Coleman map for elliptic curves

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfilment of the requirements for the
BS-MS Dual Degree Programme

by

Sameer R Kulkarni

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

May, 2016

Supervisor: Dr. Debargha Banerjee

This is to certify that this dissertation entitled Coleman map for elliptic curves towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents original research carried out by Sameer R Kulkarni at Indian Institute of Science Education and Research under the supervision of Dr. Debargha Banerjee, Assistant Professor, Department of Mathematics , during the academic year 2014-2015.

Debargha Banerjee

Dr. Debargha Banerjee

Committee:

Dr. Debargha Banerjee

Dr. Baskar Balasubramanyam

To
All my teachers

Declaration

I hereby declare that the matter embodied in the report entitled Coleman map for elliptic curves are the results of the investigations carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research Pune, under the supervision of Dr. Debargha Banerjee and the same has not been submitted elsewhere for any other degree.

Sameer R Kulkarni

Acknowledgments

First of all I would like to express my immense gratitude to my guide Dr. Debargha Banerjee. Without his tremendous patience and constant guidance I would probably have given up long ago. Next I would like to thank my college IISER Pune and in particular the Mathematics Department which have given me the best opportunities and facilities to learn mathematics. I am much obliged to Dr. Baskar Balasubramanyam for being part of my thesis advisory committee and giving valuable suggestions. I would like to thank professors Dr. Steven Spallone, Dr. Ronnie Sebastian, Dr. Krishna Kaipa, Dr. Supriya Pisolkar, Dr. Amit Hogadi, Dr. Diganta Borah, Dr. Vivek Mohan Mallick for the useful discussions I had with them. I would like to specially thank Dr. Chandrasheel Bhagwat for his support, help and guidance throughout my stay at IISER. I also benefitted from discussions I had with my friends Arun Kumar and Mihir Sheth and I thank them here. I am also grateful to all my friends, and I would like to specially mention Sagar Lokhande and Harsha Hampapura for their selfless help and support. Last but certainly not the least, I am immensely grateful to my parents for everything.

Abstract

The Coleman maps are an important tool in arithmetic geometry and Iwasawa theory. Perrin-Riou has constructed Coleman maps for any crystalline p-adic representation of Gal$(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The case of the one dimensional representation produces the simplest example of a Coleman map, described in chapter 1. Another example is that of the Tate module of an elliptic curve which is the subject of study of this thesis. We have followed the elementary proof of Shinichi Kobayashi in understanding the first derivative of the Coleman map for an elliptic curve.

Contents

Coleman map for elliptic curves

Sameer R Kulkarni

May 26, 2016

Chapter 1

Coleman power series from norm coherent sequences

In this section we construct the simplest of the many Coleman maps that arise in Iwasawa theory.
Let us fix the notation for the this section:

- $K_n = \mathbb{Q}_p(\mu_{p^n})$ and $K_\infty = \cup_{n=0}^{\infty} K_n$
- $\mathcal{G} = \mathrm{Gal}(K_\infty/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$
- $\mathcal{U}_\infty = \varprojlim_n \mathcal{O}_{K_n}^\times$ is the inverse limit of $\mathcal{O}_{K_n}^\times$ under the relative field norm map.

Definition 1.1. An element of $\mathcal{U}_\infty$ shall be called a **norm-coherent sequence of units** in the tower $(K_n)_n$.

We will prove the following theorem.

Theorem 1.1. *For every $\vec{u} = (u_n)_n$ in $\mathcal{U}_\infty$ there exists a unique $\mathrm{f}_{\vec{u}}(T)$ in $\mathbb{Z}_p[[T]]$ such that $\mathrm{f}_{\vec{u}}(\zeta_{p^n} - 1) = u_n$ for each $n \geq 0$.*

The above theorem was proved first by Coates and Wiles but soon after Coleman found a more conceptual proof in for the general case of Lubin-Tate extensions. Lubin-Tate extensions are generalisations of cyclotomic extensions: They are obtained by attaching to $\mathbb{Q}_p$ (or more generally a finite extension of $\mathbb{Q}_p$) zeros of certain special power series. The more general and cumbersome result can be found in [8], Theorem 2.2. Throughout this chapter let π_n denote $\zeta_{p^n} - 1$ and let R denote $\mathbb{Z}_p[[T]]$.

Example 1.0.1. *Let a and b be non-zero integers which are relatively coprime to p. Define*

$$\vec{c} = (c_n), \quad where \quad c_n = \frac{\zeta_{p^n}^{a/2} - \zeta_{p^n}^{-a/2}}{\zeta_{p^n}^{b/2} - \zeta_{p^n}^{-b/2}}$$

Then we can easily see that $\vec{c} \in \mathcal{U}_\infty$. It is also obvious that $c_n = \mathrm{f}_{\vec{c}}(\pi_n)$ where

$$\mathrm{f}_{\vec{c}}(T) = \frac{(1+T)^{a/2} - (1+T)^{-a/2}}{(1+T)^{b/2} - (1+T)^{-b/2}} \in \mathbb{Z}_p[[T]]^\times.$$

The uniqueness of $\mathrm{f}_{\vec{u}}(T)$ in Theorm 1.1 can be very easily derived from p**-adic Weierstrass preparation theorem**:

Theorem. *Any $f \in R$ can be written uniquely as $p^m f(T)g(T)$ where m is a non-negative integer, $f(T)$ a monic polynomial with every non-leading coefficient in the maximal ideal $p\mathbb{Z}_p$, and $g(T) \in R^\times$.*

So any power series can have only finitely many zeros and hence any two power series's agreeing at infinitely many points must be the same.

1.1 Norm and Trace operators of Coleman

Let R carry the topology induced by the maximal ideal $\mathfrak{m} = (p, T)$. That is, the open sets are generated by the unions and finite intersections of translates of the powers of the maximal ideal: the topology generated by the set $\{a + \mathfrak{m}^k, \mid k \geq 1, a \in R\}$. For $f \in R$, let $\phi(f)$ denote the power series $f((1+T)^p - 1)$. We can easily see that ϕ is a $\mathbb{Z}_p$-algebra endomorphism. Full proofs of all the statements below are in chapter 2 of [2].

Theorem 1.2. *There exist unique continuous maps $\mathcal{N}$ and ψ from R to R satisfying*

$$(\phi(\mathcal{N}(f))(T) = \prod_{\xi \in \mu_p} f(\xi(1+T) - 1)$$

$$(\phi(\psi)(f))(T) = \frac{1}{p} \sum_{\xi \in \mu_p} f(\xi(1+T) - 1)$$

In addition, ψ is a $\mathbb{Z}_p$-module homomorphism and satisfies $\psi \cdot \phi = \mathrm{id_R}$. Products are preserved under $\mathcal{N}$, consequently $\mathcal{N}(R^\times) \subseteq R^\times$.

The maps $\mathcal{N}$ and ψ above are called the **Coleman norm operator** and **Coleman Trace operator** respectively.

