БФУ им. И. Канта

Методы и алгоритмы генерации эллиптических кривых для криптографии.

Е.Малыгина (2021)

Лабораторная работа №1 (20.01.21)

Доказать следующие свойства при условии, что R, S – полиномиальные функции из $K(C)$, где C – гиперэллиптическая кривая:

1. $N(R)$ – рациональная дробь из $K(x)$.
2. Если $R = G \in K[C]$, то $N(G) \in K[x]$.
3. $N(R) = N(\bar{R})$.
4. $N(RS) = N(R)N(S)$.