Міністерство освіти і науки України

Сумський державний університет

Кафедра

Прикладної математики та моделювання складних систем

Звіт з лабораторної роботи № 3

Дисципліна

Криптографія

Студентка: Пороскун Олена Олегівна

Викладач: Козлова Ірина Іванівна

Суми, Сумська область

2021

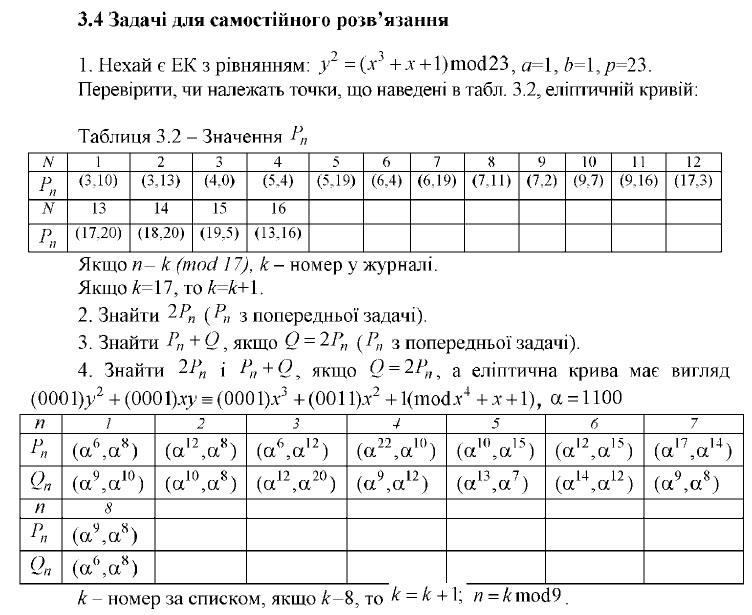
Лабораторна робота №3

**Тема**: Криптографя на еліптичних кривих

**Мета**: навчитися перевіряти належність точок еліптичній кривій, складати точки еліптичної кривої, знаходити елементи поля GF(p).

***Зміст задачі:***

1. Нехай є ЕК з рівняння: Перевірити, чи належать точки, що наведені в табл. 3.2, еліптичній кривій.



***Програмний код(C++):***

#include <iostream>

#include <math.h>

using namespace std;

int main() {

setlocale (LC\_CTYPE, "ukr");

int Pn[2];

cout << "Введiть значення Pn: ";

cin >> Pn[0] >> Pn[1];

cout << "Значення Pn = (" << Pn[0] << ", " << Pn[1] << ")"<< endl;

int x = Pn[0], y = Pn[1];

//cout << "Значення Pn: x = " << x << ", y = " << y << endl;

int a = 1, b = 1, p = 23;

int f1, f2;

f1 = pow(y, 2);

f2 = (pow(x,3) + x + 1);

f2 = f2 % p;

while (f2 < 0){

f2 = f2 + p;

}

// y^2 = (x^3 + x + 1) mod p - рiвняння елiптичної кривої

cout << "Пiдставивши значення Pn у рiвняння елiптичної кривої, маємо:" << endl;

cout << f1 << " = " << f2 << endl;

if (f1 == f2){

cout << "Отже, точка Pn = (" << x << ", " << y << ") належить елiптичнiй кривiй.";

