Tôhoku Math. J.
40 (1988), 613-616.

A REMARK ON THE RANK OF JACOBIANS OF HYPERELLIPTIC CURVES OVER Q OVER CERTAIN ELEMENTARY ABELIAN 2-EXTENSIONS

JAAP TOP*

(Received June 8, 1987)

1. Introduction. A nice question in arithmetic geometry is whether for a given abelian variety A over a number field K, relatively small extensions $L \supset K$ exist such that $\mathrm{rank}(A(L))$ is "much" bigger than $\mathrm{rank}(A(K))$. Already in 1938, Billing (see [5; p. 157] for a reference) showed that the elliptic curve $E/\boldsymbol{Q}$ given by the equation $y^2 = x^3 - x$ has rank at least m over infinitely many fields of the form $\boldsymbol{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$.

Also Néron studied these matters; his result is (see [5; p. 157]):

FACT. Given a hyperelliptic curve $\mathscr{C}$ over a number field K and a point $P \in \mathscr{C}(K)$, there exist infinitely many extensions of K of the form $L = K(\sqrt{d_1}, \cdots, \sqrt{d_m})$ such that $\mathrm{rank}(\mathscr{J}(\mathscr{C})(L)) \geqq m$.

Néron uses a specialization argument to prove this. Our aim in this paper is to show that it is quite easy to construct such extensions explicitly without using any deep theory.

2. Statement of the result and preliminaries. We give a proof of the following:

THEOREM. *Let $f \in \boldsymbol{Z}[X]$ be a separable polynomial of odd degree $\geqq 3$. Let $\mathscr{C}$ be a smooth model of the curve given by $y^2 = f(x)$ and let $\mathscr{J}$ be the jacobian of $\mathscr{C}$. For every $m \geqq 1$ one can explicitly construct infinitely many extensions of $\boldsymbol{Q}$ of the form $K = \boldsymbol{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$ for which* $\mathrm{rank}(\mathscr{J}(K)) \geqq \mathrm{rank}(\mathscr{J}(\boldsymbol{Q})) + m$.

The proof (which in fact works with $\boldsymbol{Q}$ replaced by any number field) is based on the simple observation that we have a degree two morphism $\mathscr{C} \to \boldsymbol{P}^1$ defined over $\boldsymbol{Q}$. If $x \in \boldsymbol{P}^1(\boldsymbol{Q})$, then the fiber over x in general consists of two points defined over a quadratic extension of $\boldsymbol{Q}$. The class of one such point minus the point lying over infinity yields a point in $\mathscr{J}(\mathscr{C})$. The only thing we have to check is that we can choose the points in $\boldsymbol{P}^1(\boldsymbol{Q})$ in such a way that the points in $\mathscr{J}(\mathscr{C})$ we obtain are linearly

* Supported by the Dutch Organization for the Advancement of Pure Research (ZWO).

independent of everything we already have. This will follow from the such following fact:

There are infinitely many ways to choose points $x_1, \cdots, x_m \in \boldsymbol{P}^1(\boldsymbol{Q})$ that

1. the fields $\boldsymbol{Q}(\sqrt{f(x_i)})$ are linearly disjoint, and
2. the points in $\mathscr{J}(\mathscr{C})(\bar{\boldsymbol{Q}})$ we construct are non-torsion.

To prove this fact we will use two lemmas.

LEMMA 1. *Let $A/\boldsymbol{Q}$ be an abelian variety; suppose $p \in \boldsymbol{Z}$, $p \neq 2$ is a prime number such that A has good reduction at p. Then reduction modulo p defines an injection*

$$\rho: A(\boldsymbol{Q})_{\text{torsion}} \to \bar{A}(\boldsymbol{F}_p) ,$$

with $\bar{A}$ denoting the reduction of A modulo p.

