

# Root numbers of elliptic curves over 2-adic fields

David Whitehouse\*

Institute for Advanced Study

## Abstract

We give formulas for the root number of an elliptic curve with potential good reduction over a local field of characteristic zero and residual characteristic two.

## 1 Introduction

Let  $E$  be an elliptic curve defined over a local field  $F$  with potential good reduction. Let  $\ell$  be a prime number distinct from the residual characteristic of  $F$  and consider the  $\ell$ -adic representation of  $W_F$ , the Weil group of  $F$ , on the Tate module  $V_\ell(E)$ . Once we choose a basis for  $V_\ell(E)$  and an embedding  $\mathbf{Q}_\ell \subset \mathbf{C}$  we get a representation

$$\sigma_E : W_F \rightarrow \mathrm{GL}_2(\mathbf{C})$$

which is continuous and semisimple since  $E$  has potential good reduction ([Ro2, §14]). Moreover the isomorphism class of this representation is independent of all the choices made. We define the root number of  $E/F$  to be

$$W(E/F) = \frac{\varepsilon(\sigma_E, \psi)}{|\varepsilon(\sigma_E, \psi)|}$$

where  $\psi$  is any non-trivial additive character of  $F$ . We note that  $W(E/F) = \pm 1$  and is independent of the choice of  $\psi$ .

Let  $M$  denote the minimal extension of  $F_{nr}$  over which  $E$  has good reduction. Then we know that  $M = F_{nr}(E[m])$  for any  $m > 2$  prime to the residual characteristic of  $F$ . Furthermore  $\mathrm{Ker} \sigma_E = \mathrm{Gal}(\overline{F}/M)$  and therefore  $\sigma_E$  is a faithful representation of  $W_{M/F} \cong \mathrm{Gal}(M/F_{nr}) \rtimes \langle \Phi \rangle$  where  $\Phi$  is a Frobenius element in  $\mathrm{Gal}(F_{nr}/F)$ .

The case when  $F$  has odd residual characteristic or  $E$  has potential multiplicative reduction is dealt with in [Kob], [Ro1] and [Ro3]. From now on we assume that  $F$  is a local field of characteristic 0 and residual characteristic 2. Let  $\Lambda = \mathrm{Gal}(M/F_{nr})$  then we have the following possibilities for  $\Lambda$ .

---

\*E-mail address: [dwhite@ias.edu](mailto:dwhite@ias.edu)

- $\mathbf{Z}/e\mathbf{Z}$  with  $e = 1, 2, 3, 4$  or  $6$
- $H_8$
- $\mathrm{SL}_2(\mathbf{F}_3)$

We note that  $\Lambda$  is trivial if and only if  $E$  has good reduction over  $F$ . In this case we have  $W(E/F) = +1$ . From now on we assume that  $E$  has potential good reduction but has bad reduction over  $F$ .

## 2 Notation

Let  $F$  be a finite extension of  $\mathbf{Q}_2$ . Let  $v$  denote the normalized additive valuation on  $F$  and  $|\cdot|$  the normalized multiplicative valuation on  $F$ . Let  $(\cdot, \cdot)_F$  denote the Hilbert symbol on  $F$ . Let  $E$  be an elliptic curve defined over  $F$  with potential good reduction. The equation

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

gives a (not necessarily minimal) model for  $E$  over  $F$ . We fix this model for  $E$  and set

$$f(x) = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

and we let  $g(x) = f(x/12)$ . In this model for  $E$  the 3-division polynomial  $\psi_3(x) = P(12x)$  where

$$P(x) = x^4 - 6c_4x^2 - 8c_6x - 3c_4^2.$$

We note that

$$g(x) = \frac{1}{4 \cdot 12^3} P'(x).$$

Let  $a(E/F)$  denote the exponent of the conductor of  $E$  over  $F$ .

We fix the reciprocity isomorphism between  $W_F^{ab}$  and  $F^\times$  such that arithmetic Frobenius corresponds to a uniformizer. This allows us to identify characters of  $W_F$  with characters of  $F^\times$ . If  $\chi$  is a character of  $F^\times$  then let  $a(\chi)$  denote the exponent of the conductor of  $\chi$ . For an additive character  $\psi$  of  $F$  let  $n(\psi)$  denote the largest integer such that  $\psi$  is trivial on  $\mathfrak{p}^{-n(\psi)}$ , where  $\mathfrak{p}$  is the maximal ideal of  $\mathcal{O}_F$  the ring of integers in  $F$ .

## 3 Results on $E[3]$

In this section we give some results on the structure of  $F(E[3])/F$ . We fix  $\sqrt{-3} \in \overline{F}$  and set  $\zeta = 1/2(-1 + \sqrt{-3}) \in \overline{F}$  a primitive third root of unity. We also fix  $\Delta^{\frac{1}{3}} \in \overline{F}$ . For  $1 \leq i \leq 3$  we set

$$A_i = c_4 - 12\zeta^i \Delta^{\frac{1}{3}}.$$

We fix  $\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3} \in \bar{F}$  such that

$$\sqrt{A_1}\sqrt{A_2}\sqrt{A_3} = c_6.$$

Then the roots of  $P(x)$  in  $\bar{F}$  are

$$\begin{aligned} x_0 &= \sqrt{A_1} + \sqrt{A_2} + \sqrt{A_3} \\ x_1 &= \sqrt{A_1} - \sqrt{A_2} - \sqrt{A_3} \\ x_2 &= -\sqrt{A_1} + \sqrt{A_2} - \sqrt{A_3} \\ x_3 &= -\sqrt{A_1} - \sqrt{A_2} + \sqrt{A_3}. \end{aligned}$$

and we have

$$E[3] = \{(x_i/12, \pm\sqrt{g(x_i)}) : 0 \leq i \leq 3\} \cup \{O\}.$$

We note that since  $g(x) = \frac{1}{4.12^3}P'(x)$  we have

$$g(x_i) = \frac{1}{4.12^3} \prod_{j \neq i} (x_i - x_j)$$

Let  $L = F(E[3])$  and  $L_0 = F(E[3]_x)$ , we note that  $L_0$  is the splitting field of  $P$  over  $F$  and hence Galois over  $F$ . We have  $L = L_0(\sqrt{g(x_i)})$  for any  $i$ . Therefore for each  $i$  we have

$$\frac{g(x_0)}{g(x_i)} = g_i^2$$

for some  $g_i \in L_0$ . By direct computation using

$$g(x_i) = \frac{1}{4.12^3} \prod_{j \neq i} (x_i - x_j)$$

we get

$$\begin{aligned} g_1 &= \frac{(\sqrt{A_1} + \sqrt{A_2})(\sqrt{A_1} + \sqrt{A_3})}{12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta} \\ g_2 &= \frac{(\sqrt{A_2} + \sqrt{A_1})(\sqrt{A_2} + \sqrt{A_3})}{12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta^2} \\ g_3 &= \frac{(\sqrt{A_3} + \sqrt{A_1})(\sqrt{A_3} + \sqrt{A_2})}{12\Delta^{\frac{1}{3}}\sqrt{-3}}. \end{aligned}$$

We fix  $\sqrt{g(x_0)} \in \bar{F}$  and for  $i$  with  $1 \leq i \leq 3$  we set  $\sqrt{g(x_i)} = \frac{\sqrt{g(x_0)}}{g_i}$ .

