Chapter 4

Exercise 4.1-4.5 :

$E := X_0(11) = "\ y^2+y = x^3-x^2-10x-20\ "$

Basic informations :

- conductor 11, E has split multiplicative reduction at $p=11$, and good at all other primes.

  $\Longrightarrow$ We can see that, following [Silverman, VII.6.1], $E(\mathbb{Q}_{11})/E_0(\mathbb{Q}_{11})$ has order $-v_{11}(j_E) = 5$.

  (So "5" is another important prime)

  So we see that local Tamagawa numbers $\mathrm{Tam}_p(E/\mathbb{Q}) = \begin{cases} 5 & p=11 \\ 1 & p\neq 11 \end{cases}$.

- In this exercise we focus on the prime $p=5$, where E has good ordinary reduction : $a_5 = 1 \equiv 1 \bmod 5$

  (Actually we see E is modular with associated modular form the famous
  $$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \in S_2(\Gamma_0(11))\ )$$

- **Torsion :**

  1° $E(\mathbb{Q})_{tor} \simeq \mathbb{Z}/5\mathbb{Z}$, generated by an order 5 integral point $(16,5)$.

  2° We know $E[5] \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ as abstract groups. So there is another order 5 point $Q \in E(\bar{\mathbb{Q}})[5]$.

  By SAGE, we have (by trying to solve in $\mathbb{Q}(\zeta_5)$) :

  $$E[5] = \langle \underbrace{(16:60:1)}_{P},\ \underbrace{(4\zeta_5^3+2\zeta_5^2+3\zeta_5+2 : 3\zeta_5^3-4\zeta_5^2+5\zeta_5 : 1)}_{Q} \rangle$$

  where P, Q are generators of $E[5]$ of order five.

- It can be shown that $Ш(E/\mathbb{Q})$ is trivial. (maybe by Kolyvagin's work on the (finite) upper bound of Ш.

4.1 We hope to see the Galois structure of $E[5]$.

The action of $G_{\mathbb{Q}}$ can be descented to $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ by the previous explicit computation of $E[5]$. We choose:

- $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ to be a generator, sending $\zeta_5 \mapsto \zeta_5^2$
- a temperary $\mathbb{F}_5$-basis $\{P, Q\}$ as before of $E[5]$.

Then (by SAGE), $\bar{\rho}_5 : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[5]) \xrightarrow{\sim} GL_2(\mathbb{F}_5)$:

- $\rho(\sigma)(P) = P$, $\rho(\sigma)(Q) = P + 2Q$

So the corresponding matrix for $\rho(\sigma)$ under $\{P, Q\}$ is $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

By changing the basis $\{P, Q\} \rightsquigarrow \{P' = P,\ Q' = P + Q\}$, we see

- $\rho(\sigma)(P') = P'$, $\rho(\sigma)(Q') = P + P + 2Q = 2Q'$

So the matrix in the new basis is $\begin{pmatrix} 1 & \\ & 2 \end{pmatrix}$.

Therefore, we see $E[5] = \mathbb{F}_5 \cdot P' \oplus \mathbb{F}_5 \cdot Q'$ where $G_{\mathbb{Q}}$ acts on the P'-line trivially, and on the Q'-line by the "cyclotomic character" i.e. $E[5] \simeq \mathbb{Z}/5 \oplus \mu_5$ as $G_{\mathbb{Q}}$-modules.

Note: This is the case that we seldom deal with, i.e. the reside representation is reducible (recall "$E[p]$ is irreducible" is an important hypothesis for almost all current works). There are new breakthrough on this case by Castella, Grossi, Skinner et. al very recently.

- E has two $\mathbb{Q}$-isogenies of degree 5. (actually this is equivalent to that $E[p]$ is reducible), call them E_1, E_2. Then $E_1[p]$, $E_2[p]$ has NONSPLIT $\mathbb{F}_5[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-module extensions

$$0 \longrightarrow \Sigma_1 \longrightarrow E_1[p] \longrightarrow \Psi_1 \longrightarrow 0 \qquad \checkmark$$

$$0 \longrightarrow \Psi_2 \longrightarrow E_2[p] \longrightarrow \Sigma_2 \longrightarrow 0$$

where $\cdot\ \Sigma_i \simeq \mu_5$ (so $G_{\mathbb{Q}}$-action is ramified at $p=5$)

$\cdot\ \Psi_i \simeq \mathbb{Z}/5$ (so $G_{\mathbb{Q}}$-action is trivial)

We shall see that "Iwasawaly", the three curves are quite different in nature!

Exercise 4.2-4.4 : The ultimate goal is to show that E has μ-invariant positive at $p=5$. We make the assumption more general :

- Assume $E[p]$ contains an $\mathrm{Gal}_{\mathbb{Q}}$-invariant subgroup $\mathbb{I} \simeq \mu_p$

Let Σ be the finite set containing p, ∞ and primes that E has bad reduction.

① Consider the natural map

$$\varepsilon_{\mathbb{I}} : H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_5) \longrightarrow H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[5^\infty])$$

Then $\varepsilon_{\mathbb{I}}$ has finite kernel.

Proof of ① : Postpone it later.

