ПРАКТИЧЕСКОЕ ЗАДАНИЕ 2.2.
КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Цель задания – изучить алгоритм M-кратной композиции точек на эллиптической кривой посредством его программной реализации; познакомиться с понятиями группового закона, порядка элемента в группе и генератора (порождающего элемента) группы.

Задачи

1. Напишите программу, которая демонстрирует групповой закон для остатков по модулю простого числа по отношению к операции умножения. **На вход** программа должна принимать простое число P. в качестве результата должна быть выведена такая таблица:

Демонстрация группового закона для умножения остатков по модулю P=7

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

2. Напишите программу, которая определяет порядок элемента в группе остатков по модулю простого числа. **На вход** программа должна принимать простое число P. **В качестве результата** должна быть выведена такая таблица и отмечены генераторы (числа, порядки которых равны p-1):

Порядок числа в мультипликативной группе вычетов

a	a^1	a^2	a^3	a^4	a^5	a^6	
1	1						1
2	2	4	1				3
3	3	2	6	4	5	1	6
4	4	2	1				3
5	5	4	6	2	3	1	6
6	6	1					2

У генераторов порядок числа равен числу элементов группы

3. Реализуйте алгоритм M-кратной композиции точек на эллиптической кривой. Протестируйте программу на примерах из презентации.

4. Напишите программу, которая демонстрирует групповой закон для точек на эллиптической кривой. **На вход** программа должна принимать простое число P и параметры эллиптической кривой. В качестве результата должна быть выведена такая таблица:

Демонстрация группового закона
кривая $Y^2 = X^3 + X + 3$ над полем F_7

+	(0,0)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
(0,0)	(0,0)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
(4,1)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)	(0,0)
(6,6)	(6,6)	(5,0)	(6,1)	(4,6)	(0,0)	(4,1)
(5,0)	(5,0)	(6,1)	(4,6)	(0,0)	(4,1)	(6,6)
(6,1)	(6,1)	(4,6)	(0,0)	(4,1)	(6,6)	(5,0)
(4,6)	(4,6)	(0,0)	(4,1)	(6,6)	(5,0)	(6,1)

Сумма любых точек из группы
(0,0) (4,1) (6,6) (5,0) (6,1) (4,6)
принадлежит группе
Для каждого элемента есть обратный, сумма которых равна нулевому элементу. Например,
(4,6)+(4,1)=(0,0)

5. Напишите программу, которая определяет порядок элемента в группе точек на эллиптической кривой. На вход программа должна принимать простое число P и параметры кривой. В качестве результата должна быть выведена такая таблица и отмечены генераторы (точки, порядки которых равны p-1):

Понятие генератора в группе точек на эллиптической кривой

P	[1]P	[2]P	[3]P	[4]P	[5]P	[6]P
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(4,1)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)	(0,0)
(6,6)	(6,6)	(6,1)	(0,0)	(6,6)	(6,1)	(0,0)
(5,0)	(5,0)	(0,0)	(5,0)	(0,0)	(5,0)	(0,0)
(6,1)	(6,1)	(6,6)	(0,0)	(6,1)	(6,6)	(0,0)
(4,6)	(4,6)	(6,1)	(5,0)	(6,6)	(4,1)	(0,0)

Точки (4,1) и (4,6) являются генераторами группы, поскольку все значения их m-кратной композиции различны и, следовательно, генерируют все элементы группы.

Требования к реализации:

- можно выбрать любой язык программирования;
- UI – любой (консоль, GUI, чат-бот и пр.);
- тип программного приложения – любой (консоль, desktop, web, мобильное);
- демонстрацию работы программы записать в виде GIF-файла;
- программный код и GIF разместить в репозитории GIT.