初等数论

清华大学 茹逸中

目录

目录

1.1 取模运算

取模运算即取余数运算，例如 7 mod 3 = 1 ， 8 mod 5 = 3 ， 12 mod 4 = 0 。

若 a mod b = 0 则称 a 被 b 整除。

取模运算有以下性质：

- (a + b) mod p = (a mod p + b mod p) mod p
- (a * b) mod p = ((a mod p) * (b mod p)) mod p
- 若 a 与 p 互质，则 ab mod p = ac mod p 与 b mod p = c mod p 等价（消去率）

1.2 欧几里得算法

用欧几里得算法可以计算两个数的最大公因数。

欧几里得算法基于以下定理：

(a,b) = (b,a % b)

```
gcd(a,b):
    if b = 0 return a
    return gcd(b, a % b)
```

1.3 求质数算法

- 欧拉筛法求n以内的质数

对于合数i，若它不是质数，那么它一定是某个质数j($j <= i$)的倍数。所以我们用一个bool数组记录某个数是否被筛去，然后从小到大扫描。若扫描到某个数i，它还没有被筛去时，则它是质数，且筛去所以n以内的它的倍数。

复杂度 $n/1 + n/2 + n/3 + \ldots + n/n = n\log n$

计算该级数和基于积分公式 $\int \frac{dx}{x} = \ln(x)$

质数个数估计：当n足够大时，质数的数量大约在 $n / \ln(n)$

1.3 求质数算法

线性筛法

在欧拉筛法中，我们注意到，一个合数可能会被筛掉多次，这导致了复杂度的增加。

为了将复杂度控制在线性，要让每个合数仅被其最小的质因数筛去。

从小到大进行扫描，若扫描到某个数 i ，它还没有被筛去，则它是质数。对于每个扫描到的数 i ，同时枚举此时得到的质数集合，筛去所有 i * pr[j] ，其中要求 pr[j] < i 的最小质因数。

1.3 例题

分解质因数，有 m 个询问，每个询问数都 <=n

n<=10^6, m <= 10^5

- 找到每个数的最小的质因数，然后递归分解。
- 复杂度为 x 的质因数个数 <= log(x)

2.1 费马小定理及其证明

费马小定理：若p是质数，0 < a < p，则

$$a^{p-1} \equiv 1 \ (mod\ p)$$

费马小定理的证明如下：

- 设集合L = {1,2,3,...,p-1}
- 将集合L中的每个数都乘以a，取mod p的余数，得L' = {a,2a,3a,...,(p-1)a}(mod p)
- 由消去律，因为a与p互质，所以当 $i \neq j$ 时 $ai \neq aj$ (mod p)，所以L'中仍然是互不相同的1~p-1的数，所以L = L'
- 将L和L'中的数全部相乘，得到

$$\prod_{i=1}^{p-1} i = a^{p-1} \prod_{i=1}^{p-1} i \ (\mathrm{mod\ p})$$

- 由消去律，得 $a^{p-1} \equiv 1 \ (mod\ p)$
- 证毕

2.2 欧拉定理及其证明

- 欧拉定理：对于任意数b，若(a,b) = 1，则

$$a^{\varphi(b)} \equiv 1 \ (mod\ b)$$

其中$\varphi(b)$为欧拉函数，表示小于b的数中与b互质的数的个数。

欧拉定理的证明如下：

- 设集合L = 包含了所有小于b的与b互质的数。
- 将集合L中的每个数都乘以a，取mod p的余数，得L'
- 由消去律，因为a与b互质，所以当$i \neq j$时$ai \neq aj(\mathrm{mod\ b})$，所以L = L'
- 将L和L'中的数全部相乘，得到

$$\prod_{i=1}^{p-1} i = a^{\varphi(b)} \prod_{i=1}^{p-1} i(\mathrm{mod\ p})$$

- 由消去律，得$a^{\varphi(b)} \equiv 1 \ (mod\ p)$
- 证毕

2.3 乘法逆元与模 p 域

- 在群论中，若 ab = e，其中 e 是单位元，则称 a 是 b 的左逆元，b 是 a 的右逆元。若还有 ab = ba = e，则 a 与 b 互为逆元，记为。

  对于任意质数 p，考虑到，则可定义有限域 <R,+,*>，其中 R = {1,2,…p-1}。R 中的每一个元素都可以找到乘法逆元，其逆元为。要计算时可通过计算。

在群论中，若ab = e，其中e是单位元，则称a是b的左逆元，b是a的右逆元。ab = ba = e，则a与b互为逆元，记为a = b^{-1}，或者b = a^{-1}。

