ACTA ARITHMETICA
LXIV.4 (1993)

Mordell–Weil rank of the jacobians of the curves defined by $y^p = f(x)$

by

Naoki Murabayashi (Tokyo)

1. Introduction. It is an interesting problem to study, for a given abelian variety A defined over a number field K, how the Mordell–Weil rank of $A(L)$ varies when L runs through finite extensions of K. Especially, it seems to be interesting to construct explicitly a sequence $\{L_n : n \geq 1\}$ of finite extensions of K such that $\operatorname{rank}(A(L_n))$ grows rapidly as n tends to infinity.

Recently Top ([4]) settled this problem for hyperelliptic curves C over $\mathbb{Q}$ with a $\mathbb{Q}$-rational point: he constructed explicitly infinitely many extensions of $\mathbb{Q}$ of the form $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_m})$ for which $\operatorname{rank}(J(L)) \geq \operatorname{rank}(J(\mathbb{Q})) + m$ where J denotes the jacobian variety of C.

On the other hand, it has been shown by Mazur that for any $\mathbb{Z}_l$-extension $L = \bigcup_{n=1}^{\infty} L_n$ of K, there exists a non-negative integer ϱ such that

$$\operatorname{rank}(A(L_n)) + \operatorname{corank}(H^1(\operatorname{Gal}(L/L_n), A(L))) = \varrho l^n + \text{const}$$

for sufficiently large n (see [1] or [2]). He also showed that under some conditions, $\varrho = 0$. Thus it seems not unlikely that if a sequence $\{L_n\}$ of finite l-abelian extensions of K satisfies the desired property, then the l-rank of $\operatorname{Gal}(L_n/K)$ must grow when n tends to infinity. The above result of Top ([4]) shows that this is indeed the case for the jacobians of hyperelliptic curves.

The purpose of this paper is to extend Top's result to the case of the superelliptic curves $y^p = f(x)$, where p is an arbitrary prime. In our case the fields are chosen among the Kummer extensions of exponent p.

2. Statement of the result. Our main theorem is the following:

Theorem. *Let p be a prime number, ζ_p a primitive p-th root of unity, and set $K = \mathbb{Q}(\zeta_p)$. Denote by $\mathfrak{O}_K$ the ring of integers of K. Let $f \in \mathfrak{O}_K[X]$ be a separable polynomial such that the degree of f, denoted by n, is prime to p and $\frac{1}{2}(p-1)(n-1) \geq 1$. Let C be a smooth projective model of the* *curve given by $y^p = f(x)$ and let J be the jacobian variety of C. For every $m \geq 1$ one can explicitly construct infinitely many extensions of K of the form $L = K(\sqrt[p]{d_1}, \ldots, \sqrt[p]{d_m})$ for which*

$$\mathrm{rank}(J(L)) \geq \mathrm{rank}(J(K)) + (p-1)m\,.$$

Remark 1. In the case of $p = 2$, this reduces to Top's theorem ([4]).

Remark 2. We can apply this theorem to the Fermat curve $F_p : x^p + y^p = 1$, where p is an odd prime number. In fact, putting $u := 1/(x-1)$ and $v := y/(x-1)$, F_p is birationally equivalent to the curve

$$v^p = -\prod_{i=1}^{p-1}((\zeta_p^i - 1)u - 1)\,.$$

In [5], Weil expressed the L-function $L(s, J_p/k)$ of the jacobian variety J_p of F_p over a number field k by means of Hecke L-functions. If the conjecture of Tate in [3] holds, for fields M constructed in the theorem $L(s, J_p/M)$ must have a zero at $s = 1$ of order $\geq (p-1)m$. So it is interesting to prove directly that $L(s, J_p/M)$ has a zero at $s = 1$ of order $\geq (p-1)m$. Because the action of $\mathbb{Z}[\zeta_p]$ on the Tate module of J_p commutes with the Galois action, this L-series is a $(p-1)$st power. So the factor $p-1$ in the conjectured order of vanishing is understood.

3. The proof of the theorem. Firstly we calculate the genus g of C. Consider the morphism $\theta : C \to \mathbb{P}^1$ defined by

$$\theta : (x, y) \mapsto x\,.$$

Let O be a point of C such that $\theta(O) = \infty$ and let e be the ramification index of θ at O. Then the rational function $f(x)$ on C has a pole at O of order en ($n = \deg(f)$). Since $y^p = f(x)$, p must divide en. By the assumption $(p, n) = 1$, $p \mid e$. Since θ is a Galois covering of degree p, $e = 1$ or p, hence $e = p$. So it follows that $\theta^{-1}(\infty) = \{O\}$ and $O \in C(K)$. Applying the Hurwitz formula, we have

$$g = \tfrac{1}{2}(p-1)(n-1) \geq 1\,.$$

The following two lemmas are proved by Top [4].

