Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)
Vol. IX (2010), 815-832

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 considerations. 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).