Vol. 53, No. 1 DUKE MATHEMATICAL JOURNAL © March 1986

TORSION POINTS ON ELLIPTIC CURVES OVER ALL QUADRATIC FIELDS

S. KAMIENNY

§1. Introduction. In [6] we gave a criterion for the nonexistence of a pair (E, P) consisting of an elliptic curve E and a rational point P of order p ($p \equiv 1 \pmod 4$) defined over the real quadratic field $\mathbf{Q}(\sqrt{p})$. Unfortunately, the prime $p = 17$ was exceptional for that work. We were, thus, unable to rule out the existence of an elliptic curve with a 17-torsion point rational over $\mathbf{Q}(\sqrt{17})$. In this paper we show not only that there is no elliptic curve with a rational point of order 17 defined over $\mathbf{Q}(\sqrt{17})$, but we also show that there is no elliptic curve with a rational point of order 17 defined over *any* quadratic field. In fact, we actually show that there is no elliptic curve with a rational point of order p defined over any quadratic field when $p = 17$, 19, 23, 29, or 31. The key feature that these primes have in common is the existence of a nonhyperelliptic quotient (of genus > 2) of $X_1(p)$ whose jacobian has finite Mordell–Weil group over $\mathbf{Q}$. There are a few other values of p ($p = 41$, 47, 59, and 71) that may enjoy this property, but to verify that they actually do seems to require the help of a computer.

The possibility of proving the result described above was suggested to me by a letter from B. Mazur to A. Ogg [10] about the arithmetic of Shimura curves. I would like to thank Barry Mazur for making a copy of the letter available to me. In addition, I would like to thank David Rohrlich and Chad Schoen for their assistance in verifying that the curves in question are not hyperelliptic.

§2. Modular curves and their jacobians. Let p be a prime number, and let $Y_0(p)_{/\mathbf{Q}}$ be the curve over $\mathbf{Q}$ that classifies isomorphism classes of elliptic curves together with a rational subgroup of order p. Denote by $X_0(p)_{/\mathbf{Q}}$ the complete curve obtained by adjoining the cusps 0 and ∞ to $Y_0(p)_{/\mathbf{Q}}$. Similarly, let $Y_1(p)_{/\mathbf{Q}}$ be the curve that classifies isomorphism classes of elliptic curves together with a rational point of order p, and let $X_1(p)_{/\mathbf{Q}}$ be the complete curve obtained by adjoining the $p - 1$ cusps. The curve $X_1(p)$ is naturally a cyclic cover of $X_0(p)$ of degree $(p-1)/2$. The covering map $X_1(p) \dashrightarrow X_0(p)$ is given by sending an elliptic curve and a point to the elliptic curve and the subgroup generated by that point. For an integer n dividing $(p-1)/2$ we let $X^{(n)}(p)$ denote the unique covering of $X_0(p)$ of degree n that is intermediate to the covering $X_1(p) \dashrightarrow X_0(p)$. The curve $X^{(n)}(p)$ has $2n$ cusps, half of them rational over $\mathbf{Q}$. Finally, we let $J_0(p)$ (respectively, $J_1(p)$, $J^{(n)}(p)$) denote the jacobian of $X_0(p)$ (respectively, $X_1(p)$, $X^{(n)}(p)$). The abelian variety $J^{(n)}(p)$ has good reduction at

Received February 19, 1985. Research partially supported by an N.S.F. grant.