* 代数数论阶段话说，我是不是在自己的[莫比乌斯反演](https://www.cnblogs.com/peng-ym/p/8647856.html)中挖了许多杜教筛的坑啊......
* 本文完整的总结介绍杜教筛，也算是将莫比乌斯反演中的坑全部填满吧！
* 真诚地希望来阅读这篇学习笔记的每一个人，仔仔细细的看完每一段。
* 我相信，只要认真的看完整篇文章并跟着一起思考的读者，一定能够有所收获！
* 如果您之前不会杜教筛，那么我希望这篇文章能够作为您学习杜教筛路上的有力援助，帮助您真正的了解与掌握杜教筛！
* 如果您之前早已熟知杜教筛或只有些模糊的印象，相信您一定也能有所收获！
* (PS：本文较长，请耐心阅读 ovo)

## **在OI中的意义**

* 其实，对于一般的数论题，线性筛已经非常的优秀了。
* 但是就是有那些duliuduliu出题人，硬是要把数据出到1e101e10之类的，就看你会不会杜教筛，min\_25筛，洲阁筛等各种神奇的筛法。
* 要是不会，那就要少十分左右！
* 所以，专门用杜教筛来推式子的题目很少，一般都是用杜教筛优化线性筛，弄到最后的那些分。
* 不过，杜教筛的思想对于推式子是很有帮助的。（它那种递归求解的形式，以及复杂度O(n23)O(n23) ）
* 因此，学会杜教筛也是一件挺好的事情！

## **前置技能**

* 杜教筛的前置技能挺多的......

### **各种函数**

#### **概念**

* 首先，我们需要知道有一个东西叫做**数论函数**
* 数论函数有很多种，但是我们身为**Oier**，并不需要知道它的具体的定义，具体的分类。
* 我们只需要知道，我们在**OI**中的数论中所用到的各种函数μ,φμ,φ等都是数论函数。(后面会将常见的都列举出来，当然不只这两种)。
* 当你了解**数论函数**后，你就需要知道有一类函数叫做**积性函数**。
* 还是同样的话语，我们平常所惯用的数论函数都是积性函数！
* 不过，对于积性函数的定义还是有必要了解一下。(毕竟有些函数看上去不常见，其实可能就是积性函数！)
* 积性函数定义：如果已知一个函数为数论函数，且f(1)=1f(1)=1，并且满足以下条件，若对于任意的两个互质的正整数p,qp,q都满足f(p⋅q)=f(p)⋅f(q)f(p⋅q)=f(p)⋅f(q)，那么则称这个函数为**积性函数**。
* 特殊的，如果当对于任意的正整数p,q p,q(即不一定互质)，也满足以上这个式子，则称这个函数为**完全积性函数**。
* 而我们的**杜教筛**，则是用来筛积性函数前缀和的神奇筛法！！！
* 说了这么多概念性的东西，不如来点实质性的！

#### **常见积性函数**

1. μ(n)μ(n)——莫比乌斯函数。关于这个函数，我在[莫比乌斯反演](https://www.cnblogs.com/peng-ym/p/8647856.html)中说的挺清楚的了(233)，(PS：不过我将会在下文中，从另一种角度介绍它的性质。也算是把坑给填完吧)
2. φ(n)φ(n)——欧拉函数。表示不大于n且与n互质的正整数个数，十分常见的数论函数。用数学式子表示即：φ(n)=∑ni=1[(n,i)=1]φ(n)=∑i=1n[(n,i)=1] (PS:(n,i)(n,i)表示gcd(n,i))
3. d(n)d(n)——约数个数。表示nn的约数的个数。用式子表示为：d(n)=∑d|n1d(n)=∑d|n1，也可以写作：d(n)=∑nd=1[d|n]d(n)=∑d=1n[d|n] （其实没什么太大区别啦！）
4. σ(n)σ(n)——约数和函数。 即n的各个约数之和。表示为：σ(n)=∑d|nd=∑nd=1[d|n]⋅d

(PS：接下来列举的是完全积性函数)  
(PS：代表字母可能会与他人的略有不同，似乎在数学中没有统一的字母)

1. ϵ(n)——元函数。似乎也有人把它叫作e(n)e(n)？其实无所谓啦~~我们只需要知道ϵ(n)=[n=1]ϵ(n)=[n=1]。(看到这个是不是有种莫名的熟悉感呢？到了下文中，就会发现这种熟悉感是从哪来的啦！)
2. I(n)——恒等函数。所谓恒等就是这个函数的值恒为11。
3. id(n)——单位函数。id(n)=n。

(当第一次看到这些完全积性函数的时候，是不是有人感觉这些完全积性函数毫无用处，都是一些简单的式子，只不过用符号表示了呢？在下一个前置技能——狄利克雷卷积中，你应该就会改变自己naive的想法啦~)