}

else{

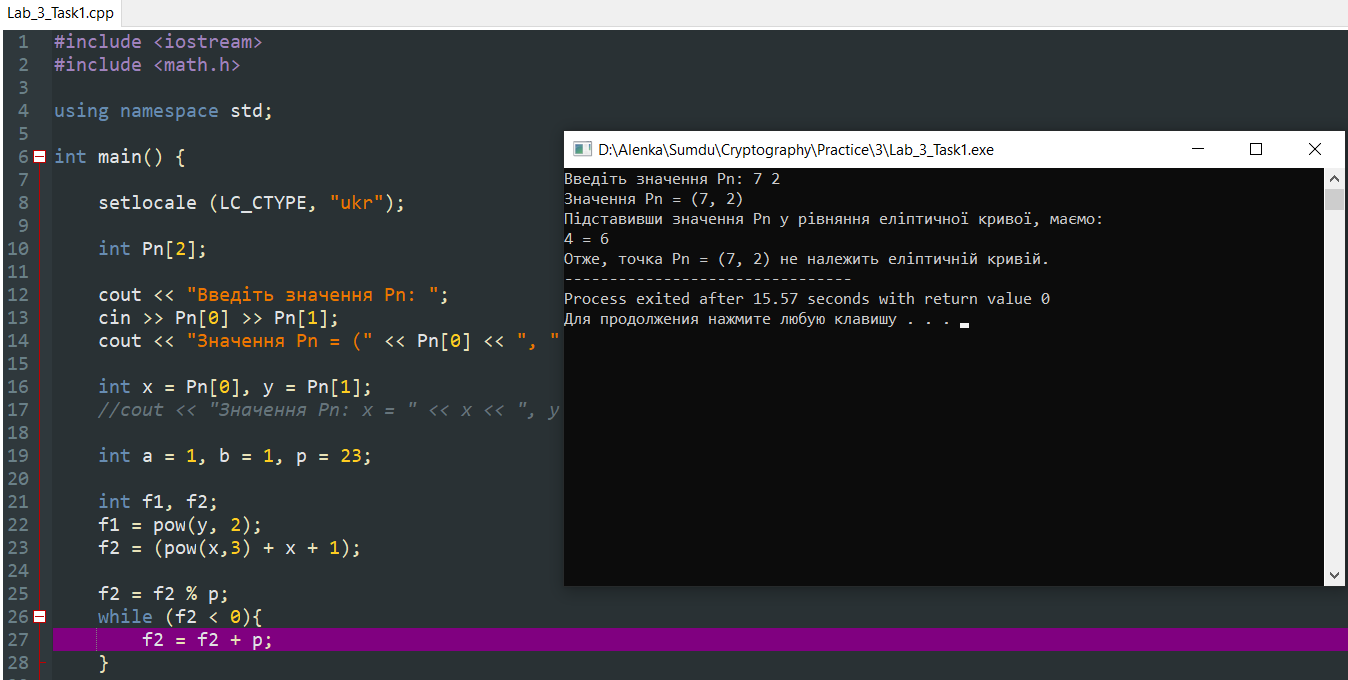
cout << "Отже, точка Pn = (" << x << ", " << y << ") не належить елiптичнiй кривiй.";

