# 第4次编程练习报告

姓名：李潇逸 学号：2111454 班级：信安法班

**编程练习1——求解最小原根并基于最小原根构造指数表**

* **源码部分：**

**#include<iostream>**

**#include<math.h>**

**#include<cmath>**

**int d2b(int n,int num,char \*a) //将十进制数n变为二进制存入char数组a中,返回二进制数的长度num**

**{**

**while(n != 0){**

**if(n % 2 == 0){**

**n /= 2;**

**a[num] = '0';**

**num++;**

**}**

**else{**

**n /= 2;**

**a[num] = '1';**

**num++;**

**}**

**}**

**return num;**

**}**

**bool su(int a) //判断a是否为素数,若是返回true,否则返回false**

**{**

**double aa;**

**int b;**

**bool flag;**

**aa = double(a);**

**b = int(sqrt(aa)) + 1;**

**for(int i = 2;i <= b;i++){**

**if(a == 2){**

**flag = true;**

**break;**

**}**

**else if(a != 2 && a % i == 0){**

**flag = false;**

**break;**

**}**

**else{**

**flag = true;**

**}**

**}**

**return flag;**

**}**

**int fast\_power(char \* binarry,int num,int a,int m) //快速幂算法,输入二进制数组binarry、数组长度、底数a、模数m**

**{**

**long long ans = 1;**

**for(int i = num - 1;i >= 0;i--){**

**if(binarry[i] == '1'){**

**ans = ans \* ans \* a;**

**ans = ans % m;**

**}**

**else{**

**ans = ans \* ans;**

**ans = ans % m;**

**}**

**}**

**return ans;**

**}**

**int gcd(int a,int b) //求a,b的最大公约数,其中a<b**

**{**

**int k = 0;**

**for(int i = 1;i <= a;i++){**

**if(a % i == 0 && b % i == 0){**

**k = i;**

**}**

**}**

**return k;**

**}**

**int min\_root(int n)**

**{**

**//分解质因数**

**int temp = n-1;**

**int \* ans = new