Potential Good Reduction of Elliptic Curves

MASANARI KIDA

Department of Mathematics, The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan

We show that there is no elliptic curve defined over the field of rational numbers that attains good reduction at every finite place under quadratic base change. We also give some examples of elliptic curves that acquire good reduction everywhere under cubic or quartic base changes.

1. Introduction

Let $E$ be an elliptic curve defined over the field of rational numbers. If the modular invariant of $E$ is a rational integer, then $E$ has potential good reduction at all primes (see Silverman, 1986, VII, 5.5). Namely, by making a base change of finite degree, the curve acquires good reduction at every prime ideal of the extension field. The aim of this paper is to study properties of this extension field. It is known that if $m$ is a rational integer greater than two which is prime to all bad primes of $E$, then $E$ has good reduction at all finite primes over the $m$-th division field of $E$ (see Silverman, 1994, IV, 10.3(b)). Once a curve attains good reduction at every prime, it continues to have good reduction under any other base changes. Thus we can take any fields containing the division field for our purpose. Since the division fields are, unfortunately, quite large in general, we are particularly interested in how small the field can be. In connection with this, it is known that if an elliptic curve defined over a number field $K$ attains good reduction everywhere under base change of degree prime to six, then the curve has good reduction everywhere over the base field $K$. In particular, it follows that there is no elliptic curve defined over $\mathbb{Q}$ that acquires good reduction everywhere under base change of degree prime to six.

Therefore, the smallest possible field for an elliptic curve over $\mathbb{Q}$ to acquire good reduction everywhere is a quadratic field. Our main theorem claims that this is impossible.

THEOREM 1.1. Let $E$ be an elliptic curve defined over $\mathbb{Q}$. If $K$ is a quadratic field, then the base change of $E$ to $K$ always has bad reduction at some prime ideal.

A proof of this theorem is given in the next section.

By this theorem, the smallest possible field is a cubic extension. This is indeed true. We give an example of an elliptic curve defined over $\mathbb{Q}$ that has good reduction everywhere over a cubic field in the third section.

* Dedicated to Professor Norio Adachi on his 60th birthday.

† E-mail: kida@sugaku.e-one.uec.ac.jp

© 2002 Elsevier Science Ltd. All rights reserved.
We set the following notation and convention, which we will use in the remainder of this paper.

Let $\mathbb{Q}_p$ be the field of $p$-adic numbers and $v_p$ the normalized $p$-adic valuation on $\mathbb{Q}_p$. A local field is a finite extension of $\mathbb{Q}_p$ in a fixed algebraic closure of $\mathbb{Q}_p$. We denote by $e(L/K)$ the ramification index if $L/K$ is an extension of local fields.

For an elliptic curve $E$ defined over a field $K$ and a finite field extension $L/K$, let $E_L$ be the base change $E \times \text{Spec}(K) \text{Spec}(L)$. If $E$ is defined over a number field, let $\text{Type}(E, \mathfrak{p})$ denote the Kodaira symbol of $E$ at a prime ideal $\mathfrak{p}$ that refers to the reduction type of the special fibre of the minimal proper regular model of $E$ at $\mathfrak{p}$. In particular, $\text{Type}(E, \mathfrak{p}) = I_0$ means that $E$ has good reduction at $\mathfrak{p}$. If the curve is defined over a local field, we often drop $\mathfrak{p}$ and simply write $\text{Type}(E)$. We denote the conductor of $E$ by $\text{Cond}(E)$. A Weierstrass model for $E$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is unique up to the coordinate change

$$\begin{cases}
    x = u^2x' + r \\
    y = u^3y' + su^2x' + t
\end{cases}$$

with $u \in K^*$ and $r, s, t \in K$. The coefficients and the basic $b$ and $c$ invariants of the new model obtained by this coordinate change are given by the formulæ in Silverman (1986, Table 2.1). It readily follows from the transformation formula for the discriminant that if an elliptic curve over a local field has good reduction, then the valuation of the discriminant is a multiple of 12.

2. Quadratic Base Change

In this section, we shall give a proof of Theorem 1.1.

To prove the theorem, we need the following lemma and propositions. The first proposition below shows that a quadratic base change is closely related to a quadratic twist.

From now on, we write $E^L$ for the quadratic twist of $E/K$ corresponding to a quadratic extension $L/K$.