Lemma 0.1. *1. Let $f \in R^\times$. Then we have $\mathcal{N}(f) \equiv f \mod pR$.*

2. If $f \equiv 1 \mod p^m R$ for some integer $m \geq 1$, then $\mathcal{N}(f) \equiv 1 \mod p^{1+n}R$.

Corollary 1.2.1. *1. Let $f \in R^\times$, and $k_1 \leq k_2$ be two non-negative integers. We have*

$$\mathcal{N}^{k_1}(f) \equiv \mathcal{N}^{k_2}(f) \pmod{p^{k_1}R}.$$

2. For any element f in $R^\times$ the limit $g = \lim_{k\to\infty} \mathcal{N}^k(f)$ exists and it satisfies $\mathcal{N}(g) = g$.

To prove Theorem 1.1 we take an arbitrary sequence $(u_n)_n$ from $\mathcal{U}_\infty$. For each u_n we have a corresponding $f_n \in R^\times$ such that $f_n(\pi_n) = u_n$. This can be done since $\mathcal{O}_{\mathbb{Q}_p(\mu_{p^n})} = \mathbb{Z}_p[\zeta_{p^n}]$. Define $g_n(T) := \mathcal{N}^n(f_{2n})(T)$. By the compactness of R, the sequence $(g_n(T))_n$ in R has a convergent subsequence, tending to $h(T)$. We have the following

Lemma 0.2. *For all $n \geq 0$ and all $m \geq n$, $g_m(\pi_n) \equiv u_n \mod p^{1+n}$.*

In particular, by taking $m \to \infty$ above, we get

$$\lim_{m\to\infty} g_m(\pi_n) = h(\pi_n) = u_n.$$

We can take $h(T)$ to be $\mathrm{f}_{\vec{u}}(T)$ and Theorem 1.1 is verified.

1.2 Significance of the Coleman map

Definition 1.2. Let D be the operator on R given by $D(f)(T) = (1+T)f'(T)$. For each $k \geq 1$, define the **higher logarithmic derivative** $\delta_k : \mathcal{U}_\infty \to \mathbb{Z}_p$ by

$$\delta_k(\vec{u}) := D^{k-1}\left(\frac{(1+T)f'_{\vec{u}}(T)}{f_{\vec{u}}(T)}\right)\Bigg|_{T=0}.$$

where $f_{\vec{u}}(T)$ is the Coleman power series corresponding to the norm coherent sequence $\vec{u}$.

Lemma 0.3. *Each δ_k is a group homomorphism satisfying*

$$\delta_k(\sigma(\vec{u})) = \chi(\sigma)^k \delta_k(\vec{u}).$$

for all $\vec{u} \in \mathcal{U}_\infty$ and $\sigma \in \mathcal{G}$.

The next result due to Kummer computes the value of higher logarithmic derivative for the cyclotomic units $\vec{c}(a,b)$ defined above (1.0.1).

Theorem 1.3.

$$\delta_k(\vec{c}(a,b)) = \begin{cases} 0 & k = 1,3,5,\dots \\ (b^k - a^k)\zeta(1-k) & k = 2,4,6,\dots \end{cases}$$

where ζ is the classical Riemann zeta function.

Proof. See chapter 2 of [2]. ♣

We can see from the above theorem how the values of the classical zeta function are related to the higher logarithmic derivatives of cyclotomic units $\vec{c}(a,b)$. In fact, we have the following theorem that makes precise how to p-adically interpolate the classical ζ function.

We derive the p-adic zeta function by interpolating the values of classical zeta function at negative integers, with a factor involving p called the Euler factor. We want to get a function from $\mathbb{Z}_p$ to the p-adic complex numbers, integral of whose k-th power over $\mathbb{Z}_p$ is related to values of the classical zeta function at negative integers. It turns out that we actually get a map from $\mathbb{Z}_p^\times$ and not $\mathbb{Z}_p$. We discuss briefly p-adic measures below:

Let X be a compact open subset of $\mathbb{Q}_p$, which will usually be $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$. A p-adic distribution μ on X is a map from the collection of compact open sets in X to $\mathbb{Q}_p$ which is disjoint additive, i.e., we have

$$\mu(\bigcup_{i=1}^{k} U_i) = \sum_{i=0}^{k} \mu(U_i)$$

whenever k is a natural number and U_i's are mutually disjoint. A *measure* on X is a distribution which is bounded, i.e., there is a $B > 0$ such that

$$|\mu(U)|_p \leq B$$

for all compact open sets U in X. An example is the *Haar distribution* μ_{Haar} on $\mathbb{Z}_p$ defined by

$$\mu_{\text{Haar}}(a + p^n\mathbb{Z}_p) = \frac{1}{p^n}.$$

We can easily see that this a distribution invariant under translation.

More generally, if $\mathfrak{B}$ is a profinite abelian group (which is mostly $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$) we can define a p-adic distribution on $\mathfrak{B}$ to be a map from the collection of compact-open sets of $\mathfrak{B}$ to $\mathbb{Q}_p$ (or $\mathbb{C}_p$) which is disjoint additive. The group $\mathfrak{B}$ has a base of neighbourhoods around the identity given by open normal subgroups $\{\mathcal{H}\}$. So any compact open subset of $\mathfrak{B}$ is a finite union of cosets of $\mathcal{H}$'s. It is hence enough to know the value of the measure on these cosets of $\mathcal{H}$. The above idea can be nicely formulated using the Iwasawa algebra of $\mathfrak{B}$.

We define the *Iwasawa algebra* of $\mathfrak{B}$ to be the inverse limit

$$\Lambda(\mathfrak{B}) := \varprojlim \mathbb{Z}_p[\mathfrak{B}/\mathcal{H}]$$

where the inverse limit is by natural projections induced by the $\mathbb{Z}_p[\mathfrak{B}/\mathcal{K}] \to \mathbb{Z}_p[\mathfrak{B}/\mathcal{H}]$ whenever $\mathcal{K}$ is a subgroup of $\mathcal{H}$.

For an element λ of $\Lambda(\mathfrak{B})$, let its image in $\mathbb{Z}_p[\mathfrak{B}/\mathcal{H}]$ be written as $\sum\limits_{x \in \mathfrak{B}/\mathcal{H}} c_{\mathcal{H}}(x)x$. We can think of λ as assigning the p-adic integer to the subset x of $\mathfrak{B}$. The inverse limit condition implies that this assignment is additive w.r.t. the cosets. Hence we can think of λ as a p-adic integral distribution on the group $\mathfrak{B}$. Since the coefficients are in $\mathbb{Z}_p$, it is also a measure.

We want to construct the p-adic analogue of the Riemann zeta function, which has a pole at 1. To take into account this fact (the p-adic zeta function also has a pole at 1.), we introduce the concept of a *pseudo-measure*.

