ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

COUNTING POINTS ON *CM* ELLIPTIC CURVES

H.M. STARK

To Wolfgang Schmidt on the occasion of his 60th birthday

1. Introduction.

Let E be an elliptic curve in Weierstrass normal form,

$$E : y^2 = 4x^3 - g_2 x - g_3 \tag{1}$$

where g_2 and g_3 are in a number field K. If $\mathfrak{P}$ is a first degree prime of K of norm p, and g_2 and g_3 are integral at $\mathfrak{P}$, we can reduce the curve (mod $\mathfrak{P}$) to a curve over the field $\mathbf{F}_p$ of p elements

$$\overline{E} : y^2 = 4x^3 - \bar{g}_2 x - \bar{g}_3$$

and we can then ask how many points are there on $\overline{E}$? It suffices to know the Frobenius automorphism of $\overline{E}$ which sends the point (x, y) on $\overline{E}$ to the point (x^p, y^p) in order to answer this question. In the case of curves with complex multiplication by an order in a complex quadratic field $k = \mathbf{Q}(\sqrt{D})$ of discriminant D, we will show how this can be done.

Since k is always a subfield of $K(\sqrt{D})$, it will be convenient for much of the paper to assume that k is a subfield of K. To avoid excess terminology, it will also be convenient to restrict ourselves to the case where E has complex multiplication by the full ring of integers of k. Let H be the Hilbert class field of k and H^+ the real subfield of H. The degree $[H : k]$ is $h(k)$, the class-number of k. A curve with complex multiplication by the full ring of integers of k may be rescaled so as to be defined over H. With correct rescalings, there are $h(k)$ such curves, all conjugate under automorphisms of the Galois group $G(H/k)$.

In this paper we consider the case that $(D, 6) = 1$ as this includes the interesting class-number one fields that were the original motivation for this paper. It is convenient to set

$$\theta = \frac{-3 + \sqrt{D}}{2},$$

Received by the editors on August 4, 1995, and in revised form on December 18, 1995.