② So in some sense we only need to work with the "smaller" $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_5)$. where we use "Kummer theory" : consider

$$1 \longrightarrow \mu_p(\mathbb{Q}_\Sigma) \longrightarrow \mathbb{Q}_\Sigma^\times \xrightarrow[x(-)^p]{} \mathbb{Q}_\Sigma^\times \longrightarrow 1$$

Then we take $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-cohomology :

$$1 \longrightarrow \frac{U_\infty}{U_\infty^p} \xrightarrow{\beta} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p(\mathbb{Q}_\Sigma)) \longrightarrow H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mathbb{Q}_\Sigma^\times)[p] \longrightarrow 0$$

Note : • $\mu_p(\mathbb{Q}_\Sigma) = \mu_p(\overline{\mathbb{Q}})$ since Σ includes the prime p.

• $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mathbb{Q}_\Sigma^\times) = 0$ by Hilbert Satz 90.

so β induces an isomorphism :

$$\beta : \frac{U_\infty}{U_\infty^p} \xrightarrow{\sim} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p) .$$

Therefore from here we see $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)$ is Λ-cotorsion since U_∞/U_∞^p is so.

Claim : The $\Lambda/p\Lambda$-module $\frac{U_\infty}{U_\infty^p}$ has $\Lambda/p\Lambda$-corank 1.

We postpone its proof. Then we deal with the μ-invariant.

- In general for a Λ-module M of finite type and torsion (eg: $M = \check{U}_\infty$ in our mind), we have (written additively)

$$M/pM \xrightarrow{\text{pseudo-isom}} \underbrace{\bigoplus_{i=1}^{r} \Lambda/(p, p^{e_i})}_{\bigoplus_{i=1}^{r} \Lambda/(p)} \oplus \underbrace{\bigoplus_{j=1}^{s} \Lambda/(p, f_j(T)^{g_j})}_{\text{finite, where } f_j(T) \text{ are distinguished polynomials.}}$$

then $\operatorname{rank}_{\Lambda/p\Lambda} M/pM$ = # of direct summands in the "μ-invariant part" $\leq \mu_M$ and the equality holds iff all e_i $(i=1,\cdots,r)$ are one. In our case, this condition is satisfied since p kills $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)^\vee$ (?) Therefore,

$$\operatorname{rank}_{\Lambda/p\Lambda} U_\infty/U_\infty^p = \mu\text{-inv. of } H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)^\vee = 1,$$

as desired!

Remark: Ignoring "(?)" in this page above, we can also show a weaker result that μ-invariant of $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)^\vee$ is positive. This suffices for Exercise 4.4 for considering the μ-invariant of the elliptic curve.

Doubt (?): In Exercise 4.2, we are required to show $\mu = 1$. But since β is ~~not necessarily surjective (or at least, I don't know how to show $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \bar{\mathbb{Q}}_\infty^\times)[p]=0$)~~ So I got stuck here. Anyway, knowing the positivity is enough for the following up exercises.

③ Next we show that the image of $\mathcal{E}_p$ lies in $Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)$. First we invoke Exercise 2.9:

$$Sel^{(p^\infty)}(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), E[p^\infty]) \longrightarrow \prod_{v\in\Sigma_{\mathbb{Q}_\infty}} H^1(\mathbb{Q}_{\infty,v}, E[p^\infty])/_{\operatorname{im}(K_v)}\right)$$

where $\Sigma_{\mathbb{Q}_\infty}$ is the set of places of $\mathbb{Q}_\infty$ lying above Σ, and $\operatorname{im}(K_v)$ is the image of local Kummer maps K_v:

$$K_v : E(\mathbb{Q}_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(\mathbb{Q}_{\infty,v}, E[p^\infty]).$$

So we deal with two cases:

Case 1: $v \in \Sigma_{\mathbb{Q}_\infty}$, $p \nmid v$. We consider the composition

$$U_\infty/U_\infty^p \xhookrightarrow[\cong]{\beta} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p) \xrightarrow{\mathcal{E}} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])$$

Consider $\varphi \in \operatorname{im}\beta \subseteq H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)$, φ is given by a cocycle

$$\varphi : \operatorname{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty) \longrightarrow \mu_p$$
$$\sigma \longmapsto \sigma(u^{1/p})/u^{1/p} \quad \text{for some } u \in \mathbb{Q}_\infty^\times.$$

($u \in \mathbb{Q}_\infty^\times$, $u^{1/p} \in \bar{\mathbb{Q}}_\infty^\times$)

Note that all units of $\mathbb{Q}_{\infty,v}$ are p-powers, we see that actually $u^{1/p} \in \mathbb{Q}_{\infty,v}$ so for $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}_{\infty,v}/\mathbb{Q}_{\infty,v})$, $\varphi(\sigma) = 1$, i.e. $\varphi|_{\operatorname{Gal}\mathbb{Q}_{\infty,v}}$ = trivial class.

Therefore we see immediately that $\mathrm{im}(\varepsilon\circ\beta)$ satisfies the local conditions defining the Selmer group at $v\nmid p$ (including archmedian primes).

