H. IMAI
KODAI MATH. J.
3 (1980), 56—58

ON THE RATIONAL POINTS OF SOME JACOBIAN VARIETIES OVER LARGE ALGEBRAIC NUMBER FIELDS

BY HIDEO IMAI

In this note we shall prove the following: Let X be a hyperelliptic curve defined over the rational number field $\boldsymbol{Q}$ and let J be its Jacobian variety. Let L be the field generated by all square roots of rational integers over $\boldsymbol{Q}$. Then the group of L-rational points $J(L)$ has an infinite rank over the rational integer ring $\boldsymbol{Z}$.

In Frey and Jarden [1], the following is conjectured: Let A be an abelian variety defined over $\boldsymbol{Q}$ and $\boldsymbol{Q}_{ab}$ the maximal abelian extension of $\boldsymbol{Q}$. Then does the group $A(\boldsymbol{Q}_{ab})$ have an infinite rank over $\boldsymbol{Z}$? Our result supports this conjecture partially.

1. Let X be a hyperelliptic curve defined by the equation (in the affine form) $y^2=f(x)$, where $f(x)$ is a monic separable polynomial of degree $2g+1$ with coefficients in $\boldsymbol{Z}$. Let $P_0=(\infty, \infty)$ be the point at infinity on X, which is rational over $\boldsymbol{Q}$. Let $z=x^g/y$ be a local uniformizing parameter at P_0. Let $\omega_i=x^{i-1}dx/y$ $(i=1, 2, \cdots, g)$ be the canonical base of the space of differential forms of the first kind on X. Writing these ω_i in terms of z and integrating ω_i formally, we get power series $\Psi_i(z)\in\boldsymbol{Q}[[z]]$ such that $\Psi_i(0)=(0)$ and $\omega_i=d\Psi_i$.

LEMMA 1.

$$\Psi_i(z)=\frac{-2}{2g-2i+1}z^{2g-2i+1}+\sum_{n>g-i}\frac{c_n^{(i)}}{2n+1}z^{2n+1} \quad \textit{with} \quad c_n^{(i)}\in\boldsymbol{Z}.$$

Proof. It is easily proved by direct computation. We outline the proof. Differentiating $z=x^g/y$ with respect to x, we have

$$dz=(gx^{g-1}-x^g f'(x)/2f(x))dx/y\,.$$

Hence we have

$$\Psi_i'(z)=1/gx^{g-i}(1-xf'(x)/2gf(x))\,.$$

We write $z=x^g/\sqrt{f(x)}$ and expand the above equation in terms of $t=1/x$. Let $\Psi_i(z)=\sum_{n=1}^{\infty}a_n z^n$ and let $h(1/x)=f(x)/x^{2g+1}-1$. After some computations we get

Received January 17, 1979

$$-2t^{g-i}\sum_{n=0}^{\infty}(th'(t)/(1+h(t)))^n=\sum_{n=1}^{\infty}na_n(t/(1+h(t)))^{(n-1)/2}.$$

Our assertion follows from this directly.

Put $\Psi(z)={}^t(\Psi_1(z),\cdots,\Psi_g(z))$ a g-dimensional column vector.

