J. Math. Soc. Japan
Vol. 32, No. 4, 1980

On the relative Mordell-Weil rank of elliptic quartic curves

By Takashi ONO

(Received Jan. 9, 1979)

Let A be an abelian variety defined over a number field k of finite degree over the rationals $\boldsymbol{Q}$. For a finite extension K of k, let A_K be the group of points of A rational over K. As is well-known, the group A_K is finitely generated [L]. For any finitely generated abelian group G, let $\mathrm{rk}(G)$ be the rank of G. We put $\rho_K(A)=\mathrm{rk}(A_K)$, the Mordell-Weil rank of A with respect to K. By the relative Mordell-Weil rank of A with respect to K/k, we shall mean the difference $\rho_{K/k}(A)=\rho_K(A)-\rho_k(A)$.

In this paper, we shall study this quantity when A is an elliptic quartic curve and K/k is a quadratic extension. Among elliptic curves under consideration, the curve $E(\kappa)$ for non-zero $\kappa\in k$ defined by equations

$$\begin{cases} X_0^2+\kappa X_1^2=X_2^2, \\ X_0^2-\kappa X_1^2=X_3^2 \end{cases}$$

has multiple interests. For example, we shall show that

$$\rho_{k(\sqrt{\lambda})/k}(E(\kappa))=\rho_{k(\sqrt{\kappa})/k}(E(\lambda))$$

whenever κ, λ are non-square elements of k. Next, let $k=\boldsymbol{Q}$, and let κ be a square free natural number. Then we shall obtain the relations

$$\rho_K(E(\kappa))=\rho_{\boldsymbol{Q}}(E(\kappa)) \quad \text{when} \quad K=\boldsymbol{Q}(\sqrt{\kappa}) \quad \text{or} \quad \boldsymbol{Q}(\sqrt{-\kappa}),$$

$$\rho_K(E(\kappa))=2\rho_{\boldsymbol{Q}}(E(\kappa)) \quad \text{when} \quad K=\boldsymbol{Q}(\sqrt{-1}).$$

In the Appendix, I have collected miscellaneous facts and comments on the (absolute) Mordell-Weil rank $\rho_{\boldsymbol{Q}}(\kappa)$ of $E(\kappa)$ where κ is a square free natural number.

1. We begin with a single lemma on any abelian variety. Let A be an abelian variety defined over a number field k. Assume that K/k is a finite galois extension with the galois group G. We then consider the homomorphism $T_{K/k}\colon A_K\to A_k$ defined by $T_{K/k}(x)=\sum_{\sigma\in G}x^\sigma$, the trace.

(1.1) LEMMA. $\rho_{K/k}(A)=\mathrm{rk}(\mathrm{Ker}\, T_{K/k})$.

PROOF. Let m be the degree of K/k. Since $mA_k \subset \mathrm{Im}\, T_{K/k}$ and A_k/mA_k is finite, we have

$$\rho_k(A)=\mathrm{rk}(\mathrm{Im}\, T_{K/k})=\rho_K(A)-\mathrm{rk}(\mathrm{Ker}\, T_{K/k}), \qquad \text{q. e. d.}$$

2. Let k be a number field. Denote by $k^{\times}$ the set of non-zero elements of k. For $M, N \in k^{\times}$ such that $M \neq N$, we shall denote by $E(M, N)$ the set of points in the projective space defined by the equations

$$\text{(2.1)} \qquad \begin{cases} X_0^2+MX_1^2=X_2^2, \\ X_0^2+NX_1^2=X_3^2. \end{cases}$$

The set $E(M, N)$ becomes an abelian variety of dimension 1. The addition $z=x+y$ on A is described as follows. The homogeneous coordinates of the sum of $x=(x_0, x_1, x_2, x_3)$ and $y=(y_0, y_1, y_2, y_3)$ is $z=(z_0, z_1, z_2, z_3)$ where

$$\text{(2.2)} \qquad \begin{cases} z_0=x_0^2y_0^2-MNx_1^2y_1^2=x_0x_1y_2y_3-x_2x_3y_0y_1, \\ z_1=x_0x_1y_2y_3+x_2x_3y_0y_1=x_1^2y_0^2-x_0^2y_1^2, \\ z_2=x_0x_2y_0y_2+Mx_1x_3y_1y_3=x_1x_2y_0y_3-x_0x_3y_1y_2, \\ z_3=x_0x_3y_0y_3+Nx_1x_2y_1y_2=x_1x_3y_0y_2-x_0x_2y_1y_3. \end{cases}$$