Case 2 : $v\in\Sigma_{\mathbb{Q}_\infty}$, v is lying over p. (This is Exercise 4.3)

Then recall the local condition can be written as

$$\mathrm{im}(\kappa_v)=\mathrm{im}(\lambda_v : H^1(\mathbb{Q}_{\infty,v}, C_p)\longrightarrow H^1(\mathbb{Q}_{\infty,v}, E[p^\infty]))$$

where C_p is the kernel of $E[p^\infty]\xrightarrow{\mathrm{red}_v}\tilde{E}[p^\infty]$ (by choosing an embedding $\bar{\mathbb{Q}}\to\bar{\mathbb{Q}}_p$) and λ_v is induced from the inclusion $C_p\subseteq E[p^\infty]$. We hope to show

$$\begin{array}{ccc} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty,\mu_p) & \xrightarrow{\iota} & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, C_p) \\ & \searrow^{\varepsilon} & \downarrow\lambda \\ & & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \end{array}$$

that ε factors through the (global) map λ by showing μ_p is contained in C_p. Then it will imply that $\mathrm{im}(\varepsilon\circ\beta)\subseteq\mathrm{im}(\lambda)$, and therefore locally at v, elements in $\mathrm{im}(\varepsilon\circ\beta)$ lies in $\mathrm{im}(\lambda_v)=\mathrm{im}(\kappa_v)$, hence satisfy the local Selmer condition at $v\mid p$.

To see $\mu_p\subseteq C_p$, we note that

- $I_{\mathbb{Q}_p}$ acts nontrivially on μ_p since p is odd.
  (Here we use essentially that μ_p is ramified at p!)
- $I_{\mathbb{Q}_p}$ acts trivially on $E[p^\infty]/C_p$ by defn of C_p, where C_p is the kernel of the reduction map.

Combing the two, we see that indeed $\mu_p\subseteq C_p$, as desired.

Combing case 1 and case 2, $\mathrm{im}(\beta\circ\varepsilon)\subseteq\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}_\infty)$. Similar to the argument of ②, we see that $\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}_\infty)^\vee$ has positive μ-invariant since it is a priori Λ-torsion by [Greenberg, PC note, Cor.4.9].

~~Doubt~~

- Actually we have only shown $\mathrm{im}(\beta\circ\varepsilon)\subseteq\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}_\infty)$, though the exercise asked me to show $\mathrm{im}(\varepsilon)\subseteq\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}_\infty)$, ~~which is even stronger~~. However, ~~the latter may be inapplicable since we do not know the general cocycles in $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty,\mu_p)$~~ β is ~~merely injective~~ already an isomorphism. □
  it is the same thing since we have see

Remark: Here is still a gap: through β is an isomorphism, Σ is in general not. Here we invoke ① that $\ker\Sigma$ is finite: by the kernel-cokernel exact sequence,

$$0 \longrightarrow \ker\beta \longrightarrow \ker(\beta\circ\Sigma) \longrightarrow \ker\Sigma \longrightarrow \cdots$$
$$\qquad\qquad \| \; 0$$

so $\ker(\beta\circ\Sigma)$ is finite. So it will not harm when we take the characteristic ideal. □

Remark:(1) This example is used by Greenberg to illustrate the proof of the general proposition:

Proposition (Greenberg, LNM, Prop. 5.7) p is an odd prime.

Assume $E/\mathbb{Q}$, good ordinary or multiplicative at p. $Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)$ is Λ-torsion. Assume $E[p^\infty]$ contains a cyclic $G_{\mathbb{Q}}$-invariant subgroup Φ of order p^m which is ramified at p, and "odd", then μ_E (at p) $\geq m$.

What we have proved is just the $m=1$ case. In the example E, E_1, E_2, only E and E_1 has a $G_{\mathbb{Q}}$-invariant sub $\Phi \simeq \mu_5$, while unfortunately E_2 does not!

and the converse of the above also holds:

Proposition (Greenberg, LNM, Prop. 5.10) Same setup.

Assume $E[p^\infty]$ contains a $G_{\mathbb{Q}}$-invariant subgroup Φ of order p which is either

- ramified at p and "even"
- unramified at p and "odd"

Then $Sel_{\Phi}^{(p^\infty)}(E/\mathbb{Q}_\infty)$ is Λ-cotorsion and $\mu_E = 0$.

This is the case of E_2. Indeed, $\mu_E = 1$, $\mu_{E_1} = 2$, $\mu_{E_3} = 0$.

Greenberg also stated a conjecture (Conj. 1.11 in [loc.cit]):

$E/\mathbb{Q}$. Assume $Sel_{\Phi}^{(p^\infty)}(E/\mathbb{Q}_\infty)$ is Λ-cotorsion, and $E[p]$ is irreducible as $\mathbb{Z}/p\mathbb{Z}$-rep of $Gal_{\mathbb{Q}}$, then $\mu_E = 0$.

This is the more classical case.

(2) We also remark that there are other invariant besides the μ-invariant.

