# 第2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——平方—乘算法**

* **源码部分：**

#include<iostream>

int d2b(int n,int num,char \*a)

{

while(n != 0){

if(n % 2 == 0){

n /= 2;

a[num] = '0';

num++;

}

else{

n /= 2;

a[num] = '1';

num++;

}

}

return num;

}

int main()

{

int a;

int n;

int m;

int num;

long long ans = 1;

char binarry[100];

std::cout<<"Calculate a^n(mod m)"<<std::endl;

std::cout<<"Please input:"<<std::endl;

std::cout<<" a=";

std::cin>>a;

std::cout<<" n=";

std::cin>>n;

std::cout<<" m=";

std::cin>>m;

num = d2b(n,0,binarry);

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;

}

}

std::cout<<a<<"^"<<n<<"(mod"<<m<<")="<<ans;

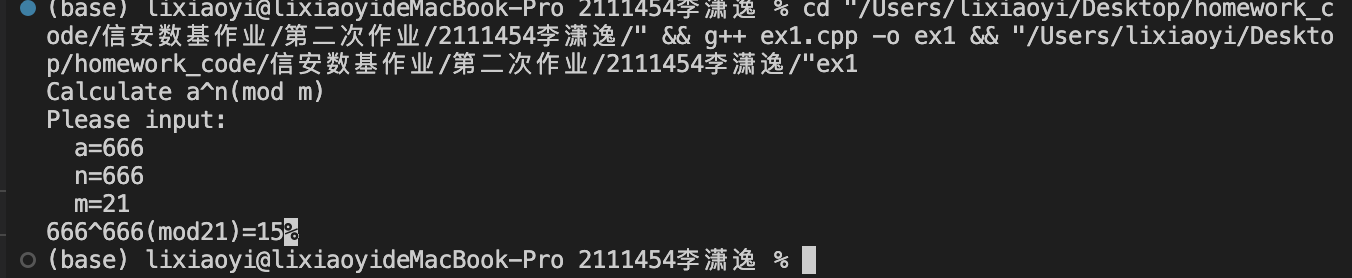
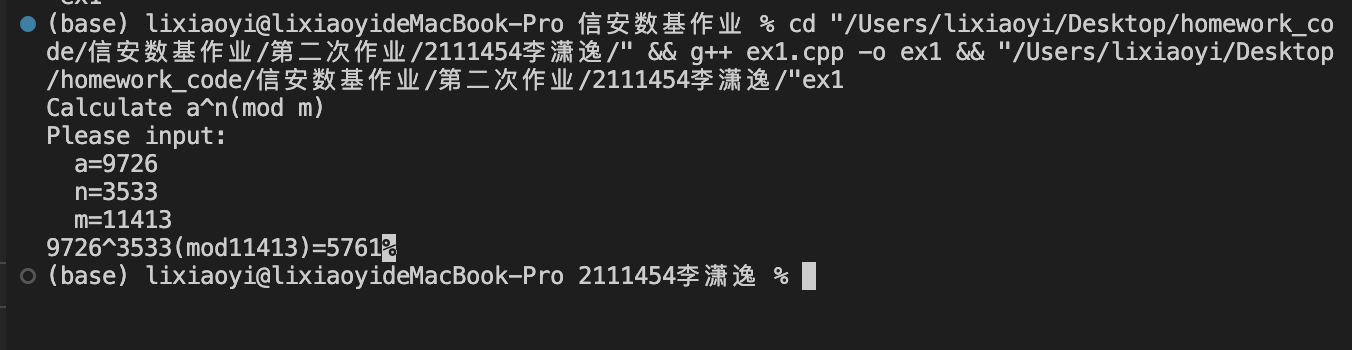
}

* **说明部分：**

构建d2b函数。该函数的作用为将输入的十进制数字转化为二进制数。

书写main函数。依次输入底数a，指数n，模数m；使用d2b函数将指数n转化为ASCII码表示的二进制数；设置一个储存结果的ans，并赋值为1。之后进行一次循环，从高位到低位遍历整个二进制，当遇到0时，ans平方后对m取模；当遇到1时，ans平方后乘a再对m取模，最后输出结果即可。

* **运行示例：**//截图



**其他：**

无

##### **编程练习2——扩展欧几里得算法**

* **源码部分：**

#include<iostream>

int gcd(int a,int b){

int k = 0;

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

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

k = i;

}

}

return k;

}

int lcm(int a,int b,int k){

int p = a / k;

int q = b / k;

return p \* q \* k;

}

void sn(int s1,int s2,int q,int r1,int r2,int num){

if(r2 == 0){

std::cout<<s2<<std::endl;

}

else{

sn(s2,s1-s2\*q,r1/r2,r2,r1%r2,num++);

}

}

void tn(int t1,int t2,int q,int r1,int r2,int num){

if(r2 == 0){

std::cout<<t2<<std::endl;

}

else{

tn(t2,t1-t2\*q,r1/r2,r2,r1%r2,num++);

}

}

int main()

{

int a;

int b;

std::cout<<"a=";

std::cin>>a;

std::cout<<"b=";

std::cin>>b;

if(a < b){

int k = gcd(a,b);

std::cout<<"gcd(a,b)="<<k<<std::endl;

std::cout<<"lcm(a,b)="<<lcm(a,b,k)<<std::endl;

std::cout<<"a^(-1)=";

tn(0,1,0,b,a,1);

std::cout<<"b^(-1)=";

sn(1,0,0,b,a,1);

}

if(a >= b){

int k = gcd(b,a);

std::cout<<"gcd(a,b)="<<k<<std::endl;

std::cout<<"lcm(a,b)="<<lcm(b,a,k)<<std::endl;

std::cout<<"a^(-1)=";

sn(1,0,0,b,a,1);

std::cout<<"b^(-1)=";

tn(0,1,0,b,a,1);

}

}

* **说明部分：**

构建sn和tn函数。两函数的作用为使用递归方法分别计算扩展欧几里得算法中的si和ti。下次传入的参数依据扩展欧几里得算法确定，直到r2=0停止。

书写main函数。依次调用所需函数即可。

* **运行示例：**//截图



* **其他：无**