Math

$n + e$

Tsinghua University

2016 年 6 月 30 日

About

- 我们不是数学家, 对于公式定理**会用**就行
- 高中阶段提升数学能力最好的地方: 联赛初赛/复赛第一试
- 建议大家在暑假期间自学高中数学**所有**内容, 百利而无一害
- 本章节基本按照 ≪ 训练指南 ≫ 的结构内容安排

- 加法原理
- 乘法原理
- 容斥原理

$$|A\cup B\cup C| = |A|+|B|+|C|-|A\cap B|-|B\cap C|-|A\cap C|+|A\cap B\cap C|$$

- 扔一枚骰子 n 次，所得点数最大值为 5 最小值为 2 的概率

$$ans = \frac{4^n - 2\times 3^n + 2^n}{6^n}$$

- 排列组合

- 欧拉筛素数

```
for(int i=2,j;(j=i*i)<=n;i++)if(!vis[i])
for(;j<=n;j+=i)vis[j]=1;
```

- 线性筛素数

```
for(int i=2;i<=n;i++){
    if(!vis[i])prime[++t]=i;
    for(int j=1;j<=t&&i*p[j]<=n;j++){
        vis[i*p[j]]=1;
        if(i%p[j]==0)break;
    }
}
```

- 好好背代码去

φ 函数

$$\varphi(n) = \sum_{i=1}^{n} [(i, n) = 1]$$

- 积性函数: $\varphi(mn) = \varphi(m)\varphi(n),\ if\ (m, n) = 1$
- 设 $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, 则

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m})$$

- 需质因数分解: n 最多只有 1 个大于 $\sqrt{n}$ 的质因数

- 欧拉筛 φ

```
for(int i=2,j;i*i<=n;i++)if(!phi[i])
for(;j<=n;j+=i)phi[j]=!phi[j]?j:phi[j]/i*(i-1);
```

- 线性筛 φ

```
for(int i=2;i<=n;i++){
    if(!phi[i])phi[p[++t]=i]=i-1;
    for(int j=1;j<=t&&i*p[j]<=n;j++){
        if(i%p[j]==0){phi[i*p[j]]=phi[i]*p[j];break;}
         phi[i*p[j]]=phi[i]*(p[j]-1);
    }
}
```

- 好好背代码去

- gcd 2246, 经典题

```
typedef long long ll;
ll gcd(ll x,ll y){return!y?x:gcd(y,x%y);}
```

- exgcd: 求整数 x,y 使得 ax+by=(a,b), 并且 |x|+|y| 最小

```
void exgcd(ll a,ll b,ll&d,ll&x,ll&y){
    !b?d=a,x=1,y=0:(exgcd(b,a%b,d,y,x),y-=x*(a/b));
}
```

- 推导见这里

%%%

- 坑: 计算机中若 a<0, 则 $a \bmod b$ 依然是负数, 与数学上的定义并不同.
- a=(a+b)%p; 可改为 if(a+=b,a>=p)a-=p;
- 模运算常数较大, 用判断语句和减法运算代替模运算

%%%

- 坑: 计算机中若 a<0, 则 $a \bmod b$ 依然是负数, 与数学上的定义并不同.
- a=(a+b)%p; 可改为 if(a+=b,a>=p)a-=p;
- 模运算常数较大, 用判断语句和减法运算代替模运算

- 真的是这样吗?

- 快速幂

```
ll power(ll t,ll k,ll p){//t^k%p
    ll f=1;
    for(t%=p;k;t=t*t%p,k>>=1)if(k&1)f=f*t%p;
    return f;
}
```

- 快速乘: 有时候 a*b 会爆 long long 并且 p 是 10^{10} 级别的
- 是可以把上面的乘号改成加号, 但是有下面这种 Trick

```
ll mul(ll a,ll b,ll p){//a*b%p
    ll tmp=(a*b-(ll)((long double)a/p*b+1e-5)*p);
    return tmp<0?tmp+p:tmp;
}
```