- λ-invariant : Why there are not so many results on λ-invariant. (?)
- $f_{E(0)}$: In class, we have seen the "refined control thm" : rk 0

Assume E good ordinary at p and $Sel^{(p^\infty)}(E/\mathbb{Q})$ is finite, then

$$f_{E(0)} \overset{\text{differs by a } p\text{-adic unit}}{\sim} \left(\prod_{l \in \Sigma_{bad}} Tam_l^{(p)} \right) \cdot |\widetilde{E}_p(\mathbb{F}_p)[p^\infty]|^2 \frac{|Sel^{(p^\infty)}(E/F)|}{|E(\mathbb{Q})[p^\infty]|^2}$$

tor

Note that under the condition, $Sel^{(p^\infty)}(E/\mathbb{Q}) = Ш(E/\mathbb{Q})[p^\infty]$.

In our case $E = X_0(11)$ and $p=5$, all these numbers are availble by the introduction of this talk. We see : $f_{E(0)} \sim 5$

$\rightsquigarrow$ So from here we see directly that $\mu_E = 1$.

Why $f_{E(0)}$ is important ? Suppose X is non-pseudonull, then :

(a) for $0 \neq \lambda \in \Lambda$, $\#\, X/\lambda X = \#\, \Lambda/(char(X), \lambda)$

(b) in particular, if f_X is a characteristic polynomial of X, then

$$\#\, X/(\gamma - 1) = \#\, \mathbb{Z}_p / f_X(0)$$

Then we have an equality on the estimate $\#\, X/(\gamma-1)X$. By Pontragin dual, $\#\, X/(\gamma-1)X = \#\, Sel(?/?_\infty)^\Gamma$, where the latter is related to the finite level invariants by control theorems. This is how we obtained the "refined control theorem". Then

as above, arithmetic invariants of $\mathbb{Q}$

$f_{E(0)}$ ~ (refined CT)

$\|$ ← Iwasawa main conjecture à la Mazur — rank zero

$\mathcal{L}_p(E/\mathbb{Q})(0)$

(construction of p-adic L-functions (MTT)) $\left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\sqrt{2}_E}$

explicit formula again

"$f_{E(0)}$" ~ (refined CT (Jetchev-Skinner-Wan)) — rk one

$\|$ ← IMC à la BDP

$\mathcal{L}_p^{BDP}(E/K)^2(0)$ $\overset{\text{BDP formula}}{=\!=}$ $\frac{1}{u_K^2 C_E^2} \left(\frac{1 - a_p(E) + p}{p} \right)^2 \log_{\omega_E}(y_K)^2$

Exercise 4.5 :

Remark. [Greenberg, LNM Thm1.10] implies that for the given $E = X_0(11)$,

$\exists\ \lambda, \mu, \nu$ such that for $n \gg 0$,

$$\left| Ш(E/\mathbb{Q}_n)[p^\infty] \right| = p^{\mu p^n + \lambda n + \nu} \quad \text{for } \mu = \mu\left(X(E/\mathbb{Q}_\infty)\right),\ \lambda = \lambda\left(X(E/\mathbb{Q}_\infty)\right) - \lambda_{MW}$$

where λ_{MW} = the maximum of $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}_n)$ as n varies. This is well-defined since $\left\{ \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}_n) \right\}_{n \in \mathbb{N}}$ is bounded by [Greenberg, Thm1.6].

However, this is not what we need for this exercise since :

- the object is $Ш(E/\mathbb{Q}_n)[p^\infty]$, not $Ш(E(\mathbb{Q}_n)[p]$ as in the exercise.
- the cardinality "=" holds for all $n \gg 0$, but it is required to show for all $n > 0$ in the exercise.

We then start with the short exact sequence for every n :

$$0 \longrightarrow E(\mathbb{Q}_n) \otimes \mathbb{Z}/p \longrightarrow Sel^{(p)}(E/\mathbb{Q}_n) \longrightarrow Ш(E/\mathbb{Q}_n)[p] \longrightarrow 0$$

Then taking $\dim_{\mathbb{F}_p}(-)$, note $\operatorname{rank}_{\mathbb{F}_p}\left(E(\mathbb{Q}_n) \otimes \mathbb{Z}/p\right) = \operatorname{rank}_{\mathbb{Z}}(\mathbb{Q}_n)$, we see

$$\begin{aligned} \dim_{\mathbb{F}_p}\left(Ш(E/\mathbb{Q}_n)[p]\right) &= \dim_{\mathbb{F}_p} Sel^{(p)}(E/\mathbb{Q}_n) - \operatorname{rank}_{\mathbb{Z}}(\mathbb{Q}_n) \\ &\geq \dim_{\mathbb{F}_p} Sel^{(p)}(E/\mathbb{Q}_n) - \lambda_{MW} \end{aligned}$$

here λ_{MW} is well-defined by [Greenberg, Thm1.6] as before. So the main term is $\dim_{\mathbb{F}_p} Sel^{(p)}(E/\mathbb{Q}_n)$. But how to relate it to Iwasawa-theoretic invariants ? (We lack a "horizontal control" : $Sel^{(p)}(E/\mathbb{Q}_n) \hookrightarrow Sel^{(p^\infty)}(E/\mathbb{Q}_n)$)

"Horizonal Control" (Claimed by Haidong) : $Sel^{(p)}(E/\mathbb{Q}_n) = Sel^{(p^\infty)}(E/\mathbb{Q}_n)[p]$.