### **狄利克雷卷积 (**∗∗**)**

#### **基本知识**

* 听名字，似乎是一个很高深的东西。
* 其实，若是不理睬这个名字，只是把它当作一个新定义的符号，你应该就会发现，狄利克雷卷积也不是那样的难理解。
* 定义：两个数论函数f和g的卷积为(f∗g)(n)=∑d|nf(d)⋅g(n/d)。前面的括号代表将f卷g，后面的括号代表范围。(PS：后面的括号一般可以省略不写，默认为n)
* 很显然，狄利克雷卷积满足以下运算规律：

1. 交换律(f∗g=g∗f)；
2. 结合律((f∗g)∗h=f∗(g∗h))；
3. 分配律((f+g)∗h=f∗h+g∗h)；

* 在记忆方面，可以类比为乘法的运算法则，其实上面这几条运算规律是可以证明的！
* 举个例子，交换律。我们看狄利克雷卷积的式子，实质上就是n的每一个约数带入f中的值，乘上与之对应的约数在g中的值。
* 显然，当交换f和g时，仅仅时枚举约数的顺序发生了改变，而每一个约数对答案的贡献是不会有改变的。因此存在交换律！
* 在大致了解了狄利克雷卷积的运算法则后，我们就需要提到上面所说的积性函数啦！
* 首先，元函数 ϵ。所谓元函数，指的就是在狄利克雷卷积中充当单位元的作用，单位元即满足：f∗ϵ=f。不要小看这个元函数，当元函数配合上结合律时就可以用来证明一些结论啦~
* 除了元函数之外，我们最为常见的则是μ,φ之类的的函数，因此我们需要十分熟练它们与一些常见的完全积性函数的卷积，以及性质。

**(PS：特别要记住一点：积性函数有一个特别重要的性质，那就是（积性函数**∗∗**积性函数）仍然为积性函数！！！这个性质可以用来判断能否被杜教筛！)**

#### **莫比乌斯函数**μ

* μ。在[莫比乌斯反演](https://www.cnblogs.com/peng-ym/p/8647856.html)中，我们曾了解过一个与μ有关的性质：∑d|nμ(d)=[n=1]我们将这个性质表示成狄利克雷卷积的形式即：μ∗I=ϵ。这在狄利克雷卷积中是一个很常用的恒等式。当然，有了它，我们也能够证明出莫比乌斯反演啦！
* 开始填坑，证明莫比乌斯反演：  
  已知：

F(n)=∑d|nf(d)

* 用狄利克雷卷积的形式表示这个式子即：F=f∗IF=f∗I  
  利用狄利克雷卷积将F卷上μ，得到：

F∗μ=f∗I∗μ

* 由于狄利克雷卷积具有结合律与交换律，因此原式可化为：

→f∗(I∗μ)=f∗ϵ=f

* 即：f=F∗μ。代入后即可证明莫比乌斯反演：f(n)=∑d|nμ(d)⋅F(n/d)同理，自然也可以得到莫比乌斯反演的另一种形式：f(n)=∑n|dμ(d/n)⋅F(d)  
  (总算填完一个大坑......)

#### **欧拉函数**φ

* φ。欧拉函数有一个很著名的性质：∑d|nφ(d)=n。
* 与以上方法类似，我们将它表示成狄利克雷卷积的形式：φ∗I=id。
* 这时候，看到这个式子我们会有一个大胆的想法，既然在这个欧拉函数与莫比乌斯函数的式子中都有I，那么我们不如将这个式子的两边同时卷上一个μ。
* 于是，我就可以开始填第二个坑了——欧拉函数与莫比乌斯函数的关系。

φ∗I=id→φ∗I∗μ=id∗μ→φ∗ϵ=id∗μ

* 即：φ=id∗μ→φ(n)=∑d|nμ(d)⋅n/d
* 我们把这个式子的两边同时除以nn，则可以推出这个巧妙的式子：

φ(n)n=∑d|nμ(d)d

* （至此，我终于把莫比乌斯反演中的坑填完啦~~23333）  
  （有关杜教筛的前置技能也说的差不多啦，终于可以步入正题啦！）

## **步入正题——杜教筛**

* 说了这么久，终于可以开始讲杜教筛啦！（是不是有一种莫名的兴奋呢？）
* 首先，我们应该弄清楚一个问题：杜教筛到底是用来干什么的？
* 杜教筛是以低于线性的时间复杂度来计算积性函数的前缀和的神奇筛法！
* 即我们需要计算的式子为：∑ni=1f(i) (f(i)为积性函数)
* PS：接下来要讲解的是杜教筛的套路式，如果不懂为什么要这样做，也没有关系。只需要明白它是怎么推过来的就行了。实在看不懂就记个结论吧......
* 推式子时间到！
* 为了解决这个问题，我们构造两个积性函数h和g。使得h=f∗g
* 现在我们开始求∑ni=1h(i)。
* 记S(n)=∑ni=1f(i)。
* 