Lemma 1. *Let A be an abelian variety defined over a number field M and let $\mathfrak{q}$ be a prime ideal of M such that*

1. *$e_{\mathfrak{q}} < q - 1$, where $e_{\mathfrak{q}}$ is the ramification index of $\mathfrak{q}$ in $M/\mathbb{Q}$ and q is a prime number for which $\mathfrak{q} \mid (q)$,*
2. *A has good reduction at $\mathfrak{q}$.*

Then reduction modulo $\mathfrak{q}$ defines an injection

$$\varrho : A(M)_{\mathrm{torsion}} \to \overline{A}(M(\mathfrak{q}))\,,$$

with $\bar{A}$ denoting the reduction of A modulo $\mathfrak{q}$ and $M(\mathfrak{q})$ denoting the residue field of $\mathfrak{q}$.

LEMMA 2. *Let $F \in \mathfrak{O}_K[X]$ be a non-constant separable polynomial. There exist infinitely many prime ideals $\mathfrak{q}$ of K for which there is $d \in \mathfrak{O}_K$ with $\mathfrak{q} \mid F(d)$ and $\mathfrak{q}^2 \nmid F(d)$ (hence $\mathfrak{q}^p \nmid F(d)$).*

From now on, we fix once and for all a prime ideal $\mathfrak{q}$ of K such that

1. $(\mathfrak{q}, p) = 1$,
2. $f \bmod \mathfrak{q} \in K(\mathfrak{q})[x]$ is separable, i.e., C (and J) have good reduction modulo $\mathfrak{q}$,
3. $p < q - 1$, where q is a prime number for which $\mathfrak{q} \mid (q)$.

Define $F(X) := q^{pn} f(X + 1/q) \in \mathfrak{O}_K[X]$ ($n = \deg(f)$). We can find $d_1, \ldots, d_m \in \mathfrak{O}_K$ such that for $1 \le i \le m$ the fields $K_i := K(\sqrt[p]{F(d_i)})$ satisfy $K_i \ne K$, and for every i there is a prime ideal of K which ramifies in K_i/K but not in K_j/K for $1 \le j \le i - 1$. Indeed, by Lemma 2 there exists a prime ideal $\mathfrak{p}_1$ of K for which $(\mathfrak{p}_1, p) = 1$ and there is $d_1 \in \mathfrak{O}_K$ with $\mathfrak{p}_1 \mid F(d_1)$ and $\mathfrak{p}_1^p \nmid F(d_1)$. Put $K_1 := K(\sqrt[p]{F(d_1)})$. Then by the theory of Kummer extensions we see that $\mathfrak{p}_1$ ramifies in K_1/K. Again, by Lemma 2 there exists a prime ideal $\mathfrak{p}_2$ of K such that $(\mathfrak{p}_2, pF(d_1)) = 1$ and there is $d_2 \in \mathfrak{O}_K$ with $\mathfrak{p}_2 \mid F(d_2)$ and $\mathfrak{p}_2^p \nmid F(d_2)$. Put $K_2 := K(\sqrt[p]{F(d_2)})$. Then $\mathfrak{p}_2$ ramifies in K_2/K but not in K_1/K. Repeating this operation we can get $d_1, \ldots, d_m \in \mathfrak{O}_K$ which satisfy the desired condition. From the condition it follows that $K_i \cap K_j = K$ if $i \ne j$ and $K_i \cap \prod_{j \ne i} K_j = K$ for $1 \le i \le m$.

