Система довгої модульної арифметики за модулем N

№	Задача	Кількість виконавців
1	Додавання, віднімання, множення, взяття оберненого елемента (за допомогою малої теореми Ферма або розширеного алгоритму Евкліда на вибір) та ділення	**2**
2	Піднесення у степінь [3] використовуючи переведення числа у форму Монтгомері [5,6]	**2**
3	Розклад числа на множники (наївний алгоритм та алгоритм Поларда) [1, С. 91]	**1**
4	Обчислення квадратного кореня числа [1, С. 99]	**1**
5	Обчислення дискретного логарифму числа за методом Baby-step giant-step [1, С. 105]	**1**
6	Обчислення дискретного логарифму числа за методом Поларда [1, С. 106]	**1**
7	Знаходження порядку елемента групи [1, С. 162, Algorithm 4.79]	**1**
8	Знаходження всіх генераторів групи [1, С. 163, Algorithm 4.80]	**1**
9	Знаходження функції Ейлера від заданого числа [1, С. 65] та функції Кармайкла від заданого числа [2]	**1**
10	Ймовірнісна перевірка числа на простоту (тести Ферма та Соловея-Штрассена) [1, С.135]	**1**
Підсистема числення на еліптичних кривих		
11	Додавання двох точок на еліптичній кривій та взяття оберненої точки [4, С.12]	**1**
12	Швидке піднесення у степінь точки [4, С. 18]	**1**
13	Визначення порядку групи, заданої еліптичною кривою (кількість точок) [4, С. 123],[8]	**2**
14	Визначення порядку заданої точки на еліптичній кривій	**1**
15	Реалізувати алгоритм генерації відкритого ключа на основі еліптичних кривих [4, С. 170]	**1**
	Всього	**18**

Умови

1) Це груповий проект, який робить кожна підгрупа окремо. Це має бути єдина програма з інтерфейсом (можна і текстовим, хоча графічний виглядав би краще). Програма повинна бути структурована (окремі бібліотеки, функції для різних задач). Більшість задач у проекті не є окремі, а використовують інші задачі, тому кооперація вітається.
2) Втім, з кожним студентом я спілкуюсь окремо, задаю питання по розумінню його задачі, базовому розумінню інших задач та знання базового теоретичного підґрунтя. Максимальна кількість балів – 20. Підгрупа з найкращим проектом додатково отримує +5 балів кожному як бонус.
3) Мова програмування C++

Література

1) Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone. Handbook of applied cryptography
2) https://en.wikipedia.org/wiki/Carmichael_function
3) https://en.wikipedia.org/wiki/Modular_exponentiation
4) Elliptic Curves, Number Theory and Cryptography (Second Edition)
5) https://en.wikipedia.org/wiki/Montgomery_modular_multiplication
6) https://www.nayuki.io/page/montgomery-reduction-algorithm
7) https://crypto.stackexchange.com/questions/33028/order-and-cofactor-of-the-base-point
8) https://en.wikipedia.org/wiki/Counting_points_on_elliptic_curves#Baby-step_giant-step