J. Math. Kyoto Univ. (JMKYAZ)
48-4 (2008), 725–746

Study of group orders of elliptic curves

By

Hidemi Sakagawa

1. Introduction

In this paper, we study the group of points modulo p of elliptic curves defined over $\mathbb{Q}$. In particular, we are interested in the frequency with which this group is cyclic. Let E be an elliptic curve over $\mathbb{Q}$ and for each prime p where E has good reduction, let $E_p(\mathbb{F}_p)$ be the group of rational points on the reduction of E modulo p. J.-P.Serre raised the question of how often this group becomes cyclic. Assuming the Generalized Riemann Hypothesis (GRH), he ([16]) showed that, for some constant C_E depending only on E, we have $f(x,E) \sim C_E \mathrm{Li}\, x$, where $f(x,E)$ denotes the number of primes $p \leq x$ such that E has good reduction at p and $E_p(\mathbb{F}_p)$ is cyclic, and Li x is the logarithmic integral. In 1980 ([10]), Ram Murty removed the GRH in the case for an elliptic curves over $\mathbb{Q}$ and with complex multiplication. In 1990 ([5]), Rajiv Gupta and Ram Murty proved unconditionally that for an elliptic curve E defined over $\mathbb{Q}$, the group $E_p(\mathbb{F}_p)$ is cyclic for infinitely many primes p if and only if E has an irrational 2-division points. By the fundamental theorem of finite abelian group, if the group order of $E_p(\mathbb{F}_p)$ is square-free, then the group becomes cyclic. Here, a natural question arises. Namely, how often the group $E_p(\mathbb{F}_p)$ becomes cyclic with non-square-free order? For this question, we will show the following result.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$. We assume that the isomorphism $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ holds for any prime q. Then, under the GRH, the primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ is a cyclic group with non-square-free order have positive density in the set of rational primes.*

By the way, the group which has the prime order clearly becomes cyclic. So another natural question is as follows. Namely, how often the group $E_p(\mathbb{F}_p)$ has prime order? As to this problem, Koblitz ([7]) conjectured the number of primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ has prime order becomes $\sim C_E \frac{x}{(\log x)^2}$, where C_E is the constant depending only on E. In 2001, assuming the GRH, Ali Miri and Kumar Murty ([13]) showed that, for an elliptic curve E over $\mathbb{Q}$ without complex multiplication, the number of primes $p \leq x$ such that $\sharp E_p(\mathbb{F}_p)$ has at most 16 prime divisors (counting multiplicity) is $\gg \frac{x}{(\log x)^2}$. However, it seems

Received January 17, 2007