数学拾遗

陈通

目录

- 数论
- 线性代数

1. 数论篇

1.1 几种质数筛法

1.1.1 埃氏筛

- 基本思路：对于每个数a (a≥2且为整数)，ka (k≥2且为整数)都不是质数
- 时间复杂度：$O(\frac{n}{2}+\frac{n}{3}+\frac{n}{4}+\frac{n}{5}+\ldots)=O(n\log n)$
- 质数个数估计： 小于等于n的质数的个数约为$\frac{n}{\ln n}$个
- 扩展：
  - 筛出一个区间[L, R]中的质数
  - 分段打表

1.1.2 优化埃氏筛

- 基本思路：对于每个质数p，则kp(k≥2且为整数)都不是质数
- 时间复杂度：$O(\frac{n}{2}+\frac{n}{3}+\frac{n}{5}+\frac{n}{7}+\ldots)=O(n\log\log n)$

1.1.3 欧拉筛法（线性筛法）

- 基本思路：
  - 每个合数仅被其最小的质因数筛去
  - 扫描所有的数，对于数a，无论a是质数还是合数，都筛去pa，其中p是质数且小于a的最小的质因数。
- 时间复杂度：$O(n)$
- 扩展：线性求积性函数

例题. 求 $\sum_{i=1}^{n} i \cdot \sigma_1(i^2)$取模

- $n \leq 10^7$
- $n \leq 10^9$，固定模数

1.2 欧几里得与扩展欧几里得算法

- 裴蜀定理：对于整数 a, b 存在整数 x, y 使得 $\gcd(a, b) = ax + by$
- 裴蜀定理推论：整数 a, b 互质的充分必要条件是存在整数 x, y 使得 ax+by=1
- 欧几里得算法（辗转相除法）
- 扩展欧几里得算法

例题. 已知 c_1, c_2, e_1, e_2, N 满足 $(e1, e2) = (m, N) = 1$，$c_1 \equiv m^{e_1} (mod\ N)$， $c_2 \equiv m^{e_2} (mod\ N)$, 求 m 。

- $N \leq 10^{18}$

1.3 费马小定理和欧拉定理

- 费马小定理：对于任意质数p和正整数a，若(a, p) = 1，则 $a^{p-1} \equiv 1$ (mod p)。
- 欧拉定理：对于任意正整数b, a，若(a, b) = 1，则 $a^{\varphi(b)} \equiv 1$ (mod b)。
- 证明：消去律，完全剩余系（简化剩余系）
- 应用：求逆元

1.4 扩展欧拉定理

- 扩展欧拉定理：对于任意正整数b, a, q，则 $a^q \equiv a^{q \bmod \varphi(b)+\varphi(b)} (mod\ b)$ 。
- 证明：考虑a的质因子与b的关系
- 应用：
  - 高次幂取模
  - 指数也是幂形式的数取模

例题. 给定p，求 $2^{2^{2^{\cdot^{\cdot^{\cdot}}}}}\ mod\ p$

1.5 原根

- 设b是正整数，a是整数且与b互质，若 $a^0, a^1, \ldots, a^{\varphi(b)-1}$互不相同，则称a为模b的一个原根。
- 若广义黎曼猜想成立，则p的最小正原根是$O(\log^{(6)} n)$级别的。通过枚举法可以快速找到原根。
- 如何快速判断a是否b的原根？
- 由于欧拉定理成立，方程$a^x \equiv 1$的一个解是$\varphi(b)$。因为它的最小正整数解$x_{min}|\varphi(b)$，逐个尝试p-1的约数即可。若$x_{min} = \varphi(b)$则a是p的原根。

1.6 线性同余方程

$$\begin{cases} x \equiv a_1 (mod\ b_1) \\ x \equiv a_2 (mod\ b_2) \\ \quad\quad \cdots \\ x \equiv a_n (mod\ b_n) \end{cases}$$

- 仅考虑方程数量为2的情况即可（方程数量大于2时可以将每两个方程合并）

$$\begin{cases} x \equiv a_1 (mod\ b_1) \\ x \equiv a_2 (mod\ b_2) \end{cases}$$

- 先考虑特殊情况 $a_1 = 0, (b_1, b_2) = 1$

$$\begin{cases} x \equiv 0(mod\ b_1) \\ x \equiv a(mod\ b_2) \end{cases}$$

- 得 $x = kb_1 \equiv a(mod\ b_2)$
- 由欧拉定理 $k \equiv ab_1^{-1} \equiv ab_1^{\varphi(b_2)-1}(mod\ b_2)$
- 所以 $x \equiv ab_1b_1^{-1} \equiv ab_1^{\varphi(b_2)}(mod\ b_1b_2)$