If we set  $P_i = (x_i/12, \sqrt{g(x_i)})$  for  $i = 0, 1, 2, 3$ , then by direct computation we have

$$P_0 \oplus P_1 = P_2$$

and

$$P_0 \oplus (-P_1) = -P_3$$

where  $\oplus$  denotes the addition law on  $E$ .

**Lemma 3.1.** *Assume that  $\text{Gal}(L_0/F)$  is abelian. Then  $\text{Gal}(L/F)$  is abelian if and only if for all  $\sigma, \tau \in \text{Gal}(L_0/F)$  we have*

$$\frac{\sigma(g_j)}{g_j} = \frac{\tau(g_i)}{g_i}$$

where  $i$  and  $j$  are such that  $\sigma(x_0) = x_i$  and  $\tau(x_0) = x_j$ .

*Proof.* Since  $\sigma(x_0) = x_i$  so  $\sigma(g(x_0)) = g(x_i)$ . Let  $\tilde{\sigma}$  be an extension of  $\sigma$  to  $L$  then

$$\tilde{\sigma}(\sqrt{g(x_0)}) = \varepsilon(\tilde{\sigma})\sqrt{g(x_i)} = \varepsilon(\tilde{\sigma})\frac{\sqrt{g(x_0)}}{g_i}$$

where  $\varepsilon(\tilde{\sigma}) = \pm 1$ . Similarly if  $\tilde{\tau}$  is an extension of  $\tau$  to  $L$  then we have

$$\tilde{\tau}(\sqrt{g(x_0)}) = \varepsilon(\tilde{\tau})\frac{\sqrt{g(x_0)}}{g_j}$$

where  $\varepsilon(\tilde{\tau}) = \pm 1$ . Therefore

$$\begin{aligned} \tilde{\sigma}(\tilde{\tau}(\sqrt{g(x_0)})) &= \tilde{\sigma}\left(\varepsilon(\tilde{\tau})\frac{\sqrt{g(x_0)}}{g_j}\right) \\ &= \varepsilon(\tilde{\tau})\varepsilon(\tilde{\sigma})\frac{\sqrt{g(x_0)}}{\sigma(g_j)g_i} \end{aligned}$$

and similarly

$$\begin{aligned} \tilde{\tau}(\tilde{\sigma}(\sqrt{g(x_0)})) &= \tilde{\tau}\left(\varepsilon(\tilde{\sigma})\frac{\sqrt{g(x_0)}}{g_i}\right) \\ &= \varepsilon(\tilde{\sigma})\varepsilon(\tilde{\tau})\frac{\sqrt{g(x_0)}}{\sigma(g_i)g_j}. \end{aligned}$$

Since  $L_0/F$  is abelian we see that  $\tilde{\sigma}$  and  $\tilde{\tau}$  commute if and only if

$$\frac{\sigma(g_j)}{g_j} = \frac{\tau(g_i)}{g_i}.$$

From which the lemma now follows. □

## 4 Determination of $\Lambda$

We recall the following result of Kraus ([Kra, Theorem 3]) which determines the structure of the group  $\Lambda$ . We note from §1 that as an abstract group  $\Lambda$  is completely determined by its order.

**Theorem 4.1.** Let  $\Delta^{\frac{1}{3}}$  be a cube root of  $\Delta$ . Set

$$A = c_4 - 12\Delta^{\frac{1}{3}} \quad B = c_4^2 + 12c_4\Delta^{\frac{1}{3}} + (12\Delta^{\frac{1}{3}})^2.$$

We have  $AB = c_6^2$ . Let  $B^{\frac{1}{2}}$  be a square root of  $B$  and put

$$C = 2(c_4 + 6\Delta^{\frac{1}{3}} + B^{\frac{1}{2}}).$$

(i) Suppose that  $v(\Delta) \equiv 0 \pmod{3}$ . Then  $\Delta^{\frac{1}{3}}$  lies in  $F_{nr}$ .

(a) Suppose that  $A$  and  $B$  are squares in  $F_{nr}$ . Then  $\#\Lambda = 2$  if  $C$  is a square in  $F_{nr}$  and  $\#\Lambda = 4$  otherwise.

(b) Suppose that  $A$  or  $B$  are not squares in  $F_{nr}$ . Then  $\#\Lambda = 4$  if  $C$  is a square in  $F_{nr}(A^{\frac{1}{2}}, B^{\frac{1}{2}})$  and  $\#\Lambda = 8$  otherwise.

(ii) Suppose that  $v(\Delta) \not\equiv 0 \pmod{3}$ . Let  $M = F_{nr}(\Delta^{\frac{1}{3}})$  denote the unique cubic extension of  $F_{nr}$ .

(a) Suppose that  $A$  and  $B$  are squares in  $M$ . Then  $\#\Lambda = 3$  if the Neron type of  $E$  is IV or IV\* and  $\#\Lambda = 6$  otherwise.

(b) Suppose that  $A$  or  $B$  are not squares in  $F_{nr}$ . Then  $\#\Lambda = 24$ .

## 5 Reducible Case

Everything in this section is implicit in [Ro1]. Assume that  $\sigma_E$  is reducible. This is true if and only if the image of  $\sigma_E$  is abelian and hence if and only if

$$W_{M/F} \cong \mathbf{Z}/e\mathbf{Z} \times \mathbf{Z}.$$

**Lemma 5.1.**  $\sigma_E$  is reducible if and only if  $\text{Gal}(L/F)$  is abelian.

*Proof.* We recall that  $\sigma_E$  is irreducible if and only if  $W_{M/F}$  is abelian. But now  $M = LF_{nr}$  and  $\text{Gal}(F_{nr}/F)$  is abelian. The result now follows.  $\square$

Since  $\det \sigma_E = |\cdot|_F$  we have

$$\sigma_E = \chi \oplus \chi^{-1} |\cdot|_F$$

for some character  $\chi$  of  $F^\times$ . In this case we have the following result.

**Lemma 5.2.**  $W(E/F) = \chi(-1)$

*Proof.* We have

$$\varepsilon(\sigma_E, \psi) = \varepsilon(\chi, \psi)\varepsilon(\chi^{-1}|\cdot|, \psi)$$

and the result follows from [Ro1, p 145].  $\square$

Let  $M_0$  be the subfield of  $M$  fixed by the closure of  $\langle \Phi \rangle$  in  $\text{Gal}(M/F)$ . Then  $M_0$  is a totally ramified cyclic extension of  $F$  of degree  $e$ . Moreover  $E$  has good reduction over  $M_0$ . Since  $M$  is the minimal extension of  $F_{nr}$  over which  $E$  has

good reduction we see that  $\ker(\chi|_{U_F}) = NU_{M_0}$ . Thus if  $\delta$  is a character of  $F^\times$  whose kernel is the group of norms from the extension  $M_0$  then

$$W(E/F) = \delta(-1).$$

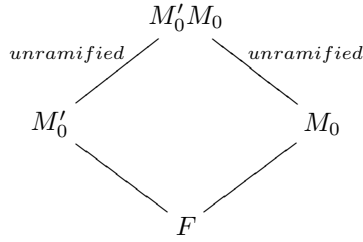
**Lemma 5.3.** *Suppose that  $M'_0$  is an extension of  $F$  over which  $E$  has good reduction and that  $e(M'_0/F) = e(M_0/F)$  then*

$$W(E/F) = \begin{cases} +1 & \text{if } -1 \in F \text{ is a norm from } M'_0 \\ -1 & \text{if } -1 \in F \text{ is not a norm from } M'_0 \end{cases}$$

