
        if x == 1 or x == n - 1:
            continue
        for j in range(s - 1):
            x = pow(x, 2, n)
            if x == 1:
                return False
            if x == n - 1:
                break
        else:
            return False
    return True
```

2