

初等数论

清华大学 茹逸中

目录

1. 数论基础

1. 取模运算
2. 欧几里得算法
3. 求质数算法

2. 费马小定理

1. 费马小定理及其证明
2. 欧拉定理及其证明
3. 乘法逆元与模 p 域
4. 原根的概念

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 $7 \bmod 3 = 1$ ， $8 \bmod 5 = 3$ ， $12 \bmod 4 = 0$ 。

若 $a \bmod b = 0$ 则称 a 被 b 整除。

取模运算有以下性质：

- ▶ $(a + b) \bmod p = (a \bmod p + b \bmod p) \bmod p$
- ▶ $(a * b) \bmod p = ((a \bmod p) * (b \bmod p)) \bmod p$
- ▶ 若 a 与 p 互质，则 $ab \bmod p = ac \bmod p$ 与 $b \bmod p = c \bmod p$ 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 $j (j \leq \sqrt{i})$ 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，它是质数，且筛去所以内的它的倍数。

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

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 $\leq n$

$n \leq 10^6, m \leq 10^5$

- ▶ 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 $\leq \log(x)$

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

$$a^{p-1} \equiv 1 \pmod{p}$$

费马小定理的证明如下：

- ▶ 设集合 $L = \{1, 2, 3, \dots, p-1\}$
- ▶ 将集合 L 中的每个数都乘以 a ，取 $\text{mod } p$ 的余数，得 $L' = \{a, 2a, 3a, \dots, (p-1)a\} \pmod{p}$
- ▶ 由消去律，因为 a 与 p 互质，所以当 $i \neq j$ 时 $ai \not\equiv aj \pmod{p}$ ，所以 L' 中仍然是互不相同的 $1 \sim p-1$ 的数，所以 $L = L'$
- ▶ 将 L 和 L' 中的数全部相乘，得到
$$\prod_{i=1}^{p-1} i = a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$$
- ▶ 由消去律，得 $a^{p-1} \equiv 1 \pmod{p}$
- ▶ 证毕

2.2 欧拉定理及其证明

欧拉定理: 对于任意数 a 与 b , 若 $(a, b) = 1$, 则

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

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 $\text{mod } b$ 的余数, 得 L'
- ▶ 由消去律, 因为 a 与 b 互质, 所以当 $i \neq j$ 时 $ai \not\equiv aj \pmod{b}$, 所以 $L = L'$
- ▶ 将 L 和 L' 中的数全部相乘, 得到

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

- ▶ 由消去律, 得 $a^{\varphi(b)} \equiv 1 \pmod{p}$
- ▶ 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 $ba = e$ ，则 a 与 b 互为逆元，记为 $b = a^{-1}$ 。

对于任意质数 p ，考虑到 p ，则可定义有限域 R ，定义有模 p 的域 $R = \{1, 2, \dots, p-1\}$ 。其中的每个元素都可以找到乘法逆元，其逆元为 a^{-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 a 是质数 p 的原根，则称 a 是质数 p 的原根。
原根有一个重要性质，即能取遍 $1, 2, \dots, p-1$ 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 a 的最小正整数解 x , 则称 a 是质数 p 的原根。

原根有一个重要性质, 即能取遍 $1, 2, \dots, p-1$ 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 $O(\log \log \log \log \log \log(x))$ 级别的, 因此可以采取逐次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

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

▶ 其中, m_1, m_2, \dots, m_n 互质。

3.1 线性同余方程组求解

▶ 对于上述方程组，令

$$M = m_1 m_2 \dots m_n$$

- ▶ 令在模意义下的模逆元素是，即 $M_i = \frac{M}{m_i}$
- ▶ 令 M_i 在模 m_i 意义下的模逆元素是 t_i ，即
- ▶ 则同余方程组的通解为 $M_i t_i \equiv 1 \pmod{m_i}$
- ▶ 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 ($p \leq 1,000,000,000$), 已知 a 和 b ($0 < a, b \leq p$), 满足
- $$a^x \equiv b \pmod{p}$$
- 求 x 。

3.2 模 p 域对数

- ▶ 令 $x = kt + m$, 其中 $t = \lfloor \sqrt{p} \rfloor$, $0 \leq m \leq t$, $1 \leq k \leq \lfloor \frac{p}{t} \rfloor$, 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 $a^0 \pmod{p}, a^1 \pmod{p}, \dots, a^t \pmod{p}$, 然后枚举 k , 计算 $a^{kt} b^{-1}$, 看是否有相等的数, 若有, 即找到了满足条件的 k 和 m 。

- ▶ 我们先预处理出 $a^0 \pmod{p}, a^1 \pmod{p}, \dots, a^t \pmod{p}$, 然后枚举 k , 计算 $a^{kt} b^{-1}$, 看是否有相等的数, 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。

- ▶ 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 ($p \leq 1,000,000,000$), 已知 a 和 b ($0 < a, b \leq p$), 满足
$$x^a \equiv b \pmod{p}$$
求 x 。

3.3 模 p 域开 n 次根

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

$$b \equiv g^c \pmod{p}$$

$$x \equiv g^t \pmod{p}$$

► 上述方程可转化为
► 上述方程可转化为

$$at \equiv c \pmod{p-1}$$

3.4 素数测试

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

谢谢
!