对于任意质数p，考虑到$a^{p-1} \equiv 1 (mod\ p)$，则可定义有限域<R,+,*>，其中R = {1,2,...p-1}。R中的每个元素a都可以找到乘法逆元，其逆元为a^{p-1}。要计算$\frac{b}{a}$时可通过计算ba^{p-1}来实现。

2.4 原根的概念

- 若 $x = p-1$ 是方程 $a^x \equiv 1 \pmod p$ 的最小正整数解，则称a是质数p的原根。

  原根有一个重要性质，即 $a, a^2, a^3 \ldots a^{p-1}$ 能取遍 1,2,...p-1 中所有的数。

  原根的某些问题中有重要作用。

2.4 原根的概念

- 若 $x = p-1$ 是方程 $a^x \equiv 1 \pmod p$ 的最小正整数解，则称a是质数p的原根。

  原根有一个重要性质，即 $a, a^2, a^3, \ldots, a^{p-1}$ 能取遍 1,2,…,p-1 中所有的数。

  原根的某些问题中有重要作用。

  根据广义Riemann猜想，一个质数的最小原根是loglogloglogloglog(x)级别的，因此可以采取逐个测试的方式来计算原根。

3.1 线性同余方程组求解

- 中国剩余定理
- 求解以下线性同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

- 其中，$m_1, m_2, \ldots, m_n$互质。

3.1 线性同余方程组求解

- 对于上述方程组，令

$$M = m_1 m_2 \ldots m_n$$

$$M_i = \frac{M}{m_i}$$

- 令在模意义下的模逆元素是，即
- 令M_i在模m_i意义下的模逆元素是t_i，即

$$M_i t_i \equiv 1 (\text{mod } m_i)$$

- 则同余方程组的通解为
- 则同余方程组的通解为

$$x = \sum_{i=1}^{n} a_i t_i M_i + kM$$

3.2 模 p 域对数

- 给定质数 p(p<1,000,000,000)，已知 a 和 b(0<a,b<p)，满足

$$a^x \equiv b \pmod p$$

求 x。

3.2 模 p 域对数

- 令 $x = kt - m$，其中 $t = \lfloor\sqrt{p}\rfloor$，$0 \le m \le t$，$1 \le k \le \lceil \frac{p}{t} \rceil$，则有
$$a^{kt-m} \equiv b \pmod p$$
- 即 $a^{kt}b^{-1} \equiv a^m \pmod p$
- 我们先预处理出 $a^0 \bmod p, a^1 \bmod p, \ldots, a^t \bmod p$，然后枚举k，计算 $a^{kt}b^{-1}$，看在 $a^0 \bmod p, a^1 \bmod p, \ldots, a^t \bmod p$ 中是否有相等的数，若有，即找到了满足条件的k和m。
- 时间复杂度 $O(\sqrt{p})$。
- 这种算法思想称之为Baby Step Giant Step。

3.3 模 p 域开 n 次根

- 给定质数 p(p<1,000,000,000)，已知 a 和 b(0<a,b<p)，满足
  $$x^a \equiv b \pmod p$$
  求 x。

3.3 模 p 域开 n 次根

- 给定质数 p(p<1,000,000,000)，已知 a 和 b(0<a,b<p)，满足

$$x^a \equiv b \pmod p$$

求 x。

3.3 模 p 域开 n 次根

- 设 p 的一个原根为 g ，则可以找到唯一的正整数 c 和唯一的正整数 t 使得

$$b \equiv g^{c} (\bmod p)$$
$$x \equiv g^{t} (\bmod p)$$

- 上述方程可转化为

- 上述方程可转化为

$$at \equiv c\big(\bmod (p-1)\big)$$

3.4 素数测试

- 给定正整数x，测试x是否质数
- $O(\sqrt{n})$朴素算法
- Miller Rabin算法，复杂度O(slogp)
- 若一个正整数p，对很多1<a<p，都有$a^{p-1} \equiv 1 \pmod{p}$，则p就有很大概率是质数。

谢谢！

初等数论

清华大学 茹逸中

目录

目录

3. 一些例题
   1. 线性同余方程组求解
   2. 模 p 域对数
   3. 模 p 域开 n 次根
   4. 素数测试

1.1 取模运算

取模运算即取余数运算，例如 7 mod 3 = 1 ， 8 mod 5 = 3 ， 12 mod 4 = 0 。

若 a mod b = 0 则称 a 被 b 整除。

取模运算有以下性质：

- (a + b) mod p = (a mod p + b mod p) mod p
- (a * b) mod p = ((a mod p) * (b mod p)) mod p
- 若 a 与 p 互质，则 ab mod p = ac mod p 与 b mod p = c mod p 等价（消去率）

