实验报告

57119101 王晨阳

第一题

运用 Miller-Rabin 素数测试算法。

Miller-Rabin 素数测试算法:

引理 1（费马小定理）：若p为质数，且$(a,p)=1$，则$a^{(p-1)} \equiv 1(mod\ p)$。若存在$a<p$，且$a^{(p-1)} \not\equiv 1(modp)$，则$p$不是素数。

引理 2（有限域上的平方根定理）：若p为奇质数且$e \geq 1$，则$x^2 \equiv 1(modp^e)$仅有两个根$x=\pm 1$，称为平凡平方根。若模n存在 1 的非凡平方根，则n为合数。

对于一个大数n，可以先考虑$a^{(n-1)} \equiv 1(modn)$。对于$n-1$，一定可以拆分成2^s+d，即$a^{n-1}=a^{2^s \times d}$。可以从$x=a^d$开始，依次平方s次，每次平方的时候模上n，按照之前的平方根定理，如果模上n的结果为 1 的话，那么x一定是 1，或者是$n-1$，如果不满足则不是素数，$x=x^2$，再次循环。每次随机选一个在2到$n-1$的数字作为a，可以重复测试。

该算法为概率测试，有一定错误率，但可以证明 30 以内所有素数全部通过可以直接判定学号范围内的数全部无判断错误。

为了进一步加快运算，采用快速幂算法进行幂运算。

学号:
57119101
运行结果:
第 1 大的素数为 10191161
第 2 大的素数为 10191133

第二题

运用欧几里得算法求出 gcd 和 lcm。

学号:
57119101
运行结果:
最大公约数为 1
最小公倍数为 582110754133675