Review of the proof of the WMW theorem

The point of view of nb. theory

Wlog assume $E[n] \subseteq K$. Have

$$0 \to E[n](\bar{k}) \to E(\bar{k}) \xrightarrow{[n]} E(\bar{k}) \to 0$$

$$\rightsquigarrow \quad 0 \to E[n] \to E(k) \xrightarrow{[n]} E(k) \to H^1(\Gamma_K, E[n])$$

$$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| $$

$$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathrm{Hom}(G_K, E[n])$$

Now let v be a place of K, with completion K_v, s.t.

1) E has good red at v
2) $v \nmid n$

We have a similar sequence

$$E(K_v) \xrightarrow{[n]} E(K_v) \xrightarrow{\delta} \mathrm{Hom}(G_{K_v}, E[n])$$

Let $\varphi \in \operatorname{im} \delta$. I claim that $\varphi(I(\bar{v}|v)) = \{0\}$.
Indeed, let $\varphi = \delta(P)$ and $\sigma \in I(\bar{v}|v)$. Then

$$\varphi(\sigma) = \sigma\left(\tfrac{1}{n}P\right) - \tfrac{1}{n}P \in E[n].$$

But $E[n] \hookrightarrow \tilde{E}_w(\mathbb{F}_w)$, and $\widetilde{\varphi(\sigma)} = \sigma\left(\widetilde{\tfrac{1}{n}P}\right) - \widetilde{\tfrac{1}{n}P}$
(where $w|v$ is a place of $K_v(\tfrac{1}{n}P)$) $\quad = \widetilde{\tfrac{1}{n}P} - \widetilde{\tfrac{1}{n}P} = 0.$

By injectivity, $\varphi(\sigma) = 0$, so φ is UNRAMIFIED at v.

The claim now follows since K has only fin'ly many ab exts of exponent $| n$ unramified outside all but finitely many places.

The pt of view of geometry

E extends to an étale scheme $\mathcal{E}$ over $\operatorname{Spec} \mathcal{O}_K\left[\frac{1}{n \prod_{v \text{ bad}} v}\right] = \overset{\operatorname{Spec}}{R}$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \overset{\shortparallel}{B}$

$$0 \to \mathcal{E}[n] \to \mathcal{E} \xrightarrow{[n]} \mathcal{E} \to 0 \quad \text{(as étale sheaves on } B)$$

$$\rightsquigarrow \quad \mathcal{E}(R) \xrightarrow{[n]} \mathcal{E}(R) \to H^1_{\text{ét}}(\operatorname{Spec} R, \mu_n^{\oplus 2})$$

But $H^1_{\text{ét}}(\operatorname{Spec} R, \mu_n^{\oplus 2}) \simeq H^1_{\text{ét}}(\operatorname{Spec} R, \mu_n)^{\oplus 2}$ $\cancel{\not\simeq R^\times}$ fits inside

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{\wedge n} \mathbb{G}_m \to 1$$

$$\rightsquigarrow \quad R^\times \to R^\times \to H^1_{\text{ét}}(R, \mu_n) \to H^1_{\text{ét}}(R, \mathbb{G}_m)$$

$$R^\times / R^{\times n} \to H^1_{\text{ét}}(R, \mu_n) \to \operatorname{Pic}(R)[n]$$
$$\shortparallel$$
$$\mathcal{Cl}(R)[n]$$

5-descent on $X_1(11)$

Recall $X_1(11)$: $y^2 + y = x^3 - x^2$

We already observed that $(0,0) =: P \in X_1(11)(\mathbb{Q})$ has order 5, and that $\# X_1(11)(\mathbb{Q})_{\text{tors}} = 5$. The 5 pts in question are easy to find: $x = 0 \rightsquigarrow y = 0, -1$ & ∞.
$x = 1 \rightsquigarrow y = 0, -1$

Thus, we have an isogeny $\phi : X_1(11) \to \cancel{X_0(11)}\ X_1(11)/\langle P \rangle$.
Incidentally, this happens to be the forgetful map

$$\phi : X_1(11) \to X_0(11).$$

By the general theory, there is $\hat{\phi} : X_0(11) \to X_1(11)$ such that $\hat{\phi} \circ \phi = [5]$.