This means that for any points $x, y \in E(M, N)$, at least one of the expressions of z is available and they represent the same point when both are available.*) The zero element is $0=(1, 0, 1, 1)$ and the inverse of x is $-x=(x_0, -x_1, x_2, x_3)$. We call x trivial if $x_1=0$. There are 4 trivial points: $(1, 0, \pm 1, \pm 1)$. They form a group isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$, where $\boldsymbol{Z}$ denotes the ring of integers. Since $M, N \in k$, $E(M, N)$ is defined over k. Let K be a quadratic extension of k. Assume that $K=k(\theta)$ with $\theta^2=m \in k$. Let σ be the conjugation of the field extension K/k.

(2.3) PROPOSITION. *There is a group isomorphism*

$$E(mM, mN)_k \approx \mathrm{Ker}\, T_{K/k}.$$

PROOF. First, consider the map $\varphi: E(mM, mN) \rightarrow E(M, N)$ defined by $\varphi(x)=(\theta^{-1}x_0, x_1, \theta^{-1}x_2, \theta^{-1}x_3)$. Since φ is an isomorphism of varieties defined over K sending the zero to the zero, by a well-known property of abelian varieties, φ becomes a group isomorphism. Let φ_k be the restriction of φ on $E(mM, mN)_k$. We must now show that $\mathrm{Im}\, \varphi_k=\mathrm{Ker}\, T_{K/k}$. Since 4 trivial points are contained

*) When the universal domain is the field of complex numbers, $E(M, N)$ is naturally parametrized by Jacobi theta-functions $\theta_i(\tau|v)$, $0 \leqq i \leqq 3$, with suitable τ determined by M, N, and the relations (2.2) are nothing but the addition theorems for these functions. Cf. Formules (LVI_i), $1 \leqq i \leqq 5$, Chapitre III, Tome II of [**T-M**].

in both sides of the equality, we shall consider only non-trivial point $y=(y_0, 1, y_2, y_3)$. We then have

$$
\begin{aligned}
y\in \mathrm{Ker}\, T_{K/k} &\Leftrightarrow y^{\sigma}=-y \\
&\Leftrightarrow (y_0^{\sigma}, 1, y_2^{\sigma}, y_3^{\sigma})=(y_0, -1, y_2, y_3) \\
&\Leftrightarrow (y_0^{\sigma}, 1, y_2^{\sigma}, y_3^{\sigma})=(-y_0, 1, -y_2, -y_3) \\
&\Leftrightarrow y_0=z_0\theta,\ y_2=z_2\theta,\ y_3=z_3\theta, \quad z_0, z_2, z_3\in k \\
&\Leftrightarrow y=\varphi_k(x) \quad \text{with } x=(mz_0, 1, mz_2, mz_3)\in E(mM, mN)_k\,,
\end{aligned}
$$

which completes the proof.

Combining (1.1) and (2.3), we get the following

(2.4) THEOREM. *Let k be a finite algebraic number field, $E(M, N)$ be the elliptic curve defined by* (2.1) *with $M, N\in k^{\times}$, $M\neq N$, and $k(\sqrt{m})$ be a quadratic extension of k, $m\in k$. Then, we have*

$$\rho_{k(\sqrt{m})/k}(E(M, N))=\rho_k(E(mM, mN))\,.$$

3. For a number $\kappa\in k^{\times}$, we put $E(\kappa)=E(\kappa, -\kappa)$. Since all invariants of $E(\kappa)$ depend only on κ, we shall simply write $\rho_K(\kappa)$, $\rho_{K/k}(\kappa)$ instead of $\rho_K(E(\kappa))$, $\rho_{K/k}(E(\kappa))$, respectively. In the multiplicative group $k^{\times}$, we write $a\sim b$ when $ab^{-1}\in(k^{\times})^2$. When $\kappa\sim\lambda$, there is, obviously, a group isomorphism $E(\kappa)\approx E(\lambda)$ defined over k. We also have a group isomorphism $E(-\kappa)\approx E(\kappa)$ defined over k. In terms of ranks, we have, for a finite extension K/k,

