ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 34, Number 2, Summer 2004

USING ELLIPTIC CURVES TO PRODUCE QUADRATIC NUMBER FIELDS OF HIGH THREE-RANK

MATT DELONG

ABSTRACT. We use a connection between the arithmetic of elliptic curves of the form $y^2 = x^3 + k$ and the arithmetic of the quadratic number fields $\mathbf{Q}(\sqrt{k})$ and $\mathbf{Q}(\sqrt{-3k})$ to look for quadratic fields with high three-rank. We give a geometric proof of known results on polynomials that give rise to infinite families of quadratic number fields possessing non-trivial lower bounds on their three-rank. We then generalize the method to produce infinitely many such polynomials. Finally, we produce specific examples of quadratic number fields with high three-rank.

1. Introduction. Previous authors have documented polynomials that give rise to infinite families of quadratic number fields possessing non-trivial lower bounds on their three-ranks [**2, 3, 8, 9**]. Their methods of proof were usually straight-forward but lengthy calculations involving ideals, or appeals to class field theory.

In this paper we give a new and shorter proof of the results on some of these families of fields. The method of proof leads us to a way of generating infinitely many such polynomials. The method is geometric in nature, and relies on a well-known connection between the arithmetic of elliptic curves of the form $y^2 = x^3 + d$ and the arithmetic of the quadratic number fields $\mathbf{Q}(\sqrt{d})$ and $\mathbf{Q}(\sqrt{-3d})$. We use a precise form of the connection, given by Satgé [**6**].

We first illustrate the method in detail on a family of Shanks [**8**]. We then discuss other previously discovered polynomials in our context. Following this, we show how to generalize our method to produce infinitely many such polynomials. Finally, we give some numerical data derived using some of our new polynomials.

The specific examples of three-ranks of quadratic fields, the orders of rational points on elliptic curves, and the conjectural upper bounds on

2000 AMS *Mathematics Subject Classification.* 11R29, 11G05.
Received by the editors on August 20, 2001.