69. *Curves of Genus 2 with a Rational Torsion Divisor of Order 23*

By Hiroyuki OGAWA

Department of Mathematics, Osaka University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 14, 1994)

§1. Introduction. Flynn [1] (resp. Leprévost [6], [7]) got infinitely many curves defined over $\boldsymbol{Q}$ with a rational torsion divisor of order $N = 11$ (resp. 13, 15, 17, 19 and 21), by constructing a curve of genus 2 defined over $\boldsymbol{Q}(t)$ with a rational torsion divisor of order N. In this paper, we shall extend these results to the case of $N = 23$. We remark that Leprévost [8] gave some curves over $\boldsymbol{Q}$ with a rational torsion divisor of order 22, 23, 24, 25, 26, 27 and 29, respectively.

Many studies have been made to find algebraic curves with a large rational torsion divisur, or abelian varieties with a large rational torsion point. In case of genus 1, lots of elliptic curves with a large rational torsion were explicitly constructed, before the appearance of the universal bound of torsion of elliptic curves over $\boldsymbol{Q}$ (resp. over any quadratic number field) by Mazur [9] (resp. by Kamienny [5]). On the other hand, Gross-Rohrich [3] and Shioda [10] constructed a family of g-dimensional abelian varieties over $\boldsymbol{Q}$ with a rational torsion point of order $2g + 1$, using Fermat varieties, and Flynn [2] and Leprévost [7] gave families of hyperelliptic curves of genus g over $\boldsymbol{Q}$ with a rational torsion divisor of order $2g^2 + 2g + 1$ and $2g^2 + 3g + 1$, respectively. As for universal bounds of torsions like Mazur's, we know only the result on torsions of abelian varieties of CM-type due to Silverberg [11], who, in the 2-dimensional case over $\boldsymbol{Q}$, showed that the order of a rational torsion point is at most $185640 = 2^3\cdot 3\cdot 5\cdot 7\cdot 13\cdot 17$.

An abelian variety without any non-trivial abelian subvarieties is called simple. Leprévost's example with a 24-torsion is not simple, by easy calculation, and those with a 25-torsion and with a 27-torsion probably not, as we can decompose their congruence zeta functions for each prime $p < 1000$. We can easily construct abelian varieties with a large torsion using the product of clliptic curves with large torsions. For example, if E and E' are two elliptic curves over $\boldsymbol{Q}$ with a rational 10-torsion and with a rational 9-torsion, respectively, then the product $E \times E'$ has a rational torsion of order $90 = 10 \times 9$. So, in search for abelian varieties with a large rational torsion, the interest would be lost without the assumption that they are simple. We remark here that the Jacobian varieties of the curves given in this paper are simple.

§2. Construction of torsion divisors with a large order. 2.1. We shall first describe briefly the method of Leprévost [6,7]. Let k be a field with $\mathrm{char}(k) \neq 2$. Let g be a positive rational integer, A a polynomial on x with