Let $Q(\mathfrak{B})$ be the localisation of $\Lambda(\mathfrak{B})$ outside the set of zero-divisors. An element

λ of $Q(\mathfrak{B})$ is called a *pseudo-measure* if

$$(g-1)\lambda \in \Lambda(\mathfrak{B})$$

for all g in $\mathfrak{B}$.

Theorem 1.4. *There exits a unique pseudo-measure $\tilde{\zeta}_p$ on $\mathcal{G}$ such that*

$$\int\limits_{\mathcal{G}} \chi(g)^k \, d\tilde{\zeta}_p = \begin{cases} 0 & k = 1, 3, \ldots \\ (1-p^{k-1})\zeta(1-k) & k = 2, 4, \ldots \end{cases}$$

Proof. This is Proposition 4.2.4 in [2]. ♣

Chapter 2

The Tate Elliptic Curve

By the theory of Weierstrass $\wp$ function for any elliptic curve E defined over $\mathbb{C}$ the solution set $E(\mathbb{C})$ is isomorphic to a torus $\mathbb{C}/\Lambda$ for some unique lattice Λ. We naturally want to look at the p-adic analogue of the above construction. A lattice is a discrete subgroup. In $\mathbb{Q}_p$ or any p-adic field (any finite extension of $\mathbb{Q}_p$) K there are no non-trivial discrete subgroups. Given any subgroup $\Lambda \hookrightarrow \mathbb{Q}_p$, 0 is a limit point in Λ since given any $a \neq 0$ the sequence $(ap^n)_{n\geq 0}$ converges to 0. So the above approach may fail.

However the multiplicative group $\mathbb{Q}_p^\times$ (and also $K^\times$) has discrete subgroups. For example, the subgroup generated by p, $p^{\mathbb{Z}}$ is a discrete subgroup in $\mathbb{Q}_p^\times$ since the only limit point of $p^{\mathbb{Z}}$ in $\mathbb{Q}_p$ is 0 which is not in $p^{\mathbb{Z}}$. In fact, if K is any finite extension $\mathbb{Q}_p$ with the norm $|\cdot|$ and $q \in K^\times$ with $|q| < 1$, then for a certain elliptic curve E_q, $E_q(\overline{K})$ is isomorphic to $\overline{K}^\times/q^{\mathbb{Z}}$.

Definition 2.1. Let K be a p-adic field and let $q \in K^\times$ with $|q| < 1$. Then we define the *Tate curve* E_q to be the curve defined by the equation

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where $a_4(q) = -s_3(q)$, and $a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}$, for

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}$$

Theorem 2.1. *(Tate)*

1. *The series $a_4(q)$ and $a_6(q)$ converge in K.*

2. *The Tate curve is an elliptic curve over K with discriminant*

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

and the j-invariant

$$j(E_q) = \frac{1}{q} + \sum_{n \geq 0} c(n) q^n$$

where each $c(n)$ is an integer.

3. *There exists a group isomorphism via an analytic map*

$$\phi : \overline{K}^{\times} / q^{\mathbb{Z}} \cong E_q(\overline{K})$$

sending

$$u \rightsquigarrow (X(u,q), Y(u,q)),\ u \in \overline{K}^{\times}$$

where

$$X(u,q) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2s_1(q)$$

$$Y(u,q) = \sum_{n \in \mathbb{Z}} \frac{(q^n u)^2}{(1 - q^n u)^3} + s_1(q)$$

and $\phi(u) = O$ if $u \in q^{\mathbb{Z}}$.

4. *The map ϕ above respects the action of the Galois group $G(\overline{K}/K)$, i.e.,*

$$\phi(\sigma(u)) = \sigma(\phi(u))$$

for all $u \in \overline{K}^{\times}, \sigma \in G(\overline{K}/K)$.

5. *For any algebraic extension L/K, ϕ induces an isomorphism*

$$L^{\times} / q^{\mathbb{Z}} \xrightarrow{\sim} E_q(L).$$

Proof. See Theorem 3.1 of [9]. ♣

We considered above a special type of curve called Tate curve. The j-invariant of the Tate curve is of the form $\equiv \frac{1}{q} \pmod{\mathbb{Z}_p[[q]]}$ so we have $\mid j(E_q) \mid > 1$ as a necessary condition for a Tate curve. By the following result of Tate the converse is also true, that is, an elliptic curve can be brought to Tate curve form if $\mid j(E_q) \mid > 1$.

Theorem 2.2. *(Tate) Let K be a finite extension of $\mathbb{Q}_p$, let E/K be an elliptic curve with $\mid j(E) \mid > 1$. Then there exists a unique $q \in K^\times$ with $\mid j(E_q) \mid > 1$ so that E is isomorphic to the Tate curve E_q via an isomorphism defined over $\overline{K}$.*

In this thesis we shall consider the Tate curve.

Chapter 3

Structure of the p-adic Tate module

3.1 p-adic representations

In this section we define a p-adic representation and give some examples:

cyclotomic character

Let $\overline{K}$ be the algebraic closure of the field K. Let σ be an element of $G(\overline{K}/K)$. The roots of the polynomial $\dfrac{x^{p^n}-1}{x^{p^{n-1}}-1}$ are permuted by σ, we get the following equation, for every natural number n:

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}, \quad \text{for some integer } a_n \perp p^n.$$

$$\begin{aligned} \zeta_{p^{1+n}}^{p} &= \zeta_{p^n} \\ \sigma(\zeta_{p^{1+n}}^{p}) = \sigma(\zeta_{p^{1+n}})^p &= \sigma(\zeta_{p^n}) \\ \zeta_{p^{1+n}}^{pa_{1+n}} = \zeta_{p^n}^{a_{1+n}} &= \zeta_{p^n}^{a_n}. \end{aligned}$$

implying that

$$a_{1+n} \equiv a_n \mod p^n, \quad \text{for all } n.$$

Hence the sequence $(\dots, a_2, a_1)$ defines an element of $\mathbb{Z}_p^\times$. This gives a map

$$G(\overline{K}/K) \xrightarrow{\chi_p} \mathbb{Z}_p^\times \tag{3.1}$$

defined by

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)}. \tag{3.2}$$

It is straightforward to see that the above map χ_p is a group homomorphism. In general it does not possess any special property like injectivity or surjectivity. The subgroup $G(\overline{K}/K(\mu_{p^\infty}))$ of $G(\overline{K}/K)$ is contained in the kernel of χ_p, therefore χ_p factors through $\dfrac{G(\overline{K}/K)}{G(\overline{K}/K(\mu_{p^\infty}))} \cong G(K(\mu_{p^\infty})/K)$. We get a map

$$G(K(\mu_{p^\infty})/K) \to \mathbb{Z}_p^\times$$

which shall also be denoted by χ_p. The new map is easily seen to be a bijection when $K = \mathbb{Q}_p$ which we shall call the (p-adic) *cyclotomic character*.

Definition 3.1.