2. Now let $J=\mathrm{Jac}(X)$ be the Jacobian variety of X. Choose an imbedding $\Lambda\colon X\to J$ defined over $\boldsymbol{Q}$ such that $\Lambda(P_0)=0$ the identity point of J. Let $y_1,\cdots,y_g$ be rational functions on J defined over $\boldsymbol{Q}$ such that they constitute a system of local uniformizing parameters at 0. Let $\eta_1,\cdots,\eta_g$ be invariant differential forms on J defined over $\boldsymbol{Q}$ such that $\omega_i=\eta_i\circ\Lambda$ $(i=1,2,\cdots,g)$. It is well known that these $\eta_1,\cdots,\eta_g$ form a base of the space of invariant differential forms on J. As η_i is closed (cf. [2], Proposition 1.3 and Lemma 1.4), there exists a formal power series $F_i(y_1,\cdots,y_g)\in\boldsymbol{Q}[[y_1,\cdots,y_g]]$ such that $F_i(0,\cdots,0)=0$ and $\eta_i=dF_i$. Let $F={}^t(F_1,\cdots,F_g)$ and let $\hat{J}$ the formal group of J. From [2], Proposition 1.1 and Theorem 1, *there is a matrix* $A\in GL_g(\boldsymbol{Q})$ such that $AF(y)\equiv y$ (mod deg 2) and $AF\colon\hat{J}\to\hat{\boldsymbol{G}}_a^g$ is a strong isomorphism over $\boldsymbol{Q}$ where $\hat{\boldsymbol{G}}_a$ is the formal group of the additive group. From [2], Proposition 1.1, we see that each component of the differential $d(AF)$ is obtained from differentiating the formal group law of $\hat{J}$. Hence for a prime p at which J and y_i,η_i $(i=1,\cdots,g)$ have good reduction, the coefficients of $d(AF)$ are p-adic integers. Hence if we write the i-th coordinate of AF as $\sum_{n_1,\cdots,n_g}a^{(i)}_{n_1,\cdots,n_g}y_1^{n_1}\cdots y_g^{n_g}$, we shall have $v_p(a^{(i)}_{n_1,\cdots,n_g})\geqq-\min_{1\leqq j\leqq g}v_p(n_j)$ were v_p is the p-adic additive valuation. From this we see that AF is convergent in sufficiently small neighbourhood of 0 in the p-adic topology. The inverse function theorem (cf. [3], LG 2.10) implies the following:

LEMMA 2. *Let p be a prime at which J and y_i, η_i $(i=1,\cdots,g)$ have good reduction, then $(AF)^{-1}$ is convergent in sufficiently small neighbourhood of* 0 *in the p-adic topology.*

3. From the equation $\omega_i=dF_i\circ\Lambda=d\Psi_i$, we have $\Psi_i=F_i\circ\Lambda$ i.e., $\Psi=F\circ\Lambda$. We take a prime p at which J and y_i, η_i have good reduction. Let $K/\boldsymbol{Q}_p$ be a finite extension, P be a K-rational point of X and let m be an integer. As $AF\colon\hat{J}\to\hat{\boldsymbol{G}}_a^g$ is an isomorphism, $m\Lambda(P)\in J(K)$ may be computed as $m\Lambda(P)=(AF)^{-1}(mA\Psi(P))$ when the right hand side converges.

Especially we consider the point $P=(1/p^\alpha,\sqrt{f(1/p^\alpha)})$ where p is a prime with the above good reduction condition and α is a sufficiently large odd integer. Let $c=p^{(2g+1)\alpha}f(1/p^\alpha)$, then $c\in\boldsymbol{Z}$ and c is coprime to p. Let $K=\boldsymbol{Q}(\sqrt{c/p})$, then P is rational over K. As p is ramified in K, we write $p=\mathfrak{p}^2$ and let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K. We consider the point P as a $K_\mathfrak{p}$-rational point. For the local parameter $z=x^g/y$, the value of z at P is given by $z_p=\sqrt{p^\alpha/c}$. From Lemma 1, $\Psi(P)=\Psi(z_p)$ is convergent in the $\mathfrak{p}$-adic topology. From Lemma 2, $(AF)^{-1}(mA\Psi(z_p))$ also coverges for sufficiently large α.

