Экзамен

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 1923:

$$476x = 7.$$

Задача 2. Известно, что

$$(19 + 34i)(19 - 34i) = (29 + 26i)(29 - 26i).$$

Разложите целое гауссово число $(19 + 34i)$ на простые множители в кольце целых гауссовых чисел $\mathbb{Z}[i]$.

Задача 3. Найдите все рациональные решения уравнения

$$\text{(а) } x^2 - 2y^2 = 1; \qquad \text{(б) } x^2 + 2y^2 = 3.$$

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

$$y^2 + xy + y = x^3 - x^2 - 3x + 3,$$

в качестве нулевого элемента выбрана бесконечно удалённая точка на кривой. Через P обозначим точку $(1, 0)$ на кривой.

(а) Найдите координаты точки $2P$.
(б) Найдите координаты суммы точек $P + Q$, где $Q = (-1, -2)$.
(в) Пусть $R = (3, -6)$. Найдите координаты точки $2R$.
(г) Найдите порядок циклической подгруппы, порождённой точкой P.