- Let L/K be a Galois extension. A **p-adic representation** V is a finite dimensional $\mathbb{Q}_p$-vector space V with a continuous $\mathbb{Q}_p$-linear action of $G = \mathrm{Gal}(L/K)$.

- Let V be a p-adic representation of G of dimension d. A **lattice** in V is a free sub-$\mathbb{Z}_p$-module of rank d.

- A $\mathbb{Z}_p$-representation of G is a finitely generated free $\mathbb{Z}_p$-module with a continuous $\mathbb{Z}_p$-linear action of $\mathbb{Z}_p$.

Example 3.1.1.

- *We have the trivial representation $\mathbb{Q}_p$, with the action of G give by $\sigma \cdot a = a$ for all $a \in \mathbb{Q}_p$ and $\sigma \in G$.*

- *Given two representations V_1 and V_2 we can define their tensor product $V_1 \otimes_{\mathbb{Q}_p} V_2$ with $\sigma \cdot (v_1 \otimes v_2) := \sigma \cdot v_1 \otimes \sigma \cdot v_2$.*

- *Given a representation V we can form its dual $V^* = \mathrm{Hom}(V, \mathbb{Q}_p)$. If $\sigma \in G$ and $\phi \in V^*$ then $\sigma \cdot \phi \in V^*$ is given by $\sigma \cdot \phi(v) := \phi(\sigma^{-1} \cdot v)$. V^* is called the dual representation of V.*

- *If M is a $\mathbb{Z}_p$ or $\mathbb{Q}_p$-representation with the action $\cdot$ of $G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, then $M(r)$ for $r \in \mathbb{Z}$ will denote the same underlying module with the new action $\star$ of $G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*

obtained by twisting $\cdot$ by the r-th power of the cyclotomic character $G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\chi} \mathbb{Z}_p^\times$.

$$\sigma \star m := \chi(\sigma)^r \cdot m.$$

*$M(r)$ is called the r-**th Tate twist** of M.*

3.1.1 Some examples

In this section we will consider some natural examples of p-adic representations and $\mathbb{Z}_p$-representations that occur in the thesis.

The Tate module of the multiplicative group $\mathbb{G}_m$

For a field F let $\mu_{p^n}(F)$ be the set of all p^n-th roots of unity in F. Consider a perfect field K. We have $\mu_{p^n}(\overline{K}) \cong \mathbb{Z}/p^n\mathbb{Z}$. We can form an inverse system of these groups: Define the the *Tate module of the multiplicative group* $\mathbb{G}_m$ to be

$$T_p(\mathbb{G}_m) := \varprojlim_{n\in\mathbb{N}} \mu_{p^n}(\overline{K}).$$

$T_p(\mathbb{G}_m)$ is a free $\mathbb{Z}_p$-module of rank 1. The Galois module structure of $T_p(\mathbb{G}_m)$ will be discussed in section 3.2 where we will see that it is isomorphic to the Tate twist of the $\mathbb{Z}_p$ by the cyclotomic character, i.e., $\mathbb{Z}_p(1)$.

The p-adic Tate module of an elliptic curve

Let p be a prime number. The *p-adic Tate module* $T = T_p(E)$ of the elliptic curve E is the inverse limit of the groups of p^n-torsion points of $E(\overline{K})$.

$$T = \varprojlim_{n\in\mathbb{N}} E(\overline{K})[p^n]$$

where the inverse limit is taken over the multiplication-by-p-map.
By Theorem 2.1, part 3 above, we get an easy way of determining the structure of the p-adic Tate module T and the action of $G = \mathrm{Gal}(\overline{K}/K)$ on it for the Tate curve $E = E_q$. First we determine the structure of $E[p^n]$ as a $\mathbb{Z}/p^n\mathbb{Z}$-module and by taking

inverse limit we get the $\mathbb{Z}_p$-module structure of T.

3.2 p-adic Tate module of the Tate curve

Let K be a finite extension of $\mathbb{Q}_p$ and let $E = E_q$ be a Tate curve defined over K. By part 3 of 2.1 above, one has

$$E_q(\overline{K})[p^n] \cong \{\overline{\alpha} \in \overline{K}^\times/q^{\mathbb{Z}} \mid \alpha^{p^n} \in q^{\mathbb{Z}}\}.$$

We fix two sequences $\varepsilon^{(n)}$ and $q^{(n)}$ for $n \geq 0$ in $\overline{K}^\times$ satisfying the relations

$$(\varepsilon^{(n)})^{p^n} = 1, \quad (q^{(n)})^{p^n} = q, \quad (\varepsilon^{(1+n)})^p = \varepsilon^{(n)} \quad \text{and} \quad (q^{(1+n)})^p = q^{(n)} \quad \forall n \geq 0,$$

with $\varepsilon^{(1)} \neq 1$. Any element α can be represented upto $q^{\mathbb{Z}}$ as $q^{(n)j_1}\varepsilon^{(n)j_2}$ for some unique integers j_1 and j_2 in $\{0, 1, \ldots, p^n - 1\}$. The automorphism $\sigma \in G(\overline{K}/K)$ acts on $\varepsilon^{(n)}$ by the cyclotomic character $\chi\colon G \to \mathbb{Z}_p^\times$, the action being

$$\sigma(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(\sigma)}.$$

We have

$$(\sigma(q^{(n)}))^{p^n} = \sigma((q^{(n)})^{p^n}) = \sigma(q) = q = (q^{(n)})^{p^n},$$

so

$$(\sigma(q^{(n)})/q^{(n)})^{p^n} = 1.$$

Hence there is a unique integer $c(n) \in \{0, 1, \ldots, p^n - 1\}$ such that

$$\sigma(q^{(n)}) = q^{(n)}(\varepsilon^{(n)})^{c(n)}.$$

So $E_q(\overline{K})[p^n]$ is a free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank 2. The Galois action is compatible with respect to taking p-th power. When we form the inverse limit of $E_q(\overline{K})[p^n]$, we get a module over the inverse limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. We write e for the inverse limit of the sequence $\varepsilon^{(n)}$ and f for the inverse limit of $q^{(n)}$. $\mathbb{Z}_p e$ is the additive notation for the module $\mathbb{Z}_p(1) := \varprojlim_n \mu_{p^n}(\overline{\mathbb{Q}}_p^\times)$. Written additively, one gets $\sigma(e) = \chi(\sigma)e$, $\sigma(f) = f + c(\sigma)e$, hence the following

Theorem 3.1.

$$T \cong \mathbb{Z}_p e \oplus \mathbb{Z}_p f$$

The action of σ w.r.t. the basis (e, f) is given by the 2×2 matrix

$$\begin{pmatrix} \chi(\sigma) & c(\sigma) \\ 0 & 1 \end{pmatrix}.$$

The map $\sigma \rightsquigarrow c(\sigma)$ is a member of $H^1(K, \mathbb{Z}_p(1))$.