**Proposition 2.1.** Let $L/K$ be a quadratic extension of number fields and $E$ an elliptic curve defined over $K$. Then we have

$$N_{L/K}(\text{Cond}(E_L)) \cdot (d_{L/K})^2 = \text{Cond}(E) \cdot \text{Cond}(E^L),$$

where $d_{L/K}$ is the relative discriminant of $L/K$ and $N_{L/K}$ is the norm map between the ideal groups.

**Proof.** In Kida (1995), an isogeny between the Weil restriction $R_{L/K}E_L$ and the product $E \times E^L$ is given. On the other hand, Milne proved in Milne (1972)

$$\text{Cond}(R_{L/K}E_L) = N_{L/K}(\text{Cond}(E_L)) \cdot (d_{L/K})^2.$$

Noting that the conductor is invariant under isogenies, we obtain the proposition. See also Umegaki (1998). \(\square\)

Since the conductors and the discriminant are decomposed into the local correspondents, this proposition is also valid in a local situation.
We also have to know the variations of some invariants under twisting.

**Lemma 2.1.** Let $E$ be an elliptic curve defined over $\mathbb{Q}_p$ and $L/\mathbb{Q}_p$ a quadratic extension. We write $L = \mathbb{Q}_p(\sqrt{d})$ with some $d \in \mathbb{Q}_p$. Let $c_i$ and $\Delta$ be the $c$-invariants and the discriminant of a model of $E$, respectively. By $c'_i$ and $\Delta'$, we denote the corresponding quantities of a model (see the proof below) of the twist $E^L$. Then we have

$$v_p(c'_i) = v_p(c_i) + \frac{i v_p(d)}{2}, \quad (i = 4, 6)$$

and

$$v_p(\Delta') = v_p(\Delta) + 6v_p(d).$$

**Proof.** Let $\eta$ be a solution of $\eta^2 = 1/d$. A model of the twisted curve corresponding to $L/\mathbb{Q}_p$ is obtained by applying the coordinate change (2) with $u = \eta, r = 0, s = a_1(\eta - 1), t = a_3(\eta^3 - 1)/2$ to the original equation of $E$ (see Connell, 1996, 4.3). The resulting equation is

$$y^2 + a_1xy + a_3y = x^3 + \left(a_2d + \frac{a_2^3(d-1)}{4}\right)x^2$$

$$+ \left(a_4d^2 + \frac{a_1a_3(d^2 - 1)}{2}\right)x + \left(a_6d^3 + \frac{a_3^2(d^3 - 1)}{4}\right).$$

Thus by the formulae in Silverman (1986, Table 2.1), we have

$$v_p(c'_i) = v_p(c_i) - v_p(\eta_i) = v_p(c_i) + iv_p(d)/2.$$

The equality for the discriminants can be obtained similarly. $\square$

Using Proposition 2.1 and Papadopoulos’s tables in Papadopoulos (1993), we can determine the possible reduction types of elliptic curves that have good reduction under quadratic base change.

**Proposition 2.2.** Let $L/\mathbb{Q}_p$ be a ramified quadratic extension and $E$ an elliptic curve defined over $\mathbb{Q}_p$ with minimal discriminant $\Delta$. Then the following two conditions are equivalent.

(i) The base change $E_L$ has good reduction.

(ii) Either $E$ or the quadratic twist $E^L$ has good reduction.

Moreover, if the above conditions hold, then the reduction type of $E$ is one of the following:

<table>
<thead>
<tr>
<th>Type($E$)</th>
<th>$E_L$ has good reduction</th>
<th>$E^L$ has good reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I_0$ or $I^*_0$ if $p \geq 3$</td>
<td>if $p \geq 3$</td>
<td>if $p \geq 3$</td>
</tr>
<tr>
<td>$I_0$ or $II^*$ with $v_2(\Delta) = 12$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
</tr>
<tr>
<td>$I_0$ or $I^*_1$ with $v_2(\Delta) = 12$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
</tr>
<tr>
<td>$I_0$ or $II$ with $v_2(\Delta) = 6$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 2$</td>
</tr>
<tr>
<td>$I^*_1$ with $v_2(\Delta) = 18$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 3$</td>
<td>if $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 3$</td>
</tr>
</tbody>
</table>
PROOF. If either $E$ or $E_L$ has good reduction, then either $E_L$ or $(E_L)_L$ has good reduction accordingly by the semi-stable reduction theorem (see Silverman, 1986, VII, 5.4). Since $E_L$ and $(E_L)_L$ are isomorphic, it implies that (i) follows from (ii).