PROOF. If not, then there exists a point $P \in A(\boldsymbol{Q})$ of prime order q which reduces to zero. Extending $A \to \operatorname{Spec}(\boldsymbol{Q})$ to an abelian scheme $\mathscr{A} \to \operatorname{Spec}(\boldsymbol{Z}_{(p)})$, and using the fact that multiplication by q: $\mathscr{A} \to \mathscr{A}$ is flat, it follows that the closure of the subgroup in $A(\boldsymbol{Q})$ generated by P defines a finite flat group scheme of rank q, say $\mathscr{N} \to \operatorname{Spec}(\boldsymbol{Z}_{(p)})$. The specialization lemma [3; p. 135] now implies that $\operatorname{ord}(P) = \operatorname{ord}(\rho(P))$, a contradiction. □

LEMMA 2. *Let $F \in \boldsymbol{Z}[X]$ be a non-constant separable polynomial. There exist infinitely many prime numbers $p \in \boldsymbol{Z}$ for which there is an $n \in \boldsymbol{Z}$ with $p \mid F(n)$ and $p^2 \nmid F(n)$.*

PROOF. Let $\Delta \in \boldsymbol{Z}$ be the discriminant of F. By assumption, $\Delta \neq 0$. Suppose p is a prime such that $p \nmid \Delta$ and $p^2 \mid F(n)$ for some n. Since $F(n + p) \equiv pF'(n) \bmod p^2$ and $F'(n) \not\equiv 0 \bmod p$ by the choice of p, we have $p \mid F(n + p)$ and $p^2 \nmid F(n + p)$. Thus the lemma will follow once we know that the set

$$\{p \in \boldsymbol{Z} \text{ prime}; \ p \mid F(n) \text{ for some } n\}$$

is infinite. This follows from [4; Appendix I, Lemma 5.5], or [6; pp. 2.7-2.8], or from the following counting argument: Suppose this set is finite, say equal to $\{p_1, \cdots, p_k\}$. Then for $N \gg 0$:

$$\begin{aligned} \#\{F(n); \ |F(n)| \leqq N\} &\leqq 1 + 2\#\{m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}; \ m \leqq N\} \\ &= 1 + 2\#\{m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}; \ \textstyle\sum \alpha_i \log p_i \leqq \log N\} \leqq \text{const} \cdot (\log N)^k , \end{aligned}$$

while on the other hand

$$\#\{F(n); \ |F(n)| \leqq N\} \geqq \text{const} \cdot N^{1/d}$$

for $d = \deg(F)$ and positive constants independent of N. This yields a contradiction. □

3. The proof. We use the notation introduced at the beginning of Section 2. Fix once and for all a prime number $p \in \boldsymbol{Z}$, $p > 2$ for which $f \bmod p$ is separable, i.e., $\mathscr{C}$ (and $\mathscr{J} = \mathscr{J}(\mathscr{C})$) have good reduction modulo p. Define $F(X) := p^{d+1} f(X + 1/p) \in \boldsymbol{Z}[X]$ $(d = \deg(f))$. Applying Lemma 2, we can find $n_1, \cdots n_m \in \boldsymbol{Z}$ such that for $1 \leqq i \leqq m$ the fields $K_i := \boldsymbol{Q}(\sqrt{F(n_i)})$ satisfy $K_i \neq \boldsymbol{Q}$, and for every i there is a prime which ramifies in K_i but in none of the others. From this we deduce $K_i \cap K_j = \boldsymbol{Q}$ if $i \neq j$.