Proof. The only fact remaining to be proved is that c is a cocycle. For that, we observe that

$$\begin{aligned}(\sigma_1\sigma_2) \cdot f &= \sigma_1 \cdot (f + c(\sigma_2)e) \\ &= \sigma_1 \cdot f + \sigma_1(c(\sigma_2)e) \\ &= f + c(\sigma_1)e + c(\sigma_2)\chi(\sigma_1)e \\ &= f + (c(\sigma_1) + \chi(\sigma_1)c(\sigma_2))e \\ &= f + c(\sigma_1\sigma_2)e\end{aligned}$$

$$\Longrightarrow c(\sigma_1\sigma_2) = c(\sigma_1) + \chi(\sigma_1)c(\sigma_2)$$

♣

Chapter 4

Formal group of an elliptic curve

In this section we define formal group laws and describe the formal group of an elliptic curve. First we'll discuss some general examples about formal groups. Let's take an elliptic curve given by the Weierstrass form:

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

Make the change of variables

$$z = -\frac{x}{y} \quad \text{and} \quad w = -\frac{1}{y}$$

so that we have

$$x = \frac{z}{w} \quad \text{and} \quad y = -\frac{1}{w}.$$

The advantage of doing so is that the point at infinity O is brought to the origin, $(0,0)$. The Weierstrass equation above then takes the form

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z,w).$$

We want to solve for w as a power series in z. That is, we want a $w(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$ satisfying

$$w(z) = f(z, w(z)).$$

To this effect we have the following

Theorem 4.1. *There exists a unique power series* $w(z) = z^3(1+A_1z+\ldots) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$

satisfying

$$w(z) = f(z, w(z)).$$

Proof. See Proposition 1.1 of [10]. ♣

Since we know w in terms of z, we can also find x and y in terms of z. We derive the following *Laurent series expansion* for x and y,

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \ldots,$$

$$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z - \ldots.$$

Considering the equation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ formally, the ordered pair $(x(z), y(z))$ provides a solution formally. We observe that in the expansion for $x(z)$ and $y(z)$ above, only finitely many terms have z in the denominator. This suggests that if we take a ring R complete with respect to a maximal ideal $\mathcal{M}$ with fraction field K and allow z to take values from $\mathcal{M}$ the ordered pair $(x(z), y(z))$ is actually a point on the elliptic curve defined over K. Hence we get a map

$$\mathcal{M} \xrightarrow{\iota} E(K), \quad z \rightsquigarrow (x(z), y(z)). \tag{4.1}$$

If for $z_1, z_2 \in \mathcal{M}$ we have $(x(z_1), y(z_1))$= $(x(z_2), y(z_2))$ then $z_1 = -\frac{x(z_1)}{y(z_1)} = -\frac{x(z_2)}{y(z_2)} = z_2$. So the map above in one-one.

We would like to have a group structure on $\mathcal{M}$ such that the map ι becomes a homomorphism. For this we need the concept of formal groups.

4.1 Formal groups

Definition 4.1. Let R be a commutative ring. Then a **one-parameter commutative formal group law** or simply a **formal group law** is a power series $F(x, y) \in R[[x, y]]$ such that

- $F(x, 0) = x$
- $F(x, y) = F(y, x)$

- $F(x, F(y, z)) = F(F(x, y), z)$

We often write $x +_F y$ for $F(x, y)$ for convenience. It can be seen that the above conditions are nothing but the requirement that the composition law $+_F$ be commutative and associative, and that 0 acts as the identity element.

We sometimes use the term *formal group* to mean a *formal group law.*

Example 4.1.1. *Let $R = \mathbb{Z}$.*

- *The formal additive group, denoted by $\widehat{\mathbb{G}}_a$, is defined by to be the usual addition*

$$F(x, y) = x + y.$$

- *The formal multiplicative group, denoted by $\widehat{\mathbb{G}}_m$, is defined by*

$$F(x, y) = x + y + xy = (1 + x)(1 + y) - 1.$$

Theorem 4.2. *If F is a formal group law over R then*

1. *$F(x, y) = x + y +$ higher degree terms.*
2. *There exists a unique power series $i(x) \in R[[x]]$ such that $x +_F i(x) = 0$.*

Proof. See Lecture 10, section 2 in [4]. ♣

Definition 4.2. Let F and G be formal group laws over R. Then a *homomorphism* from F to G is a power series $f(x) \in R[[x]]$ such that

$$f(F(x, y)) = G(f(x), f(y)) \quad \text{i.e.,} \quad f(x +_F y) = f(x) +_G f(y).$$

f is said to be an isomorphism if $\exists\, g \in R[[x]]$ such that $f(g(x)) = g(f(x))$.

We observe by looking at the linear terms in the equation $f(F(x, y)) = G(f(x), f(y))$ that f has no constant term. Further it can also be seen that f is an isomorphism if and only if $f'(0)$ is a unit in R.

Example 4.1.2. *Let $\widehat{\mathbb{G}}_m$ be the formal multiplicative group $x + y + xy$ and $\widehat{\mathbb{G}}_a$ be the additive formal group $x + y$. Consider the formal power series*

$$L(x) = \sum_{n\geq 1}(-1)^{n-1}\frac{x^n}{n} \quad \textit{and} \quad E(x) = \sum_{n\geq 1}\frac{x^n}{n!}.$$

These power series have zero constant term and it is easy to see the following identities

$$L\circ R(x) = x, \quad R\circ L(x) = x, \quad L(\widehat{\mathbb{G}}_m(x,y)) = \widehat{\mathbb{G}}_a(L(x), L(y)), \quad E(\widehat{\mathbb{G}}_a(x,y)) = \widehat{\mathbb{G}}_m(E(x), E(y)).$$

Hence we have the following isomorphisms of formal groups:

$$\widehat{\mathbb{G}}_m \underset{E}{\overset{L}{\rightleftarrows}} \widehat{\mathbb{G}}_a$$

Theorem 4.3. *If R is a local ring complete w.r.t. its maximal ideal $\mathcal{M}$ and F is a formal group law defined over R, then under the operation defined by F or $+_F$ $\mathcal{M}$ is an abelian group.*

Proof. All group axioms follow formally from the definition of formal group law and Theorem 4.2. It just remains to prove that $F(x, y)$ and $i(x)$ actually belongs to $\mathcal{M}$ when x and y are in $\mathcal{M}$. But that is obvious since R is complete w.r.t. $\mathcal{M}$. $\clubsuit$

4.2 Logarithm of a formal group

The map L from Example 4.1.2 gives us an isomorphism from $\widehat{\mathbb{G}}_m$ to $\widehat{\mathbb{G}}_a$. In other words it gives us a bijective map that converts the formal group law $\widehat{\mathbb{G}}_m$ to addition. We can in fact generalize this to any formal group provided that it is defined over a ring without torsion.