1.2 欧几里得算法

用欧几里得算法可以计算两个数的最大公因数。

欧几里得算法基于以下定理：

(a,b) = (b,a % b)

```
gcd(a,b):
    if b = 0 return a
    return gcd(b, a % b)
```

1.3 求质数算法

- 欧拉筛法求n以内的质数

对于合数i，若它不是质数，那么它一定是某个质数j(j<=i)的倍数。所以我们用一个bool数组记录某个数是否被筛去，然后从小到大扫描。若扫描到某数i，它还没有被筛去时，则它是质数，且筛去所以n以内的它的倍数。

复杂度 $n/1 + n/2 + n/3 + \ldots + n/n = n \log n$

计算该级数和基于积分公式 $\int \frac{dx}{x} = \ln(x)$

质数个数估计：当n足够大时，质数的数量大约在 $n / \ln(n)$

1.3 求质数算法

线性筛法

在欧拉筛法中，我们注意到，一个合数可能会被筛掉多次，这导致了复杂度的增加。

为了将复杂度控制在线性，要让每个合数仅被其最小的质因数筛去。

从小到大进行扫描，若扫描到某个数 i ，它还没有被筛去，则它是质数。对于每个扫描到的数 i ，同时枚举此时得到的质数集合，筛去所有 i * pr[j] ，其中要求 pr[j] < i 的最小质因数。

1.3 例题

分解质因数，有 m 个询问，每个询问数都 <=n

n<=10^6, m <= 10^5

- 找到每个数的最小的质因数，然后递归分解。
- 复杂度为 x 的质因数个数 <= log(x)

2.1 费马小定理及其证明

- 费马小定理：若p是质数，0 < a < p，则

$$a^{p-1} \equiv 1 \ (mod\ p)$$

费马小定理的证明如下：

- 设集合L = {1,2,3,…,p-1}
- 将集合L中的每个数都乘以a，取mod p的余数，得L' = {a,2a,3a,…,(p-1)a}(mod p)
- 由消去律，因为a与p互质，所以当$i \neq j$时$ai \neq aj (\mathrm{mod\ p})$，所以L'中仍然是互不相同的1~p-1的数，所以L = L'
- 将L和L'中的数全部相乘，得到

$$\prod_{\mathrm{i}=1}^{p-1} i = a^{p-1} \prod_{\mathrm{i}=1}^{p-1} i (\mathrm{mod\ p})$$

- 由消去律，得$a^{p-1} \equiv 1 \ (mod\ p)$
- 证毕

2.2 欧拉定理及其证明

- 欧拉定理：对于任意数b，若(a,b) = 1，则

$$a^{\varphi(b)} \equiv 1\ (mod\ b)$$

其中$\varphi(b)$为欧拉函数，表示小于b的数中与b互质的数的个数。

欧拉定理的证明如下：

- 设集合L = 包含了所有小于b的与b互质的数。
- 将集合L中的每个数都乘以a，取mod p的余数，得L′
- 由消去律，因为a与b互质，所以当$i \neq j$时$ai \neq aj$(mod b)，所以L = L′
- 将L和L′中的数全部相乘，得到

$$\prod_{i=1}^{p-1} i = a^{\varphi(b)} \prod_{i=1}^{p-1} i (\mathrm{mod\ p})$$

- 由消去律，得$a^{\varphi(b)} \equiv 1\ (mod\ p)$
- 证毕

- 欧拉定理：对于任意数 b，若 (a,b) = 1，则

其中为欧拉函数，表示小于 b 的数中与 b 互质的数的个数。

欧拉定理的证明如下：

- 设集合 L = 包含了所有小于 b 的与 b 互质的数。
- 将集合 L 中的每个数都乘以 a，取 mod p 的余数，得 L′
- 由消去律，因为 a 与 b 互质，所以当，所以 L = L′
- 将 L 和 L′ 中的数全部相乘，得到

(mod p)

- 由消去律，得
- 证毕

2.3 乘法逆元与模 p 域

- 在群论中，若 $ab = e$，其中 e 是单位元，则称 a 是 b 的左逆元，b 是 a 的右逆元。若还有 $ab = ba = e$，则 a 与 b 互为逆元，记为 $b = a^{-1}$。

