Michiel Kosters - Mathematisch Instituut, Universiteit Leiden
mkosters@math.leidenuniv.nl, January 7, 2013

Generating the rational points of an elliptic curve over $\mathbf{F}_q$ by looking at x-coordinates

1. Abstract

Let $E/\mathbf{F}_q$ be an elliptic curve given by a Weierstrass equation. In this talk we will discuss a theorem which says that the points of $E(\mathbf{F}_q)$ with x-coordinates in a coset of a subgroup of $\mathbf{F}_q$ of size at least $6\sqrt{q}$ generate $E(\mathbf{F}_q)$, unless one is in a very specific case. We will discuss this exception in more detail.