$$\rho_K(\lambda)=\rho_K(\kappa) \quad \text{if} \quad \lambda\sim\kappa \quad \text{in } k\,, \tag{3.1}$$

$$\rho_K(-\kappa)=\rho_K(\kappa)\,. \tag{3.2}$$

As a special case of (2.4), we have

$$\rho_{k(\sqrt{\lambda})/k}(\kappa)=\rho_k(\lambda\kappa) \quad \text{for } \lambda\nsim 1. \tag{3.3}$$

Since the right hand side of the equality in (3.3) is symmetric in κ and λ, we have the "reciprocity":

$$\rho_{k(\sqrt{\lambda})/k}(\kappa)=\rho_{k(\sqrt{\kappa})/k}(\lambda) \quad \text{for } \lambda\nsim 1,\ \kappa\nsim 1. \tag{3.4}$$

(3.5) If $-1\nsim 1$ in k, then $\rho_{k(\sqrt{-1})}(\kappa)=2\rho_k(\kappa)$.

In fact, by (3.2), (3.3), we have $\rho_{k(\sqrt{-1})/k}(\kappa)=\rho_k(-\kappa)=\rho_k(\kappa)$, q. e. d.

(3.6) If $\lambda\nsim 1$, $-\lambda\nsim 1$, then $\rho_{k(\sqrt{\lambda})/k}(\kappa)=\rho_{k(\sqrt{-\lambda})/k}(\kappa)$.

In fact, by (3.2), (3.3), we have $\rho_{k(\sqrt{\lambda})/k}(\kappa)=\rho_k(\lambda\kappa)=\rho_k(-\lambda\kappa)=\rho_{k(\sqrt{-\lambda})/k}(\kappa)$, q. e. d.

Now, if κ, $-\kappa\nsim 1$, then we have, by (3.1), (3.3), (3.6),

$$\rho_{k(\sqrt{\kappa})/k}(\kappa)=\rho_{k(\sqrt{-\kappa})/k}(\kappa)=\rho_k(1)\,. \tag{3.7}$$

Suppose, in particular, that $k=\boldsymbol{Q}$ and that κ is a square free natural number. As is well-known, we have $\rho_{\boldsymbol{Q}}(1)=0$ (Fibonacci-Fermat). Therefore, (3.5) and (3.7) imply that

(3.8)
$$\rho_K(\kappa)=2\rho_{\boldsymbol{Q}}(\kappa) \quad \text{when } K=\boldsymbol{Q}(\sqrt{-1}),$$
$$\rho_K(\kappa)=\rho_{\boldsymbol{Q}}(\kappa) \quad \text{when } K=\boldsymbol{Q}(\sqrt{\kappa}) \text{ or } \boldsymbol{Q}(\sqrt{-\kappa}).$$

Appendix.

(I) The torsion subgroup.

In the Appendix, we consider the case $k=\boldsymbol{Q}$ only and collect some results on the (absolute) Mordell-Weil rank $\rho_{\boldsymbol{Q}}(\kappa)$ of the elliptic curve $E(\kappa)$, where κ being a square free natural number. We begin with the determination of the torsion subgroup $E_t(\kappa)_{\boldsymbol{Q}}$ of $E(\kappa)_{\boldsymbol{Q}}$. We first remark that, in (2.2), since x_0, $y_0\neq 0$ for $k=\boldsymbol{Q}$, the first expression for the addition $z=x+y$ in the group $E(\kappa)_{\boldsymbol{Q}}$ is always available. Each point of $E(\kappa)_{\boldsymbol{Q}}$ can be represented by the coordinates $x=(x_0, x_1, x_2, x_3)$ where all $x_i\in\boldsymbol{Z}$ and g. c. d. of x_i is 1. We shall call such coordinates primitive. The primitive coordinates of a point are uniquely determined up to ± 1. We denote by $E_0(\kappa)_{\boldsymbol{Q}}$ the set of trivial points, i. e. the points with $x_1=0$. It consists of 4 points $(1, 0, \pm 1, \pm 1)$ and forms a group isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$.