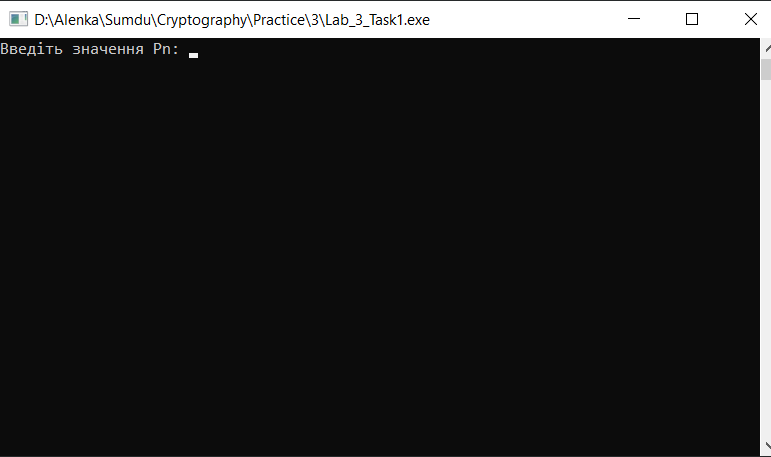
}

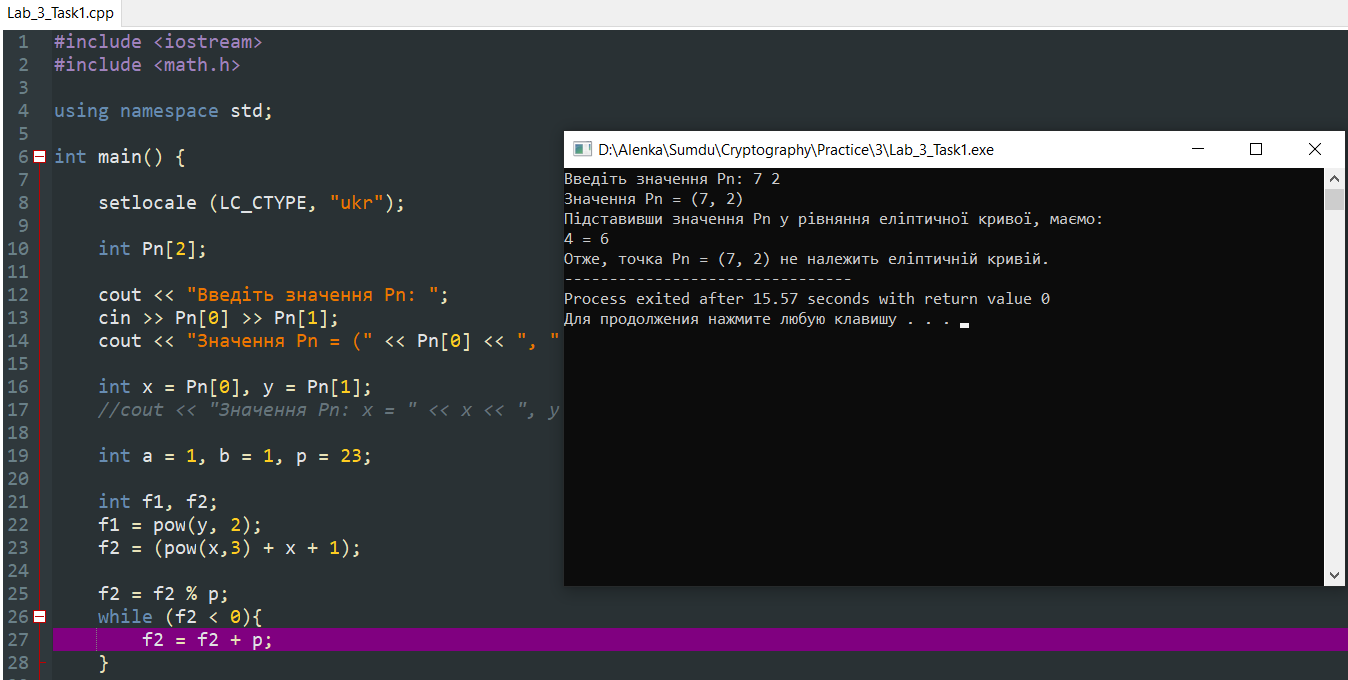
return 0;

}

***Прінт-скрін виконання програми:***

******

******

******

2. Знайти (з попередньої задачі).

***Програмний код(C++):***

#include <iostream>

#include <math.h>

using namespace std;

int main() {

setlocale (LC\_CTYPE, "ukr");

int Pn[2];

cout << "Введiть значення Pn: ";

cin >> Pn[0] >> Pn[1];

cout << "Значення Pn = (" << Pn[0] << ", " << Pn[1] << ")"<< endl;

int x = Pn[0], y = Pn[1];

//cout << "Значення Pn: x = " << x << ", y = " << y << endl;

int a = 1, b = 1, p = 23;

int lambda, x2, y2;

// x1 = x2, y1 = y2, 2Pn = Pn + Pn = (x, y) + (x, y) = 2(x, y)

//lambda = ((y2 - y1) / (x2 - x1)) % p;

lambda = 0;

// x2 = (lambda^2 - 2\*x)mod p або x3 = (lambda^2 - x1 - x2) mod p

x2 = (pow(lambda, 2) - 2\*x);

x2 = x2 % p;

while (x2 < 0){

x2 = x2 + p;

}

//y2 = (lambda\*(x - x2) - y) mod p або y3 = (lambda\*(x1 - x3) - y1) mod p

y2 = (lambda\*(x - x2) - y) % p;

while (y2 < 0){

y2 = y2 + p;

