Orders of CM elliptic curves modulo $p$
with at most two primes

HENRYK IWANIEC AND JORGE JIMÉNEZ URROZ

Abstract. In this paper of 1988 N. Koblitz conjectured that given an elliptic
curve $E$ over the rationals, the order of the group of $\mathbb{F}_p$ points of its reduction
modulo $p$, $|E(\mathbb{F}_p)|$, is a prime number for infinitely many primes $p$. Since then
a wide number of research articles has been dedicated to understand and solve
this conjecture. In this paper we give the best result known nowadays. We can
prove quantitatively that for infinitely many primes $p$ the reduction of the curve
$y^2 = x^3 - x$ modulo $p$ has order which is eight times an almost prime number.
The problem turns out to be the equivalent to the twin prime conjecture in the
Gaussian domain. The result could be extended to any CM curve with certain
considerations. We also point out the relation of the result with certain considera-
tions. We also point out the relation of the result with the cyclicity of $E(\mathbb{F}_p)$, and
the Lang Trotter conjecture.

Mathematics Subject Classification (2010): 11N36 (primary); 11G07, 14G50
(secondary).

1. Introduction and statement of results

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. There is a huge variety of papers
dedicated to the study of this object, and we can safely say that the main interest
to do so is that, in fact, apart from an algebraic curve, it can be equipped with a
compatible structure as a finitely generated Abelian group. For example, we know
that $E(\mathbb{Q})$, the set of $\mathbb{Q}$-rational points of $E$, can be seen as the direct product
$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$. Let us mention here that, while the torsion is very well
understood, the mathematical community is making a great effort in trying to un-
derstand the rank $r$ of this group with certain generality.

Since the operations of the group are algebraic functions defined over the same
field as the curve, we can also consider the structure of the set of points, not over
$\mathbb{Q}$, but over different fields of interest. In this sense, let $N$ be the conductor of the
curve and $p$ be a prime of good reduction for $E$ (that is, $p \nmid N$). We denote by $E_p$
the reduction of $E$ modulo $p$. This is an elliptic curve defined over $\mathbb{F}_p$ and, as in

The first author was supported in part by NSF grant DMS-03-01168. The second by DGICYT
Received June 23, 2009; accepted in revised form November 19, 2009.