*Proof.* Our conditions on  $M'_0$  imply that

$$M'_0 F_{nr} = M = M_0 F_{nr}.$$

Therefore we have the following field diagram



Let  $y \in U_F$  then we have

$$y \text{ is a norm from } M'_0 \iff y \text{ is a norm from } M'_0 M_0$$

and

$$y \text{ is a norm from } M_0 \iff y \text{ is a norm from } M'_0 M_0.$$

From which the result follows. □

## 6 Imprimitve Case

Everything in this section is implicit in [Ro1]. In this case there exists a quadratic extension  $F_1$  of  $F$  and a character  $\theta$  of  $F_1^\times$  such that

$$\sigma_E = \text{Ind}_{F_1/F} \theta$$

Let  $\alpha$  denote the character of  $F^\times$  associated to the extension  $F_1$ , i.e.  $\alpha$  is the character of  $F^\times$  whose kernel is precisely the group of norms from  $F_1^\times$ . Given an additive character  $\psi$  of  $F$  let  $\psi_{F_1}$  denote the additive character of  $F_1$  given by composing  $\psi$  with the trace map from  $F_1$  to  $F$ .

**Lemma 6.1.**  $W(E/F) = W(\theta, \psi_{F_1})W(\alpha, \psi)$

*Proof.* Since  $\varepsilon$  factors are inductive in degree zero we have

$$\varepsilon(\text{Ind}_{F_1/F}(\theta - 1_{F_1}), \psi) = \varepsilon(\theta - 1_{F_1}, \psi_{F_1}).$$

That is

$$\frac{\varepsilon(\sigma_E, \psi)}{\varepsilon(1_F, \psi)\varepsilon(\alpha, \psi)} = \frac{\varepsilon(\theta, \psi_{F_1})}{\varepsilon(1_{F_1}, \psi_{F_1})}$$

from which the result follows.  $\square$

Now we assume that  $\Lambda$  is abelian but that  $\sigma_E$  is not reducible. In this case we have  $\Lambda = \mathbf{Z}/e\mathbf{Z}$  with  $e = 3, 4$  or  $6$  and  $W_{M/F} = \Lambda \rtimes \langle \Phi \rangle$ , with the product not direct. Now the group  $W_{M/F}$  contains  $\Lambda \times \langle \Phi^2 \rangle$  as an abelian normal subgroup and hence we deduce that

$$\sigma_E = \text{Ind}_{H/F} \theta$$

for some character  $\theta$  of  $H^\times$ , where  $H$  is the unramified quadratic extension of  $F$ . By the above result we have

$$W(E/F) = W(\theta, \psi_H)W(\alpha, \psi)$$

where  $\alpha$  is the unramified quadratic character of  $F^\times$ . We recall the following result of Frohlich and Queyrut as stated in [KT, Theorem 2.6].

**Theorem 6.2.** *Let  $\chi$  be a character of a quadratic extension  $F'$  of  $F$ , and suppose that  $\chi$  is trivial when restricted to  $F^\times$ . Let  $y$  be an element of  $F'^\times$  such that  $\text{Tr}_{F'/F}(y) = 0$ . Then*

$$\varepsilon(\chi, \psi) = c(\psi)\chi(y)$$

where  $c(\psi)$  is a constant which depends only on  $\psi$ .

Note that  $c(\psi)$  is positive (take  $\chi$  to be the trivial character). From the formula for the determinant of an induced representation we have

$$|\cdot|_F = \alpha |\theta|_{F^\times}.$$

Let  $\tilde{\alpha}$  denote the quadratic unramified character of  $H^\times$ , then  $\tilde{\alpha}|_{F^\times} = \alpha$  and hence the character

$$\phi = \theta \tilde{\alpha} |\cdot|_H^{-1}$$

of  $H^\times$  is trivial when restricted to  $F^\times$ . Let  $y \in H$  such that  $\text{Tr}_{K/F}(y) = 0$ . Then from Theorem 6.2 we have

$$\varepsilon(\phi, \psi_H) = c(\psi_H)\phi(y).$$

On the other hand  $\tilde{\alpha}|\cdot|_H^{-1}$  is unramified and hence

$$\varepsilon(\phi, \psi_H) = \varepsilon(\theta, \psi_H)\tilde{\alpha}(\varpi_H^{a(\theta)+n(\psi_H)})|\varpi_H^{a(\theta)+n(\psi_H)}|_H^{-1}.$$

Therefore

$$W(\theta, \psi_H) = \frac{\theta(y)}{|\theta(y)|} (-1)^{a(\theta) + n(\psi)}$$

since  $n(\psi_H) = n(\psi)$  as  $H/F$  is unramified. We also have

$$W(\alpha, \psi) = (-1)^{n(\psi)}.$$

Hence

$$W(E/F) = \frac{\theta(y)}{|\theta(y)|} (-1)^{a(\theta)}.$$

From the formula for the conductor of an induced representation we deduce that  $a(E/F) = 2a(\theta)$  and hence

$$W(E/F) = \frac{\theta(y)}{|\theta(y)|} (-1)^{\frac{a(E/F)}{2}}.$$

Now we write

$$y = \varpi_F^{v_H(y)} u$$

with  $u \in U_H$ . Then

$$\frac{\theta(y)}{|\theta(y)|} = \left( \frac{\theta(\varpi_F)}{|\theta(\varpi_F)|} \right)^{v_H(y)} \theta(u) = (-1)^{v_H(y)} \theta(u)$$

since  $\theta|_{F^\times} = |\cdot|_F \alpha$ . We know that

$$\sigma_E|_H = \theta \oplus \theta^{-1} | \cdot |_H$$

and  $E/H$  achieves good reduction over some totally ramified cyclic extension  $H_1$  of degree  $e$  over  $H$ . Thus  $\text{Ker}(\theta|_{U_H}) = NU_{H_1}$  and hence if we take  $\delta$  to be any character of  $H^\times$  whose kernel is the group of norms in  $H$  from  $H_1^\times$  then

$$W(E/F) = (-1)^{\frac{a(E/F)}{2}} (-1)^{v_H(y)} \delta \left( \frac{y}{\varpi_F^{v_H(y)}} \right).$$

## 7 Other Results

We recall a couple of results here that will be useful later.

**Lemma 7.1.** *Let  $E$  be an elliptic curve over  $F$  and let  $K$  be a Galois extension of  $F$  of odd degree then  $W(E/F) = W(E/K)$ .*

*Proof.* See the proof of [KT, Proposition 3.4]. □

**Lemma 7.2.** (*[Tun, Lemma 5.5]*) *Let  $K$  be a local field of residue characteristic 2. There exists a Galois extension  $E$  of  $K$  such that  $\text{Gal}(E/K) \cong S_3$  if and only if  $K$  does not contain the cube roots of unity, in which case  $E$  is unique. There are ramified normal cubic extensions of  $K$  if and only if  $K$  contains the cube roots of unity, in which case there are three nonisomorphic extensions of this type.*

**Lemma 7.3.** *The following are equivalent*

- (i)  $a(E/F) = 2$
- (ii)  $E$  is of Neron type IV or IV\*
- (iii)  $\#\Lambda = 3$ .

