Экзамен II

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Продолжительность экзамена — 3 часа. Можно пользоваться ручкой, бумагой, материалами лекций и семинаров и (если очень хочется) системой SageMath или её аналогом (хотя ни в одной задаче не требуется сложных вычислений). Каждый пункт оценивается в 2 балла.

Задача 1. Решите задачу дискретного логарифмирования в аддитивной группе вычетов по модулю 1955:

$$480x = 10.$$

Задача 2. Известно, что

$$(31 + 3\sqrt{2})(31 - 3\sqrt{2}) = (39 + 17\sqrt{2})(39 - 17\sqrt{2}).$$

Разложите число $(31 + 3\sqrt{2})$ на простые множители в кольце $\mathbb{Z}[\sqrt{2}]$.

Задача 3. Найдите все рациональные решения уравнения

$$\text{(а) } 2x^2 - y^2 = 1; \qquad \text{(б) } x^2 + y^2 = 2.$$

Задача 4. Сколько решений по модулю p имеет сравнение

$$x^2 - y^2 \equiv 1 \pmod{p}?$$

Через p обозначается простое число (ответ будет зависеть от p).

Задача 5. Эллиптическая кривая задана уравнением

$$y^2 = x^3 + 1,$$

в качестве нулевого элемента выбрана бесконечно удалённая точка на кривой. Через P обозначим точку $(2, 3)$ на кривой.

(а) Найдите координаты точки $2P$.
(б) Найдите координаты суммы точек $P + Q$, где $Q = (0, 1)$.
(в) Пусть $R = (-1, 0)$. Найдите координаты точки $2R$.
(г) Найдите порядок циклической подгруппы, порождённой точкой P.