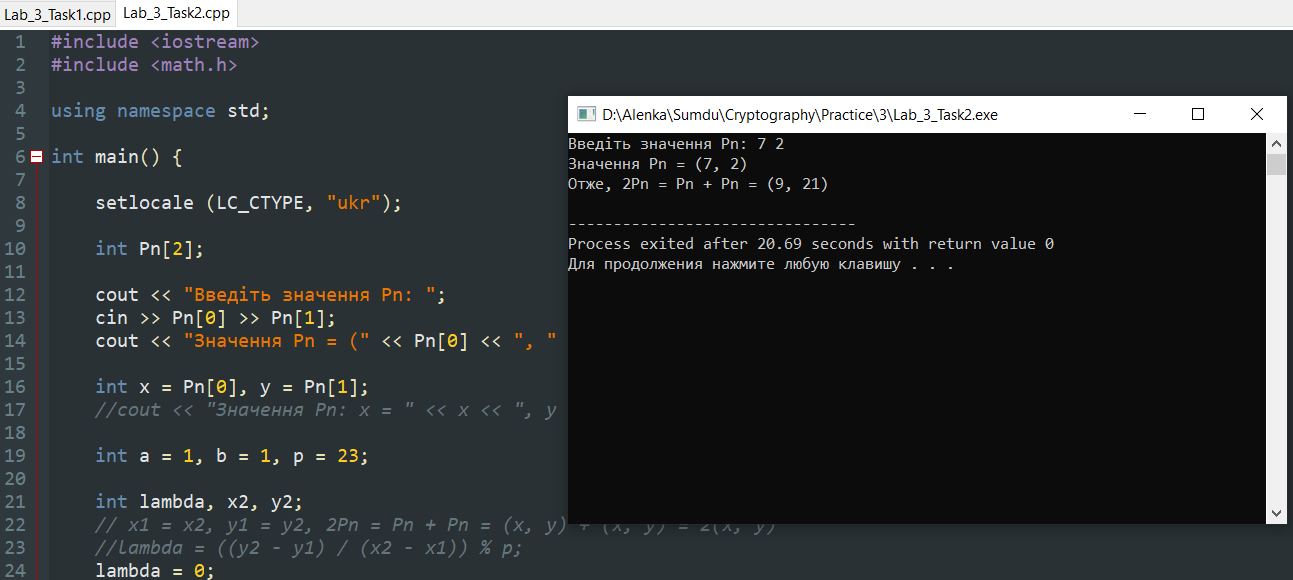
}

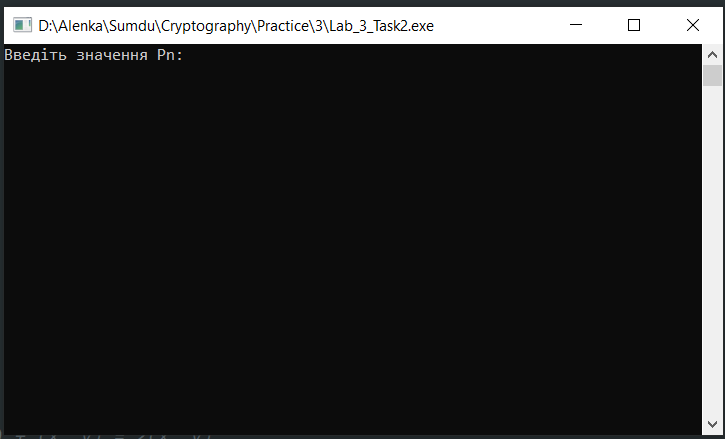
cout << "Отже, 2Pn = Pn + Pn = (" << x2 << ", " << y2<< ")"<< endl;

