TOKYO J. MATH.
VOL. 28, NO. 2, 2005

Parametric Families of Elliptic Curves with Cyclic $\mathbf{F}_p$-Rational Points Groups

Naoya NAKAZAWA

Osaka Prefecture University

(Communicated by H. Tsuji)

1. Introduction

In elliptic cryptography, it is needed for a given finite field F, to construct an elliptic curve whose group of F-rational points is cyclic of a large order. An approach to construct such elliptic curves is, for a given elliptic curve E defined over an algebraic number field K, to determine a set $S_{E,K}$ of prime ideals $\mathfrak{p}$ of K such that group $\bar{E}(\mathbf{F}_{\mathfrak{p}})$ of rational points of the reduction $\bar{E}$ of E modulo $\mathfrak{p}$ is cyclic. R. Gupta and M. R. Murty [3] obtained a result for this problem in probabilistic point of view. However, in general, the problem to determine the set $S_{E,K}$ is not easy. In the case E has complex multiplication and an ordinary good reduction at $\mathfrak{p}$, it is noted the group structure of $\bar{E}(\mathbf{F}_{\mathfrak{p}})$ is determined by the trace of Frobenius endomorphism (cf. [9]). In this case, the trace can be computed easily from the quadratic norm representation of a prime number (cf. [4], [5], [6], [7]). Therefore, in this case, we can give a family of prime ideals contained in $S_{E,K}$. For example see [2].

The purpose of this article is, without the properties of complex multiplication, to construct a family of elliptic curves E defined over $\mathbf{Q}$ such that for prime numbers of the form $p = 2^\alpha 3^\beta 5^\gamma q^\delta + 1$($q$:an odd prime) $\bar{E}(\mathbf{F}_p)$ are cyclic. The key for considering this problem is the next theorem.

THEOREM 1 (cf. [3]). *For an elliptic curve $E/\mathbf{Q}$ and a positive integer n, let $E[n]$ be the set of n-division points and $K_n(E)$ be the field generated over $\mathbf{Q}$ by all points of $E[n]$. Let p be a prime number such that E has good reduction at p and $\bar{E}(\mathbf{F}_p)$ the group of rational points on the reduction of E modulo p. Then we have*

(a) *$\bar{E}(\mathbf{F}_p)$ is cyclic if and only if p does not split completely in $K_l(E)$ for any prime l.*

(b) *The cyclotomic field $\mathbf{Q}(\zeta_n)$ is contained in $K_n(E)$ for any n.*

COROLLARY 2. *If a prime p of the form $p = 2^\alpha q_1^{\beta_1} \cdots q_m^{\beta_m} + 1$ $(q_1, \cdots, q_m$:odd primes) does not split completely in $K_2(E), K_{q_1}(E), \cdots, K_{q_m}(E)$, then $\bar{E}(\mathbf{F}_p)$ is cyclic.*

Received January 15, 2004; revised May 27, 2004