**Lemma 7.4.** *Assume that  $\#\Lambda = 3$  then*

$$W(E/F) = \begin{cases} +1 & \text{if } \mu_3 \in F \\ -1 & \text{if } \mu_3 \notin F \end{cases}$$

*Proof.* If  $\#\Lambda = 3$  then  $E$  achieves good reduction over the cubic extension  $F(\Delta^{\frac{1}{3}})$  of  $F$ . Therefore if  $\mu_3 \subset F$  then  $F(\Delta^{\frac{1}{3}})/F$  is a normal cubic extension and hence by Lemma 7.1 we have

$$W(E/F) = W(E/F(\Delta^{\frac{1}{3}})) = +1.$$

Now assume that  $\mu_3 \not\subset F$ . Then by Lemma 7.2 there are no cubic Galois extensions of  $F$  and hence from §5 we deduce that  $\sigma_E$  is irreducible. Now  $H = F(\sqrt{-3})$  is the unramified quadratic extension of  $F$  and hence from §6 we deduce that

$$W(E/F) = -\delta(\sqrt{-3}) = -1$$

since  $\delta^3$  is trivial and we know that  $W(E/F) = \pm 1$ . □

## 8 $P$ has a root in $F$

Assume that  $P$  has a root  $x' \in F$ . Then  $(x'/12, \sqrt{g(x')}) \in E[3]$ . From [Kra, Proposition 3] we deduce that  $E$  has good reduction over

- $F(\sqrt{g(x')})$  if  $v(\Delta) \equiv 0 \pmod{3}$
- $F(\sqrt{g(x')}, \Delta^{\frac{1}{3}})$  if  $v(\Delta) \not\equiv 0 \pmod{3}$

Therefore if  $v(\Delta) \equiv 0 \pmod{3}$  then

$$W(E/F) = (-1, g(x'))_F.$$

We now assume that  $v(\Delta) \not\equiv 0 \pmod{3}$ . First suppose  $\mu_3 \subset F$  then  $F(\Delta^{\frac{1}{3}})$  is a cubic Galois extension of  $F$  and hence by Lemma 7.1 we have

$$W(E/F) = W(E/F(\Delta^{\frac{1}{3}})).$$

Now, if  $E$  has good reduction over  $F(\Delta^{\frac{1}{3}})$ , then  $W(E/F(\Delta^{\frac{1}{3}})) = +1$ . But then since  $E$  has good reduction over  $F(\Delta^{\frac{1}{3}})$  so  $F(\sqrt{g(x')})/F$  must be unramified and hence in this case we have  $(-1, g(x'))_F = +1$ . On the other hand if  $E$  still has bad reduction over  $F(\Delta^{\frac{1}{3}})$  then

$$\begin{aligned} W(E/F(\Delta^{\frac{1}{3}})) &= (-1, g(x'))_{F(\Delta^{\frac{1}{3}})} \\ &= (-1, g(x'))_F. \end{aligned}$$

Thus in either case  $W(E/F) = (-1, g(x'))_F$ .

We now assume that  $\mu_3 \not\subset F$ . If  $F(\sqrt{g(x')})/F$  is unramified then  $E$  has good reduction over  $F(\Delta^{\frac{1}{3}})$  and hence by Lemma 7.4

$$W(E/F) = -1.$$

Thus we are left to consider the case that  $F(\sqrt{g(x')})$  is a ramified quadratic extension of  $F$ . In this case we see that  $F(\sqrt{g(x')}, \Delta^{\frac{1}{3}})$  is a totally ramified extension of  $F$  of degree 6. Hence  $\#\Lambda = 6$  and  $\text{Gal}(L/F)$  is not abelian since  $L$  contains  $F(\Delta^{\frac{1}{3}})$  which is not Galois over  $F$ . Therefore in this case

$$W(E/F) = (-1)^{\frac{\alpha(E/F)}{2}} \delta(\sqrt{-3})$$

where  $\delta$  is a character of  $F(\mu_3)^\times$  with kernel the group of norms from  $F(\mu_3, \Delta^{\frac{1}{3}}, \sqrt{g(x')})^\times$ . Now,  $\delta^3$  is the character of  $F(\mu_3)^\times$  with kernel the group of norms from  $F(\mu_3, \sqrt{g(x')})^\times$ . Since  $\delta^3(\sqrt{-3}) = \delta(\sqrt{-3})$  we deduce that

$$\begin{aligned} W(E/F) &= (-1)^{\frac{\alpha(E/F)}{2}} (\sqrt{-3}, g(x'))_{F(\mu_3)} \\ &= (-1)^{\frac{\alpha(E/F)}{2}} (3, g(x'))_F. \end{aligned}$$

## 9 $P$ splits into the product of two irreducible quadratics over $F$

Now assume that  $P$  splits into the product of two irreducible quadratics over  $F$ . This is equivalent to  $P$  not having any roots in  $F$  and some  $A_k$  being a square in  $F$ . We fix  $\Delta^{\frac{1}{3}} \in F$  such that  $\sqrt{A_3} \in F$ .

First assume that  $\mu_3 \subset F$ . Since  $P$  has no root in  $F$  so  $L_0 = F(\sqrt{A_1})$  is quadratic over  $F$ . Therefore  $F(E[3]) = F(\sqrt{A_1}, \sqrt{g(x_0)})$  has degree 4 and is abelian over  $F$  by [Kra, Proposition 3]. Now

$$e(L/F) = \begin{cases} 2 & \text{if } F(\sqrt{A_1})/F \text{ is unramified} \\ 4 & \text{if } F(\sqrt{A_1})/F \text{ is ramified} \end{cases}$$

First assume that  $e(L/F) = 2$ . In this case  $F(\sqrt{A_1})/F$  is unramified and hence there exists  $x \in F(\sqrt{A_1})$  such that  $N_{F(\sqrt{A_1})/F} x = -1$  and

$$W(E/F) = (x, g(x_0))_{F(\sqrt{A_1})}.$$

Now if  $F(\sqrt{A_2})/F$  is ramified, let  $\delta$  be a character of  $F^\times$  with kernel equal to the group of norms in  $F$  from  $F(\sqrt{A_1}, \sqrt{g(x_0)})^\times$  then

$$W(E/F) = \delta(-1).$$

Now assume that  $\mu_3 \notin F$ . In this case we have the following possibilities.

- $\text{Gal}(L_0/F) \cong \mathbf{Z}/2\mathbf{Z}$ , in which case  $L_0 = F(\mu_3)$
- $\text{Gal}(L_0/F) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$

In the first case  $L_0/F$  is unramified and so by [Kra, Proposition 3]  $e(L/F) = 2$ . Therefore we have  $F(\sqrt{A_1}) = F(\mu_3) = F(\sqrt{5})$  and  $A_1$  and  $A_2$  are squares in  $F(\sqrt{5})$ . In this case we have

$$W(E/F) = (2 + \sqrt{5}, g(x_0))_{F(\mu_3)}.$$

Now consider the second case. By [Kra, Proposition 3]  $e(L/F) = 4$  and hence  $L$  has degree 8 over  $F$ .

