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 Fermat's Little Theorem

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

2 伪素数

2.1 Carmichael伪素数

由Fermat's Little Theorem可知，若对于任意整数a，有$a^p \equiv a \pmod{p}$，则p可能为素数。但是，若p为合数，仍有可能满足$a^p \equiv a \pmod{p}$。此时，p被称为Carmichael伪素数。

2.1.1 Fermat素数检测

1. 给定奇整数$n \geq 3$和安全参数t。
2. 随机选取整数b,$(b, n) = 1, 2 \leq b \leq n - 2$.
3. 计算$r = b^{n-1} \pmod{n}$。
4. 若$r \neq 1$，则n为合数。
5. 若$r = 1$，则n可能为素数，重复步骤2-4，共重复t次。

2.2 算法实现

```
def fermat(n, k):
    if n == 2:
        return True
    if n % 2 == 0:
        return False
    for i in range(k):
        a = random.randint(2, n - 2)
        if pow(a, n - 1, n) != 1:
            return False
    return True
```

2.2.1 平方因子检测

设n为一个有平方因子的整数，则存在整数a，使得$a^2 \equiv 1 \pmod{n}$，且$a \not\equiv \pm 1 \pmod{n}$。此时，$n$被称为Carmichael数。

2.3 Euler伪素数

设n是一个正奇合数，设整数b与n互素，若$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$，则$n$被称为Euler伪素数。

2.3.1 Solovary-Strassen素数检测

1. 给定奇整数$n \geq 3$和安全参数t。
2. 随机选取整数b,$(b, n) = 1, 2 \leq b \leq n - 2$.
3. 计算$r = b^{\frac{n-1}{2}} \pmod{n}$。
4. 若$r \neq \pm 1 \pmod{n}$，则n为合数。

5. 计算Jacobi符号$(\frac{b}{n})$。

6. 如果$r \neq s$，则n为合数。

7. 若$r \equiv \pm 1 \pmod{n}$，则n可能为素数，重复步骤2-4，共重复t次。

2.3.2 算法实现

```
def solovay_strassen(n, k):
    if n == 2:
        return True
    if n % 2 == 0:
        return False
    for i in range(k):
        a = random.randint(2, n - 2)
        if pow(a, (n - 1) // 2, n) != jacobi(a, n) % n:
            return False
    return True
```

3 强伪素数

设一个奇合数n,且有表达式$n-1=2^s d$，其中d为奇数。若对于任意整数a，有

$$a^d \equiv 1 \pmod{n}$$

或

$$a^{2^r d} \equiv -1 \pmod{n}$$

，则n被称为强伪素数。

3.1 Miller-Rabin素数检测

1. 给定奇整数$n \geq 3$和安全参数t。

2. 随机选取整数b,$(b,n)=1, 2 \leq b \leq n-2$.

3. 计算$r = b^{n-1} \pmod{n}$。

4. 若$r \neq 1$，则n为合数。

5. 若$r = 1$，则n可能为素数，重复步骤2-4，共重复t次。

3.2 算法实现

3.3 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
```

4