

G_1 a subgroup of the additive group of points of an elliptic curve E/\mathbb{F}_p