## Day1 AM 数论

###### P6.素数(Prime)

**性质：**有无穷多个素数

**素数密度：**

**数论函数：**定义域为N+，陪域为复数的函数称为数论函数。

**积性函数：**若有数论函数f(x)，对于所有互质的正整数对，均满足，则称f(x)为积性函数。

**完全积性函数：** 若有数论函数f(x)，对于所有正整数对，均满足，则称f(x)为积性函数。

**常见数论函数：**

l(x)：对于任意正整数x，函数值恒为1. ->

e(x)：对于任意正整数x，若x=1，则函数值为1，否则为0. ->

n(x)：（常函数）对于任意正整数x，函数值恒为x. –>

**以上为完全积性函数**

d(x)：对于正整数x，函数值为其正因子个数.

φ(x)：对于正整数x，函数值为小于等于n且与n互质的正整数的个数.

μ(x)：莫比乌斯函数，见后.

σx(n)：（除数函数）n的正因数的x次幂之和，即 。

**σ.ps：**σ0(n)：n的正因数的数目。

σ1(n)：n的正因数之和（包括自己）。

**以上为积性函数**

###### P8.费马小定理(Fermat's little theorem)

若p是素数，且a,p互质，则 。

###### P9.Miller-Rabin素数测试(Miller–Rabin Primality Test)

费马小定理的逆定理并不一定成立，但大多数情况下是成立的。

**ps：逆定理(Format测试)：**若存在0<a<p，使得 ，那么就说明p不是素数。

但是有些合数并不能找到这样的a，如561,1105,1729，这些合数被称为Carmichael数(强伪素数)，非常少，在10^8内的整数中仅有255个。

**End ps。**

于是我们得到了定理的直接应用，对于待验证的数p，不断取，验证是否等于1。

**定理二(二次探测定理)：**若(0<x<p)且p为素数，则

**证明：**若，则

因为p为质数，所以(x+1)与(x-1)不同时整除p

若，则；否则, 则。

**Miller-Rabin**

就是结合了费马小定理和定理二。

设，即将p-1表示成二进制下t后面再加k个0。

随机选取一个数a，计算，然后令a不断\*2，结合定理二判断：

若当前，但是\*2前，那么这个数就是合数(违背定理二)。

这样乘k次，最后的a就是,再判断a是否为1(费马小定理)：若不为1，是素数。

**正确性/性质：**

Carmichael数存在能证明它是合数的证据。

若n是一个奇合数,则n为合数的证据数目至少为。

经过t轮测试，误判的概率为。

###### P12.狄利克雷卷积(Dirichlet Product)

**定义：**设f(n),g(n)是两个数论函数，它们的Dirichlet乘积也是一个数论函数，其定义为：

简记为。函数f(n)与g(n)的Dirichlet卷积亦可记为：

**性质1：**两个积性函数的狄利克雷卷积仍是积性函数 ；反之，若g(n)与(f\*g)(n)都是积性函数，则f(n)亦为积性函数。

若g(n)为完全积性函数，且，则。即若  
  
则

**性质2：**满足交换律：

**性质3：**满足结合律：

**性质4：**满足分配率：

**证明(?)：**

即

**性质5：**对于所有数论函数f(n)，均有，故l(n)在狄利克雷卷积中有单位元的作用，简称l(n)为单位数论函数或称卷积单位元。

**常见卷积形式：**1.任何函数卷积单位元仍为它本身。

2. ->

3. ->

4. ->

###### P16.莫比乌斯函数(Möbius function)

**定义：**（定义域为N+）

**性质1：**μ(n)为积性函数

**性质2：**

**证明：**1.n=1时，显然

2.n≠1时，将n分解可以得到 。

μ值不为0的只有所有质因子次数都为1的因子，其中质因子个数为i的有个，即有

**二项式定理：**

那么令x=-1，y=1，代入

得证。

或是直接将μ看做容斥的系数。

**性质3：**对于任意正整数n，有

**证明：**

###### P17.莫比乌斯反演(Möbius Inversion Formula)

**公式：**

**证明：**

step1：即将 展开；

step2：因为step1中的d是n的所有因子，k是 的所有因子，即k也是n的所有因子，所以step2中可以更换枚举顺序，此时d就是 的所有因子；

step3：由 可得，当且仅当 ，即k=n时，有。

**形式2：**

证明同理。常用这种形式。

###### P21.欧拉函数(Euler'so/Euler's totient function)

**性质1：**φ(n)为积性函数

**性质2：**

**证明1：**设集合M={1,2,…,n-1,n}

尝试将集合中的数分类，每个数都能按照与n的最大公约数来划分

不妨设我们当前讨论M中与n最大公约数为d的数有多少个

设dx∈M,且gcd(dx,n)=d

则gcd(x,n/d)=1,且x属于集合M’={1,2,…,n/d}

这样x的所有可能个数显然就是φ(n/d)