∑i=1nh(i)=∑i=1n∑d|ig(d)⋅f(id)→=∑d=1ng(d)⋅∑i=1⌊n/d⌋f(i)

→∑i=1nh(i)=∑d=1ng(d)⋅S(⌊nd⌋)

* 接着，我们将右边式子的第一项给提出来，可以得到：

∑i=1nh(i)=g(1)⋅S(n)+∑d=2ng(d)⋅S(⌊nd⌋)∑i=1nh(i)=g(1)⋅S(n)+∑d=2ng(d)⋅S(⌊nd⌋)

→g(1)S(n)=∑i=1nh(i)−∑d=2ng(d)⋅S(⌊nd⌋)→g(1)S(n)=∑i=1nh(i)−∑d=2ng(d)⋅S(⌊nd⌋)

* 其中的h(i)=(f∗g)(i)h(i)=(f∗g)(i);
* 这就是杜教筛的惯用套路式。经各种分析，只要当你的h(i)h(i)的前缀和很好求，能在较短的时间内求出，那么当我们对后面的式子进行整除分块时，求S(n)S(n)的复杂度为O(n23)O(n23)
* 当我们知道了这个套路式后，可能会思考，我们应该如何选择这个gg与hh呢？
* 对于这个疑问，我没有太好的回答。只能说，依靠平时对于狄利克雷卷积中的各种式子的熟悉，以及仔细观察式子的能力啦！（当然我下面也会介绍一种小方法啦~~OVO）
* 知道了这个套路式总要练练手吧！

### **应用**

(PS：以下例子中，假设线性筛均跑不过)

一：求S(n)=∑ni=1μ(i)S(n)=∑i=1nμ(i)；

* 根据那个套路式：g(1)S(n)=∑ni=1(f∗g)(i)−∑nd=2g(d)⋅S(⌊nd⌋)g(1)S(n)=∑i=1n(f∗g)(i)−∑d=2ng(d)⋅S(⌊nd⌋)，我们只需要找一个积性函数gg使得这个函数与μμ的卷积的前缀和容易求。如果你认真的看了上文，应该就可以很轻松的想到一个积性函数II。
* 我们知道μ∗I=ϵμ∗I=ϵ，很显然，单位元的前缀和非常好求，就是11，并且II十分方便整除分块。所以我们把这个积性函数带入上述式子中可以得到：

S(n)=1−∑d=2nS(⌊nd⌋)S(n)=1−∑d=2nS(⌊nd⌋)

* 因此，我们就学会了杜教筛莫比乌斯函数的前缀和啦！

二：求S(n)=∑ni=1φ(i)S(n)=∑i=1nφ(i)

* 与求莫比乌斯函数的思路类似。
* 我们在脑海中找到一个与欧拉函数有关的卷积式子：φ∗I=idφ∗I=id
* 我们可以发现，在筛欧拉函数前缀和所选择的积性函数gg同样也是II哟！代入得：

S(n)=∑i=1ni−∑d=2nS(⌊nd⌋)S(n)=∑i=1ni−∑d=2nS(⌊nd⌋)

* 前面那个式子可以利用等差数列求和公式O(1)O(1)的计算出结果，后面同样利用整除分块。  
  所以，我们又学会了如何筛欧拉函数的前缀和啦！

三：求S(n)=∑ni=1i⋅φ(i)S(n)=∑i=1ni⋅φ(i)

* 这个式子是不是无法一眼看出需要配什么积性函数了呢？
* 我们考虑狄利克雷卷积的形式：∑d|n(d⋅φ(d))⋅g(nd)∑d|n(d⋅φ(d))⋅g(nd)
* 我们看前面这个dd不太爽，考虑后面配出一个积性函数使得这个dd能够被约掉。因此，我们尝试将gg配成idid。这样就可以把dd给弄没！代入得：

∑d|n(d⋅φ(d))⋅nd=∑d|nn⋅φ(d)→=n∑d|nφ(d)=n2∑d|n(d⋅φ(d))⋅nd=∑d|nn⋅φ(d)→=n∑d|nφ(d)=n2

* 我们惊喜的发现，似乎配对了！！！  
  得：

S(n)=∑i=1ni2−∑d=2nd⋅S(⌊nd⌋)S(n)=∑i=1ni2−∑d=2nd⋅S(⌊nd⌋)

* 对于这个式子，我们前面可以利用平方和的公式O(1)O(1)算出结果，后面的式子利用等差数列求和公式进行整除分块。  
  因此，我们可以通过以上的思路求得这个看似无法筛的积性函数的前缀和！