int[n]; //若为n-1的质因数赋值为1否则为0**

**int num = 0; //质因数的个数**

**while(temp != 1){**

**double t = temp;**

**if(su(t)){**

**if(ans[temp] != 1){**

**num++;**

**ans[temp] = 1;**

**}**

**break;**

**}**

**else{**

**for(int i = 2;i <= temp/2;i++){**

**if(su(double(i)) && temp % i == 0){**

**if(ans[i] != 1){**

**num++;**

**ans[i] = 1;**

**}**

**temp /= i;**

**}**

**}**

**}**

**}**

**char \*\* t = new char\*[num]; //存储n除以各个质因数的二进制形式**

**//初始化**

**for(int i = 0;i < num;i++){**

**t[i] = new char[100];**

**}**

**int \* num1 = new int[num]; //存储n处以各个质因数二进制的长度**

**int z = num;**

**for(int i = 1;i <= n-1;i++){**

**if(ans[i] == 1){ //当第i个位置是质因数,将n/i转化为二进制**

**num1[z-1]=d2b(n/i,0,t[z-1]);**

**z--;**

**}**

**}**

**int minroot = 0;**

**for(int i = 2;i < n;i++){**

**bool flag;**

**for(int j = 0;j < num;j++){**

**if(fast\_power(t[j],num1[j],i,n) == 1){**

**flag = false;**

**break;**

**}**

**else{**

**flag = true;**

**}**

**}**

**if(flag == true){**

**minroot = i;**

**break;**

**}**

**}**

**return minroot;**

**}**

**int main()**

**{**

**int n;**

**std::cout<<"Please input n(n>0):";**

**std::cin>>n;**

**int minroot = min\_root(n);**

**std::cout<<"The min privitive root of "<<n<<": g="<<minroot<<std::endl;**

**std::cout<<"The ind\_table of "<<n<<" based on g="<<minroot<<" is:"<<std::endl;**

**int ten = n / 10;**

**int \* ans = new int[n];**

**for(int