- 乘法逆元: 若 $a \cdot b \equiv 1 \pmod{p}$, 则 $a \equiv \frac{1}{b} \pmod{p}$
- 欧拉定理: $a^{\varphi(m)} \equiv 1 \pmod{m}$, *when* $(a, m) = 1$
- 特殊情况即为费马小定理: $a^{p-1} \equiv 1 \pmod{p}$
- 因此

  $$inv[a] = \frac{1}{a} \equiv a^{p-2} \pmod{p}$$

  快速幂实现即可
- 用 exgcd: 求方程 $ax + py = (a, p) = 1$ 的解 (x,y), 其中必定包含 $(\frac{1}{a}, 0)$, 两边同时对 p 取模即可

- 线性求逆元: 跟上面求 φ 一样做也行, 但是有下面这种方法

```
inv[1]=1;
for(int i=2;i<=n;i++)inv[i]=p-(p/i*inv[p%i])%p;
```

- 推导: 设 $ai+b=p\equiv 0 \pmod p$, 则有 $a=\lfloor \frac{p}{i} \rfloor, b=p \bmod i$, 并且

$$\frac{1}{i}\equiv -\frac{a}{b} \pmod p$$

就是上面的代码了

BSGS-素数版

- 解方程

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

- 取 $k = \sqrt{p}$, 如果有解, 则 x 必定能够表示为 $ck + d$ 的形式
- 方程化为

$$(a^k)^c \equiv \frac{b}{a^d} \pmod{p}$$

- 计算并用 hash 表存储 $\frac{b}{a^0}, \frac{b}{a^1}, \cdots, \frac{b}{a^k}$ 的值, 枚举 c 的值, 看看有没有相等的情况, 输出来就好了.
- 一个 Trick: 把 $ck + d$ 改成 $ck - d$, 方程化为

$$(a^k)^c \equiv b \times a^d \pmod{p}$$

就不用求逆元了

exBSGS

- 膜 Miskcoo

中国剩余定理

- 有 n 个方程，第 i 个方程为 $x \equiv a_i \pmod{m_i}$，求最小的 x
- 类似插值的方法：设 $M = \prod_{i=1}^{n} m_i$, $M_i = M/m_i$, $t_i M_i \equiv 1 \pmod{m_i}$

  则在 $\pmod{M}$ 的意义下，该方程组只有一个解

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

中国剩余定理

- m_i 不互质？就要用 exgcd 合并方程组
- $n \bmod m_1 = a_1,\ n \bmod m_2 = a_2,\ t = (m_1, m_2)$
- $n = m_1x + a_1 = m_2y + a_2,\ m_1x - m_2y = a_2 - a_1$
- 若 $a_1 \not\equiv a_2 \pmod t$，则无解
- 将方程两边同时除以 t，记新方程为 $ax + by = c$
- 用 exgcd 得到该方程的一组特解 (x_0, y_0)，通解为 $x = x_0 + k \cdot b$，k 为整数
- $m_1(x_0 + k \cdot b) + a_1 = n$
- 合并后的方程为 $(m_1 \cdot b)k + m_1x_0 + a_1 = n$
- 即 $n \bmod (m_1 \cdot b) = m_1x_0 + a_1$

Miller-Rabin 素性测试

- 这里有介绍
- 它是一个概率算法
- 还是一个大模板背下来就好了……

反演

- 看这里
- 本质是~~推式子~~容斥

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

你应当要想起下面这些东西:

1. c[n][k]=c[n][n-k]
2. c[i][j]=c[i-1][j]+c[i-1][j-1]
3. c[n][k+1]=c[n][k]$\times \frac{n-k}{k+1}$
4. $$(a+b)^n = \sum_{k=0}^{n} C_n^k \times a^k \times b^{n-k}$$

Problem Set

5. 有重复元素的全排列. 有 n 个不同元素, 其中第 i 个元素有 a_i 个, 则全排列个数为:

$$\binom{a_1+a_2+\cdots+a_n}{a_1,a_2,\cdots,a_n}=\frac{(a_1+a_2+\cdots+a_n)!}{a_1!a_2!\cdots a_n!}$$

