31.1-10

设：

则：

同理：

故：

31.2-5





即满足上面式子的最小n为：

所以由Lame定理可知：EUCLID(a,b)至多执行次递归调用。因为该算法达到gcd(a,b)时终止，所以可以修改Lame定理的为，定理一样成立。同上证明，只是b变成了b/gcd(a,b)。所以该函数至多运行了次递归调用。

31.4-1



由： 



即：  为解

31.5-2

题意等价于：





、





31.7-2





由于d的范围限制，所以k=1或k=2。

这样就可以解出来： k=1或2

然而又知道：

以上两个式子联立p、q分别为：



由于只涉及到了加减乘除开方平方运算，所以计算可以控制在n的位数的多项式时间。

31.8-3

由题意：



非平凡表明x mod n不是1和n-1。假设命题不成立，则两个数中至少存在一个平凡约数（1或者n），则可以知道x-1与x+1中至少有一个被n整除。

如果是x-1，则 n|(x-1)，导出x mod n为1，矛盾！

如果是x+1，则n|(x+1)，导出x mod n为n-1，也矛盾！

所以假设不成立。即gcd(x-1,n)与gcd(x+1,n)都是n的非平凡约数。