当d跑遍n的所有因子时，n/d也跑遍n的所有因子，因为每个数与n的最大公约数是确定的，所以每个数分类时只会被分一次

所以，可得

**证明2：**设

首先，当n=1时，f(1)=1，性质显然成立

当n=p时(p为质数) ，显然成立

当n=p^k时，

**ps：**

**ps.证明：**一个数要不与n=互质，则不含质数p。而包含质数p的一共有个：1\*p, 2\*p, …, 。

**ps 2：**

**ps 2.证明：**

等比数列，公比为p，所以前n项和为

**End ps.**

对于一般形式n=

因为φ(n)为积性函数，根据莫比乌斯反演的充要性，得f(n)为积性函数。

则

**性质3：**1~n中与n互质的数的和为

**证明：**由引理：若，则（证明可用反证法）；则由于i，n-i总是成对出现，且和为n，则 .

(详见：<http://blog.csdn.net/Clove_unique/article/details/53152473> )

###### P27.离散对数 BSGS(Baby-Step-Giant-Step)

**问题：**给定a,b,p，求出一个最小的非负整数0<x<p，使得 .（这只考虑p为质数的情况下，且a,p互质）

**解：**令 ，，则

移项，得 ；

首先，从0~m枚举j，将得到的 存入map或Hash表；

然后，从1~m枚举i，计算，若map或Hash表中有一个值与其相等，此时得到的 一定是最小值。

**讨论：1.无解的情况？**

方程有解的充要条件是p为质数且a,p互质，即费马小定理的条件，见2.

**2.为什么m取即可？**

首先要证明：

即要证明

由费马小定理知当p为素数且a,p互质时，，推出p为质数且a,p互质这个条件，并证明结论 。

即我们得到，枚举x的话最大枚举到p即可，即，i,j的最大值也为m。

**3.为什么第一个枚举到的 一定是最小值？**

首先枚举j时算出来的值可能重复，那么我们在map或Hash表中就会覆盖旧的值，此时j是更大的。要使 最小即j要最大。

**4.为什么从0~m枚举j，而从1~m枚举i？**

i不能为0，否则 会出现负数的情况。

###### ps:扩展BSGS

**问题：**给定a,b,p，求出一个最小的非负整数0<x<p，使得 .（a,p无限制）

**解：**设 ，则

若 ，唯一可能的解为x=0，即如果B=1，方程有解。

若 且d=1，此时a,p互质，直接用BSGS求即可。

若 且d≠1，有

此时a与 仍有可能不互质，继续分解，直至

如果 ，则唯一可能解为 。

如果 ，首先暴力枚举 ，看是否为解。显然 。

对于 的情况，有

然后换元，令 , ,，得

此时a与p’互质，用BSGS解方程即可，原方程的解为 。

###### P28.杜教筛

**1.莫比乌斯函数前缀和：求**

我们有

step1：利用μ的性质，分出一个1，多算的就是 这部分了；

step2：两种写法等价，换下写法，来进行step3。

step3：换种写法后可以看出就是所有以i的≠i的因子为自变量的μ的和。

step4：转为计算2~n的所有因子d会对答案贡献多少次，即1~n中因子d会出现次。但是之前因子是不包括i的，这并没有考虑，全算了，所以d不从1开始，即减掉了计算多余的。

一共只会访问个状态，状态S(x)的转移复杂度是，转移总数为 。显然后半部分大于前半部分，可以忽略前半部分。用积分近似求得复杂度为。

如果可以将 的部分预处理出来，那么转移的复杂度就是 。

如果预处理复杂度为，那么k取 时，能将复杂度降至。

这种优化复杂度的思想很多时候都能用。

**ps：实现：**常数影响过大，可以用map记忆化搜索；不过注意到参数只会是n的约数，所以可以在n>k时返回一个sum[n/x]，可以省去一个log。数组范围大约 即可。

**2.欧拉函数前缀和**

用到 ，其余同理。

###### P35.扩展欧拉定理(广义欧拉定理，降幂大法)

若 ，则

<http://blog.csdn.net/guhaiteng/article/details/52670606>

<http://blog.csdn.net/synapse7/article/details/19610361>