The curve $\mathscr{C}$ is equipped with a K_i-rational point P_i, namely the point corresponding to $(n_i + 1/p, \sqrt{f(n_i + 1/p)})$ on $y^2 = f(x)$. Letting O denote the point in $\mathscr{C}(\boldsymbol{Q})$ corresponding to the point at infinity on the plane model, we define

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

Let $K := K_1 \cdot \ldots \cdot K_m$ and take a basis $Q_1, \cdots, Q_r$ of $\mathscr{J}(\boldsymbol{Q})$ modulo torsion. We claim that $D_1, \cdots, D_m, Q_1, \cdots, Q_r$ are independent points in $\mathscr{J}(\boldsymbol{Q})$. Suppose not. Then there is a relation

$$\lambda_1 D_1 + \cdots + \lambda_m D_m + \mu_1 Q_1 + \cdots + \mu_r Q_r = 0 .$$

This implies that $\lambda_1 D_1 = -\lambda_2 D_2 - \cdots - \mu_r Q_r$ is rational over $K_1 \cap K_2 \cdot \ldots \cdot K_m = \boldsymbol{Q}$.

Let $\mathscr{J}^1$ denote "the" quadratic twist of $\mathscr{J}$ over K_1; this is just the jacobian of the curve $F(n_1)y^2 = f(x)$. From the commutative diagram

$$\begin{array}{ccc} \mathscr{J}(K_1) & \xrightarrow{\text{twist}} & \mathscr{J}^1(K_1) \\ \downarrow{\scriptstyle [\lambda_1]} & & \downarrow{\scriptstyle [\lambda_1]} \\ \mathscr{J}(K_1) & \xrightarrow{\text{twist}} & \mathscr{J}^1(K_1) \end{array}$$

it now follows that both $\lambda_1 D_1$ and its image under twisting are $\boldsymbol{Q}$-rational (since the nontrivial element of $\mathrm{Gal}(K_1/\boldsymbol{Q})$ acts on D_1 by multiplication by -1). Hence $\lambda_1 D_1$ is a torsion point (of order $\leqq 2$), so in particular if $\lambda_1 \neq 0$ then D_1 is a torsion point. This contradicts Lemma 1 if we reduce modulo p. Hence we deduce $\lambda_1 = 0$, and by the same reasoning $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$, so by the choice of the Q_i's, our relation is trivial. This proves the theorem. □

REMARK 1. Recently Chahal [1] published a proof of the theorem above in the case $\deg(f) = 3$, i.e., $\mathscr{C}$ is an elliptic curve. His proof depends on a highly nontrivial result of Ribet, and also I cannot find

an argument in his paper explaining why the points that are constructed are actually independent.

REMARK 2. In concrete examples elementary abelian 2-extensions of Q as above which are needed to increase the rank by a given amount may have a much smaller degree. For example, let E/Q be the elliptic curve given by $y^2 = x^3 - x$. Take $x_i \in Z$, $x_i > 1$, $x_i \equiv 6 \bmod 8$ in such a way that for $d_i := x_i^3 - x_i$, the fields $Q(\sqrt{d_i})$ are linearly disjoint. Then $\operatorname{rank}(E(Q(\sqrt{d_i}))) \geqq 1$. The conjecture of Birch and Swinnerton-Dyer predicts that this rank is even (compare [2; p. 84]). So one expects

$$\operatorname{rank} E(Q(\sqrt{d_1}, \cdots, \sqrt{d_m})) \geqq 2m .$$

REFERENCES

[1] J. S. CHAHAL, The Mordell-Weil rank of elliptic curves, Tôhoku Math. J. 39 (1987), 101–103.
[2] N. KOBLITZ, Introduction to Elliptic Curves and Modular Forms, GTM 97, Springer-Verlag, 1984.
[3] B. MAZUR, Rational isogenies of prime degree, Invent. Math. 44 (1978), 129–162.
[4] D. MUMFORD, Abelian Varieties, Oxford Univ. Press, 1974.
[5] A. NÉRON, Problémes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, Bull. Soc. Math. France 80 (1952), 101–166.
[6] J. P. SERRE, Autour du théorème de Mordell-Weil II, Publ. Math. de l'Université Pierre et Marie Curie, 1981.

MATHEMATICAL INSTITUTE
UNIVERSITY OF UTRECHT
BOX 80.010
3508 TA UTRECHT
THE NETHERLANDS