(I. 1) THEOREM. *$E_t(\kappa)_{\boldsymbol{Q}}=E_0(\kappa)_{\boldsymbol{Q}}$. In other words, $\rho_{\boldsymbol{Q}}(\kappa)>0$ if $E(\kappa)_{\boldsymbol{Q}}$ contains a non-trivial point.*

We need two lemmas: (I. 2), (I. 3). (I. 2) is needed to prove the first half of (I. 3). The proof of lemmas is left to readers as an exercise.

(I. 2) LEMMA. *If $x=(x_0, x_1, x_2, x_3)\in E(\kappa)_{\boldsymbol{Q}}$ is non-trivial, then all $x_i\neq 0$.*

(I. 3) LEMMA. *If $x=(x_0, x_1, x_2, x_3)$ is non-trivial and primitive, then $2x=(x_0^4+\kappa^2x_1^4, 2x_0x_1x_2x_3, x_0^2x_2^2+\kappa x_1^2x_3^2, x_0^2x_3^2-\kappa x_1^2x_2^2)$ is also non-trivial and primitive.*

PROOF OF (I. 1). It is enough to show that any non-trivial x is not a torsion element. Assuming $x=(x_0, x_1, x_2, x_3)$ primitive, put $\mu(x)=|x_1|$. By (I. 3), $2x$ is non-trivial and primitive, and so we have $\mu(x)=|x_1|<\mu(2x)=2|x_0||x_1||x_2||x_3|$. In this way, we obtain an ascending sequence

$$\mu(x)<\mu(2x)<\mu(2^2x)<\mu(2^3x)<\cdots,$$

which shows that x is not a torsion element, q. e. d.

(II) To find κ with $\rho_{\boldsymbol{Q}}(\kappa)>0$.

In view of (I. 1), to get a number κ with $\rho_{\boldsymbol{Q}}(\kappa)>0$, it is enough to find a non-trivial point of $E(\kappa)_{\boldsymbol{Q}}$. A practical method for this is to take a Pythagorean pair $\{a, b\}$, i. e. natural numbers a, b such that $a>b$, $(a, b)=1$ and $a\not\equiv b \pmod 2$, and call κ the square free number such that

(II. 1)
$$\kappa c^2=ab(a^2-b^2), \quad c\in\boldsymbol{N}.$$

Then, $x=(a^2+b^2, 2c, a^2-b^2+2ab, a^2-b^2-2ab)$ is a non-trivial point of $E(\kappa)_Q$. What is important is that conversely one can associate a Pythagorean pair $\{a, b\}$ to any non-trivial point $x=(x_0, x_1, x_2, x_3)\in E(\kappa)_Q$. Observe first that x_1 is even but all x_0, x_2, x_3 are odd and that $(x_i, x_j)=1$, $i\neq j$. Put $X_i=|x_i|$. Next, put $a=(1/2(X_0+1/2(X_2\mp X_3)))^{1/2}$, $b=(1/2(X_0-1/2(X_2\mp X_3)))^{1/2}$ according as $1/2(X_2\pm X_3)$ is even. One then verifies that $\{a, b\}$ is a Pythagorean pair satisfying (II. 1) with $c=(1/2)X_1$. We have therefore proved that

(II. 2) $$\rho_Q(\kappa)>0\Leftrightarrow\kappa\sim ab(a^2-b^2) \text{ for a Pythagorean pair } \{a, b\}.$$

(III) To prove that $\rho_Q(\kappa)=0$ for some κ.

