数学

吴耀轩

北京大学

Section 1

BSGS

给定质数p，给定a和b，$(a, p) = 1$。

求最小的非负整数x，使得$a^x \equiv b \pmod{p}$。

根据欧拉定理$a^{\varphi(p)} \equiv 1 \pmod p$，当$a^x \equiv b \pmod p$有解，最小非负整数解必然在$[0, \varphi(p))$中。

记$m = \lfloor \sqrt{\varphi(p)} \rfloor$，任意$x \in [0, \varphi(p))$都可以分解成$im + j$的形式，其中$0 \le i \le m, 0 \le j < m$。

枚举i的取值，$a^x \equiv b \pmod p \Leftrightarrow a^j \equiv a^{-im} b \pmod p$。

何以得出是否有$0 \le j < m$，满足$a^j \equiv a^{-im} b \pmod p$：将$a^0, a^1, a^2, \ldots, a^{m-1}$ 压入Hash-Table，在Hash-Table中询问即可。

算法思想：分块

算法复杂度：$O(\sqrt{\varphi(p)})$

算法缺陷：不能做p不是质数的情况

Section 2

Miller-Rabin

给定n，判断n是否为素数。

在进行Miller-Rabin探测之前，先筛去n是偶数的情况，只需要考虑n是奇数。

于素数p而言，任意$x = 1, \ldots, p-1$，都有$x^p \equiv x \pmod{p}$，而于合数，这个等式不一定成立。根据这个性质，如果找到了$1 \le x < n$，$x^n \not\equiv x \pmod{n}$，说明$n$一定是合数。

然而存在一些Carmichael数，如561，其本身是合数，但x 取遍$1, \ldots, n-1$都满足$x^n \equiv x \pmod{n}$。

考虑$x^2 \equiv 1 \pmod{n}$ 的根，若n为奇素数，只有1和$n-1$两根；若n是奇合数，一定存在其他的根。

设$n-1 = 2^r * d$，其中d是奇数。若存在$0 \le k < r$，$a^{2^k * d} \not\equiv 1, -1 \pmod{n}$，但是$a^{2^{k+1} * d} \equiv 1 \pmod{n}$，可推断$n$一定是合数。

任选一个a，若n是素数，一定可以通过二次探查和费马定理的测试；若n是合数，出现矛盾的概率是$\frac{1}{2}$。

选取k组a进行探测，算法的错误率为2^{-k}。

对于$int32$范围内的数，使用$2, 7, 61$探测即可；对于$int64$范围内的数，使用前10个素数作为探测基底即可保证算法成功。

Section 3

Pollard-rho

给定n，要求对n质因数分解。

- 若Miller-Rabin测试n 为素数，可以停止分解。
- 随机基底a和c，生成序列$x_0 = a, x_i = x_{i-1}^2 + c \pmod{n}$，可以认为$\{x_i\}$是随机序列。
- 若出现$(x_i - x_{2i+1}, n) \neq 1$，此时停止算法，令$d = (x_i - x_{2i+1}, n)$，若$d \neq n$，那么$d$就是$n$的一个非平凡因子，$n$被分为$d$和$n/d$相乘的结果，递归下去对$d$及$n/d$继续分解。
- 若$d = n$，那么重新选一组基底a与c，再次重复过程。
- 复杂度$O(n^{1/4} poly(n))$

生日悖论：每个人的生日都是1到n之间的正整数，期望$\sqrt{N}$个人中至少有两个人生日相同。

假设n是合数，$n = n_1 n_2$，设$y_i = x_i \pmod{n_1}$。

则$\{y_i\}$会在$\sqrt{n}_1$ 步内进入循环，此时有$n_1 \mid x_i - x_j$，而多半x_i 还没有进入 $\bmod n$的循环，$(x_i - x_j, n)$就是n的一个平凡因子，而$n_1 \le \sqrt{n}$，则rho算法会在$O(n^{1/4})$步内分解成功。

Section 4

Linear-Shaker

要求筛出小于n的所有素数。

传统的筛法是用i筛去所有i的倍数，复杂度$O(n \ln n)$，每个数被其每个因子都筛了一遍。

线性筛是用i筛去i的部分倍数，假设i的最大素因子为p_0，$\leq p_0$的素因子为$p_1, \ldots, p_j$，线性筛的过程中i只筛去了$ip_0, \ldots, ip_j$。注意到若i的最小素因子为p，那么i只会被i/p筛去，复杂度$O(n)$。