We define

$$P_i^{(j)} := (d_i + 1/q, \zeta_p^j \sqrt[p]{f(d_i + 1/q)}) \in C(K_i)$$

$(1 \le i \le m\,,\ 0 \le j \le p - 1)$ and

$$D_i^{(j)} := [P_i^{(j)} - O] \in \operatorname{Pic}^0(C)(K_i) = J(K_i)\,.$$

Consider the automorphism σ of C defined by

$$(x, y) \mapsto (x, \zeta_p y)$$

and define the endomorphism φ of J by

$$\varphi([D]) = [\sigma(D)]$$

where $D = \sum_R n_R R$ is a divisor of degree 0 on C and $\sigma(D) = \sum_R n_R \sigma(R)$. Let $\operatorname{End}(J)$ denote the endomorphism ring of J and put $\operatorname{End}^0(J) := \operatorname{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$. We define the $\mathbb{Q}$-algebra homomorphism

$$\Phi : \mathbb{Q}[T] \to \operatorname{End}^0(J)\,, \qquad T \mapsto \varphi\,.$$

Now we claim that

$$\operatorname{Ker} \Phi = (T^{p-1} + T^{p-2} + \ldots + 1)\,.$$

Indeed, for any $R = (x, y) \in C$, we have

$$(\varphi^{p-1} + \varphi^{p-2} + \ldots + 1)([R - O]) = [(x, y) + (x, \zeta_p y) + \ldots + (x, \zeta_p^{p-1} y) - pO] = [\mathrm{div}(z \circ \theta)] = 0$$

where z is a rational function on $\mathbb{P}^1$ for which $\mathrm{div}(z) = x - \infty$. Since $J = \mathrm{Pic}^0(C)$ is generated by the set $\{[R - O] : R \in C\}$,

$$(T^{p-1} + T^{p-2} + \ldots + 1) \subseteq \mathrm{Ker}\,\Phi\,.$$

The claim holds, because $\mathbb{Q}[T]$ is a P.I.D. and $T^{p-1} + T^{p-2} + \ldots + 1$ is irreducible in $\mathbb{Q}[T]$. So we get the injective $\mathbb{Q}$-algebra homomorphism, denoted by the same letter Φ:

$$\Phi : K \hookrightarrow \mathrm{End}^0(J)\,, \qquad \zeta_p \mapsto \varphi\,.$$

LEMMA 3. *$D_i^{(0)}, \ldots, D_i^{(p-2)}$ are independent points in $J(K_i)$ for $1 \le i \le m$.*

Proof. Suppose that they are not independent. Then there is a nontrivial relation

$$\lambda_0 D_i^{(0)} + \ldots + \lambda_{p-2} D_i^{(p-2)} = 0\,.$$

This implies that $\varphi'(D_i^{(0)}) = 0$ where $\varphi' := \lambda_0 + \lambda_1\varphi + \ldots + \lambda_{p-2}\varphi^{p-2} \in \mathrm{End}(J)$. Since $\varphi' \in \Phi(K^\times)$, φ' is a unit of $\mathrm{End}^0(J)$, i.e., an isogeny of J. Hence $\mathrm{Ker}\,\varphi'$ is finite, so $D_i^{(0)} \in J(K_i)_{\mathrm{torsion}}$. Let $\mathfrak{Q}_i$ be a prime ideal of K_i lying over $\mathfrak{q}$. Then $e_{\mathfrak{Q}_i} \le p < q-1$. Moreover, J has good reduction modulo $\mathfrak{Q}_i$ and $D_i^{(0)}$ mod $\mathfrak{Q}_i$ is the identity element of $\bar{J}$. By Lemma 1, $D_i^{(0)}$ is the identity element of J, i.e., there is a rational function w on C such that $\mathrm{div}(w) = P_i^{(0)} - O$. So C must be isomorphic to $\mathbb{P}^1$; this contradicts $g \ge 1$ and proves the lemma. ∎

Let $L := K_1 \cdot \ldots \cdot K_m$ and take a basis $Q_1, \ldots, Q_r$ of $J(K)$ modulo torsion. We show that $D_1^{(0)}, \ldots, D_1^{(p-2)}, \ldots, D_m^{(0)}, \ldots, D_m^{(p-2)}, Q_1, \ldots, Q_r$ are independent points in $J(L)$. We assume that there is a relation

$$\lambda_1^{(0)} D_1^{(0)} + \ldots + \lambda_1^{(p-2)} D_1^{(p-2)} + \ldots + \lambda_m^{(0)} D_m^{(0)} + \ldots + \lambda_m^{(p-2)} D_m^{(p-2)} + \mu_1 Q_1 + \ldots + \mu_r Q_r = 0\,.$$

Putting $D_i := \lambda_i^{(0)} D_i^{(0)} + \ldots + \lambda_i^{(p-2)} D_i^{(p-2)}$ $(1 \le i \le m)$, this implies that

$$D_1 = -D_2 - \ldots - \mu_r Q_r \in J(K_1 \cap K_2 \cdot \ldots \cdot K_m) = J(K)\,.$$