6. 可重复选择的组合. 有 n 个不同元素, 每个元素可以选多次, 一共选 k 个元素, 求方案数.
   - 设第 i 个元素选 x_i 个, 则问题转化为求方程 $x_1+x_2+\cdots+x_n=k$ 的非负整数解的个数
   - 令 $y_i=x_i+1$, 等价于求方程 $y_1+y_2+\cdots+y_n=k+n$ 的正整数解的个数
   - 隔板问题: ans=c[n+k-1][n-1]=c[n+k-1][k]

Appendix

表 5.4　居首位的 10 个二项系数等式

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$,	整数$n \geqslant k \geqslant 0$.	阶乘展开
$\binom{n}{k} = \binom{n}{n-k}$,	整数$n \geqslant 0$，整数k.	对称
$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}$,	整数$k \neq 0$.	吸收／抽出
$\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}$,	整数k.	加法／归纳
$\binom{r}{k} = (-1)^k\binom{k-r-1}{k}$,	整数k.	上求反
$\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}$,	整数m,k.	三项修正
$\sum_k \binom{r}{k} x^k y^{r-k} = (x+y)^r$,	整数$r \geqslant 0$ 或$\lvert x/y \rvert < 1$.	二项定理
$\sum_{k \leqslant n} \binom{r+k}{k} = \binom{r+n+1}{n}$.	整数n.	类似求和

- 百度百科这里抄讲的还是可以的

数列

- $F_{n+2} = F_{n+1} + F_n,\ \ F_0 = 0,\ \ F_1 = 1$
  0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, ······
- $C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!} = \frac{4n-2}{n+1}C_{n-1}$

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$$

1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, ······

方法

- 主要是 DP, 思路在 DP 那一讲讲过了 (考虑子问题与原问题之间的关联性)
- 不会 DP?

方法

- 主要是 DP, 思路在 DP 那一讲讲过了 (考虑子问题与原问题之间的关联性)
- 不会 DP? 找规律!

- 请勿看答案
- 眼球技术
- n 次多项式差分 n+1 次之后就变成了 0，可以返推回去：1111
- 普通插值方法
- k 次方幂和本质上是一个 k+1 次关于 n 的多项式，使用线性插值的方法即可解决本问题
- 详见 ≪ 多项式及求和 ≫ From 杜瑜皓
- 常系数递推多项式？暴力枚举多少项递推，然后高斯消元，检验是否能接着递推：1982
- 剩下的超几何函数我表示不会搞，并没有研究过，欢迎讨论

平等博弈的两个规则:

1. 一个状态是必败状态 (0), 当且仅当它的所有后继都是必胜状态 (1)
2. 一个状态是必胜状态 (1), 当且仅当它至少有一个后继状态是必败状态 (0)

记当前游戏局面的状态为 x, 则 $SG(x) = mex\{S\}$, 其中 S 表示 x 的所有后继状态的 SG 函数值的集合, mex 函数表示当前集合中未出现过的最小非负整数

- SG(x)=0 当且仅当 x 为必败状态

游戏的 nim 和: 把所有状态异或起来的 SG 值

举个栗子

- 有 N 堆石子, 每堆有 a_i 个, 两个玩家轮流取石子, 每次只能从任意一堆中拿走至少一个石子, 当然也可以全部拿走. 谁不能拿谁就输了. 问先手的胜负情况
- 比如 $N = 3,\ a_1 = 1,\ a_2 = 2,\ a_3 = 3$
- 单堆 nim 游戏满足 SG(x)=x, 多堆 nim 游戏把状态异或起来, 转化成单堆问题
- 结论: 直接异或

举个栗子

- 有 N 堆石子，每堆有 a_i 个，两个玩家轮流取石子，每次只能从任意一堆 (i) 中拿走至少一个石子，最多只能拿走 $\lfloor \frac{a_i}{2} \rfloor$ 个石子. 谁不能拿谁就输了. 问先手的胜负情况
- 比如 $N = 3,\ a_1 = 1,\ a_2 = 2,\ a_3 = 5$

```
SG[0]=SG[1]=0;
for(int i=2;i<=n;printf("SG[%d]=%d\n"i,SG[i]),i++){
    memset(vis,0,i+1);
    for(int j=1;j<<1<i;j++)vis[SG[i-j]]=1;
    for(;vis[SG[i]];SG[i]++);
}
```