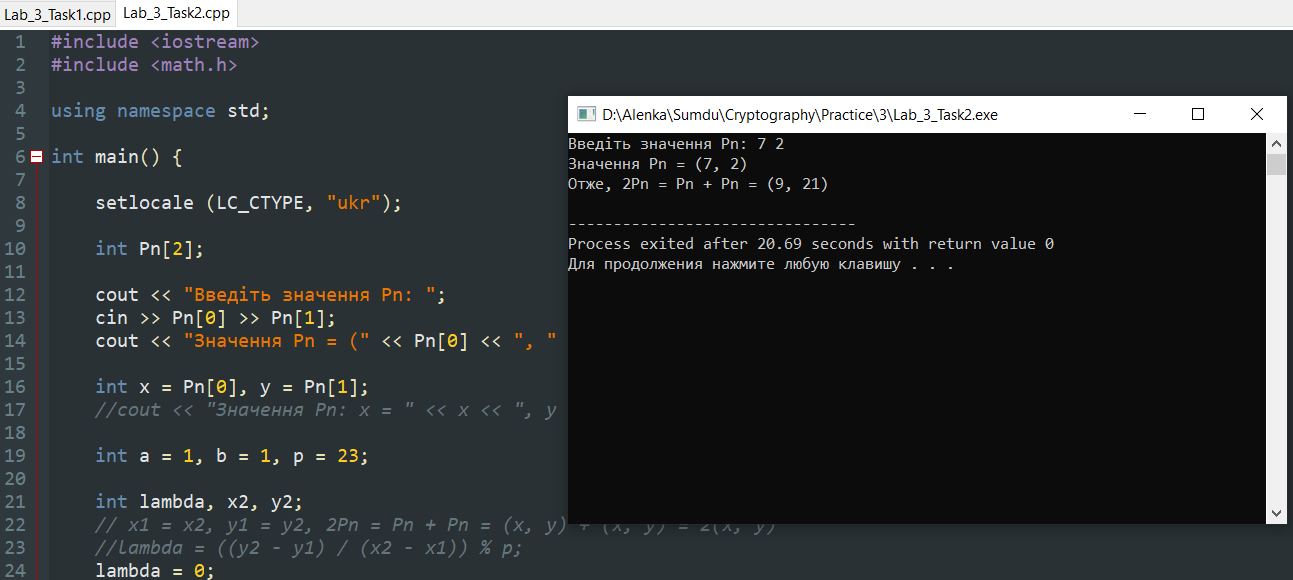
return 0;

}

***Прінт-скрін виконання програми:***

******

******

******

3. Знайтиз попередньої задачі).

***Програмний код(C++):***

#include <iostream>

#include <math.h>

using namespace std;

// перетворення вiд'ємної остачi

int absRemain(int rem, int d){

while(rem < 0){

rem = rem + d;

}

return rem;

}

int main() {

setlocale (LC\_CTYPE, "ukr");

int Pn[2];

cout << "Введiть значення Pn: ";

cin >> Pn[0] >> Pn[1];

cout << "Значення Pn = (" << Pn[0] << ", " << Pn[1] << ")"<< endl;

int x1 = Pn[0], y1 = Pn[1];

int a = 1, b = 1, p = 23;

int lambda1, x2, y2;

// x1 = x2 = x, y1 = y2 = y, 2Pn = Pn + Pn = (x, y) + (x, y) = 2(x, y)

//lambda = ((y2 - y1) / (x2 - x1)) % p;

lambda1 = 0;

// x2 = (lambda^2 - 2\*x)mod p або x3 = (lambda^2 - x1 - x2) mod p

x2 = (pow(lambda1, 2) - 2\*x1);

x2 = x2 % p;

x2 = absRemain(x2, p);

//y2 = (lambda\*(x - x2) - y) mod p або y3 = (lambda\*(x1 - x3) - y1) mod p

y2 = (lambda1\*(x1 - x2) - y1) % p;

y2 = absRemain(y2, p);

cout << "Q = 2Pn = Pn + Pn = (" << x2 << ", " << y2 << ")"<< endl << endl;

// Pn + Q = (x3, y3)

// lambda = ((y2 - y1) / (x2 - x1)) % p;

//cout << "x1 = " << x1 << ", y1 = " << y1 << endl;

//cout << "x2 = " << x2 << ", y2 = " << y2 << endl;

int lambda2, x3, y3;

lambda2 = ((y2 - y1) / (x2 - x1)); // % p;

//cout << "lambda2 = " << lambda2 << endl

int rem = ((y2 - y1) % (x2 - x1));