Let F be a formal group defined over a torsion-free ring R. We want to get a power series $L(x) = L_F(x)$ such that $L(x +_F y) = L(x) + L(y)$, i.e., L should act as logarithm for the operation F. We will see that $L(x)$ may not actually have coefficients in R. We want

$$L(F(x, y)) = L(x) + L(y)$$

Taking the partial derivative with respect to the first variable x we get

$$L'(F(x,y))F_1(x,y) = L'(x)$$

Put $x = 0$.

$$\begin{aligned} L'(F(0,y))F_1(0,y) &= L'(0) \\ L'(y)F_1(0,y) &= L'(0) \\ L'(y) &= \frac{L'(0)}{F_1(0,y)} \end{aligned}$$

This suggests that we use $\int \frac{L'(0)}{F_1(0,y)}\,dy$ as a suitable candidate for $L(y)$. We check below that $\int \frac{L'(0)}{F_1(0,y)}\,dy$ is indeed the right choice.

Theorem 4.4. *If F is a formal group defined over a torsion-free ring R then there exists an isomorphism $L(x) : F \overset{\cong}{\to} \widehat{G}_a$ with coefficients in $R \otimes \mathbb{Q}$.*

Proof. Begin with the associative law for F:

$$F(x, F(y,z)) = F(F(x,y),z).$$

Taking partial derivative w.r.t. x and putting $x = 0$ we get

$$\begin{aligned} F_1(x, F(y,z)) &= F_1(F(x,y),z)F_1(x,y) \\ F_1(0, F(y,z)) &= F_1(F(0,y),z)F_1(0,y) \\ F_1(0, F(y,z)) &= F_1(y,z)F_1(0,y) \\ \frac{L'(0)}{L'(F(y,z))} &= F_1(y,z)\frac{L'(0)}{L'(y)} \end{aligned}$$

Since L is an isomorphism $L'(0)$ is a unit so we get

$$\begin{aligned} L'(y) &= F_1(y,z)L'(F(y,z)) \\ \int L'(y)\,dy &= \int L'(F(y,z))F_1(y,z)\,dy \\ L(y) &= L(F(y,z)) + C(z) \end{aligned}$$

To evaluate $C(z)$ we just put $y = 0$. $C(z) = L(0) - L(F(0,z)) = -L(z)$ since $L(0) = 0$.

Therefore we have

$$L(F(y,z)) = L(y) + L(z)$$

♣

Since we are integrating a power series to $L(x)$ the coefficients involve denominators containing natural numbers. So $L(x)$ has coefficients in $R \otimes \mathbb{Q}$.

Corollary 4.4.1. *Any two formal groups over a $\mathbb{Q}$-algebra are isomorphic.*

4.3 Formal group of an elliptic curve

Now we can give a group structure on $\mathcal{M}$ so that the map ι defined above (Equation 4.1) is a group homomorphism. We work with (z, w) coordinates. Let $w_1 = w(z_1)$ and $w_2 = w(z_2)$. By elementary calculations we see that the sum of the points (z_1, w_1) and (z_2, w_2) is of the form (z_3, w_3) where $z_3 = F(z_1, z_2)$ where $F(z_1, z_2)$ belongs to $\mathbb{Z}[a_1, \dots, a_6][[z]]$ and is of the form $z_1 + z_2 +$ higher degree terms.

$$F(z_1, z_2) = z((z_1, w(z_1)) +_E (z_2, w(z_2))).$$

From the above equation it is evident that F satisfies the axioms of formal group law.

Definition 4.3. The set $\mathcal{M}$ with the power series F defined above is called the **formal group of the elliptic curve** E. The group structure thus induced on $\mathcal{M}$ will be denoted by $\widehat{E}(\mathcal{M})$.

Chapter 5

A particular group of local units

In this section we want to construct a norm coherent sequence $(d_n)_n$ of units in the cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}_p$ which will be useful in the construction of the Coleman map later.

Definition 5.1. Let p be a prime number. A Galois extension K/F is said to be a $\mathbb{Z}_p$-extension if the Galois group of K/F is isomorphic to the additive group of $\mathbb{Z}_p$.

Let $p > 2$ be a prime number. The Galois group of $\mathbb{Q}_p(\mu_{p^\infty})$ over $\mathbb{Q}_p$ is isomorphic to

$$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p).$$

Let

$$\Delta := \mu_{p-1} \text{ and } \Gamma := 1 + p\mathbb{Z}_p, \quad \text{so that} \quad \mathbb{Z}_p^\times = \Delta \times \Gamma.$$

If $a \in 1 + p\mathbb{Z}_p$ and not in $1 + p^2\mathbb{Z}_p$, then the map

$$x \rightsquigarrow a^x$$

gives a topological isomorphism from $\mathbb{Z}_p$ to $\Gamma = 1 + p\mathbb{Z}_p$ [3]. Under this map the (closed) subgroups $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$ correspond to $1 + p^{1+n}\mathbb{Z}_p$. Let us denote $1 + p^{1+n}\mathbb{Z}_p$ by Γ^{p^n} and $\Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ by Γ_n.

The subgroup Δ is closed and hence corresponds uniquely to a subfield of $\mathbb{Q}_p(\mu_{p^\infty})$. Let k_∞ be the unique extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_p(\mu_{p^\infty})$ such that $G(k_\infty/\mathbb{Q}_p) = \Gamma \cong \mathbb{Z}_p$. We have constructed a $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. A $\mathbb{Z}_p$-extension constructed like this by adjoining p-th power roots of unity is called a *cyclotomic $\mathbb{Z}_p$-extension.*

All the closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$ for some $n \geq 0$ or the zero subgroup 0. Let the subfield of k_∞ corresponding to the subgroup $p^n\mathbb{Z}_p$ be denoted by k_n and let $k_0 := \mathbb{Q}_p$. Then $G(k_n/\mathbb{Q}_p) = \Gamma/\Gamma^{p^n}$ is the cyclic group of order p^n. We fix a topological generator γ of Γ (e.g., $1+p$ or any element in $\Gamma - \Gamma^p$). Then each Γ_n is generated by $\gamma \mod \Gamma^{p^n}$.

Let $\wp_n$ denote the maximal ideal of the integer ring $\mathcal{O}_n = \mathcal{O}_{k_n}$ of k_n. Let $\mathcal{U}_n^1 := 1 + \wp_n$ be the subgroup of $\mathcal{O}_n^\times$ of principal units.