LEMMA 3. *For almost all primes p, if an odd integer α is taken sufficiently large, $m\Lambda(P)$ is not $\boldsymbol{Q}$-rational for any non-zero integer m where $P=(1/p^{\alpha}, \sqrt{f(1/p^{\alpha})})$.*

Proof. We exclude the prime $p=2$, the primes at which J, y_i, η_i have bad reduction and the primes p such that there exists a non p-unit a_{ij} for the matrix $A=(a_{ij})$. For a prime p, take an odd integer α sufficiently large so that in the expansion $\Psi(z_p)$, the term $-2z_p$ has smaller $\mathfrak{p}$-adic valuation than any other terms ($-2z$ is the smallest degree term in the expansions of the coordinates of $\Psi(z)$). We take α more large if necessary, so that the last coordinate of $(AF)^{-1}(\Psi(z_p))$ has $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}(z_p)$ (note that $AF(y)\equiv y \bmod \deg 2$). Suppose $m\Lambda(P)=Q$ was a $\boldsymbol{Q}$-rational point of J. Then the value Q_i of y_i at Q is a rational number. Hence $v_{\mathfrak{p}}(Q_i)$ is an even integer (for the $\mathfrak{p}$-adic valuation, $v_{\mathfrak{p}}(p)=2$). On the other hand it can be seen easily from what the above said, that some coordinate of $m\Lambda(P)=(AF)^{-1}(mA\Psi(P))$ has $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}(z_p)+v_{\mathfrak{p}}(m)$ which is an odd integer since $v_{\mathfrak{p}}(z_p)=\alpha$ is odd. This is a contradiction.

THEOREM. *Let $L=\boldsymbol{Q}(\sqrt{d}\mid d\in\boldsymbol{Z})$. Then the group of L-rational points $J(L)$ has an infinite rank over $\boldsymbol{Z}$.*

Proof. The proof is entirely similar to that of [1], Theorem 2.2. We include it for the convenience of reader. For a prime number p_i, put $c_i=p_i^{(2g+1)\alpha_i}f(1/P_i^{\alpha_i})$ as before, with α_i a sufficiently large odd integer. We take an infinite sequence of primes $\{p_n\}_{n=1}^{\infty}$ such that J and y_i, η_i have good reduction at p_n, and that $\boldsymbol{Q}(\sqrt{c_1/p_1}, \cdots, \sqrt{c_n/p_n})\cap\boldsymbol{Q}(\sqrt{c_{n+1}/p_{n+1}})=\boldsymbol{Q}$ for all n. For example, take inductively a prime p_{n+1} unramified in $\boldsymbol{Q}(\sqrt{c_1/p_1}, \cdots, \sqrt{c_n/p_n})/\boldsymbol{Q}$ with the above good reduction condition. Put $P_i=(1/p_i^{\alpha_i}, \sqrt{f(1/P_i^{\alpha_i})})$, then we claim that $\{\Lambda(P_i)\}_{i=1}^{\infty}$ are linearly independent over $\boldsymbol{Z}$. Suppose there was a relation $m_1\Lambda(P_1)+\cdots+m_n\Lambda(P_n)=0$ with $m_n\neq 0$. Write this as $m_1\Lambda(P_1)+\cdots+m_{n-1}\Lambda(P_{n-1})=-m_n\Lambda(P_n)$. The left hand side is $\boldsymbol{Q}(\sqrt{c_1/p_1}, \cdots, \sqrt{c_{n-1}/p_{n-1}})$-rational and the right hand side is $\boldsymbol{Q}(\sqrt{c_n/p_n})$-rational. Hence $m_n\Lambda(P_n)$ must be a $\boldsymbol{Q}$-rational point. This contradicts to Lemma 3.

REFERENCES

[1] G. FREY AND M. JARDEN, Approximation theory and the rank of abelian varieties over large algebraic number fields, Proc. London Math. Soc. 28 (1974), 112-128.

[2] T. HONDA, On the theory of commutative formal groups, J. Math. Soc. Japan, 22 (1970), 213-246.

[3] J-P. SERRE, Lie algebras and Lie group, Benjamin Inc. New York, (1965).

DEPARTMENT OF MATHEMATICS
COLLEGE OF GENERAL EDUCATION
TOHOKU UNIVERSITY
KAWAUCHI, SENDAI, JAPAN.