Семинар 9. Сложение точек на кривых

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Определение 1. *Выберем точку O на конике C и объявим O нулевым элементом. Для двух точек P и Q на конике C определим их сумму $P+Q$ следующим образом. Проведём через точку O прямую l, параллельную прямой PQ, и в качестве $P+Q$ возьмём вторую точку пересечения прямой l с коникой C.*

Задача 1. Как дополнить определение сложения в случае, когда у прямой l и коники C нет "второй точки" пересечения?

Задача 2. (а) Задайте явными формулами сложение точек на окружности $\{x^2+y^2=1\}$ на вещественной плоскости.

(б) Запараметризуем точки окружности таким образом: $P(\varphi)=(\cos\varphi,\sin\varphi)$. Какую точку нужно выбрать в качестве нулевого элемента, чтобы для всех $\varphi\in\mathbb{R}$ выполнялось тождество

$$P(\varphi)+P(\psi)=P(\varphi+\psi)?$$

Задача 3. (а) Задайте явными формулами сложение точек на гиперболе $\{x^2-2y^2=1\}$ на вещественной плоскости.

(б) Используйте пункт (а), чтобы построить бесконечную серию целочисленных решений уравнения Пелля:

$$x^2-2y^2=1.$$

(в) Найдите все обратимые элементы в кольце $\mathbb{Z}[\sqrt{2}]$.

Задача 4. Пусть p — простое число. Будем рассматривать "окружность" $\{x^2+y^2=1\}$ как проективную конику C над полем из p элементов. Найдите группу точек на C для

(а) $p=2$; (б) $p=3$; (в) $p=5$.