Define

$$\ell(x) := \ln(1+x) + \sum_{k\geq 0}\sum_{\delta\in\Delta} \tfrac{(1+x)^{p^k\delta}-1}{p^k}.$$

Lemma 0.4.

$$\ell(x) \in \mathbb{Q}_p[[x]].$$

Proof.

$$\ell(x) = \ln(1+x) + \sum_{j\geq 1} x^j\Big(\sum_{k\geq 0}\frac{1}{p^k}\sum_{\delta\in\Delta}\binom{p^k\delta}{j}\Big).$$

Expanding $(1+x)^{p^k\delta}$ using binomial series and collecting like powers of x we get

$$\ell(x) = \ln(1+x) + \sum_{j\geq 1} x^j\Big(\sum_{k\geq 0}\tfrac{1}{p^k}\sum_{\delta\in\Delta}\binom{p^k\delta}{j}\Big) = \ln(1+x) + \sum_{j\geq 1} A_j x^j.$$

It is sufficient to check that $A_j \in \mathbb{Q}_p \,\forall\, j \geq 1$. Because $A_j = \sum\limits_{k\geq 0}\frac{1}{p^k}\sum\limits_{\delta\in\Delta}\binom{p^k\delta}{j}$ it suffices to check that the kth term $\frac{1}{p^k}\sum\limits_{\delta\in\Delta}\binom{p^k\delta}{j}$ tends to 0 in $\mathbb{Q}_p$ as $k \to \infty$.

$$A_j = \frac{1}{j!}\Big[\sum_{\delta\in\Delta}\frac{p^{kj}\delta^j}{p^k} \pm \sum_{\delta\in\Delta}\frac{p^{kj-k}\delta^{j-1}}{p^k}(\text{integer}) \pm \ldots \pm \sum_{\delta\in\Delta}\frac{p^k\delta}{p^k}(\text{integer})\Big].$$

All the terms in the above sum are divisible by p^k except the last term which vanishes due to the presence of $\sum\limits_{\delta\in\Delta}\delta = 0$. Hence $A_j \to 0$ as $k \to \infty$ and the claim is proved. ♣

In addition $\ell(x)$ satisfies the following properties:

Lemma 0.5. *1.* $\ell(x) = x +$ *higher degree terms*

2. $\ell'(x) \equiv 1 \mod x\mathbb{Z}_p[[x]]$

3. $\ell((1+x)^p - 1) \equiv p\ell(x) \mod p\mathbb{Z}_p[[x]]$

Proof. The first property is straightforward. To prove the second we differentiate $\ell(x)$ to get $\ell'(x) = \frac{1}{1+x} + \sum\limits_{j\geq 1} jA_j x^j$. Since $A_j = \sum\limits_{k\geq 0} \frac{1}{p^k} \sum\limits_{\delta\in\Delta} \binom{p^k\delta}{j}$, we get $jA_j = \sum\limits_{k\geq 0}\sum\limits_{\delta} \binom{p^k\delta-1}{j-1}\delta$. Each summand is a p-adic integer since if $x \in \mathbb{Z}_p$ and $n \in \mathbb{N}$ then $\binom{x}{n}$ is also in $\mathbb{Z}_p$ [3]. And since we already know A_j converges jA_j belongs to $\mathbb{Z}_p$ for all $j \geq 2$. $A_1 = 0$ as can be seen by putting $x = 0$ in the definition of $\ell(x)$. (3) follows similarly. ♣

The properties (1), (2) & (3) listed above together satisfy the hypothesis for Theorem 8.3(iii) in [5] with the Eisenstein polynomial $u(t)$ being $t - p$. Hence there exists a formal group $\mathcal{F}$ over $\mathbb{Z}_p$ that has ℓ as its logarithm. The formal group $\widehat{\mathbb{G}}_m$ is a formal group over $\mathbb{Z}_p$ whose logarithm $L(x) = \ln(1+x)$ also satisfies the conditions (1), (2) & (3) above. Hence by Theorem 8.2(ii) of [5] the power series $\iota(x) := \exp\circ\ell(x) - 1$ belongs to $\mathbb{Z}_p[[x]]$ and acts as an isomorphism from $\mathcal{F}$ to $\widehat{\mathbb{G}}_m$.
We are now ready to define the local units. Pick an ε from $p\mathbb{Z}_p$ such that $\ell(\varepsilon) = p$ and define

$$\begin{aligned} c_n &:= \iota((\zeta_{p^{1+n}} - 1) +_{\mathcal{F}} \varepsilon) \\ &= \exp(\ell((\zeta_{p^{1+n}} - 1) +_{\mathcal{F}} \varepsilon)) - 1 \\ &= \exp(\ell(\zeta_{p^{1+n}} - 1) + \ell(\varepsilon)) - 1 \\ &= e^p e^{\ell(\zeta_{p^{1+n}} - 1)} - 1. \end{aligned}$$

The element c_n is fixed under the action of Δ, so belongs to $\widehat{\mathbb{G}}_m(\wp_n)$. We define $d_n := 1 + c_n \in \mathcal{U}_n^1 = e^p e^{\ell(\zeta_{p^{1+n}}-1)}$ which satisfies the relation

$$\log_p(d_n) = \ell(\varepsilon) + \ell(\zeta_{p^{1+n}} - 1) = p + \sum_{\substack{k\geq 0\\ \delta\in\Delta}} \frac{\zeta^{\delta}_{p^{1+n-k}} - 1}{p^k}.$$

Lemma 0.6. *1. $(d_n)_n$ is a norm coherent sequence and $d_0 = 1$.*

2. Let u be a (topological) generator of $\mathcal{U}_0^1$. Then as a $\mathbb{Z}_p[\Gamma_n]$ module, d_n and u generate U_n^1, and d_n generate $(\mathcal{U}_n^1)^{N=1}$ where N is the norm from k_n to $\mathbb{Q}_p$.

Proof. For the first claim, We have $d_n = e^p e^{\ell(\zeta_{p^{1+n}}-1)}$ and $d_{n-1} = e^p e^{\ell(\zeta_{p^n}-1)}$.

$$\mathrm{N}_{n/n-1}(d_n) = \prod_{\sigma\in \mathrm{G}(k_n/k_{n-1})} \sigma(e^p e^{\ell(\zeta_{p^{1+n}}-1)}) = e^{p^2} \prod_{\sigma\in \mathrm{G}(k_n/k_{n-1})} e^{\ell(\sigma(\zeta_{p^{1+n}})-1)}.$$

Hence it is enough to show that

$$p^2 + \sum_{\sigma \in \mathrm{G}(k_n/k_{n-1})} (\ell(\sigma(\zeta_{p^{1+n}}) - 1)) = p + \ell(\zeta_{p^n} - 1).$$

But this follows from the structure of $\mathrm{G}(k_n/k_{n-1})$ which is the set $\{\gamma^{j+p^n} | 0 \leq j \leq p-1\}$. The equation $d_0 = 1$ follows from $\ell(\zeta_p - 1) = -p$ which is verified directly.
For the second claim we inductively show that $(\sigma(\iota^{-1}(c_n)))_{\sigma \in \Gamma_n}$ generate $\mathcal{F}(\wp_n)$ as a $\mathbb{Z}_p$-module.

$$\begin{tikzcd}
\mathcal{F} \arrow[r, "\iota = \exp \circ \ell(\cdot) - 1", "\cong"'] \arrow[dr, "\ell", "\cong"'] & \widehat{\mathbb{G}}_m \\
& \widehat{\mathbb{G}}_a \arrow[u, "\cong", "\exp(\cdot)-1"']
\end{tikzcd}$$