- 0, 0, 1, 0, 2, 1, 3, 0, 4, 2, 5, 1, 6, 3, 7, 0, 8, 4, 9, 2, 10,⋯⋯
- 0, 0, 1, 0, 2, 1, 3, 0, 4, 2, 5, 1, 6, 3, 7, 0, 8, 4, 9, 2, 10,⋯⋯

1. 计数方法
2. 数论
3. 组合数学
4. 概率论
   - 高考真题
   - 生日攻击
   - 随机转移状态机：马尔可夫链
5. 线性代数
6. 微积分

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$$E(X + Y) = EX + EY$$

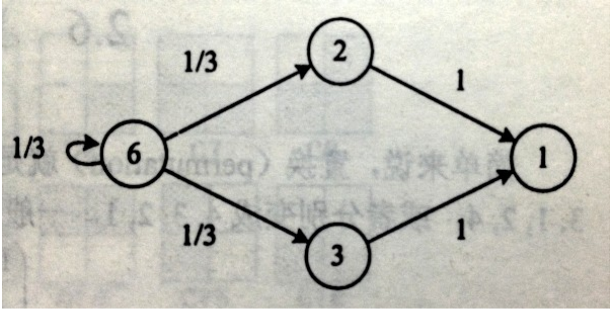
- 数学期望 EX: 对于所有情况求个平均数

- (2016 全国卷 I, 理数 4) 某公司的班车在 7:00, 8:00, 8:30 发车, 小明在 7:50 至 8:30 之间到达发车站乘坐班车, 且到达发车站的时刻是随机的, 则他等车时间不超过 10 分钟的概率是?
- (2010 天津,18 改) 某射手每次射击击中目标的概率是 2/3, 且各次射击的结果相互独立, 互不影响. 记 4 次中击中的次数为 X, 求 X 的分布列与数学期望

- 生日悖论: 如果一个房间里有 23 个或 23 个以上的人, 那么至少有两个人的生日相同的概率要大于 50%. 对于 60 或者更多的人, 这种概率要大于 99%.
- 生日攻击: 一个 40 比特长的消息摘要是很不安全的, 因为仅仅用 2^{20} 次随机 Hash 可至少以 1/2 的概率找到一个碰撞. 为了抵抗生日攻击, 通常建议消息摘要的长度至少应取为 128 比特, 此时生日攻击需要约 2^{64} 次 Hash. 安全的 Hash 标准的输出长度选为 160 比特是出于这种考虑.
- 一句话: 如果你在 n 个数中随机选数, 那么最多选 $\sqrt{n}$ 次就能以大概率选到相同的数
- BZOJ-3098

1. 计数方法
2. 数论
3. 组合数学
4. 概率论
   - 高考真题
   - 生日攻击
   - 随机转移状态机：马尔可夫链
5. 线性代数
6. 微积分

- 给出一个正整数 N，每次可以在不超过 N 的素数中随机选择一个 p，如果 p 是 N 的约数，则 N:=N/p，否则 N 不变
- 问平均情况下需要多少次随机选择，才能把 N 变成 1?



- $f(6) = 1 + f(6) \times 1/3 + f(3) \times 1/3 + f(2) \times 1/3$

- 图是 DAG, 可以直接算. 边界: f(1)=0
- 不是 DAG 怎么办? 高斯消元

- 就是一个二维数组呀
- 简介
- 矩阵的行列式: 把矩阵 A[n][n] 拿去消元, 消成上三角矩阵, 再把对角线上的数乘起来就是行列式的值 (注意不能随便把一行同 *C, 不然的话 det 也会跟着 *C)
- 比如