Granting this, we can turn to $Sel^{(p^\infty)}(E/\mathbb{Q}_n)$: by Mazur's control thm, we have for good ordinary prime p,

$$0 \longrightarrow K \longrightarrow Sel^{(p^\infty)}(E/\mathbb{Q}_n) \longrightarrow Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n} \longrightarrow C \longrightarrow 0$$

where K and C are of finite cardinality. Note that $(-)[p]$ is left exact on torsion groups, we have

$$0 \longrightarrow K[p] \longrightarrow Sel^{(p^\infty)}(E/\mathbb{Q}_n)[p] \xrightarrow{\varphi_n} Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n}[p].$$

$$\| \text{ horizontal control}$$

$$Sel^{(p)}(E/\mathbb{Q}_n)$$

We then turn to $Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n}[p]$. Denote by $X(E/\mathbb{Q}_\infty)$ the Pontragin dual of $Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)$. then by Pontragin duality,

$$Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n}[p] = \mathrm{Homcts}\left((X/p)_{\Gamma_n}, \mathbb{Q}_p/\mathbb{Z}_p\right),$$

whose $\mathbb{F}_p$-dimension is the same as $\dim_{\mathbb{F}_p}(X/p)_{\Gamma_n}$

Now for our explicit elliptic curve E, we can show that $\mu_E = 1$, $\lambda_E = 0$ (see the remark after our solution of this), so actually there is an exact sequence

$$0 \longrightarrow K' \longrightarrow X \longrightarrow \Lambda/p \longrightarrow C' \longrightarrow 0$$

where K', C' are of finite cardinality. Then moding p and take Γ_n-coinvariant, we have (note that they are only right exact):

$$(K'/p)_{\Gamma_n} \xrightarrow{\text{"}\xi_n\text{"}} (X/p)_{\Gamma_n} \longrightarrow \Lambda/(p, \omega_n(T)) \xrightarrow{\eta_n} (C'/p)_{\Gamma_n} \to 0$$

Then taking $\dim_{\mathbb{F}_p}$ along this exact sequence, we see (by taking an epi-mono decomposition of "ξ" and "η"):

$$\dim_{\mathbb{F}_p}(X/p)_{\Gamma_n} = \underbrace{\dim_{\mathbb{F}_p}(\operatorname{im}\xi_n)}_{\text{bdd finite independent of } n \text{ (dep on only } \#K')} + \dim_{\mathbb{F}_p} \ker(\eta_n)$$

$$= \dim_{\mathbb{F}_p}(\ker\xi) + \dim_{\mathbb{F}_p} \Lambda/(p, \omega_n(T))$$

As $\omega_n(T) = (T+1)^{p^n} - 1$, we see easily that $\dim_{\mathbb{F}_p} \Lambda/(p, \omega_n(T)) = p^n$.

More explicitly: as

- $0 \to \ker\eta_n \to \Lambda/(p, \omega_n(T)) \to (C'/p)_{\Gamma_n} \to 0$
- $0 \to \ker\xi_n \to (K'/p)_{\Gamma_n} \to \operatorname{im}\xi_n \to 0$

we see

$$\dim_{\mathbb{F}_p}(X/p)_{\Gamma_n} = \underbrace{\left(\dim(K'/p)_{\Gamma_n} - \ker\xi_n\right)}_{\text{(i)}} + \underbrace{\dim_{\mathbb{F}_p} \Lambda/(p, \omega_n(T))}_{\text{main term}} - \underbrace{\dim_{\mathbb{F}_p}(C'/p)_{\Gamma_n}}_{\text{(ii)}}$$

and (i) is bounded by "K'" and "C'" independent of n, and the main term is of $\dim_{\mathbb{F}_p} p^n$.

Putting everything together, we see

$$\dim_{\mathbb{F}_p} Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n}[p] = \dim_{\mathbb{F}_p}(X/p)_{\Gamma_n} \geq p^n + D_1$$

D_1 is a constant coming from (i) & (ii)

(note: it could be either positive or negative).

and

$$\dim_{\mathbb{F}_p} Sel^{(p)}(E/\mathbb{Q}_n) \overset{\text{"horizontal control"}}{=\!=} \dim_{\mathbb{F}_p} Sel^{(p^\infty)}(E/\mathbb{Q}_n)[p]$$

$$= \dim_{\mathbb{F}_p} K[p] + \dim_{\mathbb{F}_p}(\ker \wp_n)$$

$$= \underbrace{\dim_{\mathbb{F}_p} K[p]}_{\text{(iii)}} + \underbrace{\dim_{\mathbb{F}_p} Sel^{(p^\infty)}(E/\mathbb{Q}_\infty)^{\Gamma_n}[p]}_{\text{main term}} - \underbrace{\dim_{\mathbb{F}_p} \operatorname{im} \wp_n}_{\text{(iv)}}$$

and (iii) is bounded by "K", (iv) by "C", so then $\geq p^n + D_1 + D_2$ where D_2 comes from (iii) and (iv) is a constant. To sum up, we have seen

$$\dim_{\mathbb{F}_p}\left(Ш(E/\mathbb{Q}_n)[p]\right) \geq p^n + \underbrace{D_1 + D_2 - \lambda_{MW}}_{\text{altogether be the constant } c \text{ in the exercise}}.$$

□

Remark:

(1) For $\mu_E = 1$, it follows from the refined control theorem on the computation of $f(0)$, where f is the characteristic power series. Knowing $Sel^{(p^\infty)}(E/\mathbb{Q})$ is trivial, we see $f(0) \sim 5$. Note that it may contain constant term of distinguished polynomials at first glance. But as we have seen in Exercise 4.4 that $\mu_E > 0$, the only option is that $\mu_E = 1$.

