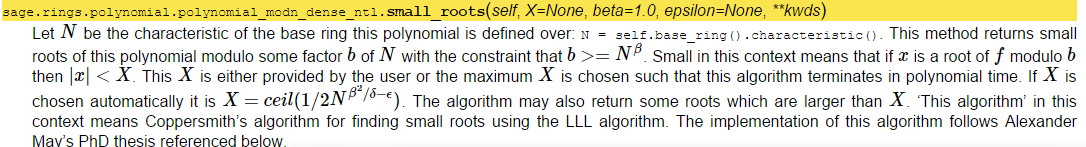
C:\Users\wy\AppData\Local\Temp\1505896188(1).png

这里的X：

、

ceil() === 向上取整

**Coppersmith定理攻击**

Coppersmith定理指出在一个e阶的mod n多项式f(x)中，如果有一个根小于n1en1e ，就可以运用一个O(log n)的算法求出这些根。

这个定理可以应用于RSA算法。如果e = 3并且在明文当中只有三分之二的比特是已知的，这种算法可以求出明文中所有的比特。

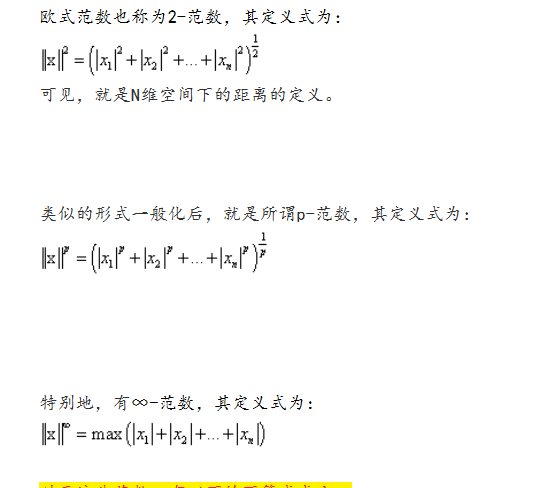
并未找到真题。

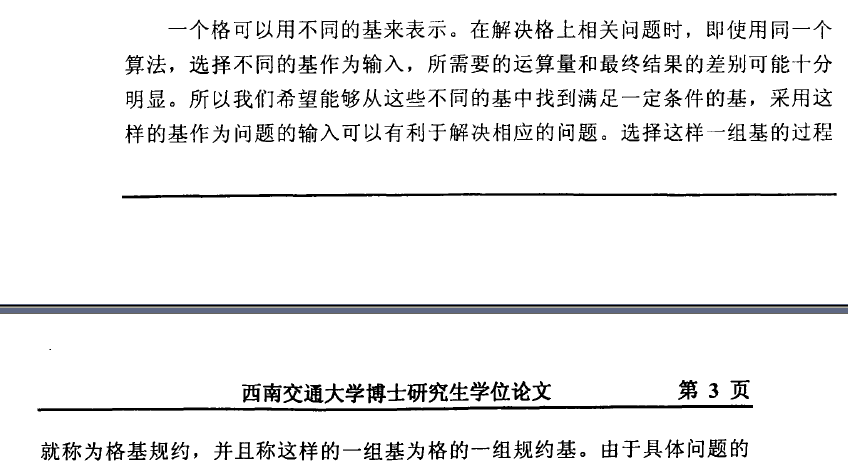
格基约化：

ceil

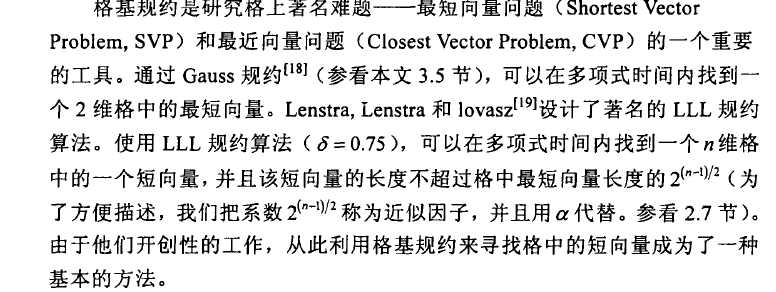
*C:\Users\wy\AppData\Local\Temp\1505932245(1).png*