**Lemma 9.1.**  *$L$  is not abelian over  $F$ .*

*Proof.* In this case we have  $L_0 = F(\sqrt{A_1} + \sqrt{A_2}, \sqrt{A_1} - \sqrt{A_2})$  with  $F(\sqrt{A_1} + \sqrt{A_2})$  and  $F(\sqrt{A_1} - \sqrt{A_2})$  quadratic extensions of  $F$ . Let  $\sigma_1$  be the element of  $\text{Gal}(L_0/F)$  with fixed field  $F(\sqrt{A_1} + \sqrt{A_2})$  and let  $\sigma_2$  be the element of  $\text{Gal}(L_0/F)$  with fixed field  $F(\sqrt{A_1} - \sqrt{A_2})$ . Then we note that  $\sigma_1(x_0) = x_0$  and  $\sigma_2(x_0) = x_3$ . We have

$$\sigma_1(g_3) = \frac{(\sqrt{A_3} + \sqrt{A_2})(\sqrt{A_3} + \sqrt{A_1})}{12\Delta^{\frac{1}{3}}\sigma_1(\sqrt{-3})}$$

and

$$\sigma_2(g_0) = 1$$

Therefore by Lemma 3.1  $\sigma_1$  and  $\sigma_2$  commute if and only if

$$\frac{(\sqrt{A_3} + \sqrt{A_2})(\sqrt{A_3} + \sqrt{A_1})}{12\Delta^{\frac{1}{3}}\sigma_1(\sqrt{-3})} = \frac{(\sqrt{A_3} + \sqrt{A_1})(\sqrt{A_3} + \sqrt{A_2})}{12\Delta^{\frac{1}{3}}\sqrt{-3}}$$

Which is if and only if  $\sigma_1(\sqrt{-3}) = \sqrt{-3}$ . Therefore if  $\text{Gal}(L/F)$  is abelian then  $F(\sqrt{A_1} + \sqrt{A_2}) = F(\sqrt{-3})$  and hence  $P$  has a root in  $F_{nr}$ . But then by [Kra, Proposition 3]  $L_0/F$  is unramified. Contradiction!  $\square$

Therefore  $L = F(\mu_3, \sqrt{A_1} + \sqrt{A_2}, \sqrt{g(x_0)})$ . Let  $\delta$  be a character of  $F(\mu_3)^\times$  with kernel the group of norms from  $F(\mu_3)(\sqrt{A_1} + \sqrt{A_2}, \sqrt{g(x_0)})$  then

$$W(E/F) = (-1)^{\frac{\alpha(E/F)}{2}} \delta(\sqrt{-3}).$$

## 10 $P$ is irreducible over $F$

Now assume that  $P$  is irreducible over  $F$ . This is equivalent to  $A_i$  not being a square in  $F$  for all  $i$ . The resolvent polynomial of  $P$  is

$$h(x) = x^3 - \frac{\Delta}{3^3}$$

and the discriminant of  $P$  is  $-\frac{\Delta^2}{3^3}$ . From Galois theory (see for example [DF, pg 594]) we have the following

- If  $\mu_3 \notin F$  and  $\Delta$  is not a cube in  $F$  then  $\text{Gal}(L_0/F) \cong S_4$ .
- If  $\mu_3 \in F$  and  $\Delta$  is not a cube in  $F$  then  $\text{Gal}(L_0/F) \cong A_4$ .
- If  $\mu_3 \in F$  and  $\Delta$  is a cube in  $F$  then  $\text{Gal}(L_0/F) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
- If  $\mu_3 \notin F$ ,  $\Delta$  is a cube in  $F$  and  $P$  is irreducible over  $F(\mu_3)$  then  $\text{Gal}(L_0/F) \cong D_8$ .
- If  $\mu_3 \notin F$ ,  $\Delta$  is a cube in  $F$  and  $P$  is reducible over  $F(\mu_3)$  then  $\text{Gal}(L_0/F) \cong \mathbf{Z}/4\mathbf{Z}$ .

We first assume that  $\mu_3 \in F$ . Note that by Lemma 7.1 we have

$$W(E/F) = W(E/F(\Delta^{\frac{1}{3}})).$$

Hence we can reduce to the case that  $\Delta$  is a cube in  $F$ . Now  $L_0 = F(\sqrt{A_1}, \sqrt{A_2})$  is biquadratic over  $F$ . We note that  $e(L/F) = 4$  or  $8$  and  $L$  has degree 8 over  $F$  by [Kra, Proposition 3].

**Lemma 10.1.**  *$L$  is not abelian over  $F$ .*

*Proof.* Take  $\sigma_1, \sigma_2 \in \text{Gal}(L_0/F)$  with fixed fields  $F(\sqrt{A_1})$  and  $F(\sqrt{A_2})$  respectively. Then  $\sigma_1(x_0) = x_1$  and  $\sigma_2(x_0) = x_2$ . We compute

$$\sigma_1(g_2) = \frac{(-\sqrt{A_2} + \sqrt{A_1})(-\sqrt{A_2} - \sqrt{A_3})}{12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta^2}$$

and

$$\sigma_2(g_1) = \frac{(-\sqrt{A_1} + \sqrt{A_2})(-\sqrt{A_1} - \sqrt{A_3})}{12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta}$$

Therefore we have  $\frac{\sigma_1(g_2)}{g_2} = \frac{\sigma_2(g_1)}{g_1}$  if and only if

$$\frac{(-\sqrt{A_2} + \sqrt{A_1})(-\sqrt{A_2} - \sqrt{A_3})}{(\sqrt{A_2} + \sqrt{A_1})(\sqrt{A_2} + \sqrt{A_3})} = \frac{(-\sqrt{A_1} + \sqrt{A_2})(-\sqrt{A_1} - \sqrt{A_3})}{(\sqrt{A_1} + \sqrt{A_2})(\sqrt{A_1} + \sqrt{A_3})}$$

which is if and only if

$$\frac{-\sqrt{A_2} + \sqrt{A_1}}{\sqrt{A_2} + \sqrt{A_1}} = \frac{(-\sqrt{A_1} + \sqrt{A_2})}{(\sqrt{A_1} + \sqrt{A_2})}$$

Which is not true. Hence by lemma 3.1 we deduce that  $\text{Gal}(L/F)$  is not abelian.  $\square$

Therefore  $\sigma_E$  is induced from a character of some quadratic extension of  $F$ .