(2) Also, continue the arguments above, we see the distinguished polys part ~~if f has constant terms~~ disappears, so $\lambda_E = 0$.

Actually the p in the solution above is only $p=5$ for the particular elliptic curve $E = X_0(11)$. But in the exercise we are required to show for all prime p. ∎

Exercise 4.7-4.8

The subtlety is at the algebraic part. We first make some general discussion:

- Suppose X is a finitely generated torsion Λ-module. Then by the structure theorem, X is pseudo-isomorphic to

$$X^{\#} = \bigoplus_{i=1}^{r} \Lambda/p^{e_i} \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{n_j}), \quad f_j: \text{distinguished polynomials}.$$

Then we solely work on $\omega_0(T) = T$ case below: consider $\operatorname{rank}_{\mathbb{Z}_p} X/TX$, then:

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p} X/TX &= \operatorname{rank}_{\mathbb{Z}_p} X^{\#}/TX^{\#} \\ &= \sum_{i=1}^{r} \operatorname{rank}_{\mathbb{Z}_p} \Lambda/(p^{e_i}, T) + \sum_{j=1}^{t} \operatorname{rank}_{\mathbb{Z}_p}\left(\Lambda/(\omega_0(T), f_j^{n_j})\right)\end{aligned}$$

Then note that

(1) We compute $\Lambda/(p^{e_i}, T) = \mathbb{Z}/p^{e_i}$ is a finite set, so it will not contribute to the "$\operatorname{rank}_{\mathbb{Z}_p}$"-part.

(2) The subtlety is on the distinguished polynomial part. We assume now that $\exists\ 0 \le s \le t$ ($s=0$, we mean there are no such polynomials) such that

$$T \mid f_1, \cdots, f_s, \quad T \nmid f_{s+1}, \cdots, f_t$$

Then for $s+1 \le j \le t$, $\Lambda/(T, f_j^{n_j})$ is finite [Washington, Lemma 13.7], so again they will not contribute to the "$\operatorname{rank}_{\mathbb{Z}_p}$"-part. What remains is the first part: for $1 \le j \le s$,

$$\operatorname{rank}_{\mathbb{Z}_p} \Lambda/(T, f_j^{n_j}) = \operatorname{rank}_{\mathbb{Z}_p} \Lambda/(T) = 1$$

So actually $\operatorname{rank}_{\mathbb{Z}_p} X/TX = s$, where $s = \#$ of direct summand such that f_j is divisible by T. Therefore,

$$\operatorname{rank}_{\mathbb{Z}_p} X/TX \le \underbrace{\operatorname{ord}_T(\operatorname{char}_\Lambda X)}_{:= \text{the exact power } l \text{ such that } T^l \,\|\, \operatorname{char}_\Lambda X}.$$

Moreover, the equality holds if and only if all the "T-divisible part" power n_j are one.

Remark: One may doubt if we can generalize it for $\omega_n(T) = (1+T)^{p^n} - 1$?

But unfortunately it may not be easy: write

$$\omega_n(T) = T \cdot \omega_n^b(T), \quad \omega_n^b(T) = T^{p^n-1} + \binom{p^n}{1} T^{p^n-2} + \cdots + \binom{p^n}{p^{n-1}} T + p$$

and note $\omega_n^b(T)$ is an p-Eisenstein polynomial, hence irreducible. Then we carry out the same argument as before:

- $\wedge/(p^{e_i}, \omega_n(T))$ is finite? I'm not sure!

  If we assume $e_i = 1$, then $\wedge/(p, \omega_n(T)) = \dfrac{\mathbb{F}_p[\![T]\!]}{(1+T)^{p^n}-1}$

  $= \mathbb{F}_p[\![T]\!]/T^{p^n}$ freshman's dream

  $\simeq \mathbb{F}_p^{\oplus p^n}$

  which is finite. But for higher e_i, we would have $\mathbb{Z}/p^{e_i}[\![T]\!]/((1+T)^{p^n}-1)$, but the freshman's dream is not available since non-leading coefficients of ω_n^b has only p-valuation 1, not p^{e_i}.

- For the distinguished poly part, ~~if we again consider s such that~~

  ~~$\omega_n(T) \mid f_1, \cdots, f_s$, $\omega_n(T) \nmid f_{s+1}, \cdots, f_t$~~

  ~~then since $\omega_n(T)$ is reducible we further consider~~

  ~~$f_1, \cdots, f_u$ such that $\gcd(f_j,$~~

  analogously, we need to consider three cases:

  (a) $(\omega_n(T), f_j) = 1$, say $f_{s+1}, \cdots, f_t$.