The criterion (II. 2), together with its proof, can be used to prove that $\rho_Q(\kappa)=0$ for a certain κ. In fact, starting with a non-trivial primitive x of $E(\kappa)_Q$, if any, construct the Pythagorean pair as above. Then, we have $\kappa((1/2)x_1)^2=ab(a^2-b^2)$. Now, among many distributions of factors of κ as factors of a, b, (a^2-b^2), if $\kappa|b$ is the only possibility, then we have $a=y_0^2$, $b=\kappa y_1^2$, $a+b=y_2^2$, $a-b=y_3^2$, which implies that $\mu(y)<\mu(x)$, i.e. the method of infinite decent works. For example, the matter is trivial when $\kappa=1$ and hence $\rho_Q(1)=0$ (Fibonacci-Fermat). Let $\kappa=2$: $2c^2=ab(a^2-b^2)$. If $2|a$, then $a^2-b^2\equiv-1 \pmod 4$ cannot be square. On the other hand, $2\nmid(a^2-b^2)$ because $a\not\equiv b \pmod 2$, and so $2|b$ is the only possibility, i.e. $\rho_Q(2)=0$. Next, let κ be a prime $p\equiv3 \pmod 8$: $pc^2=ab(a^2-b^2)$. If $p|a$, then we have $a=px^2$, $b=y^2$ and so $px^2+y^2=u^2$, $px^2-y^2=v^2$. The last equality implies that $\left(\frac{-1}{p}\right)=+1$ which contradicts $p\equiv3 \pmod 8$. Similarly $p\nmid(a+b)$. Finally, if $p|(a-b)$, then we have $a=x^2$, $b=y^2$ and so $x^2+y^2=u^2$, $x^2-y^2=pv^2$, which implies that $2x^2\equiv u^2 \pmod p$, i.e. $\left(\frac{2}{p}\right)=1$, a contradiction, again. Hence $p|b$ is the only possibility, i.e. $\rho_Q(p)=0$ when $p\equiv3 \pmod 8$, a prime. By a similar but a little more complicated argument, one can prove that $\rho_Q(\kappa)=0$ if $\kappa=2q$, q a prime$\equiv5 \pmod 8$; $\kappa=p_1p_2$, p_i a prime$\equiv3 \pmod 8$; $\kappa=2q_1q_2$, q_i a prime$\equiv5 \pmod 8$.

(IV) An observation.

Among natural numbers less than 100 there are 61 square free numbers and among the latter $\rho_Q(\kappa)=0$ for 25 values: $\kappa=1$, 2, 3, 10, 11, 17, 19, 26, 33, 35, 42, 43, 51, 57, 58, 59, 66, 67, 73, 74, 82, 83, 89, 91, 97 and $\rho_Q(\kappa)>0$ for 36 values: $\kappa=5$, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47, 53, 55, 61, 62, 65, 69, 70, 71, 77, 78, 79, 85, 86, 87, 93, 94, 95.*)

Limiting ourselves to odd primes, we obtain the following table:

*) I learned this list of numbers from [**B**] p. 155. Not all of the list can be explained immediately by the methods or facts mentioned in (II), (III): in fact, to use the criterion (II.2) for this purpose the ordinary 12-digit desk calculator is too small.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
mod 8	3	5	7	3	5	1	3	7	5	7	5	1	3	7
$\rho_Q(p)$	0	+	+	0	+	0	0	+	+	+	+	+	0	+

p	53	59	61	67	71	73	79	83	89	97
mod 8	5	3	5	3	7	1	7	3	1	1
$\rho_Q(p)$	+	0	+	0	+	0	+	0	0	0

If $p \equiv 3 \pmod 8$, then $\rho_Q(p)=0$ as we proved in (III). When $p \equiv 1 \pmod 8$, both cases can happen: in fact, $\rho_Q(p)=0$ for $p=17, 73, 89, 97$ but $\rho_Q(41)>0$ because $41c^2=ab(a^2-b^2)$ for the Pythagorean pair $\{a, b\}=\{5^2, 4^2\}$ and $c=60$. On the other hand, one observes that $\rho_Q(p)>0$ for all $p<100$ such that $p\equiv 5$ or $7 \pmod 8$. It is natural to guess that this is true for all $p \equiv 5$ or $7 \pmod 8$.

References

[L] S. Lang, Diophantine Geometry, Interscience Publishers, New York, 1962.

[T-M] J. Tannery and J. Molk, Eléments de la Théorie des Fonctions Elliptiques, 4 vols., Paris, Gauthiers-Villars, 1896.

[B] A. Beiler, Recreations in the Theory of Numbers, Dover Publications, New York 1966.

Takashi ONO

Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland 21218
U.S.A.