Rmks

① $X_0(11)$: $y^2 + y = x^3 - x^2 - 10x - 20$,

② How to compute $\phi : X_1(11) \longrightarrow X_0(11)$? Not too bad, use Vélu's formulas (in particular, if $G \subseteq E$ is a finite subgroup, the fn. field of E/G is generated by $\sum_{Q \in G \setminus \{\infty\}} (x \circ \tau_Q - x(Q)) + x =: X$

$\sum_{Q \in G \setminus \{\infty\}} (y \circ \tau_Q - y(Q)) + y =: Y$

$$\phi(x,y) = \left(\frac{x^5 - 2x^4 + 3x^3 - 2x + 1}{(x(x-1))^2}, \frac{x^6y - 3x^5y + x^4y - x^4 - 3x^3y - x^3 + 6x^2y + 3x^2 - 6xy - 3x + 2y + 1}{(x(x-1))^3} \right)$$

③ How to compute $\hat{\phi}$? Actually, I will only need its kernel. Thus, we just need to push $X_1(11)[5]$ through ϕ and read the resulting x-coordinates. I don't have a fantastically smart way to do this: The result is that $\ker \hat{\phi}$ is the set $\{\infty\} \cup \{ P : x(P)^2 + x(P) - 29/5 \} =: H$

④ Note that $H \not\simeq \mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}$. In fact, it's necessarily μ_5, by the Weil pairing: ρ_5 looks like $\begin{pmatrix} 1 & * \\ 0 & \chi_5 \end{pmatrix}$

⑤ The usual torsion analysis shows that $X_0(11)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$ generated by the pt $(5,5)$
(To see this: $\# X_0(11)(\mathbb{F}_2) = \# X_0(11)(\mathbb{F}_3) = 5$) (Or, if we don't like reducing mod 2, $\# X_0(11)(\mathbb{F}_7) = 10$)

⑥ Isogenies preserve the rk, so we expect rk $X_0(11)(\mathbb{Q}) = 0$. ~~This~~ Since $X_0(11)$ has 2 cusps, both rational, this proves that there are precisely 3 ell. curves over $\mathbb{Q}$ that admit an 11-isog. over $\mathbb{Q}$. ($\hat{\bar{\mathbb{Q}}}$-iso classes of)

(Their j-inv. are -121, $\underset{\text{CM } -11}{-32768}$, -24729001)

⑦ Since $\ker \hat{\phi} \simeq \mu_5$ has only 1 pt over $\mathbb{Q}$, we KNOW that $\hat{\phi} : X_0(11)(\mathbb{Q}) \longrightarrow X_1(11)(\mathbb{Q})$ is injective.

On the other hand, ϕ has ker of order 5, so we expect that:

(a) - $\hat{\phi}$ is surjective

(b) - ϕ has cokernel $\dfrac{X_0(11)(\mathbb{Q})}{\phi(X_1(11)(\mathbb{Q}))} \simeq \mathbb{Z}/5\mathbb{Z}$.

We'll show ~~that~~ (a) and (b). Together, they imply that $[5]_{X_0(11)} = \phi \circ \hat{\phi}$ has cokernel $\mathbb{Z}/5\mathbb{Z}$. Writing

$$X_0(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}^r$$

we then obtain $r = 0$, hence also $\operatorname{rk} X_1(11)(\mathbb{Q}) = 0$, as desired.

(b) Consider the exact sequence

$$0 \to \mathbb{Z}/5\mathbb{Z} \cdot (0,0) \to X_1(11)(\bar{\mathbb{Q}}) \xrightarrow{\phi} X_0(11)(\bar{\mathbb{Q}}) \longrightarrow 0$$

Take Gal cohomology:

$$\begin{array}{ccccc} X_1(11)(\mathbb{Q}) & \xrightarrow{\phi} & X_0(11)(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G_{\mathbb{Q}}, \mathbb{Z}/5\mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow \text{Res} \\ X_1(11)(\mathbb{Q}_p) & \xrightarrow[\phi]{} & X_0(11)(\mathbb{Q}_p) & \xrightarrow{\delta} & H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z}) \end{array}$$

Reasoning as in WMW, for $p \neq 5, 11$ $\operatorname{Res}_{G_{\mathbb{Q}_p}}(\delta P)$ is unramified

But in fact, $\langle(0,0)\rangle \hookrightarrow$ reduction mod 5 (look at the physical pts!), so imm δ consists of classes that are unram. outside 11.

Now some alg nb theory: who are the $\mathbb{Z}/5\mathbb{Z}$-exts of $\mathbb{Q}$ ramified only at 11? There's only $\mathbb{Q}(\zeta_{11})^+$, by Kronecker-Weber (they lie inside ~~the~~ some $\mathbb{Q}(\zeta_n)$; since p ramifies $\Leftrightarrow p \mid n$, we have $n = 11^h$, and the
(choose $4 \mid n$ or n odd)
11-adic tower only contains $\mathbb{Q}(\zeta_{11})^+$ as an $\mathbb{F}_5$-subext)

Once we fix $\ker \varphi$, there are at most 5^4 morphisms $G_{\mathbb{Q}} \longrightarrow \mathbb{Z}/5\mathbb{Z}$ with the given kernel, so the image of δ lands inside a 1-dim'l $\mathbb{F}_5$-subspace.