  对于任意质数 p，考虑到 $a^{p-1} \equiv 1 \pmod p$，则可定义有限域 <R,+,*>，其中 $R = \{1,2,\ldots p-1\}$。R 中的每一个元素都可以找到乘法逆元，其逆元为 a^{p-1}。要计算 $\frac{b}{a}$ 时可通过计算 ba^{p-1} 来实现。

2.4 原根的概念

- 若 $x = p-1$ 是方程 $a^x \equiv 1\ (mod\ p)$ 的最小正整数解，则称a是质数p的原根。

  原根有一个重要性质，即 $a, a^2, a^3, \ldots, a^{p-1}$ 能取遍1,2,...,p-1中所有的数。

  原根的某些问题中有重要作用。

2.4 原根的概念

- 若 $p-1$ 是满足 $a^x \equiv 1 \pmod p$ 的最小正整数解，则称a是质数p的原根。

  原根有一个重要性质，即 $a, a^2, a^3 \ldots a^{p-1}$ 能取遍1,2,...p-1中所有的数。

  原根的某些问题中有重要作用。

  根据广义Riemann猜想，一个质数的最小原根是logloglogloglog(x)级别的，因此可以采取逐个测试的方式来计算原根。

3.1 线性同余方程组求解

- 中国剩余定理
- 求解以下线性同余方程组

$$
\begin{cases}
x \equiv a_1 (\bmod m_1) \\
x \equiv a_2 (\bmod m_2) \\
\quad \cdots \\
x \equiv a_n (\bmod m_n)
\end{cases}
$$

- 其中，$m_1, m_2, \ldots, m_n$ 互质。

3.1 线性同余方程组求解

- 对于上述方程组，令

$$M = m_1 m_2 \dots m_n$$

$$M_i = \frac{M}{m_i}$$

- 令M_i在模m_i意义下的模逆元素是t_i，即

$$M_i t_i \equiv 1 (\mathrm{mod}\ m_i)$$

- 则同余方程组的通解为

- 则同余方程组的通解为

$$x = \sum_{i=1}^{n} a_i t_i M_i + kM$$

3.2 模 p 域对数

- 给定质数 p(p<1,000,000,000)，已知 a 和 b(0<a,b<p)，满足

$$a^x \equiv b \pmod p$$

求 x。

3.2 模 p 域对数

- 令 $x = kt - m$，其中 $t = \lfloor\sqrt{p}\rfloor$，$0 \le m \le t$，$1 \le k \le \left\lceil\frac{p}{t}\right\rceil$，则有
$$a^{kt-m} \equiv b \pmod p$$
- 即 $a^{kt}b^{-1} \equiv a^m \pmod p$
- 我们先预处理出 $a^0 \bmod p, a^1 \bmod p, \ldots, a^t \bmod p$，然后枚举k，计算 $a^{kt}b^{-1}$，看在 $a^0 \bmod p, a^1 \bmod p, \ldots, a^t \bmod p$ 中是否有相等的数，若有，即找到了满足条件的k和m。
- 时间复杂度 $O(\sqrt{p})$。
- 这种算法思想称之为Baby Step Giant Step。

- 令 其中 ，则有
- 即
- 我们先预处理出 ，然后枚举 k ，计算 ，看在中是否有相等的数 ，若有，即找到了满足条件的 k 和 m 。
- 时间复杂度。
- 这种算法思想称之为 Baby Step Giant Step 。

3.3 模 p 域开 n 次根

- 给定质数 $p(p<1,000,000,000)$，已知 a 和 $b(0<a,b<p)$，满足

$$x^a \equiv b \pmod{p}$$

求 x。

3.3 模 p 域开 n 次根

- 给定质数 p(p<1,000,000,000)，已知 a 和 b(0<a,b<p)，满足 $x^a \equiv b \pmod p$ 求 x。

3.3 模 p 域开 n 次根

- 设 p 的一个原根为 g，则可以找到唯一的正整数 c 和唯一的正整数 t 使得

- 设p的一个原根为g，则可以找到唯一的正整数c和唯一的正整数t使得

$$b \equiv g^{c} (\mathrm{mod}\, p)$$
$$x \equiv g^{t} (\mathrm{mod}\, p)$$

- 上述方程可转化为

- 上述方程可转化为

$$at \equiv c\big(\mathrm{mod}\ (p-1)\big)$$

3.4 素数测试

- 给定正整数x，测试x是否质数
- $O(\sqrt{n})$朴素算法
- Miller Rabin算法，复杂度O(slogp)
- 若一个正整数p，对很多1<a<p，都有$a^{p-1} \equiv 1 \pmod{p}$，则p就有很大概率是质数。

谢谢！