Section 5

Chinese Reminder Thereom

$$x \mod n_1 = x_1$$

$$x \mod n_2 = x_2$$

……

$$x \mod n_k = x_k$$

其中$n_1, \ldots, n_k$两两互质，求x的一个合法解。

令$N = n_1 n_2 \ldots n_k$，$m_i = N/n_i$，$t_i = m_i^{-1} \pmod{n_i}$。

$$x = \sum_i x_i m_i t_i \pmod{N}$$

容易验证当$j = i$时，$m_i t_i \equiv 1 \pmod{n_i}$，当$j \neq i$时，$m_i t_i \equiv 0 \pmod{n_j}$，则$x$一定是原方程的一组解。

Section 6

Quadratic residue

给定y和奇质数p，求x，使得$x^2 \equiv y \pmod{p}$。

欧拉判别法：

- 若$y^{\frac{p-1}{2}} \equiv 1 \pmod p$，则$y$在模奇素数$p$下有二次剩余
- 若$y^{\frac{p-1}{2}} \equiv -1 \pmod p$，则$y$ 在模奇素数p下没有二次剩余
- 勒让德符号$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$
- $1..p-1$中有$\frac{p-1}{2}$个数的勒让德符号为1，另有$\frac{p-1}{2}$ 为-1。

Cipolla's Algorithm.

- 不断随机a，使得$(\frac{a^2-y}{p})=1$
- 令$\omega=\sqrt{a^2-y}$，$x=(a+\omega)^{(p+1)/2}$
- $x^2\equiv(a+\omega)^p*(a+\omega)\equiv(a+\omega)\sum_j\binom{p}{j}a^j\omega^{p-j}\equiv(a-\omega)(a+\omega)\equiv a^2-\omega^2\equiv y\pmod p$

unknown

给定长度为n的高精度数字a，请判断a是不是完全平方数。

$n \leq 1000$

unknown

给定长度为n的高精度数字a，请判断a是不是完全平方数。

$n \leq 1000$

暴力高精度?

Section 7

Multiplicative function

狄利克雷卷积：

$$(fg)(n) = \sum_{d|n} f(d)g(n/d)$$

积性函数的性质：

- $\forall (a,b)=1, f(ab)=f(a)f(b)$
- 积性函数的卷积仍然是积性函数

$$n = p1^{k1} p2^{k2} \dots pm^{km}$$

普通函数：

$$1(n) = 1, id(n) = n, e(n) = [n = 1]$$

除数函数：

$$\sigma_k(n) = \sum_{d|n} d^k$$

欧拉函数：

$$\varphi(n) = n * \frac{p1 - 1}{p1} \dots \frac{pm - 1}{pm}$$

莫比乌斯函数：

$$\mu(n) = [k1 \le 1][k2 \le 1] \dots [km \le 1](-1)^m$$

- $\sum_{d|n} \mu(d) = [n = 1] \Rightarrow \mu * 1 = e$
- $\sum_{d|n} \varphi(d) = n \Rightarrow \varphi * 1 = id$