- 再考虑特殊情况 $a_1 \neq 0, (b_1, b_2) = 1$

$$\begin{cases} x \equiv a_1 (mod\ b_1) \\ x \equiv a_2 (mod\ b_2) \end{cases}$$

- 令 $x' = x - a_1$

$$\begin{cases} x' \equiv 0 (mod\ b_1) \\ x' \equiv a_2 - a_1 (mod\ b_2) \end{cases}$$

- 所以
$x \equiv (a_2 - a_1) b_1 b_1^{-1} + a_1 \equiv (a_2 - a_1) b_1^{\varphi(b_2)} + a_1 (mod\ b_1 b_2)$

- 再考虑特殊情况 $(b_1, b_2) \neq 1$
- 记 $d = (b_1, b_2), x'' = \frac{x'}{d}, b_1' = \frac{b_1}{d}, b_2' = \frac{b_2}{d}$
- 显然，若$d \nmid a_2 - a_1$，则方程无解。记 $c = \frac{a_2 - a_1}{d}$

$$\begin{cases} x'' \equiv 0(mod\ b_1') \\ x'' \equiv c(mod\ b_2') \end{cases}$$

- $x \equiv dc'b_1'b_1'^{-1} + a_1 \equiv c'b_1'^{\varphi(b_2)} + a_1(mod\ gb_1'b_2')$

1.7 第一类指数同余方程

$$a^x \equiv b(mod\ p)$$

- 朴素算法：枚举 $O(p)$

- 大步小步算法(BSGS)
- 考虑分块，记 $x = us + v$，取$s = \lfloor \sqrt{p} \rfloor$。
- $a^x = (a^s)^u \cdot a^v \equiv b(mod\, p)$
- 预处理 $(a^{-s})^0, (a^{-s})^1, (a^{-s})^2, \ldots$ 和 $a^0, a^1, a^2, \ldots$
- 枚举v，通过哈希表查找u。
- 时间复杂度$O(\sqrt{p})$

1.8 第二类指数同余方程

$$x^q \equiv b(mod\ p)$$

- 朴素算法：枚举+快速幂 $O(p\log q)$

- 假设a是p的一个原根，通过第一类指数同余方程的解法求得$b \equiv a^m$
- 令$x \equiv a^y$，则$a^{qy} \equiv a^m$
- $qy \equiv m(mod\ (p-1))$
- 若q与p-1互质，$y \equiv mq^{-1}(mod\ (p-1))$
- 若q与p-1不互质，则有可能有多解或者无解。

1.9 二次剩余

$$x^2 \equiv n(mod\ p)$$

- 有解则必有两解
- 威尔逊定理
- 勒让德符号 $\left(\frac{n}{p}\right)$
- 二次探测定理（欧拉判别法）

- 二次互反律
- Cipolla's Algorithm

例题. 给定a和质数p。求最小n，满足斐波那契数列的第n项 $Fib_n \equiv a(mod\, p)$。

- $p \leq 2 \times 10^9$, 且$(p\ mod\ 10)$为完全平方数。

1.10 Miller Rabin算法

- 给定正整数n，测试n是否质数
- 朴素算法 $O(\sqrt{n})$
- 直接使用费马小定理判断——存在Carmichael数

- Miller Rabin算法基于以下两个定理：费马小定理 + 二次探测定理
- 设$n-1=2^s d$
- 若n是质数，则对于任意的正整数a, 0 < a < n有$a^{n-1}\equiv 1(mod\ n)$
- 多次运用二次探测定理，可得以下两个公式之一成立
  - $a^d\equiv 1$
  - $a^{d\cdot 2^r}\equiv -1(0\le r<s)$
- 若这两条式子均不成立，则n是合数
- 误判概率上限：$(\frac{1}{4})^k$

1.11 Pollard Rho算法

- 分解（质）因数
- 朴素算法：确定性算法、随机化算法
- 生日悖论
- 随机函数
- 弗洛伊德判环
- 维护两个指针

2. 线性代数篇

2.1 向量与向量空间

- 向量
- 向量空间
- 线性变换

2.2 矩阵

- 矩阵的加法
- 矩阵的数乘
- 矩阵的乘法
- 矩阵的转置
- 矩阵快速幂

2.3 线性基

- 张成
- 线性相关和线性无关
- 线性基是满足线性无关的极大子集
- 线性基中元素的个数就是线性空间的维度
- 矩阵的秩
- 满秩与线性无关

2.4 线性方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n} = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n} = b_2 \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn} = b_m \end{cases}$$