(i)  $e(L/F) = 4$ : Therefore  $H = F(\sqrt{A_k})$  is the unramified quadratic extension of  $F$  for some  $k$ , fix  $k$ . Let  $\delta$  be a character of  $F(\sqrt{A_k})^\times$  with kernel the group of norms from  $F(\sqrt{A_k})(\sqrt{A_i}, \sqrt{g(x_0)})^\times$ , with  $i \neq k$ . Then

$$W(E/F) = (-1)^{\frac{a(E/F)}{2}} (-1)^{v_H(\sqrt{A_k})} \delta \left( \frac{\sqrt{A_k}}{\varpi_F^{v_H(\sqrt{A_k})}} \right)$$

(ii)  $e(L/F) = 8$ : In this case  $\text{Gal}(L/F) \cong H_8$  and  $\sigma_E$  is induced from a character of  $F(\sqrt{A_i})^\times$  for each  $i$ . For each  $i$  we can write

$$\sigma_E = \text{Ind}_{F(\sqrt{A_i})/F} \chi_i$$

for some character  $\chi_i$  of  $F(\sqrt{A_i})^\times$ . Let  $\tau_i$  be the non-trivial element of  $\text{Gal}(F(\sqrt{A_i})/F)$  then

$$\sigma_E|_{F(\sqrt{A_i})} = \chi_i \oplus \chi_i^{\tau_i}.$$

Since  $E$  has good reduction over  $L$  we have

$$\chi_i = \alpha_i \omega_i$$

where  $\alpha_i$  is one of the two characters of  $F(\sqrt{A_i})^\times$  associated to the quartic cyclic extension  $L/F(\sqrt{A_i})$  and  $\omega_i$  is unramified. Now

$$\chi_i^{\tau_i} = \alpha_i^{\tau_i} \omega_i.$$

Since  $\det(\sigma_E|_{F(\sqrt{A_i})}) = |\cdot|_{F(\sqrt{A_i})}$  we deduce that

$$\alpha_i^{\tau_i} = \alpha_i^{-1}$$

and

$$\omega_i^2 = |\cdot|_{F(\sqrt{A_i})}.$$

Therefore

$$\omega_i = |\cdot|_{F(\sqrt{A_i})}^{\frac{1}{2}}$$

or

$$\omega_i = \delta_i | \cdot |_{F(\sqrt{A_i})}^{\frac{1}{2}}$$

where  $\delta_i$  is the unramified quadratic character on  $F(\sqrt{A_i})^\times$ . Since  $L = F(E[3])$  we see that  $\sigma_E|_L$  must be trivial mod 3. Therefore we deduce that

$$\omega_i = \begin{cases} \delta_i | \cdot |_{F(\sqrt{A_i})} & \text{if } \sqrt{q} \equiv 2 \pmod{3} \\ | \cdot |_{F(\sqrt{A_i})} & \text{if } \sqrt{q} \equiv 1 \pmod{3} \end{cases}$$

Let  $\psi$  be a non-trivial additive character of  $F$  then

$$W(E/F) = (-1)^m W(\delta_{F(\sqrt{A_i})/F}, \psi) W(\alpha_i, \psi_{F(\sqrt{A_i})})$$

where

$$m = \begin{cases} a(L/F(\sqrt{A_i})) + n(\psi_{F(\sqrt{A_i})}) & \text{if } \sqrt{q} \equiv 2 \pmod{3} \\ 0 & \text{if } \sqrt{q} \equiv 1 \pmod{3} \end{cases}$$

Now assume that  $\mu_3 \not\subset F$ . We first show that we can reduce to the case that  $\Delta$  is a cube in  $F$ . So suppose that  $\Delta$  is not a cube in  $F$ . In this case we have  $\text{Gal}(L_0/F) \cong S_4$  and therefore  $\text{Gal}(L_0/F(\mu_3))$  is not abelian. Therefore we deduce that  $\sigma_E$  is either imprimitive or else is induced from a character of a ramified quadratic extension of  $F$ . Applying [Kut, Proposition 5.1.8] and [Kut, Lemma 5.2.4] together with the fact that  $W(E/F) = \pm 1$  we deduce that

$$W(E/F) = (-1)^{a(E/F)} W(E/F(\Delta^{\frac{1}{3}})).$$

We now assume that  $\Delta$  is a cube in  $F$ .

(i)  $P$  is reducible over  $F(\mu_3)$ . So  $\text{Gal}(L_0/F) \cong \mathbf{Z}/4\mathbf{Z}$  and we have  $F(\sqrt{A_3}) = F(\mu_3)$ .

**Lemma 10.2.** *We have  $\text{Gal}(L/F) \cong \mathbf{Z}/8\mathbf{Z}$ .*

*Proof.* We have  $K = F(\mu_3, \sqrt{A_1})$  and  $\text{Gal}(K/F) \cong \mathbf{Z}/4\mathbf{Z}$ . Let  $\tau \in \text{Gal}(L/F)$  be such that  $\tau|_K$  has order 4. We wish to show that  $\tau$  has order 8. We have  $\tau(\sqrt{-3}) = -\sqrt{-3}$ ,  $\tau(\sqrt{A_1}) = \sqrt{A_2}$  and  $\tau(\sqrt{A_2}) = -\sqrt{A_1}$ . Therefore we have  $\tau(x_0) = x_2$  and hence

$$\tau(g(x_0)) = g(x_2) = \frac{g(x_0)}{g_2^2}$$

Therefore we can assume that  $\tau(\sqrt{g(x_0)}) = \frac{\sqrt{g(x_0)}}{g_2}$ . Therefore we have

$$\tau^4(\sqrt{g(x_0)}) = \frac{\sqrt{g(x_0)}}{g_2 \tau(g_2) \tau^2(g_2) \tau^3(g_2)}$$

Now

$$\begin{aligned}
g_2\tau(g_2) &= \frac{(\sqrt{A_2} + \sqrt{A_1})(\sqrt{A_2} + \sqrt{A_3})}{12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta^2} \frac{(-\sqrt{A_1} + \sqrt{A_2})(-\sqrt{A_1} - \sqrt{A_3})}{-12\Delta^{\frac{1}{3}}\sqrt{-3}\zeta} \\
&= \frac{(A_2 - A_1)(\sqrt{A_2} + \sqrt{A_3})(-\sqrt{A_1} - \sqrt{A_3})}{432\Delta^{\frac{2}{3}}} \\
&= \frac{(\zeta^2 - \zeta)(\sqrt{A_2} + \sqrt{A_3})(\sqrt{A_1} + \sqrt{A_3})}{36\Delta^{\frac{1}{3}}}
\end{aligned}$$

And

$$\tau^2(g_2)\tau^3(g_2) = \frac{(\zeta^2 - \zeta)(-\sqrt{A_2} + \sqrt{A_3})(-\sqrt{A_1} + \sqrt{A_3})}{36\Delta^{\frac{1}{3}}}$$

Therefore

$$\begin{aligned}
g_2\tau(g_2)\tau^2(g_2)\tau^3(g_2) &= \frac{(\zeta^2 - \zeta)^2(A_3 - A_2)(A_3 - A_1)}{1296\Delta^{\frac{2}{3}}} \\
&= \frac{-3(12\Delta^{\frac{1}{3}}(\zeta^2 - 1))(12\Delta^{\frac{1}{3}}(\zeta - 1))}{1296\Delta^{\frac{2}{3}}} \\
&= -1
\end{aligned}$$

Therefore we have  $\tau^4(\sqrt{g(x_0)}) = -\sqrt{g(x_0)}$  and hence  $\tau$  has order 8.  $\square$

Therefore we have  $e(L/F) = 2$  or  $4$ . Moreover we have  $e(L/F) = 2$  if and only if  $F(\mu_3, \sqrt{A_1})$  is unramified over  $F(\mu_3)$ . If  $e(L/F) = 2$  then  $L_0 = F(\mu_5)$ . Let  $x \in F(\mu_5)$  be such that

$$N_{F(\mu_5)(\sqrt{g(x_0)})/F(\mu_5)} x = -1$$

then

$$W(E/F) = (x, g(x_0))_{F(\mu_5)}.$$

If  $e(L/F) = 4$  let  $\delta$  be a character on  $F(\mu_3)^\times$  corresponding to  $L/F(\mu_3)$  then

$$W(E/F) = \delta(2 + \sqrt{5}).$$

(ii)  $P$  is irreducible over  $F(\mu_3)$ . In this case we have  $\text{Gal}(L_0/F) \cong D_8$  and  $\text{Gal}(L_0/F(\mu_3)) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Therefore we deduce that  $e(L/F) = 4$  or  $8$ . However, if  $e(L/F) = 4$  then  $\text{Gal}(L/F(\mu_3))$  is abelian, but this is not so by Lemma 10.1. Therefore we deduce that  $e(L/F) = 8$  and  $L$  has degree 16 over  $F$ , hence  $\text{Gal}(L/F)$  is isomorphic to the 2 Sylow subgroup of  $\text{GL}_2(\mathbf{F}_3)$  which is generated by the matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

with the relation  $ABA^{-1} = B^3$ .