<u>Conclusion</u>: $\dfrac{X_0(11)(\mathbb{Q})}{\phi(X_1(11)(\mathbb{Q}))} \hookrightarrow \mathbb{Z}/5\mathbb{Z}$. On the other hand, torsion pts come from torsion pts, and all the torsion pts of $X_1(11)(\mathbb{Q})$ lie in $\ker \varphi$, so

$$\mathbb{Z}/5\mathbb{Z} \simeq X_0(11)(\mathbb{Q})_{\text{tors}} \hookrightarrow \frac{X_0(11)(\mathbb{Q})}{\phi(X_1(11)(\mathbb{Q}))}$$

$$\Rightarrow \frac{X_0(11)(\mathbb{Q})}{\phi(X_1(11)(\mathbb{Q}))} \simeq \mathbb{Z}/5\mathbb{Z}, \text{ that is, (b).}$$

<u>Geometry</u> We have $0 \to \mathbb{Z}/5\mathbb{Z} \to \mathcal{E}_1 \longrightarrow \mathcal{E}_0 \to 0$ in the étale site of $\mathbb{Z}[\frac{1}{5\cdot 11}]$, and even in the flat site of $\mathbb{Z}[\frac{1}{11}] =: R$

Thus, $\mathcal{E}_1(R) \xrightarrow{\phi} \mathcal{E}_0(R) \to H^1_{fppf}(R, \mathbb{Z}/5\mathbb{Z})$
(since $\mathbb{Z}/5\mathbb{Z}$ is smooth) $= H^1_{et}(\mathbb{Z}[\frac{1}{11}], \mathbb{Z}/5\mathbb{Z})$, and we conclude as above.

(a) Now for the hard part. For the dual isogeny $\hat{\phi}$ we have

$$0 \to \mu_5 \to X_0(11)(\overline{\mathbb{Q}}) \xrightarrow{\hat{\phi}} X_1(11)(\overline{\mathbb{Q}}) \to 0,$$

which gives

$$\begin{tikzcd}
X_0(11)(\mathbb{Q}) \arrow[r, "\hat{\phi}"] \arrow[d, hook] & X_1(11)(\mathbb{Q}) \arrow[r] \arrow[d, hook] & H^1(G_{\mathbb{Q}}, \mu_5) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 5} \\
X_0(11)(\mathbb{Q}_p) \arrow[r, "\hat{\phi}_p"'] & X_1(11)(\mathbb{Q}_p) \arrow[r] & H^1(G_{\mathbb{Q}_p}, \mu_5) \simeq \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 5}
\end{tikzcd}$$

<u>Lemma</u> Let $L = \mathbb{Q}_p(\mu_5)$. The natural map $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 5} \to L^\times/L^{\times 5}$ is injective

<u>Proof</u> We have to show that $L^{\times 5} \cap \mathbb{Q}_p^\times = \mathbb{Q}_p^{\times 5}$. Consider

$$1 \to \mu_5 \to L^\times \to L^{\times 5} \to 1, \quad G := Gal(L/\mathbb{Q}_p) \hookrightarrow \mathbb{Z}/4\mathbb{Z}.$$

The LES in cohom. gives

$$1 \to \mu_5(\mathbb{Q}_p) \to \mathbb{Q}_p^\times \to L^{\times 5} \cap \mathbb{Q}_p^\times \to H^1(G, \mu_5) = (0),$$ where

the (0) comes from $(|G|, |\mu_5|) = 1$ $\square$

<u>Claim</u> For $p \neq 11$, ~~$\hat{\phi}_p$ is surjective~~ the cokernel of $\hat{\phi}_p$ is unramified

<u>Proof</u> We have a commutative diagram

$$\begin{tikzcd}
X_0(11)(\mathbb{Q}_p) \arrow[r, "\hat{\phi}"] \arrow[d, hook] & X_1(11)(\mathbb{Q}_p) \arrow[r, "\delta"] \arrow[d, hook] & \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 5} \arrow[d, hook] \\
X_0(11)(L) \arrow[r, "\hat{\phi}_L"'] & X_1(11)(L) \arrow[r, "\delta"'] & L^\times/L^{\times 5}
\end{tikzcd}$$

~~Suppose $\hat{\phi}$ surj $\Leftrightarrow \delta \equiv 1$ Suppose $\delta(P) \neq 1$ for some $P \in X_1(11)(\mathbb{Q}_p)$. Then by diagram chasing $\delta(P) \neq 1$ also~~

~~when we consider $P \in X_1(11)(L)$. But ϕ~~

Suppose that $\delta_{\mathbb{Q}_p}(P)$ involves p. Then the same is true for $\delta_L(P)$ when P is considered as a pt of $X_1(11)(L)$.