i = 0;i <= n;i++){**

**char binarry[100];**

**int num = d2b(i,0,binarry);**

**if(fast\_power(binarry,num,minroot,n) == 1){**

**ans[fast\_power(binarry,num,minroot,n)] = n;**

**}**

**else if(fast\_power(binarry,num,minroot,n) == minroot){**

**ans[fast\_power(binarry,num,minroot,n)] = 1;**

**}**

**else{**

**ans[fast\_power(binarry,num,minroot,n)] = i;**

**}**

**}**

**for(int i = 0;i <= ten+1;i++){**

**if(i == 0){**

**for(int j = 0;j < 11;j++){**

**if(j == 0){**

**printf("%8s"," ");**

**}**

**else{**

**printf("%8d",j-1);**

**}**

**}**

**}**

**else{**

**for(int j = 0;j < 11;j++){**

**if(j == 0){**

**printf("%8d",i-1);**

**}**

**else if((i-1)\*10+j-1<1 || (i-1)\*10+j-1>n-1){**

**printf("%8s","-");**

**}**

**else{**

**if(ans[(i-1)\*10+j-1] == n){**

**printf("%8d",0);**

**}**

**else if(ans[(i-1)\*10+j-1] == 0){**

**printf("%8s","-");**

**}**

**else{**

**printf("%8d",ans[(i-1)\*10+j-1]);**

**}**

**}**

**}**

**}**

**std::cout<<std::endl;**

**}**

**}**

* **说明部分：**

构建d2b函数。目的是将输入的十进制数字转化为二进制的字符串，同时返回该二进制字符串的长度。

构建su函数。目的是判断输入的数字是否为素数，若为素数则返回true，否则返回false。

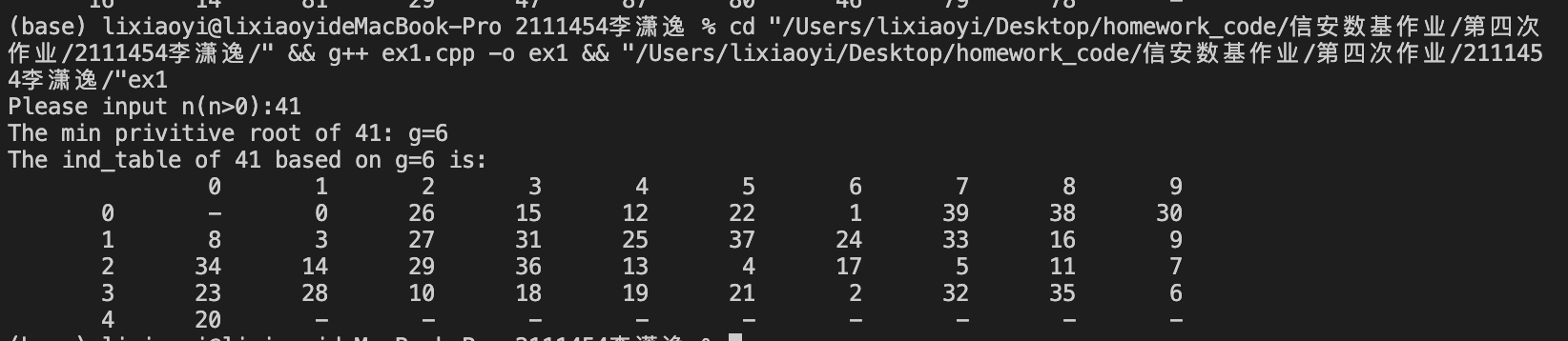
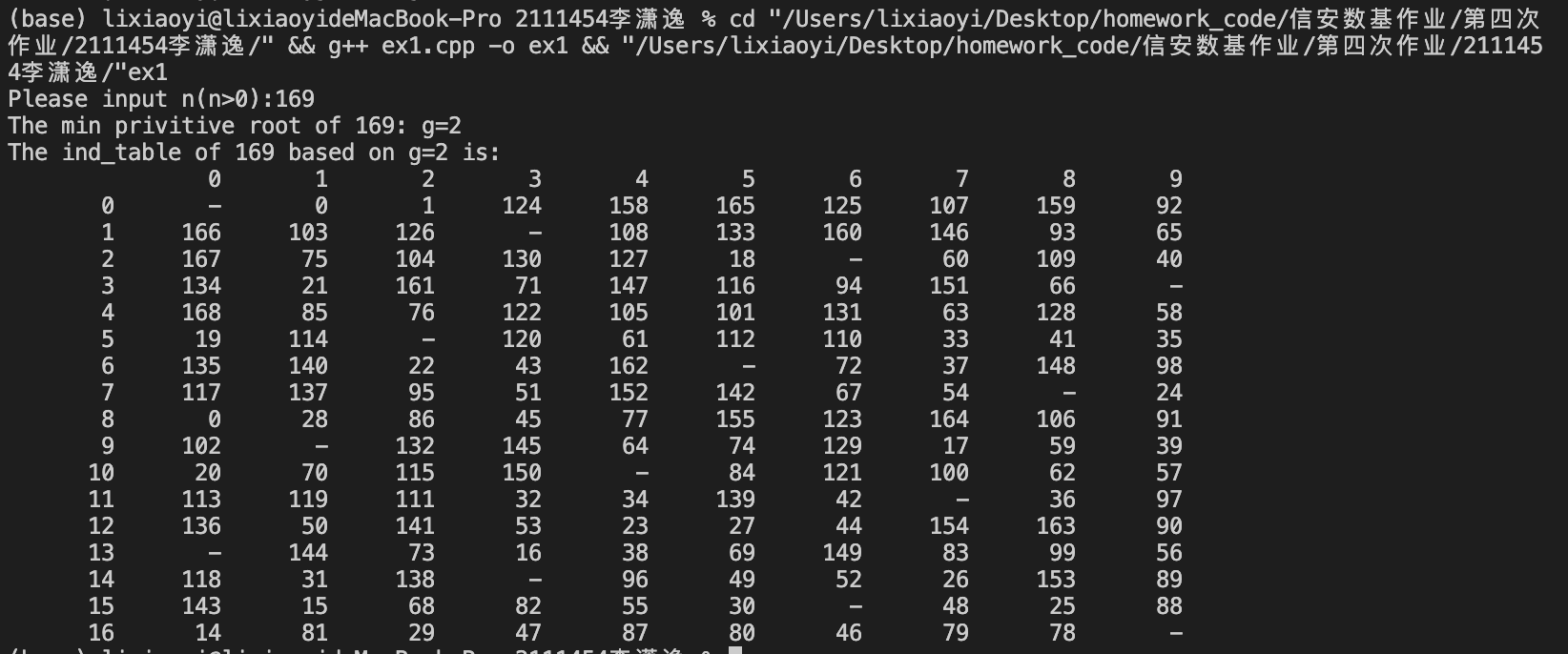
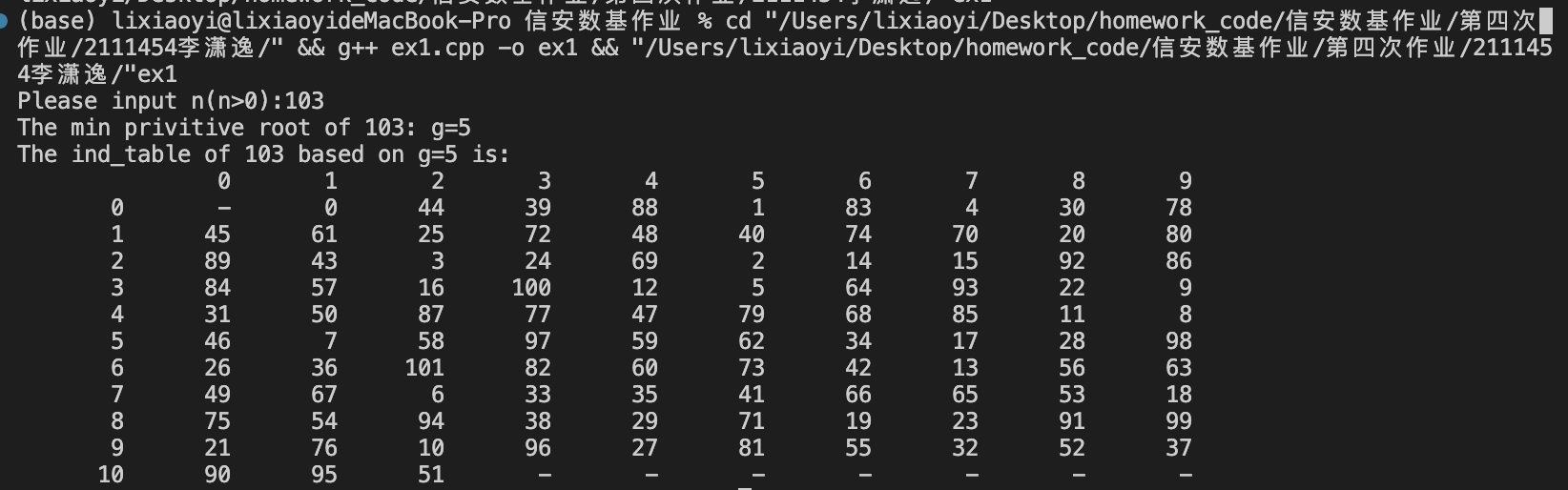
构建fast\_power函数。目的是通过传入的二进制字符串、字符串长度、底数和模数进行快速幂算法，快速输出高次幂的同余数。

构建gcd函数。目的是返回输入的最大公约数。

构建min\_root函数。目的是返回输入数字的最小元根。

主函数部分进行基础的输入即可。

* **运行示例：**//截图



**其他：**

无