//cout << "rem = " << rem << endl;

int Z = 0;

if (rem != 0) {

cout << "Знаходимо в полi G(" << p << ") обернений елемент Z, розв'язавши порiвняння:" << endl;

cout << abs(x2 - x1) << " \* Z" << " = 1 mod " << p << endl;

int key = (abs(x2 - x1) \* Z);

key = key % p;

while (key != 1) {

Z++;

key = (abs((x2 - x1)) \* Z) % p;

}

cout << "Це порiвняння має розв'язок при Z = " << Z << ", тому " << endl;

lambda2 = ( abs(y2 - y1) \* Z ) % p;

}

else {

lambda2 = lambda2 % p;

}

lambda2 = absRemain(lambda2, p);

cout << "lambda = " << lambda2 << endl << endl;

x3 = (pow(lambda2, 2) - x1 - x2);

x3 = x3 % p;

x3 = absRemain(x3, p);

y3 = (lambda2\*(x1 - x3) - y1) % p;

y3 = absRemain(y3, p);

cout << "x3 = " << x3 << endl;

cout << "y3 = " << y3 << endl << endl;

cout << "Отже, Pn + Q = Pn + 2Pn = (" ;

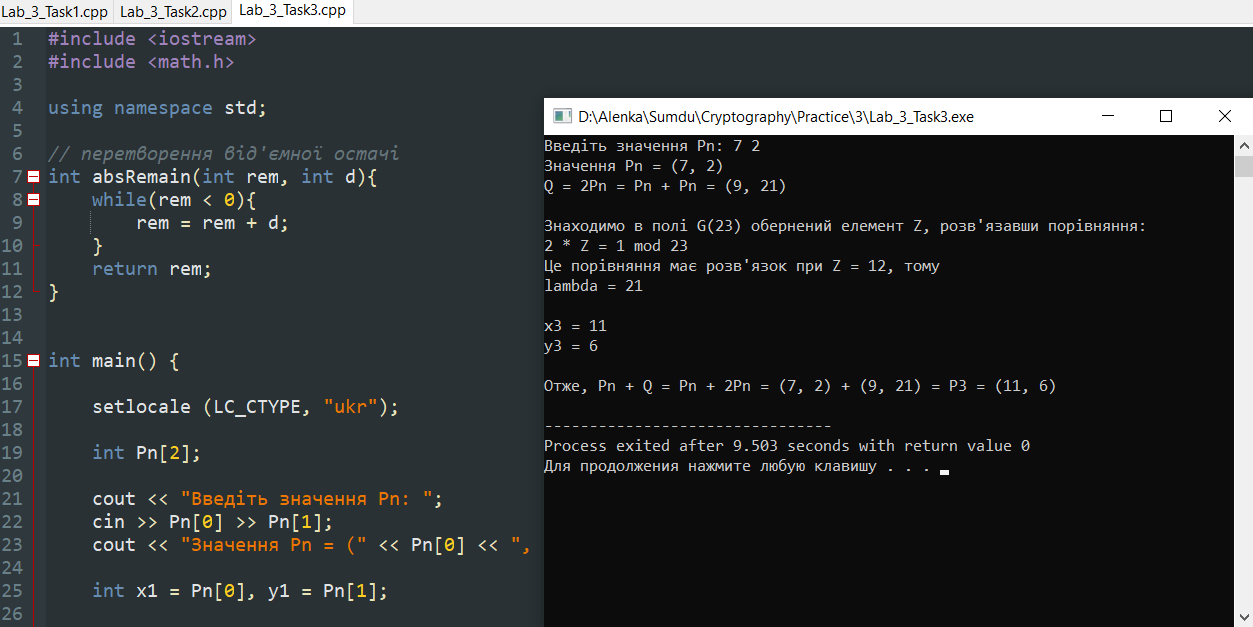
cout << x1 << ", " << y1 << ") + (" << x2 << ", " << y2 << ") = ";