Conversely, we assume (i). If Type($E_L$) = $I_0$ or equivalently Cond($E_L$) is trivial, then by Proposition 2.1 we have

$$v(E_L) = 0.$$ (3)

By the semi-stable reduction theorem, if $E_L$ has good reduction, then $E$ must have good or additive reduction over $\mathbb{Q}_p$. If $E$ has good reduction, then $E_L$ has good reduction. Thus we concentrate our attention on the additive reduction case.

If $p \geq 3$, then the ramification in $L/\mathbb{Q}_p$ is tame. Therefore, equation (3) yields

$$p^2 = \text{Cond}(E) \cdot \text{Cond}(E_L).$$ (4)

In addition to this, if $p \geq 5$, then it is known that Cond($E$) = $p^2$ by Silverman (1994, IV, 10.2). Thus equation (4) implies Cond($E_L$) = 1. Namely, the twist $E_L$ has good reduction over $\mathbb{Q}_p$. This is (ii). By Lemma 2.1, we see that $E_L$ has good reduction if and only if $v_p(\Delta) + 6 \equiv 0 \pmod{12}$. By the minimality of $\Delta$, then it implies $v_p(\Delta) = 6$. Then by checking up on Table 4.1 in Silverman (1994), this happens exactly when Type($E$) = $I_0$. This completes the proof for $p \geq 5$.

If $p = 3$, then it is necessary that $2v_3(\Delta) \equiv 0 \pmod{12}$. From (4), $v_3(\text{Cond}(E)) \leq 2$ is also necessary. Looking up Table II in Papadopoulos (1993), we have two possibilities Type($E$) = $I_0^*$ or $I_0^{**}$ with $\nu > 0$. But if Type($E$) = $I_0^*$ ($\nu > 0$), then the twist has multiplicative reduction by Proposition 1 in Comalada (1994) and thus $E_L$ also has multiplicative reduction. Therefore we again obtain Type($E$) = $I_0$. If Type($E$) = $I_0^*$, then we have Type($E_L$) = $I_0$ by Comalada (1994, Proposition 1). Thus we have proved the proposition for $p = 3$.

Suppose now that $p = 2$. We first consider the case $v_2(d_{L/\mathbb{Q}_2}) = 2$. Equation (3) yields

$$2^4 = \text{Cond}(E) \cdot \text{Cond}(E_L).$$ (5)

Thus we have $v_2(\text{Cond}(E)) \leq 4$. Together with the condition $2v_2(\Delta) \equiv 0 \pmod{12}$, we look up Table IV in Papadopoulos (1993) to find the following two possibilities:

- Type($E$) = $II^*$ with $v_2(\Delta) = 12$;
- Type($E$) = $I_0^{**} + 12k$ with $v_2(\Delta) = 12 + 12k$.

Here in the latter case, only $k = 0$ is possible. Indeed, in the case, we have $v(c_k) = 2 \cdot 4$, $v(c_k) = 2 \cdot 6$, $v(\Delta) = 2(12 + 2k) = 12 \cdot 2(1 + k)$ where $v$ is the normalized valuation of $L$ (thus $v(2) = 2$ holds). Let $\pi$ be a prime element of $L$. Then, to have Type($E_L$) = $I_0$, $2(k + 1)$ applications of the coordinate change (2) with $u = \pi$ are necessary. After the applications, we obtain $v(c_k) = 8 - 4 \cdot 2(k + 1) = -8k \geq 0$ and $v(c_k) = 12 - 6 \cdot 2(k + 1) = -12k \geq 0$ by Silverman (1986, Table 2.1). From this, it follows $k = 0$. In both cases, the exponent of the conductor is $4$ (see again Papadopoulos, 1993, Table IV). Thus from (5) we have Cond($E_L$) = 1.

Finally, we consider the case where $p = 2$ and $v_2(d_{L/\mathbb{Q}_2}) = 3$. By (3), we have

$$2^6 = \text{Cond}(E) \cdot \text{Cond}(E_L).$$ (6)

This yields $v_2(\text{Cond}(E)) \leq 6$. By using the condition $2v_2(\Delta) \equiv 0 \pmod{12}$, it follows $v_2(\text{Cond}(E)) \geq 4$ by Table IV in Papadopoulos (1993). We now search for the possible
We shall show that $I^\ast$ and $E$ of Proposition 2.2 for all prime numbers. Let $S$ be the set of the prime numbers at which $E$ has bad reduction:

$$S = \{p \mid \text{Type}(E, p) \neq I_0\}.$$
We define a quadratic field $L$ over $\mathbb{Q}$ in the following manner. If $2 \not\in S$, then we put
$m = \prod_{p \in S} p$ and

$$
L = \mathbb{Q}(\sqrt{m}) \quad \text{if } m \equiv 1 \pmod{4},
$$
$$
L = \mathbb{Q}(\sqrt{-m}) \quad \text{if } m \equiv 3 \pmod{4}.
$$