Now consider  $F_1 = F(\sqrt{-3A_3})$ , a ramified quadratic extension of  $F$  contained in  $L$ . By part (i) above we see that  $\text{Gal}(L/F_1) \cong \mathbf{Z}/8\mathbf{Z}$  and hence that  $\sigma_E$  is induced from a character  $\chi$  of  $F_1^\times$ . We can write  $\chi = \alpha\omega$  where  $\omega$  is an unramified character and  $\alpha$  is one of the four characters associated to the extension  $L/F_1$ . Now we have  $\sigma_E|_{F_1} = \chi \oplus \chi^\tau$  where  $\tau$  is the non-trivial element of  $\text{Gal}(F_1/F)$  and we have  $\chi^\tau = \alpha^\tau\omega$ .

**Lemma 10.3.** *We have  $\alpha^\tau = \alpha^3$ .*

*Proof.* Since  $L/F$  is Galois we see that  $\alpha^\tau$  is also associated to the extension  $L$  of  $F_1$ . Under the isomorphism of  $\text{Gal}(L/F)$  with the 2-Sylow subgroup of  $\text{GL}_2(\mathbf{F}_3)$ ,  $F_1$  is the field fixed by  $B$ , and since  $ABA^{-1} = B^3$  the result follows.  $\square$

We have  $\det(\sigma_E|_{F_1}) = |\cdot|_{F_1}$  and hence we have  $\alpha^4\omega^2 = |\cdot|_{F_1}$ . Now  $\alpha^4$  is the unramified quadratic character of  $F_1^\times$ . Hence if  $\varpi_{F_1}$  is a uniformizer in  $F_1$  then we have  $\omega(\varpi_{F_1})^2 = -q^{-1}$ . We can assume, by changing  $\alpha$  if necessary that  $\omega(\varpi_{F_1}) = iq^{-\frac{1}{2}}$ . We now wish to determine  $\alpha$ . First we make explicit the embedding  $\text{Gal}(L/F_1) \hookrightarrow \text{GL}_2(\mathbf{F}_3)$  given by the action of Galois on  $E[3]$ . Let  $P_0 = (x_0/12, \sqrt{g(x_0)})$  and  $P_1 = (x_1/12, g(x_1))$ . We take  $\theta$  to be the element of  $\text{Gal}(L/F_1)$  such that  $\theta(\sqrt{A_3}) = -\sqrt{A_3}$ ,  $\theta(\sqrt{A_1}) = \sqrt{A_2}$ ,  $\theta(\sqrt{A_2}) = -\sqrt{A_1}$  and  $\theta(\sqrt{g(x_0)}) = \sqrt{g(x_2)}$ . Then we have

$$\theta(P_0) = (x_2, \sqrt{g(x_2)}) = P_0 \oplus P_1$$

and

$$\theta(P_1) = (x_0, \sqrt{g(x_0)}) = P_0.$$

Hence with respect to the basis  $\{P_0, P_1\}$  of  $E[3]$ ,  $\theta$  corresponds to the matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

We have  $\text{Gal}(L/F_1) = \langle \theta \rangle$ , now  $\alpha$  is a faithful character of this group and we are trying to determine exactly which character  $\alpha$  is. We set  $z = \exp\left(\frac{2\pi i}{8}\right)$ . Then we can assume that either  $\alpha(\theta) = z$  or  $\alpha(\theta) = z^5$ . Now let  $\phi \in W_{F_1}$  such that  $\phi$  is equal to  $\theta$  when restricted to  $L$ . Then we see that  $\phi$  must induce an odd power of Frobenius on the maximal unramified extension of  $F_1$ , since  $\theta$  is non-trivial on the unramified quadratic extension of  $F$ . Under the representation  $\sigma_E|_{F_1}$  we have

$$\phi \mapsto \begin{pmatrix} \alpha(\theta)(iq^{-\frac{1}{2}})^{2a+1} & \\ & \alpha(\theta)^3(iq^{-\frac{1}{2}})^{2a+1} \end{pmatrix}.$$

Therefore

$$\begin{aligned} \text{Tr}(\sigma_E|_{F_1}(\phi)) &= (\alpha(\theta) + \alpha(\theta)^3)(iq^{-\frac{1}{2}})^{2a+1} \\ &= (\alpha(\theta) + \alpha(\theta)^3)(-q^{-1})^a(iq^{-\frac{1}{2}}) \end{aligned}$$

Now we can write  $q = 2^{2k+1}$ , since  $\mu_3 \not\subset F$  and then we have

$$\begin{aligned}\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) &= (\alpha(\theta) + \alpha(\theta)^3)(iq^{-\frac{1}{2}})^{2a+1} \\ &= (\alpha(\theta) + \alpha(\theta)^3)(-2^{-2k-1})^a (i2^{-\frac{2k+1}{2}}).\end{aligned}$$

Now if  $\alpha(\theta) = z$  then we have

$$\begin{aligned}\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) &= (z + z^3)(-2^{-2k-1})^a (i2^{-\frac{2k+1}{2}}) \\ &= i\sqrt{2}(-2^{-2k-1})^a (i2^{-\frac{2k+1}{2}}) \\ &= -2^{-k}(-2^{-2k-1})^a.\end{aligned}$$

While on the other hand, if  $\alpha(\theta) = z^5$  then we have

$$\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) = 2^{-k}(-2^{-2k-1})^a.$$

But now, under the action of Galois on  $F_1(E[3])$  we see that the trace of  $\theta$  is 1 mod 3. Hence we need

$$\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) \equiv 1 \pmod{3}.$$

Now if  $\alpha(\theta) = z$  then we have

$$\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) = -2^{-k}(-2^{-2k-1})^a \equiv -(-1)^k \pmod{3}$$

and if  $\alpha(\theta) = z^5$  then we have

$$\mathrm{Tr}(\sigma_E|_{F_1}(\phi)) = 2^{-k}(-2^{-2k-1})^a \equiv (-1)^k \pmod{3}.$$

Therefore we have the following result.

**Lemma 10.4.** *With everything as above we have  $\sigma_E = \mathrm{Ind}_{F_1/F} \alpha\omega$  where  $\alpha$  is the character of  $\mathrm{Gal}(L/F_1)$  such that*

$$\alpha(\theta) = \begin{cases} \exp(2\pi i/8), & \text{if } k \text{ is even;} \\ \exp(-2\pi i/8), & \text{if } k \text{ is odd.} \end{cases}$$

And we can now give the formula for the root number of  $E$ .