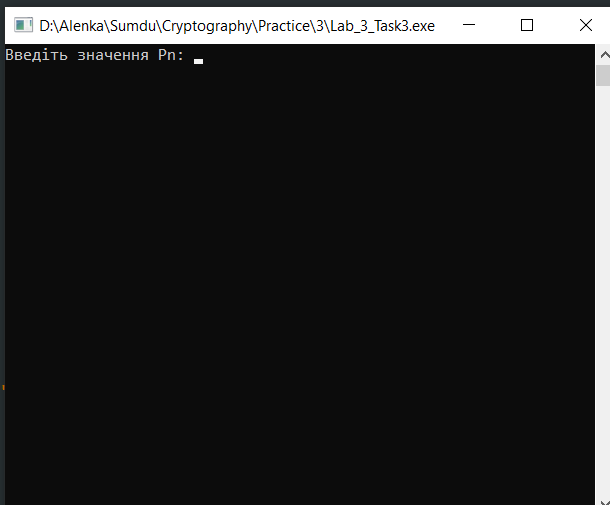
cout << "P3 = (" << x3 << ", " << y3 << ")" << endl;

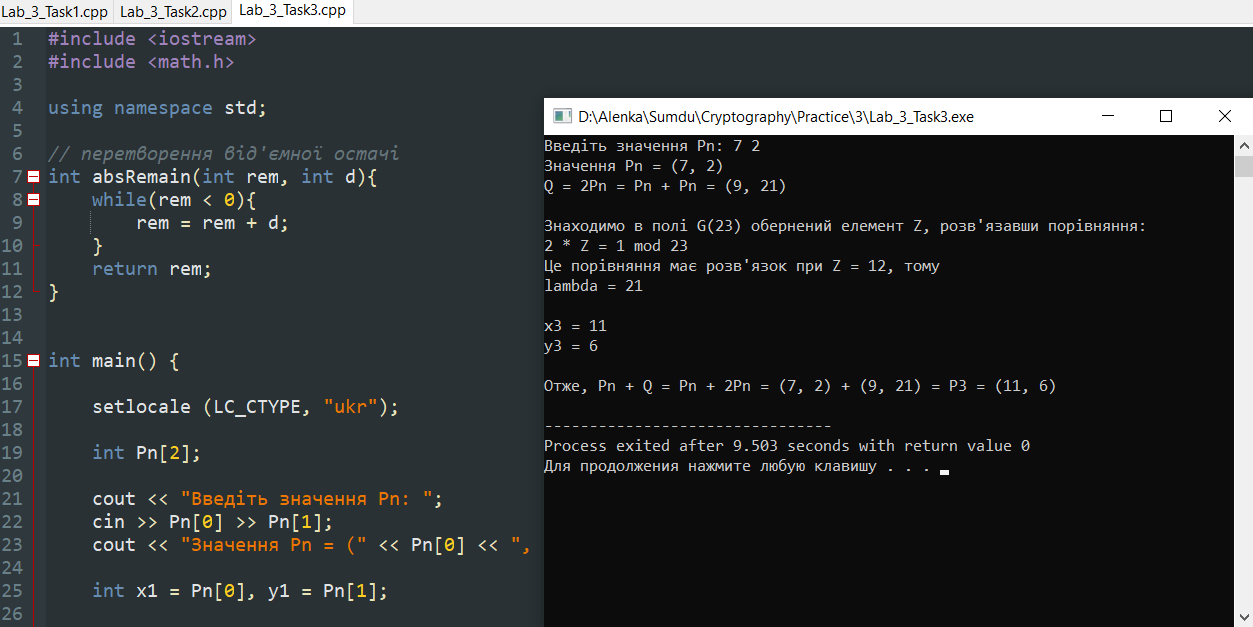
return 0;

}

***Прінт-скрін виконання програми:***

******



******

***Контрольне питання***

9. Запишіть елементи поля GF(7).

GF(p) = {0, 1, …, p-1}

GF(7) = {0, 1, 2, 3, 4, 5, 6}

***Висновок***

Виконуючи лабораторну роботу, навчилися перевіряти належність точок еліптичній кривій, складати точки еліптичної кривої та складати програму розв’язування цих задач, а також знаходити елементи поля GF(p).

***Додаток***