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 & -4 \\ -2 & 2 & 1 \\ -3 & 4 & -2 \end{bmatrix}$$

$$det(\boldsymbol{A}) = \begin{vmatrix} 1 & 2 & -4 \\ 0 & 6 & -7 \\ 0 & 10 & -14 \end{vmatrix} = \begin{vmatrix} 1 & 2 & -4 \\ 0 & 6 & -7 \\ 0 & 0 & -\frac{7}{3} \end{vmatrix} = -14$$

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots a_{2n}x_n &= b_2 \\
&\vdots \\
a_{n1}x_1 + a_{n2}x_2 + \cdots a_{nn}x_n &= b_n
\end{aligned}
$$

$$\downarrow$$

$$
\begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}
=
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

$$\downarrow$$

$$\boldsymbol{Ax} = \boldsymbol{b},\ \ \boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b}$$

- 消元大家小学就会了吧?
- 可以用于模方程组和异或方程组
- 自由基?

- 大家记一下结论就好了
- A[x][y]=-(xy 之间是否连边)
- A[x][x]=x 的点度
- 删掉 A 的任意一行一列之后，求行列式，det(**A**) 的值即为所求

- 丢链接跑
- 就是一大模版，背下来就好了

求零点

- 二分法太慢
- 牛顿迭代:

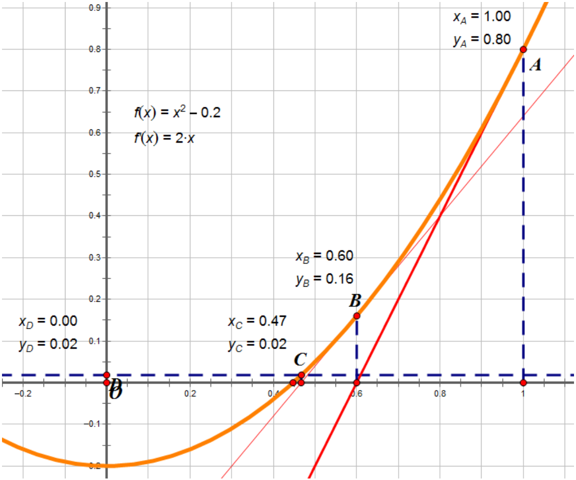
$$x = x_0 - \frac{f(x_0)}{f'(x_0)}$$

  收敛速度快, 不用上下界.
- 黑科技: 徒手开根号 ($\sqrt{C}$)
- 等价于求函数 $f(x) = x^2 - C$ 的零点

$$x = x_0 - \frac{x_0^2 - C}{2x_0} = \frac{1}{2}(x_0 + \frac{C}{x_0})$$

- 3 次就有 6 位小数的精度 (如果你一开始的值够准的话)

原理



$x_A = 1.00$
$y_A = 0.80$
A
$f(x) = x^2 - 0.2$
$f'(x) = 2\cdot x$
$x_B = 0.60$
$y_B = 0.16$
B
$x_D = 0.00$
$y_D = 0.02$
$x_C = 0.47$
$y_C = 0.02$
C
D
O

手算性能提升

- $e^x \sim 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$
- $\sin x \sim x - \frac{x^3}{3!} + \frac{x^5}{5!} - + \dots$
- $\cos x \sim 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - + \dots$
- $\tan x \sim x + \frac{x^3}{3} + \frac{2x^5}{15}$
- 以上结果均来源于麦克劳林展开

- 三分法，无需多言．只要单峰即可
- 求个导，可以转成二分法 (如果能求导的话)
- 求个偏导，就能算出多元函数的极值了
  FJOI 出过不要不服：题面 题解
- 条件极值？拉格朗日乘数法直接爆搞
  NOI 出过不要不服：题面 题解

自适应辛普森积分

- 对于二次及以下的函数，恒有

$$\int_l^r f(x)\,dx = \frac{r-l}{6}[f(l) + 4f(\frac{l+r}{2}) + f(r)]$$

- 其他奇奇怪怪的函数只要暴力递归，如果误差在一定范围内就认为已经求到了精确值
- 主要应用：各种面积并

格林公式

- 广告一定要点
- 主要应用：还是各种面积并