But this means that the field of def'n of the inverse images $\hat{\phi}_L^{-1}(P)$ is ramified. This is not the case by the usual argument, provided that $\ker \hat{\phi}_L$ injects in the reduction. This is certainly true for $p \neq 5, 11$.

For $p=5$, courtesy of Ilaria: the field $L(\hat{\phi}_L^{-1}(P))$ is of the form $L(\sqrt[5]{\alpha})$. The claim is that $v_5(\alpha) \equiv 0 \ (5)$

If $v_5(\alpha) > 0$, its disc is divisible at least by p^6;

if $v_5(\alpha) = 0$, the disc has strictly lower valuation.

If I didn't miscompute, the disc has valuation 5 in this case.

Geometry: exactly the same as before,

$$0 \to \mu_5 \to \mathcal{E}_0 \xrightarrow{\hat{\phi}} \mathcal{E}_1 \to 0 \quad \text{on the fppf site of } \mathbb{Z}[1/11]$$

$\hookrightarrow$ Weil pairing

$$\rightsquigarrow \quad X_0(11)(\mathbb{Q}) \xrightarrow{\hat{\phi}} X_1(11)(\mathbb{Q}) \to H^1(\mathbb{Z}[1/11], \mu_5)$$

$$H^1(\mathbb{Z}[1/11], \mu_5) = \langle 11 \rangle / \langle 11 \rangle^5$$

This gives $\dfrac{X_1(11)(\mathbb{Q})}{\hat{\phi}(X_0(11)(\mathbb{Q}))} \hookrightarrow \mathbb{F}_5$, but this is still not enough! The wild claim is now that $X_0(11)(\mathbb{Q}_{11}) \xrightarrow{\hat{\phi}} X_1(11)(\mathbb{Q}_{11})$ is ONTO!

Claim 1 Let $E := X_1(11)$. We have $E(\mathbb{Q}_{11}) = E_0(\mathbb{Q}_{11})$

Proof Recall that $X_1(11) \; : \; y^2 + y = x^3 - x^2$

What's the singularity? $\begin{cases} 2y+1 = 0 \\ 3x^2 - 2x = 0 \\ y^2 + y = x^3 - x^2 \end{cases}$ $\begin{cases} y = -1/2 \\ x = 2/3 \\ -1/4 = \frac{8}{27} - \frac{12}{27} \\ \quad\;\; = -\frac{4}{27} \end{cases}$

(and indeed, $-\frac{1}{4} = -\frac{4}{27}$ in $\mathbb{F}_{11}$)

Translating, we set $X := x - 2/3$, $Y := y + 1/2$ and get

$$Y^2 = X^3 + X^2 + 11/108$$

If $(X, Y) \equiv (0,0) \mod 11$ contradiction, because

$$1 = v_{11}\left(\frac{11}{108}\right) = v_{11}\left(Y^2 - X^3 - X^2\right) \geq 2 \qquad \square$$

Rmk This is a special instance of the "converse" to Hensel's lemma: if R is a DVR, $\mathcal{X} \to \operatorname{Spec} R$ is regular, and $P : \operatorname{Spec} R \longrightarrow \mathcal{X}$ is a section, then $P \bmod \pi$ is a smooth point of $\mathcal{X}_{(R/\pi)}$

Claim 2 $\tilde{X}_0(11)^{ns}(\mathbb{F}_{11}) \xrightarrow{\hat{\phi}} \tilde{X}_1(11)^{ns}(\mathbb{F}_{11})$ is onto.

Proof Both have size $10 = \# \mathbb{G}_m(\mathbb{F}_{11})$. It suffices to check that $\hat{\phi}$ is injective. But $\ker \hat{\phi}$ consists of pts with $x^2 + x - \frac{29}{5} = 0$. Mod 11, the sols are $x = -1/2$ on $X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$.

$y^2 + y = 8$ $\quad y = -1/2$. Now, what's the sing pt of $X_0(11)/\mathbb{F}_{11}$?

