96. On the Rank of an Elliptic Curve in Elementary 2-extensions

By Masanari KIDA

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

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 13, 1993)

1. Let E be an elliptic curve (i.e., an abelian variety of dimension one) defined over an algebraic number field k. For any finite field extension K of k, we denote by $E(K)$ the group of K-rational points of E. We define *the Mordell-Weil rank over* K *of* E *by*

$$\mathrm{rank}(E\,;K) = \dim_{\boldsymbol{Q}} E(K) \otimes_{\boldsymbol{Z}} \boldsymbol{Q},$$

which is known to be finite.

The extension K/k is called an *elementary* 2-*extension* if it is a (Galois) (pro-) 2-extension with the Galois group of exponent 2.

This note grew out of an effort to generalize Ono's theorem [7] on the relative Mordell-Weil rank (his $E(\kappa)$ is our E_κ) and its aim is to construct elliptic curves whose Mordell-Weil rank becomes infinite in a tower of elementary 2-extensions.

We should note here that Kurčanov ([4],[5]) constructed elliptic curves defined over $\boldsymbol{Q}$ whose ranks are infinite or stable in a $\boldsymbol{Z}_p$-extension based on the theory of Mazur.

2. Let k be an algebraic number field and suppose we are given a (finite or infinite) subset $\Sigma = \{d_\lambda\}_{\lambda\in\Lambda}$ of $k^\times/(k^\times)^2$. We can assign a quadratic extension $k_\lambda = k(\sqrt{d_\lambda})$ to each d_λ in the set Σ.

For any non-empty finite subset S of Λ, we set

$$k_S = k\left(\sqrt{\prod_{i\in S} d_i}\right) \text{ and } k(S) = k(\{\sqrt{d_i} \mid i \in S\}).$$

We call the set Σ a *primitive set* if $[k(S):k] = 2^{\#S}$ holds for all finite subsets S of Σ. If Σ is primitive, then the fields k_T's $(T \neq \phi,\ T \subseteq S)$ are exactly $2^{\#S} - 1$ different quadratic extensions over k in $k(S)$. For an elliptic curve E defined over k, we denote by E^S the twist of E by the quadratic character of k_S/k.

The following proposition is the key to our construction.

Proposition 1. *Suppose that* $\Sigma = \{d_\lambda\}_{\lambda\in\Lambda}$ *is primitive and let* S *be any finite subset of* Λ. *Then we have*

$$\mathrm{rank}(E\,;k(S)) = \sum_{T\subseteq S} \mathrm{rank}(E^T\,;k),$$

where the sum is taken for all subsets T *of* S.

Proof. Put $S = \{1,2,\dots,m\}$ and $S' = \{1,2,\dots,m-1\}$. When $m=1$, the proposition is classical (for instance, see [1]). It is easy to see that $[k(S):k(S')] = 2$ and $k(S) = k(S')(\sqrt{d_m})$. Therefore we obtain

$$\mathrm{rank}(E\,;k(S)) = \mathrm{rank}(E\,;k(S')) + \mathrm{rank}(E^{\{m\}}\,;k(S'))$$

$$= \sum_{T' \subseteq S'} \operatorname{rank}(E^{T'}; k) + \sum_{T' \subseteq S'} \operatorname{rank}(E^{\{m\} \cup T'}; k)$$
$$= \sum_{T \subseteq S} \operatorname{rank}(E^{T}; k)$$

as claimed.

Remark. Proposition 1 may follow from a general result of A. Satoh [9].

Now we can start the explicit construction.

Let n be a square-free positive integer and E_n the elliptic curve over $\boldsymbol{Q}$ defined by

$$E_n : y^2 = x^3 - n^2 x.$$

It is easy to see that the structure of the subgroup $E_n(\boldsymbol{Q})_{\text{tors}}$ of the points of finite order in $E_n(\boldsymbol{Q})$ is $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$. And it is well-known that finding a point of infinite order on E_n is equivalent to determining whether n is the area of some right triangle with rational sides. In a classical language, we know that $\operatorname{rank}(E_n; \boldsymbol{Q}) \geq 1$ if and only if n is a *congruent number*, concerning which we have the following result.

Proposition 2 ([6] Corollary 5.15). *Let p_1, p_3, p_5 and p_7 denote prime numbers congruent to* 1, 3, 5 *and* 7 (mod 8), *respectively.*

The following are all congruent numbers:

$$p_5,\ p_7,\ p_3p_7,\ p_3p_5,$$
$$\text{and } p_1p_5 \text{ when } \left(\frac{p_1}{p_5}\right) = -1.$$

From now on, we assume $k = \boldsymbol{Q}$. When we write $n = p_i (i = 1,3,5,7)$, this will mean that n is a prime number congruent to i (mod 8). Let $\Sigma = \{q_j\}_{j \in N}$ be an infinite set of prime numbers and set $S_m = \{1,2,\ldots,m\}$. The set Σ is primitive.

Our main theorem is as follows.

Theorem. *If the number n and the set Σ satisfies one of the conditions below, then $\operatorname{rank}(E_n; \boldsymbol{Q}(S_m))$ becomes arbitrarily large as m goes to infinity.*

(1) $n = 1$ *or* p_3, *and infinitely many* q_j*'s are congruent to* 5 *or* 7 (mod 8).