- $A_{m\times n} \cdot x_{n\times 1} = b_{m\times 1}$

- 高斯消元
- 主元与自由元
- 解的数量
- 解的数值稳定性

2.5 行列式

方阵$A_{(n\times n)}$，定义A的行列式为

$$|A| = \sum_{p_1,p_2,\dots p_n} (-1)^{p_1,p_2,\dots p_n} a_{1p_1} a_{2p_2} \dots a_{np_n}$$

- 意义：（行）列向量的面积，特征值的乘积

- 上三角矩阵的行列式
- 行列式的计算
- 初等变换行列式的值不变
  1. 用一非零的数乘以某一行
  2. 把一个方程的倍数加到另一个行
  3. 互换两个行的位置
- 高斯消元

- 应用：
  - 矩阵树定理
  - 求三角形面积
  - 解方程

- 积和式

$$\sum_{p_1,p_2,\ldots p_n} a_{1p_1}a_{2p_2}\ldots a_{np_n}$$

- 行列式的无系数版本
- 不易计算
- 奇偶性与行列式相同

2.6 矩阵的逆

- 逆矩阵：对于方阵A，若存在方阵B满足$AB = BA = I$，称B为A的逆，记作A^{-1}。
- 逆矩阵存在等价于行列式不为0
- 矩阵的逆的计算方法

$$A|I \rightarrow I|A^{-1}$$

2.7 余子式与伴随矩阵

- 余子式： 将方阵A划去第i行第j列，得到的n-1阶行列式称为元素a_{ij}余子式，记作$M_{i,j}$。
- 代数余子式：令$A_{ij}=(-1)^{i+j}M_{ij}$， 称A_{ij}为元素a_{ij}的代数余子式。
- 行列式按第i行展开：

$$|A|=\sum_{j=1}^{n}a_{ij}A_{ij}$$

- 伴随矩阵：第i行第j列为A_{ji}的矩阵为矩阵A的伴随矩阵，记作A*。
- 伴随矩阵的重要性质：若矩阵A可逆，

$$A^* = |A|A^{-1}$$

例题. 给定有向带权图，求所有以n号点为根的内向树，所选边的边权之和。

- $n \leq 300$

例题. 给出一张二分图，这张二分图完美匹配的个数是奇数，求删掉第 $i(1 \le i \le m)$ 条边后完美匹配个数的奇偶性。

- $n \le 2000$

2.8 换基与矩阵的相似

- 换基的目的：使矩阵变为更易于计算的形式
- 对于方阵A、B，若存在矩阵P，使 $A = P^{-1}BP$，则称A与B相似
- $A^m = (P^{-1}BP)^m = P^{-1}B^mP$

例题. 给定a_0, a_1，$a_i = 3a_{i-1} - 2a_{i-2}$，求$a_n$模$10^{1000}$。

- $n \le 10^{18}$

2.9 特征值与特征向量

- 不变子空间
- 特征值和特征向量：对于矩阵A和数λ，若存在非零向量v使得$Av = \lambda v$，则称λ为A的**特征值**，v为A相对于λ的**特征向量**。
- $(T - \lambda I)v = 0$

- λ为A的特征值的充要条件是$|T - \lambda I| = 0$
- 上三角矩阵的特征值就是它主对角线上的元素

例题. 一个培养皿分为n个区域，一开始第1个区域有一个细胞，在每个单位时间，第i个区域的每个细胞会分裂并进入第j个区域 a_{ij} 个。细胞只会进入编号大于等于当前编号的区域。保证$a_{ii} \neq a_{jj}$。求T个时刻后细胞数量，取模。

- $n \leq 200, T \leq 10^{100000}$

2.10 特征多项式

- 特征多项式：$p_T(x) = |xI - T|$
- $p_T(x) = a_n x^n + ... + a_0 = (x - \lambda_1)...(x - \lambda_n)$
- 凯莱-哈密顿定理(Cayley–Hamilton theorem)：$p_T(T)$ = 0
- 极小多项式

2.11 齐次线性递推

- 已知$s_1, \ldots, s_k$， $s_m = \sum_{i=1}^{k} a_i \cdot s_{m-i}$，求$s_n$。
- 朴素算法：$O(nk)$
- 矩阵快速幂：$O(k^3 \log n)$
- 优化？

- 特征多项式：$p(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$
- 目标：求 A^n
- 令$f(x) = x^n \ mod \ p(x)$，则$A^n = f(A)$
- $A^n(s_0, \ldots, s_{-k+1})^T = f(A)(s_0, \ldots, s_{-k+1})^T = \sum_{i=1}^{k} [f_i] s_i$

谢谢！