$X_0(11)^{sing}$: $\begin{cases} 2y + 1 = 0 \\ 3x^2 - 2x + 1 = 0 \\ -1/4 = x^3 - x^2 + x + 2 \end{cases}$ and $x = y = 5 = -1/2$ is a common solution!

$\Rightarrow \ker \hat{\phi}$ is trivial on the non-sing part $\qquad \square$

Claim 3 a. $E_1(\mathbb{Q}_{11}) \subseteq E_0(\mathbb{Q}_{11})$ with index 10

b. $E_1(\mathbb{Q}_{11})$ is a pro-11 group.

Proof

a. $E_0(\mathbb{Q}_{11}) / E_1(\mathbb{Q}_{11}) \simeq \tilde{E}(\mathbb{F}_{11}) \simeq \mathbb{F}_{11}^\times$

b. This is basically Hensel's lemma. Clearly

$$E_1(\mathbb{Q}_{11}) = \varprojlim \ker\left(E(\mathbb{Z}/11^r\mathbb{Z}) \to E(\mathbb{F}_{11})\right);$$

it suffices to show that $\nearrow$ is an 11-group, hence, by induction, that $\# \ker\left(E(\mathbb{Z}/11^{r+1}\mathbb{Z}) \to E(\mathbb{Z}/11^r\mathbb{Z})\right) = 11$. Since ∞ is a smooth pt of E, the nb. of lifts from $\mathbb{Z}/11^r\mathbb{Z}$ to $\mathbb{Z}/11^{r+1}\mathbb{Z}$ is a power of 11 (in fact, 11): in local coordinates, $E: f(x,y) = 0$, with $\infty \leftrightarrow (0,0)$, and $\frac{\partial f}{\partial x}(0,0) \not\equiv 0 \ (11)$. It follows that $x_{lift} = 11^r \cdot a$, $y_{lift} = 11^r \cdot b$ with

$$0 \equiv f(x_{lift}, y_{lift}) \equiv \frac{\partial f}{\partial x}(0,0) \cdot a \cdot 11^r + \frac{\partial f}{\partial y}(0,0)\, b \cdot 11^r \mod 11^{r+1}$$

$$\Rightarrow \quad 0 \equiv \frac{\partial f}{\partial x}(0,0) \cdot a + \frac{\partial f}{\partial y}(0,0) \cdot b \ (11),$$

so it's a 1-dim'l $\mathbb{F}_{11}$-vector space. □

Claim 4 $X_0(11)(\mathbb{Q}_{11}) \xrightarrow{\hat{\phi}} X_1(11)(\mathbb{Q}_{11})$ is onto.

Proof The image of $\hat{\phi}$ contains $\operatorname{im} \hat{\phi} \circ \phi = \operatorname{im} [5]$, and $[5]$ is bijective on $(X_1(11)(\mathbb{Q}_{11}))_1$ by Claim 3. So the img of $\hat{\phi}$ contains $(X_1(11)(\mathbb{Q}_{11}))_1$, and on the other hand it projects surjectively onto $\tilde{X}_1(11)(\mathbb{F}_{11})$. Since $X_1(11)(\mathbb{Q}_{11}) = X_1(11)(\mathbb{Q}_{11})_0$, we are done! □

The end

We now know that in the diagram

$$\begin{tikzcd} X_0(11)(\mathbb{Q}) \arrow[r, "\hat{\phi}"] \arrow[d, "\rho"] & X_1(11)(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d, "\mathrm{Res}\,\rho"] & \mathbb{Q}^\times/\mathbb{Q}^{\times 5} \arrow[d, "\mathrm{Res}"] \\ X_0(11)(\mathbb{Q}_{11}) \arrow[r, "\hat{\phi}_{11}"'] & X_1(11)(\mathbb{Q}_{11}) \arrow[r, "\delta_{11}"'] & \mathbb{Q}_{11}^\times/\mathbb{Q}_{11}^{\times 5} \end{tikzcd}$$

the arrow $\hat{\phi}_{11}$ is onto, hence δ_{11} is the trivial morphism. Thus, $\mathrm{Res}\circ\delta(P) = \delta_{11}(\mathrm{Res}\,P) = 0$, hence $\delta(P) \in \mathbb{Q}_{11}^{\times 5}$, and in particular $v_{11}(\delta(P)) \equiv 0\ (5)$. But we already knew $v_q(\delta(P)) \equiv 0\ (5)\quad \forall q \neq 11$, so $\delta(P) \in \mathbb{Q}^{\times 5}$: δ is trivial, hence $\hat{\phi}_{\mathbb{Q}}$ is onto!