(2) $n = p_1$, *and infinitely many* q_j*'s are congruent to* 5 (mod 8) *and* $\left(\frac{n}{q_j}\right) = -1$.

(3) $n = p_5$, *and infinitely many* q_j*'s are congruent to* 3 (mod 8) *or else they are congruent to* 1 (mod 8) *and* $\left(\frac{q_j}{n}\right) = -1$.

(4) $n = p_7$, *and infinitely many* q_j*'s are congruent to* 3 (mod 8).

Proof. As we saw in Proposition 1, one has

$$\operatorname{rank}(E_n; \boldsymbol{Q}(S_m)) = \sum_{T \subseteq S_m} \operatorname{rank}(E_n^T; \boldsymbol{Q}) \geq \sum_{j \in S_m} \operatorname{rank}(E_n^{\{q_j\}}; \boldsymbol{Q}).$$

An explicit computation shows that

$$E_n^{\{q_j\}} = E_{nq_j}.$$

Combining with the remark on the congruent number above, we obtain

$$\operatorname{rank}(E_n; \boldsymbol{Q}(S_m)) \geq \#\{l = nq_j \mid j \in S_m,\ l \text{ is a congruent number}\}.$$

By Proposition 2 and the conditions of the theorem, the right hand side becomes arbitrarily large as m goes to infinity. This completes the proof.

3. In this section, we consider the following question.

For the elliptic curve E_n, is there an elementary 2-extension such that the rank under the extension is unchanged?

We have the following example.

Example 1. Put $E = E_1$ and let p, q be prime numbers congruent to 3 modulo 8. Then we have

$$\mathrm{rank}(E\,;\,\boldsymbol{Q}(\sqrt{p}, \sqrt{q})) = \mathrm{rank}(E\,;\,\boldsymbol{Q}) = 0.$$

In fact, p, q, pq are all non-congruent numbers (cf. [10]).

Example 2. Let p, q, r be prime numbers congruent to 3 modulo 8 whose product pqr is not 1419 and less that 4500. $\left(\text{Note that } 1419 = 3\cdot 11\cdot 43 \text{ is the area of the right triangle with rational sides } \left(72, \frac{473}{12}, \frac{985}{12}\right). \text{ See [3]}\right)$. Then we have

$$\mathrm{rank}(E_r\,;\,\boldsymbol{Q}(\sqrt{p}, \sqrt{q})) = \mathrm{rank}(E_r\,;\,\boldsymbol{Q}) = 0.$$

As in Example 1, it is shown that r, pq, qr, rp are non-congruent numbers. For the product pqr, we can check that it is not congruent by the method described in Theorem 3.3 and Corollary 3.4 of [10] which gives us an upper bound for the rank of E_n. A machine computation using this algorithm shows that Example 2 is valid for many such p, q, r.

One may naturally ask also the following question.

Can we find an infinite set of prime numbers congruent to 3 (mod 8) *such that any product of primes in the set is a non-congruent number?*

If this is true, we can construct an elementary 2-extension of *infinite* degree which gives an affirmative answer to the question posed in the beginning of this section. But the author has no evidence for it to be valid.

Acknowledgement. I wish to thank Professor Takashi Ono for suggesting me the problem and also for his warm encouragement and valuable advice.

References

[1] Birch, B. J.: Elliptic curves and modular functions. Symposia Math., **4**, 27–32 (1970).

[2] Koblitz, N.: Introduction to Elliptic Curves and Modular Forms. Springer-Verlag, New York, Berlin, Heidelberg, Tokyo (1984).

[3] Kramarz, G.: All congruent numbers less that 2000. Math. Ann., **273**, 337–340 (1986).

[4] Kurčanov, P.: Elliptic curves of infinite rank over Γ-extensions. Mat. Sbornik, **90**(132), 320–324 (1973) (in Russian); English trans.: Math. USSR Sb., **19**, 320–324 (1973).

[5] ——: The rank of elliptic curves over Γ-extensions. ibid., **93**(135), 460–466 (1974) (in Russian); English trans.: ibid., **22**, 465–472 (1974).

[6] Monsky, P.: Mock Heegner points and congruent numbers. Math. Zeit., **204**, 45–68 (1990).

[7] Ono, T.: On the relative Mordell-Weil rank of elliptic quartic curves. J. Math. Soc. Japan, **32**, 665–670 (1980).

[8] ——: Variations on a Theme of Euler—quadratic forms, elliptic curves and Hopf

maps. Jikkyo Syuppan, Tokyo (1980) (in Japanese) (English translation is to appear).

[9] Satoh, A.: A note on Mordell-Weil groups under Kummer extensions. Abstract of the autumn meeting of Japan Mathematical Society. pp. 104–105 (1992).

[10] Serf, P.: Congruent numbers and elliptic curves. Computational Number Theory. Walter de Gruyter and Co., Berlin, New York, pp. 227–238 (1991).

[11] Schneiders, U., and Zimmer, H. G.: The rank of elliptic curves upon quadratic extension. ibid., pp. 239–260 (1991).