<http://photo.blog.sina.com.cn/showpic.html#blogid=633a407d0100gkli&url=http://s6.sinaimg.cn/orignal/633a407d4798269aa5c15&690>

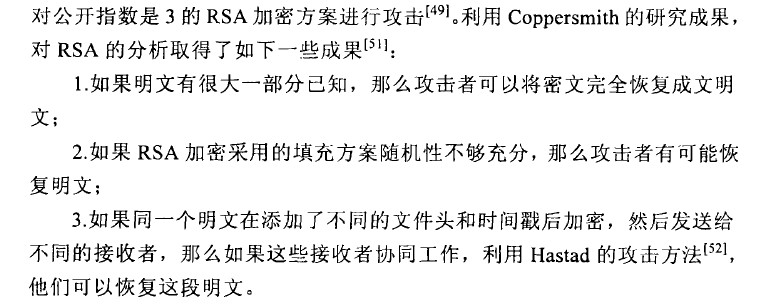
**

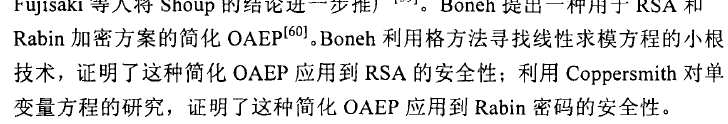


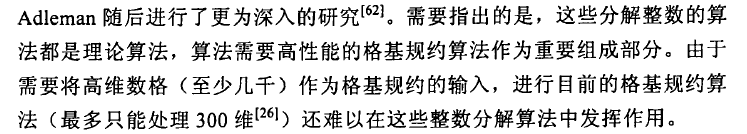
格基规约把基中包含格中极可能短的向量作为一个重要的指标。

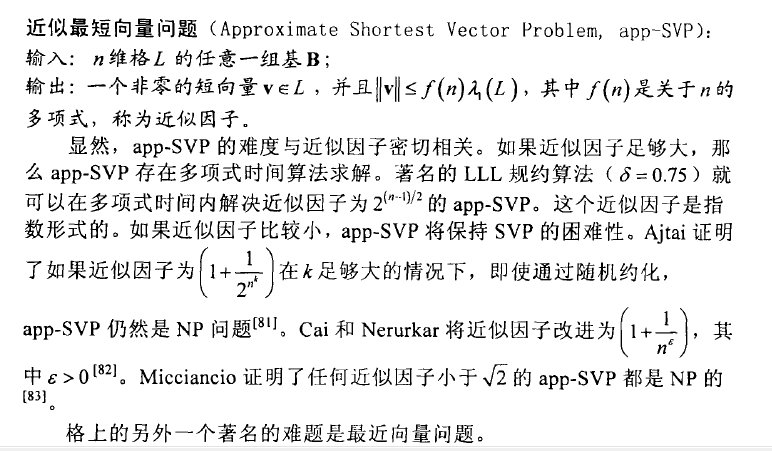


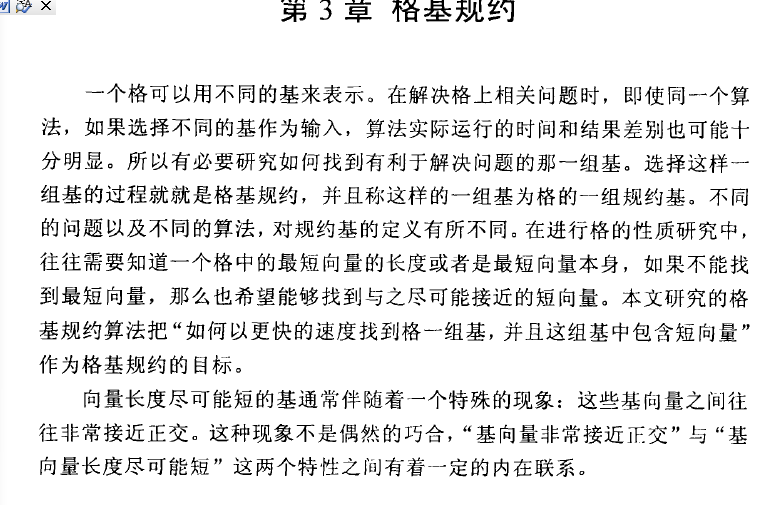
基格规约理论

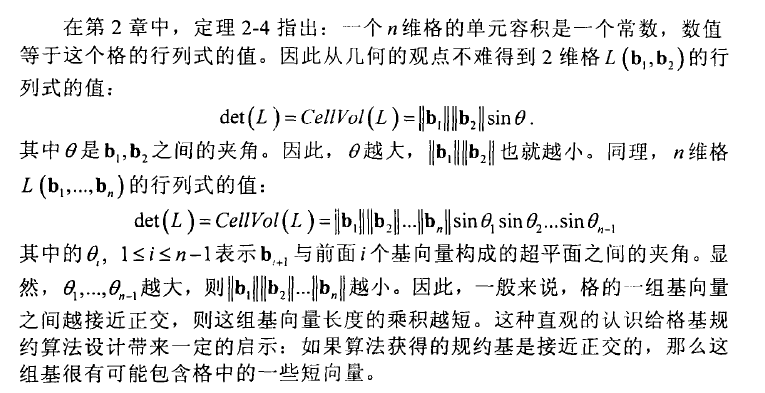










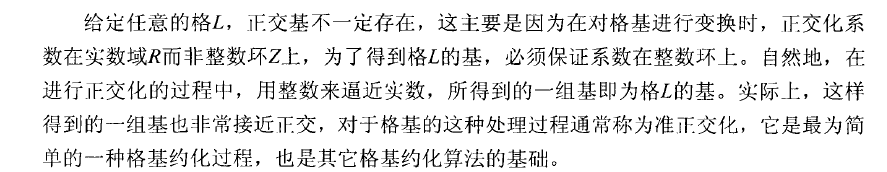


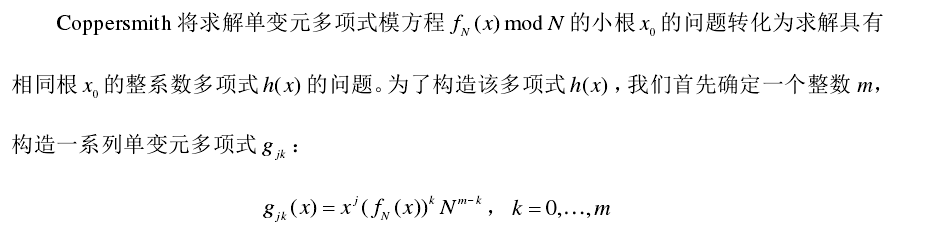
格是空间中离散点的集合。

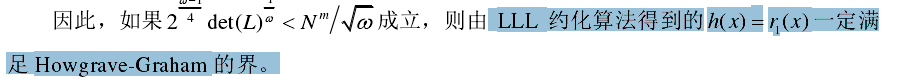
准正交化

**[多项式时间](https://baike.baidu.com/item/%E5%A4%9A%E9%A1%B9%E5%BC%8F%E6%97%B6%E9%97%B4" \t "_blank)（Polynomial time）**在计算复杂度理论中，指的是一个问题的[计算时间](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%97%B6%E9%97%B4" \t "_blank)*m*(*n*)不大于问题大小*n*的多项式倍数。任何抽象机器都拥有一复杂度类，此类包括可于此机器以多项式时间求解的问题。

例如：时间复杂度为O(nlog(n))、O(n^3)的算法都是[多项式时间](https://www.baidu.com/s?wd=%E5%A4%9A%E9%A1%B9%E5%BC%8F%E6%97%B6%E9%97%B4&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y3nWm3njIBmW6YujcvrADz0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWnYnHmznf" \t "_blank)算法，时间复杂度为O(n^log(n))、O(n!)、O(2^n)的算法是指时间算法。







C:\Users\wy\AppData\Local\Temp\1506439295(1).png

