46th Annual Iranian Mathematics Conference
25-28 August 2015
Yazd University

Some question on the reduction of elliptic curves

Jorge Jimenez
Polytechnic University Catalonia, Barcelona, Spain

Abstract

An elliptic curve E over the rationals gives, in a natural way, a family of elliptic curves over finite fields simply considering the reduction Ep of the curve modulo prime numbers. And many interesting question arises regarding this family. For example, one could ask for the number of primes up to X so that Ep has a prime number of points, and try to solve an open problem stated long back by Koblitz. Recall that this question has a direct interest in building elliptic curves interesting for cryptographic purposes. Another problems related with this family are the famous Sato-Tate conjecture, or the Lang-Trotter conjectures on the trace of the Frobenius element and the Frobenius ring. In the talk, after a review of the ingredients, i will talk about some contributions that i could do, on these problems.