- 怎么求φ, μ的前n项？
- 怎么求φ, μ的前缀和？

Section 8

Primitive root

给定n，若a满足$(a,n)=1$ 且$1,a,a^2,\ldots,a^{\phi(n)-1}$ 在 $\bmod n$下都互不相同，则称a是n的一个原根。

性质：

- 2,4,p^n,2p^n 有原根，p是奇素数
- 若n有原根，原根的数量为$\varphi(\varphi(n))$ 个

如何判断a是不是n的原根？暴力算a的幂次？

如何判断a是不是n的原根？暴力算a的幂次？

如何找到n的一个原根？

Section 9

Combination

$\binom{n}{m}$表示从n个与区分的物品中无顺序地选取m 个物品的方法。

- 物品有区分
- 选取有顺序

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

- 杨辉三角
- 预处理阶乘及逆元
- 求$\binom{10^9}{10^8} \pmod{21^{18}}$

Section 10

Recurrence relation

- 有一些问题只需要用较少的状态就可以刻画问题
- 较大规模的问题由较小的问题推得
- 线性递推可以利用矩阵乘法优化

unknown

给定一张N个点M条边的有向图，Q次询问图中从每个点出发的长度为K 的路径各有多少条。

$N \leq 100, Q \leq 10, K \leq 100$

unknown

给定一张N个点M条边的有向图，Q次询问图中从每个点出发的长度为K 的路径各有多少条。

$N \le 100, Q \le 10, K \le 100$

矩阵乘法？

unknown

给定一张N个点M条边的有向图，Q次询问图中从每个点出发的长度为K 的路径各有多少条。

$N \leq 100, Q \leq 10, K \leq 100$

矩阵乘法？

分块优化？

Section 11

Principle of inclusion-exclusion

容斥原理：

$$F(A\cup B\cup C) = F(A)+F(B)+F(C)-F(A\cap B)-F(A\cap C)-F(B\cap C)+F(A\cap B\cap C)$$

Section 12

Binomial inversion

二项式反演：

$$f_n=\sum_{i=0}^{n}(-1)^i\binom{n}{i}g_i \Leftrightarrow g_n=\sum_{i=0}^{n}(-1)^i\binom{n}{i}f_i$$

$$f_n=\sum_{i=0}^{n}\binom{n}{i}g_i \Leftrightarrow g_n=\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}f_i$$

bzoj2839 集合计数

n个元素的集合有2^n种子集，现从2^n个子集中选出若干子集，求有多少种方法，使得选出集合的交元素个数为K。

$n, K \leq 10^6$，对10^9+7取模。

bzoj2839 集合计数

n个元素的集合有2^n种子集，现从2^n个子集中选出若干子集，求有多少种方法，使得选出集合的交元素个数为K。

$n, K \leq 10^6$，对10^9+7取模。

怎么化到二项式反演？

bzoj4487 JSOI2015染色问题

有$n * m$的矩阵，C种染料，每个格子可以不染或染成任意颜色，求有多少种方案使得：

- 每一行至少有一个格子被染色
- 每一列至少有一个格子被染色
- 每种颜色至少在棋盘上出现一次

bzoj4487 JSOI2015染色问题

有$n*m$的矩阵，C种染料，每个格子可以不染或染成任意颜色，求有多少种方案使得：

- 每一行至少有一个格子被染色
- 每一列至少有一个格子被染色
- 每种颜色至少在棋盘上出现一次

答案为$\sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=0}^{C}(-1)^{i+j+k}k^{(n-i)(m-j)}$

Section 13

Probability Thereom

- 概率独立的事件可以分开考虑
- 期望具有线性性

jsk1483G Clear the room

给定$n * m$的网格，(i, j)中物品价值为w_{ij}。小G有K次操作，每次随机从网络中独立地选取两个格子，然后将这两个格子中构成的矩形中还没有被拿走的物品全部拿走。求K次操作后拿走物品价值和的期望。

$n, m \leq 500, K \leq 10^9$。

jsk1483G Clear the room

给定$n * m$的网格，(i, j)中物品价值为w_{ij}。小G有K次操作，每次随机从网络中独立地选取两个格子，然后将这两个格子中构成的矩形中还没有被拿走的物品全部拿走。求K次操作后拿走物品价值和的期望。

$n, m \leq 500, K \leq 10^9$。

利用期望线性，计算每一个格子被拿走的概率。

Section 14

Gaussian

对矩阵作行变换的过程被称为行变换。

- 将一行乘以非零数
- 将一行的倍数加到另一行上
- 交换两行

怎么用高斯消元解线性方程组？

怎么用高斯消元解线性方程组？

- 将变量前的系数连同等式右侧常数写成矩阵
- 对矩阵作行变换消成阶梯形矩阵
- 从最下侧的方程反解答案

Section 15

Determinant

- 设$p_1, \ldots, p_n$是n阶排列，那么$1, \ldots, n$在$p_1, \ldots, p_n$中各恰好出现一次
- $\sigma(p_1, \ldots, p_n)$ 表示排列中逆序对出现的次数
- 方阵A的行列式是一个值

$$det(A) = \sum_{i_1, \ldots, i_n \ is \ a \ permutation} (-1)^{\sigma(i_1, \ldots, i_n)} A_{1,i_1} A_{2,i_2} \ldots A_{n,i_n}$$