**Proposition 10.5.** *With notation and assumptions as above we have*

$$W(E/F) = i^{n(\psi_{F_1})+a(\alpha)} W(\delta_{F_1/F}, \psi) W(\alpha, \psi_{F_1}).$$

## 11 Summary

Putting this all together we have the following results.

**Proposition 11.1.** *Assume that  $\mu_3 \subset F$ . Then with notation as above we have the following.*

(i) *P has a root in F: Let  $x' \in F$  be a root of P then*

$$W(E/F) = (-1, g(x'))_F.$$

(ii) *P splits into the product of two irreducible quadratics over F: Fix  $\Delta^{\frac{1}{3}} \in F$  such that  $\sqrt{A_3} \in F$ .*

- *If  $F(\sqrt{A_1})/F$  is unramified then let  $x \in F(\sqrt{A_1})$  such that  $N_{F(\sqrt{A_1})/F}x = -1$ , then*

$$W(E/F) = (x, g(x_0))_{F(\sqrt{A_1})}.$$

- *If  $F(\sqrt{A_1})/F$  is ramified then let  $\delta$  be a character of  $F^\times$  whose kernel is the group of norms from  $F(\sqrt{A_1}, \sqrt{g(x_0)})$  then*

$$W(E/F) = \delta(-1).$$

(iii) *P is irreducible over F: Let  $F' = F(\Delta^{\frac{1}{3}})$ .*

- *If  $H = F'(\sqrt{A_k})/F'$  is unramified for some k then let  $\delta$  be a character of  $F'(\sqrt{A_k})^\times$  with kernel the group of norms in  $F'(\sqrt{A_k})^\times$  from  $F'(\sqrt{A_k})(\sqrt{A_i}, \sqrt{g(x_0)})^\times$  with  $i \neq k$ . Then*

$$W(E/F) = (-1)^{\frac{a(E/F)}{2}} (-1)^{v_H(\sqrt{A_k})} \delta \left( \frac{\sqrt{A_k}}{\varpi_{F'}^{v_H(\sqrt{A_k})}} \right).$$

- *If  $F'(\sqrt{A_k})/F'$  is ramified for all k let  $\psi$  be an additive character of  $F'$ , let  $\delta$  be the character of  $F'^\times$  associated to the quadratic extension  $F'(\sqrt{A_1})/F'$  and let  $\alpha$  be a character of  $F'(\sqrt{A_1})^\times$  associated to the extension  $F'(\sqrt{A_1})(\sqrt{A_2}, \sqrt{g(x_0)})$  then*

$$W(E/F) = (-1)^m W(\delta, \psi) W(\alpha, \psi_{F'(\sqrt{A_1})})$$

where

$$m = \begin{cases} a(L/F'(\sqrt{A_1})) + n(\psi_{F'(\sqrt{A_1})}) & \text{if } \sqrt{q} \equiv 2 \pmod{3} \\ 0 & \text{if } \sqrt{q} \equiv 1 \pmod{3}. \end{cases}$$

**Proposition 11.2.** *Assume that  $\mu_3 \not\subset F$ . Then with notation as above we have the following.*

(i) *P has a root in F: Let  $x' \in F$  be a root of P.*

- *If  $F(\sqrt{g(x')})/F$  is unramified then*

$$W(E/F) = -1.$$

- If  $F(\sqrt{g(x')})/F$  is ramified then

$$W(E/F) = (-1)^{\frac{a(E/F)}{2}} (3, g(x'))_F.$$

(ii)  $P$  splits into the product of two irreducible quadratics over  $F$ : Fix  $\Delta^{\frac{1}{3}} \in F$  such that  $\sqrt{A_3} \in F$ .

- If  $F(\sqrt{A_1})/F$  is unramified then

$$W(E/F) = (2 + \sqrt{5}, g(x_0))_{F(\mu_3)}.$$

- If  $F(\sqrt{A_1})/F$  is ramified then let  $\delta$  be a character of  $F(\mu_3)^\times$  whose kernel is the group of norms from  $F(\mu_3)(\sqrt{A_1} + \sqrt{A_2}, \sqrt{g(x_0)})$  then

$$W(E/F) = (-1)^{\frac{a(E/F)}{2}} \delta(\sqrt{-3}).$$

(iii)  $P$  is irreducible over  $F$ : Let  $F' = F(\Delta^{\frac{1}{3}})$ . We set  $m = 0$  if  $\Delta^{\frac{1}{3}} \in F$ , and  $m = a(E/F)$  otherwise.

(a)  $P$  is reducible over  $F'(\mu_3)$ .

- If  $F'(\mu_3, \sqrt{A_1})/F'$  is unramified then  $F'(\mu_3, \sqrt{A_1}) = F'(\mu_5)$ . Let  $x \in F'(\mu_5)$  such that  $N_{F'(\mu_5)(\sqrt{g(x_0)})/F'(\mu_5)} x = -1$  then

$$W(E/F) = (x, g(x_0))_{F'(\mu_5)} (-1)^m.$$

- If  $F'(\mu_3, \sqrt{A_1})/F'$  is ramified let  $\delta$  be a character on  $F'(\mu_3)^\times$  corresponding to  $L/F'(\mu_3)$ . Then

$$W(E/F) = \delta(2 + \sqrt{5}) (-1)^m.$$

(b)  $P$  is irreducible over  $F'(\mu_3)$ . We set  $F'_1 = F'(\sqrt{-3A_3})$ . Let  $\alpha$  be the character of  $\text{Gal}(L/F'_1)$  given above and let  $\delta$  be the quadratic character of  $F'^\times$  corresponding to the extension  $F'_1$ . Then

$$W(E/F) = i^{n(\psi_{F'_1}) + a(\alpha)} W(\delta, \psi) W(\alpha, \psi_{F_1}) (-1)^m.$$

## References

- [Con] I. Connell, *Calculating Root Numbers of Elliptic Curves over  $Q$* , Manusc. Math. **82** (1994), 93-104.
- [DF] D. Dummitt, R. Foote, *Abstract Algebra*, Prentice Hall, 1991.
- [Hal] E. Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3*, C. R. Acad. Sci. Paris Série, I Math. **326** (1998), 1047-1052.

- [Kob] S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Math. Ann. **323** (2002), 609-623.
- [KT] K. Kramer and J. Tunnell, *Elliptic curves and local  $\varepsilon$ -factors*, Compos. Math. **46** (1982), 307-352.
- [Kra] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manusc. Math. **69** (1990), 353-385.
- [Kut] P. Kutzko, *The local Langlands conjecture for  $GL(2)$* , Ann. of Math. **112** (1980), 381-412.
- [Ro1] D. E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87** (1993), 119-151.
- [Ro2] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic curves and related topics, 125-157, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994.
- [Ro3] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. **100** (1996), 311-349.
- [Tat] J. Tate, *Number Theoretic Background*, in Automorphic Forms, Representations and  $L$ -functions, Proc. Symp. in Pure Math. **XXXIII** Part 2 (1979), 3-26.
- [Tun] J. B. Tunnell, *On the local Langlands Conjecture for  $GL(2)$* , Invent. Math. **46** (1978), 179-200.