If $2 \in S$, we put $m = (\prod_{p \in S} p)/2$ and

$$
L = \mathbb{Q}(\sqrt{\pm 2m}) \quad \text{if Type}(E, 2) = \text{II or I}_2^8,
$$
$$
L = \mathbb{Q}(\sqrt{m}) \quad \text{if Type}(E, 2) = \text{II}^* \text{ or I}_2^* \text{ and if } m \equiv 3 \pmod{4},
$$
$$
L = \mathbb{Q}(\sqrt{m}) \quad \text{if Type}(E, 2) = \text{II}^* \text{ or I}_2^* \text{ and if } m \equiv 1 \pmod{4},
$$

where the sign of $2m$ is chosen such that the quadratic twist $E^L$ has good reduction at $2$. Then it is easy to see that $L/\mathbb{Q}$ is ramified exactly at primes in $S$ and that, if Type$(E, 2) = \text{II or I}_2^8$, then $v_2(d_{L/\mathbb{Q}}) = 3$ and, if Type$(E, 2) = \text{II}^* \text{ or I}_2^*$, then $v_2(d_{L/\mathbb{Q}}) = 2$.

Let us consider the twist $E^L$ of $E$ corresponding to $L/\mathbb{Q}$. If a prime number $q$ is not contained in $S$, then $v_q(\text{Cond}(E^L)) = 0$ by Proposition 2.1. If $q \in S$, then by Proposition 2.2 (ii), we have $v_q(\text{Cond}(E^L)) = 0$. Consequently, the twist $E^L$ is an elliptic curve defined over $\mathbb{Q}$ that has good reduction everywhere. This contradicts a well-known theorem of Tate (see Ogg, 1966).

It may be appropriate to make a remark on $L$ in the above proof. The field $L$ may be different from the quadratic field $K$. The important point here is that we can control the ramification of $L$ so that the twist $E^L$ has a desired property for using Proposition 2.2.

### 3. Examples

In this section, we give some examples of elliptic curves that acquire good reduction everywhere over relatively small fields.

In the following, we often use a notation like $p_p$. This stands for a prime ideal lying above a prime number $p$. We also use a capital correspondent $P_p$, by which we mean a prime ideal of a larger field also lying above $p$. We hope that the fields to which these ideals belong are always clear from the context.

#### 3.1. Cubic Fields

**Example 1.** We first consider an elliptic curve over $\mathbb{Q}$ defined by

$$E : y^2 = x^3 + x^2 - 114x - 127.$$  

This curve is 196B1 in Cremona (1997) and has bad reduction at two and seven. More precisely, we have

$$\text{Type}(E/\mathbb{Q}, 2) = \text{IV}, \quad \text{Type}(E/\mathbb{Q}, 7) = \text{IV}^*.$$  

Making a base change to the cubic field $K_1 = \mathbb{Q}(\sqrt[3]{14})$, we obtain Type$(E_{K_1}, p) = I_0$ for all prime ideals $p$ of $K_1$. In fact, we find a following model over $K_1$

$$y^2 + (\sqrt[3]{14})^2 xy + y = x^3 + 3(\sqrt[3]{14})^2 x + 12,$$

whose discriminant generates $p_1^{12}$. Obviously this model is not a global minimal model.
Moreover, we can show that there is no global minimal model for this elliptic curve over $K_1$.

On the other hand, the base change to $K_2 = \mathbb{Q}(\sqrt[3]{28})$ has a global minimal model
\[ y^2 + \sqrt[3]{28}xy + y = x^3 \]
with discriminant 1. This model was first found by Connell (Connell, 1996, Chapter 1).

The curve $E$ acquires good reduction everywhere over a cubic field with even smaller discriminant. Actually $E$ has good reduction everywhere over the field $K_3$ defined by
\[ f(X) = X^3 + 52X^2 + 444X + 7596. \]
The field discriminant is $-2^3 \cdot 3^2 \cdot 13^3$. The field $K_3$ is a subfield of the 3-division field of $E$. The division field coincides with the splitting field of $f(X)$. Since the point $(16, 49)$ on the curve is of order three, the 3-division field is relatively small in this case.