性质：

- 若方阵A有一行是另一行的若干倍，$det(A) = 0$
- 将方阵A的某一行若干倍加到另一行上，行列式不变
- 交换方阵的两行，行列式变为相反数
- 上三角矩阵的行列式恰为对角线的乘积

如何求A的行列式？

如何求A的行列式？
将矩阵作高斯消元，答案就是对角线上的乘积或其相反数。
复杂度$O(n^3)$。

Section 16

Matrix-Tree

给定无向图$G = (E, V)$，求该图有多少种生成树？

生成树：从E中选取$|V| - 1$ 条边，使得选取的边构成一颗树。

Matrix-Tree定理：

- 记D为度数矩阵，D_{ii}表示i连接的变数
- 记A为邻接矩阵，A_{ij}表示i和j之间边数
- 基尔霍夫矩阵$K = D - A$，记K_0为K删去最后一行一列，生成树数量恰为$det(K_0)$

Section 17

Burnside and Polya

LightOJ1419 Necklace

有长度为n的环形项链，每个珠子的颜色都可以是$1 \to K$，请问有多少种本质不同的染色方式。如果其中一个染色方案通过旋转可以得到另一个方案，则这两种方式被认为是本质相同的。

$n \leq 1000, K \leq 10^9$。

LightOJ1419 Necklace

有长度为n的环形项链，每个珠子的颜色都可以是$1 \to K$，请问有多少种本质不同的染色方式。如果其中一个染色方案通过旋转可以得到另一个方案，则这两种方式被认为是本质相同的。

$n \leq 1000, K \leq 10^9$。

Burnside引理：$|\Pi/G| = \frac{1}{|G|}\sum_{g}|fixed(g)|$

LightOJ1419 Necklace

有长度为n的环形项链，每个珠子的颜色都可以是$1 \to K$，请问有多少种本质不同的染色方式。如果其中一个染色方案通过旋转可以得到另一个方案，则这两种方式被认为是本质相同的。

$n \le 1000, K \le 10^9$。

Burnside引理：$|\Pi/G| = \frac{1}{|G|}\sum_{g}|fixed(g)|$

这是嘛玩意儿?!!

LightOJ1419 Necklace

有长度为n的环形项链，每个珠子的颜色都可以是$1 \to K$，请问有多少种本质不同的染色方式。如果其中一个染色方案通过旋转可以得到另一个方案，则这两种方式被认为是本质相同的。

$n \le 1000, K \le 10^9$。

Burnside引理：$|\Pi/G| = \frac{1}{|G|}\sum_g |fixed(g)|$

这是嘛玩意儿?!! 本质不同的方案数=$|\Pi/G|$，G就是n种旋转方式，$|fixed(g)|$就是表示在某个旋转下方案不变的数量。

Section 18

SG

- 公平博弈问题中，用SG来描述当前局面操作者的胜负关系。
- 若SG为0，则先手必败，否则先手必胜。
- 若同时又N个游戏同时进行，那么N个游戏的总SG为$SG_1 \oplus \cdots \oplus SG_N$。
- 如果先手经过一步操作后能到达的局面对应的SG值分别为$SG_1, \ldots, SG_M$，那么当前游戏的SG值为$mex\{SG_1, \ldots, SG_M\}$

bzoj1874 BeiJing2009 取石子游戏

n堆石子，每堆石子有a_i个，两个人轮流取石子，每次可以取的数量可以是$b_1, b_2, \ldots, b_m$，求双方都是最优策略下先手胜负。

$n, b_i \leq 10, a_i \leq 1000$

bzoj1874 BeiJing2009 取石子游戏

n堆石子，每堆石子有a_i个，两个人轮流取石子，每次可以取的数量可以是$b_1, b_2, \ldots, b_m$，求双方都是最优策略下先手胜负。

$n, b_i \leq 10, a_i \leq 1000$

转化到sg函数？

bzoj1016 JSOI2008 最小生成树计数

bzoj2654 tree

bzoj1004 HNOI2008Cards