  (b) $(\omega_n(T), f_j) = \omega_n^b(T)$, say $f_{u+1}, \cdots, f_s$

  (c) $(\omega_n(T), f_j) = \omega_0(T) = T$, say $f_{u+1}, \cdots, f_u$.

  Then (d) $(\omega_n(T), f_j) = \omega_n(T)$, say $f_1, \cdots, f_v$.

- $\operatorname{rank}_{\mathbb{Z}_p} \wedge/(\omega_n(T), f_j^{n_j}) = \begin{cases} 1 & \text{in case (c)} \\ p^n - 1 \ (= \deg \omega_n^b(T)) & \text{in case (b)} \\ 0 & \text{in case (a)} \\ p^n & \text{in case (d)} \end{cases}$.

The wierd (exceptional) case (b)(d) makes us hard to conclude anything helpful. ~~If we add a quite strong hypothesis that $p^n - 1$~~

So it seems that only $\omega_0(T) = T$ works quite well. □

① Exercise 4.7 : Kato's inclusion actually gives

$$\mathrm{char}_\Lambda\big(X(E/\mathbb{Q})\big) \subseteq (\mathcal{L}_p(E/\mathbb{Q}))$$

Then we see $\mathrm{ord}_T\big(\mathrm{char}_\Lambda(X)\big) \leq \mathrm{ord}_T\big(\mathcal{L}_p(E/\mathbb{Q})\big) \overset{\text{by defn}}{=} \mathrm{ord}_{s=1} g_E(\kappa_0^{s-1}-1)$

$$= \mathrm{ord}_{s=1} \mathcal{L}_p(E/\mathbb{Q},s) .$$

By previous discussions, we have seen

$$\mathrm{rank}_{\mathbb{Z}_p} X/TX \leq \mathrm{ord}_T\big(\mathrm{char}_\Lambda(X)\big) .$$

The left hand side $= \mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}_\infty)^\Gamma\Big)$

$= \mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q})\Big)$ by Mazur's control theorem.

Then going through the fundamental short exact sequence,

$$0 \longrightarrow E(\mathbb{Q})\otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[p^\infty] \longrightarrow 0$$

we get $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \leq \Big(\mathrm{Sel}^{(p^\infty)}(E/\mathbb{Q})\Big)^{\mathrm{cork}_{\mathbb{Z}_p}}$ (note : here we are needless to consider the "Ш"), so combine them altogether, we see that

$$\mathrm{rank}_{\mathbb{Z}}\big(E(\mathbb{Q})\big) \leq \mathrm{ord}_{s=1} L_p(E/\mathbb{Q}) .$$

s=1

Remark.

(1) One may ask if we can further get upper bound in terms of $\mathrm{ord}_{s=1} L(E/\mathbb{Q},s)$.

But it seems hard ? Indeed, we know

$$\mathcal{L}_p(E/\mathbb{Q},1) = g_E(0) = (1-\beta_p p^{-1})^2 L(E/\mathbb{Q},1)/\Omega_E$$

so we know $\mathcal{L}_p(E/\mathbb{Q},1) \neq 0 \Leftrightarrow L(E/\mathbb{Q},1) \neq 0$ —— (MTT)

But what about information on the precise order ?

(2) $\mathcal{L}_p(E/\mathbb{Q})$ is first (?) constructed by Mazur-Tate-Teitelbaum, then they raised a "p-adic analogue" of BSD conjecture, now known as MTT conjecture :

(a) $\mathrm{ord}_{s=1} \mathcal{L}_p(E/\mathbb{Q},s) = \begin{cases} \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}), & p \text{ good ordinary} \\ \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})+1 & p \text{ pmd of split reductie reduction.} \end{cases}$

(b) In the second case, the leading coef of $\mathcal{L}_p(E/\mathbb{Q})$ is

$$\underbrace{\mathcal{L}_p(E)}_{\text{"}\mathcal{L}\text{-invariant of } E/\mathbb{Q}_p\text{"}} \cdot \#Ш(E/\mathbb{Q}) \cdot \frac{\mathrm{Reg}_p^{sch}(E)}{|E(\mathbb{Q})_{tor}|^2} \cdot \Big(\prod_{l \text{ bad}} \mathrm{Tam}_l(E/\mathbb{Q})\Big) \cdot \Omega_E$$

It is (in some sense) now a Theorem of Greenberg-Steven ! ($p \geq 5$)

- Global proof : Hida theory (on universal deformation) by [GS]
- Local proof : Kato-Kurihara-Tsuji, Colmez (of course w/ "Kato's element")

② Exercise 4.8

This time, we should start with the converse inclusion given by Skinner-Urban (under quite a lot assumptions) :

$$\mathrm{char}_\Lambda(X(E/\mathbb{Q}_\infty)) \overset{?}{\supseteq} (\mathcal{L}_p(E/\mathbb{Q})) \quad \text{---} (*)$$

Dating back to previous arguments, we see that the vital inequality

$$\text{"}\mathrm{rank}_{\mathbb{Z}_p} X/TX \leq \mathrm{ord}_T(\mathrm{char}_\Lambda(X))\text{"}$$

is not consistent with the inclusion here ! We need a stronger observation :

Fact : $X(E/\mathbb{Q}_\infty)$ has no nonzero pseudo-null submodule.