### 3.2. QUARTIC FIELDS

**Example 2.** We next consider the following curve
\[ E': y^2 = x^3 + 78x - 1352. \]
The discriminant of this (global minimal) model is $-2^9 \cdot 3^6 \cdot 13^3$ and the conductor of the curve is $2^8 \cdot 3^2 \cdot 13^2$. The reduction types are
\[
\begin{align*}
\text{Type}(E'/\mathbb{Q}, 2) &= \text{III}, \\
\text{Type}(E'/\mathbb{Q}, 3) &= \text{I}^*_9, \\
\text{Type}(E'/\mathbb{Q}, 13) &= \text{III}.
\end{align*}
\]
There is no rational torsion point on the curve.

By a quadratic extension $K = \mathbb{Q}(\sqrt[3]{26})$ over $\mathbb{Q}$, the reduction types change to
\[
\begin{align*}
\text{Type}(E_K', \mathfrak{p}_2) &= \text{I}^*_9, \\
\text{Type}(E_K', \mathfrak{p}_3) &= \text{I}^*_9, \\
\text{Type}(E_K', \mathfrak{p}_{13}) &= \text{I}_0
\end{align*}
\] and $v_{\mathfrak{p}_2}(\Delta_{E_K'}) = 18$.

Then by a cyclic quartic extension $L = \mathbb{Q}(\sqrt{78 + 15\sqrt{26}}) \supset K \supset \mathbb{Q}$, we can show $\text{Type}(E_L', \mathfrak{P}) = \text{I}_0$ for all prime ideals $\mathfrak{P}$ of $L$.

This example shows that Theorem 1.1 does not hold if we replace the base field $\mathbb{Q}$ by an arbitrary algebraic number field.

The quadratic twist of $E_K'$ corresponding to $L/K$
\[ y^2 = x^3 + 78(78 + 15\sqrt{26})^2 x - 1352(78 + 15\sqrt{26})^3 \]
has good reduction everywhere. Since $d_{L/K} = \mathfrak{p}_2^5 \mathfrak{p}_3 \mathfrak{p}_{13}$, the field $L$ fits the condition for the bad primes becoming good by twisting (see Comalada, 1994). Many examples of this kind are found in Kida (2001).

**Example 3.** The following curve is 49A2 in Cremona (1997):
\[ E'' : y^2 + xy = x^3 - x^2 - 37x - 78. \]
The only bad prime is seven and the Kodaira type at 7 is III.

Since the curve has complex multiplication in the imaginary quadratic order of discriminant $-28$, the division fields tend to be relatively small. Thus we expect that the curve acquires good reduction everywhere over a field of small degree.
Let $K = \mathbb{Q} (\sqrt{-7})$ and $L = \mathbb{Q} (\sqrt[4]{-7})$. We compute $\text{Type}(E''_K, p_7) = I_0$ and $\text{Type}(E''_L, \mathfrak{p}_7) = I_0$. In fact, there is a global minimal model over $L$

$$y^2 - \vartheta x y + \frac{(1 + 2\vartheta + \vartheta^2)}{2} y = x^3 - \left(\frac{3 + \vartheta^2}{2}\right) x^2 + \left(\frac{19 - \vartheta - 5\vartheta^2 - \vartheta^3}{4}\right) x + \left(\frac{-7 - \vartheta - 3\vartheta^2 - \vartheta^3}{4}\right)$$

where $\vartheta = \sqrt[4]{-7}$. The discriminant of the model is $-1$.

But, unlike the previous example, the quadratic twist of $E''_K$ corresponding to $L/K$ has bad reduction of type $I^*_4$ at the prime ideals lying above $2$. This is because the prime ideals lying above $2$ ramify in $L/K$. If there were a quadratic extension of $L$ in which only $\mathfrak{p}_7$ ramifies, the corresponding twist would have good reduction everywhere over $K$. But there is no such extension, since the ray class number of $K$ modulo $p_7$ is $3$, thus is prime to $2$. Furthermore, it is known that there is no elliptic curve having good reduction everywhere over $K$. This is a result proved in Setzer (1978) and Stroeker (1983).

All computations in the above examples are done by using tiny elliptic curve calculator (TECC) (Kida, 2000) running on KASH (Daberkow et al., 1997).

Acknowledgements

This research was supported in part by grant-in-aid for Encouragement of Young Scientists (No. 11740009), Ministry of Education, Science, Sports and Culture, Japan.

References


Received 8 August 2000

Accepted 22 May 2002