线性筛 与 线性递推

Ⅰ. 目录

Ⅱ. 线性筛 – 素数

一. Eratosthenes 筛法：

最简单的筛法，代码极度简洁，时间复杂度：$O(n\cdot\log(\ln(n)))$

代码参考：http://paste.ubuntu.com/20117186/

二. Euler 筛法：

代码稍显复杂，但时间复杂度为 $O(n)$。对于某些暴力数据，只能使用该种筛法

时间复杂度证明：http://paste.ubuntu.com/20117581/[1]

代码参考：http://paste.ubuntu.com/20118999/

Ⅲ. 线性筛 – 莫比乌斯函数

一. 莫比乌斯函数的定义：https://zh.wikipedia.org/wiki/

二. 线性筛法：

如果我们使用“Euler 筛法”类似的筛法，不难发现[2]：

1. 我们可以筛出每一个质数
2. 对每一个能被 p^2 整除的合数，其进行唯一分解后，可以被他最小的质因子筛去
3. 对于 $\mu(x)\neq 0$ 的合数，其正负一定会被逐渐更新

时间复杂度证明：同“Euler 筛法”

代码参考：http://paste.ubuntu.com/20124475/

Ⅳ. 线性递推 – 欧拉函数

一. 欧拉函数的定义[3]：https://zh.wikipedia.org/wiki

二. 相关引理[4]：

1. $\varphi(p^k)=p^k-p^{k-1}$

   证明：在小于 p^k 的正整数中，p 的正整数倍有 p^{k-1} 个，而只有这些数不与 p^k 互质，得证。

2. 欧拉函数是积性函数

   证明：见《具体数学》第 111 页

三. 单个求解欧拉函数：

---

[1] 节选自何昊天的 blog

[2] 因为时间关系，这里的证明从略

[3] 不同的文献中对于其定义不尽相等，这里取 wiki 的定义为准

[4] 下文中的 p 在未说明的情况下均代表质数

1. 数学依据：

$$\varphi(m)=\prod_{p|\mathrm{m}}\varphi(p^k)=\prod_{p|m}p^k(1-\frac{1}{p})=(\prod_{p|m}p^k)\cdot(\prod_{p|m}(1-\frac{1}{p}))=m\cdot\prod_{p|m}(1-\frac{1}{p})$$

2. 代码实现：

因为此方法需要预处理出素数表，或者使用 mille-rubin 等素数判断方法，所以无论是时间复杂度或是编程复杂度均不如线性递推欧拉函数，故不提供此版本的程序

四. 线性递推欧拉函数：

仍然使用类似于“Euler 筛法”，我们分两种情况讨论

1. 当前枚举的素数 pri 与当前处理的数 i 互质

根据引理二得：$\varphi(i\cdot pri)=\varphi(i)\cdot\varphi(pri)$

2. 当前枚举的素数 pri 与当前处理的数 i 不互质

由枚举顺序得，$i=pri\cdot k$，则有： $\varphi(i\cdot pri)=\varphi(k\cdot pri^2)=\varphi(k)\cdot\varphi(pri^2)$

由引理一得：$\varphi(k)\cdot\varphi(pri^2)=\varphi(k)\cdot(pri^2-pri)$

化简得：$\varphi(k)\cdot(pri^2-pri)=\varphi(k)\cdot\varphi(pri)\cdot pri=\varphi(i)\cdot pri$

综上，$\varphi(i\cdot pri)=\varphi(i)\cdot pri$

于是，我们便可以使用类似于“Euler 筛法”的算法，线性递推欧拉函数了

时间复杂度证明：同“Euler 筛法”

代码参考：http://paste.ubuntu.com/20135730/

Ⅴ. Reference

一. 《具体数学》· 第四章

二. 何昊天的博客：http://techotaku.lofter.com/post/4856f0_634219b