Let τ be the element of $\mathrm{Gal}(K_1/K)$ defined by

$$\tau : \sqrt[p]{f(d_1 + 1/q)} \mapsto \zeta_p \sqrt[p]{f(d_1 + 1/q)}\,.$$

Then since $D_1^{(0)} + \ldots + D_1^{(p-2)} + D_1^{(p-1)} = 0$ in J, we have

$$\begin{aligned} D_1^\tau &= \lambda_1^{(0)} D_1^{(1)} + \ldots + \lambda_1^{(p-3)} D_1^{(p-2)} + \lambda_1^{(p-2)} D_1^{(p-1)} \\ &= -\lambda_1^{(p-2)} D_1^{(0)} + (\lambda_1^{(0)} - \lambda_1^{(p-2)}) D_1^{(1)} + \ldots + (\lambda_1^{(p-3)} - \lambda_1^{(p-2)}) D_1^{(p-2)} . \end{aligned}$$

Since $D_1^\tau = D_1$, Lemma 3 implies that

$$\begin{aligned} \lambda_1^{(0)} &= -\lambda_1^{(p-2)} , \\ \lambda_1^{(1)} &= \lambda_1^{(0)} - \lambda_1^{(p-2)} , \\ &\vdots \\ \lambda_1^{(p-2)} &= \lambda_1^{(p-3)} - \lambda_1^{(p-2)} . \end{aligned}$$

Hence for

$$B := \begin{pmatrix} 1 & 0 \ldots\ldots\ldots\ldots & & 0 & 1 \\ -1 & 1 & 0 \ldots\ldots & 0 & 1 \\ 0 & -1 & 1 \quad 0 \ldots & 0 & 1 \\ \vdots & & \ddots \ddots & & \vdots \\ & & -1 & 1 & 1 \\ 0 \ldots\ldots\ldots & & 0 & -1 & 2 \end{pmatrix} \in M_{p-1}(\mathbb{Z}) ,$$

we have

$$B \begin{pmatrix} \lambda_1^{(0)} \\ \lambda_1^{(1)} \\ \vdots \\ \lambda_1^{(p-2)} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} .$$

LEMMA 4. $\det B = p$.

P r o o f. For any integer $h \geq 1$ let $B^{(h)}$ be the $h \times h$ matrix defined as above. By induction on h we prove that $\det B^{(h)} = h + 1$. In case $h = 1$, since $B^{(1)} = (2)$, the claim is true. Assuming $\det B^{(h-1)} = h$, we have

$$\det B^{(h)} = \det B^{(h-1)} + \det \left.\begin{pmatrix} 0 \ldots\ldots\ldots\ldots & & 0 & 1 \\ -1 & 1 \quad 0 \ldots & 0 & 1 \\ 0 & \ddots \ddots & & \vdots \\ \vdots & -1 & 1 & 1 \\ 0 \ldots\ldots & 0 & -1 & 2 \end{pmatrix}\right\} h-1 \text{ rows}$$

$$= \ldots = \det B^{(h-1)} + \det \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} = h + 1 .$$

Hence the claim holds. So $\det B = \det B^{(p-1)} = p$. This completes the proof of the lemma. ■

By Lemma 4, it follows that

$$\lambda_1^{(0)} = \ldots = \lambda_1^{(p-2)} = 0\,.$$

By the same reasoning,

$$\lambda_i^{(0)} = \ldots = \lambda_i^{(p-2)} = 0$$

for every i. Moreover, by the choice of $Q_1, \ldots, Q_r$, we have

$$\mu_1 = \ldots = \mu_r = 0\,.$$

Hence our relation is trivial. This proves the theorem.

References

[1] Yu. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys 26 (6) (1971), 7–78.

[2] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. 18 (1972), 183–266.

[3] H. P. F. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, in: Proceedings of a conference on local fields (Driebergen, 1966), Springer, 1967, 132–157.

[4] J. Top, *A remark on the rank of jacobians of hyperelliptic curves over* $\mathbb{Q}$ *over certain elementary abelian* 2*-extensions*, Tôhoku Math. J. 40 (1988), 613–616.

[5] A. Weil, *Jacobi sums as Grössencharaktere*, Trans. Amer. Math. Soc. 73 (1952), 487–495.

DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCE AND ENGINEERING
WASEDA UNIVERSITY
3-4-1, OKUBO SHINJUKU-KU, TOKYO
169 JAPAN

Received on 28.7.1992
and in revised form on 21.1.1993 (2287)