Actually this holds for all good ordinary prime p (See [Greenberg, LNM, Prop.4.15]) (note : Prop.4.8 loc.cit may not be enough.). With this fact in mind, we run again on

$$0 \longrightarrow X \xrightarrow{\theta} X^\# \longrightarrow \mathrm{coker}\,\theta \longrightarrow 0$$

and catch a snake on :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & X^\# & \longrightarrow & \mathrm{coker}\,\theta & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \times T} & & \downarrow{\scriptstyle \times T} & & \downarrow{\scriptstyle \times T} & & \\ 0 & \longrightarrow & X & \longrightarrow & X^\# & \longrightarrow & \mathrm{coker}\,\theta & \longrightarrow & 0 \end{array}$$

to see :

$$\cdots \longrightarrow \mathrm{coker}[T] \xrightarrow{\delta} X/TX \xrightarrow{\bar{\theta}} X^\#/TX^\# \longrightarrow \frac{\mathrm{coker}\,\theta}{T\,\mathrm{coker}\,\theta} \longrightarrow 0$$

and a little bit modification :

$$0 \longrightarrow \mathrm{im}\,\delta \longrightarrow X/TX \xrightarrow{\bar{\theta}} X^\#/TX^\# \longrightarrow \frac{\mathrm{coker}\,\theta}{T\,\mathrm{coker}\,\theta} \longrightarrow 0$$

Note that the left-most and right-most term is finite, we see directly

$$\mathrm{rank}_{\mathbb{Z}_p} X/TX = \mathrm{rank}_p X^\#/TX^\#$$

It seems that we have obtained something trivial. But now we are not satisfied : we count instead of taking $\mathbb{Z}_p$-rank :

$$\#\,\mathrm{im}(\delta)\cdot \#\,X^{\#}/TX^{\#} = \#\,X/TX \cdot \#\,\frac{\mathrm{coker}\,\theta}{T\,\mathrm{coker}\,\theta}.$$

Note that $\mathrm{coker}\,\theta$ is finite, hence $\#\,\frac{\mathrm{coker}}{T\cdot\mathrm{coker}} = \#\,\mathrm{coker}\,[T]$, but $\mathrm{im}(\delta)$ is a quotient of $\#\,\mathrm{coker}\,[T]$, which is smaller. So we see

$$\times \quad \boxed{\#\,X^{\#}/TX^{\#} \geq \#\,X/TX} \quad \leftarrow \text{(not enough)}$$

that $\#\,X^{\#}/TX^{\#}$ and $\#\,X/TX$ differs by a finite number, which means X/TX is infinite if and only if $X^{\#}/TX^{\#}$ is infinite !!

So we count $X^{\#}/TX^{\#}$, the arguments at the begining tells us that if $T \mid \mathrm{char}_{\Lambda}(X(E/\mathbb{Q}))$, then $X^{\#}/TX^{\#}$ is infinite. Now with Skinner-Urban's inclusion (*) in hand, we see that

$$L(E/\mathbb{Q},1)=0 \underset{\text{interpolating property}}{\Longleftrightarrow} L_p(E/\mathbb{Q},1)=0$$

$$\Longleftrightarrow T \mid L_p(E/\mathbb{Q},1)$$

$$\underset{[SU]\ \text{inclusion}}{\Longrightarrow} T \mid \mathrm{char}_{\Lambda}(X(E/\mathbb{Q})),$$

So the condition is satisfies and $\#\,X/TX$ is infinite. By Mazur's control theorem, this is precisely that $\mathrm{corank}_{\mathbb{Z}_p}\,Sel^{(p^\infty)}(E/\mathbb{Q})$ is ~~infinite~~ positive.

Again we invoke the fundamental exact sequence

$$0 \longrightarrow E(\mathbb{Q})\otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow Sel^{(p^\infty)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[p^\infty] \longrightarrow 0$$

Then $\mathrm{cork}_{\mathbb{Z}_p}$ of $Sel^{(p^\infty)}(E/\mathbb{Q})$ ($\Leftarrow$ is infinite) implies that at least ~~one~~ one of $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ and $\mathrm{cork}_{\mathbb{Z}_p} Ш(E/\mathbb{Q})[p^\infty]$ is infinite.

- if $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ is infinite, then we are done.
- or $\mathrm{cork}_{\mathbb{Z}_p} Ш(E/\mathbb{Q})[p^\infty]$ is infinite, which implies $Ш(E/\mathbb{Q})[p^\infty]$ = infinite.

  If $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))=0$, then this means for any good ordinary prime, $Ш(E/\mathbb{Q})[p^\infty]$ is infinite.

Therefore if we assume a priori that ~~$Ш(E/\mathbb{Q})[p^\infty]$~~ $Ш(E/\mathbb{Q})[p^\infty]$ is ~~finite~~ for one single good ordinary prime p, then $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ is infinite. □