The case $n = 0$ is immediate from the fact that $\mathcal{U}^1$ is generated by u. For $n \geq 1$, we first prove that

$$\frac{\mathcal{F}(\wp_n)}{\mathcal{F}(\wp_{n-1})} \cong \frac{\ell(\wp_n)}{\ell(\wp_{n-1})} \cong \frac{\wp_n}{\wp_{n-1}}.$$

We have the following diagram

$$\begin{tikzcd}
\mathbb{Q}_p(\mu_{p^{1+n}}) \arrow[dd, dash, "p^n(p-1)"'] \arrow[dr, dash, "p-1"] & \\
& k_n \arrow[dl, dash, "p^n"] \\
\mathbb{Q}_p &
\end{tikzcd}$$

The extension

$$\begin{tikzcd}
\mathbb{Q}_p(\mu_{p^{1+n}}) \arrow[d, dash, "p-1"'] \\
k_n
\end{tikzcd}$$

is tamely ramified and hence the restriction of the trace map to respective integer rings is surjective. Write $x \in \mathcal{F}(\wp_n)$ as

$$x = \mathrm{Tr}_{\mathbb{Q}_p(\mu_{p^{1+n}})/k_n}\left(\sum_{i=0}^{p^{1+n}-1} a_i\zeta_{p^{1+n}}^i\right) = \sum_{\delta\in\Delta}\sum_{i=0}^{p^{1+n}-1} a_i\zeta_{p^{1+n}}^{i\delta}.$$

We then have

$$x^p \equiv y \mod p\mathcal{O}_{k_n},$$

where $y = \sum_{\delta\in\Delta}\sum_{i=0}^{p^n-1} a_i\zeta_{p^n}^{i\delta} \in \wp_{n-1}$. For $k \geq 1$ we have the following congruence

$$\sum_{\delta\in\Delta}\frac{(1+x)^{p^k\delta}-1}{p^k} \equiv \sum_{\delta\in\Delta}\frac{(1+x^p)^{p^{k-1}\delta}-1}{p^k} \equiv \sum_{\delta\in\Delta}\frac{(1+y)^{p^{k-1}\delta}-1}{p^k} \mod \wp_n.$$

From the above we have $\sum_{\delta\in\Delta}\frac{(1+x)^{p^k\delta}-1}{p^k} \in \wp_n + k_{n-1}$. By studying the coefficients of $\ell(x)$ it is easy to deduce that $\ell(x)$ converges when $x \in \wp_n$. Since $\ell(x)$ converges, the tail of the series after sufficiently long will belong to $\wp_n$. That is, for some k_0 sufficiently big we have $\sum_{k\geq k_0}\sum_{\delta\in\Delta}\frac{(1+x)^{p^k\delta}-1}{p^k} \in \wp_n$. Therefore $\ell(x) \in \wp_n + k_{n-1}$, meaning

$$\ell(\wp_n) \subseteq \wp_n + k_{n-1}. \tag{5.1}$$

The group $\widehat{\mathbb{G}}_m$ has no non-trivial torsion element (it has no prime-to-p-torsion by Proposition 3.2.b of [10] and has no p-power torsion because if it contained a p^k-torsion point then ζ_{p^k} and hence ζ_p would belong to $\wp_n$ hence k_n and this is impossible by degree considerations) and since $\mathcal{F}(\wp_n)$ is isomorphic to $\widehat{\mathbb{G}}_m$, $\mathcal{F}(\wp_n)$ also has no torsion point. Hence the map ℓ is injective on $\mathcal{F}(\wp_n)$, and can be easily seen to be compatible with the Galois action. This gives

$$(\wp_n) \cap k_{n-1} = \ell(\wp_{n-1}). \tag{5.2}$$

Using Equation 5.1 and Equation 5.2 we get the following injection:

$$\ell(\wp_n)/\ell(\wp_{n-1}) \hookrightarrow (\wp_n + k_{n-1})/k_{n-1} \cong \wp_n/\wp_{n-1}.$$

From elementary calculations it is seen that $\sum_{\delta\in\Delta}\sum_{k\geq 1}\frac{\zeta_{p^{1+n}}^{\delta}-1}{p^k}$ belongs to k_{n-1} as it is fixed by any element of $1+p^n\mathbb{Z}_p$ so we have

$$\ell(\iota^{-1}(c_n)) = p + \ell(\zeta_{p^{1+n}} - 1) \equiv \sum_{\delta\in\Delta}(\zeta_{p^{1+n}}^{\delta} - 1) \mod k_{n-1}.$$

Since $\sum\limits_{\delta\in\Delta}(\zeta_{p^{1+n}}^{\delta} - 1) \mod k_{n-1}$ generates ${\wp}/{\wp_{n-1}}$ as a $\mathbb{Z}_p[\Gamma_n]$, hence the map above is a bijection. Thus $\ell(\iota^{-1}(\sigma(c_n)))_{\sigma\in\Gamma_n}$ generate $\mathcal{F}(\wp_n)/\mathcal{F}(\wp_{n-1})$. By induction, ε and $\ell(\iota^{-1}(\sigma(c_n)))_{\sigma\in\Gamma_n}$ generate $\mathcal{F}(\wp_n)$. Since $\widehat{\mathbb{G}}_m$ is isomorphic to $\mathcal{F}$ over $\mathbb{Z}_p$, we have proved the second statement. $\clubsuit$

Since d_n has norm 1 Hilbert's theorem 90 gives x_n from k_n such that $d_n = \gamma(x_n)/x_n$. Put $\pi_n = \prod\limits_{\delta\in\Delta}(\zeta_{p^{1+n}}^{\delta} - 1)$. We can see directly from the definition that $(\pi_n)_n$ is a norm coherent sequence of uniformizers of k_n. Hence x_n can be written as $\pi_n^{e_n}u_n$ for $e_n\in\mathbb{Z}$ and $u_n\in(\mathcal{U}_n^1)^{\mathrm{N}=1}$.
The following result will be useful later.

Theorem 5.1. *With the notation introduced above, one has*

$$p \equiv e_n(p-1)\log_p\chi(\gamma) \mod p^{1+n}$$

Proof. Define

$$G(x) = \exp(p)\exp\circ\ell(x) = \exp\circ\ell(x +_{\mathcal{F}} \varepsilon) \in 1 + (p,\, x)\mathbb{Z}_p[[x]]$$

and for $\sigma\in\Gamma$

$$G_\sigma(x) = G((1+x)^{\chi(\sigma)} - 1).$$

By item 2, we can write u_n as $\prod\limits_{\sigma,a}(\sigma(d_n))^a$. Putting $H(x) = \prod\limits_{\sigma,a} G_\sigma(x)^a$ where a, σ are the same as those appearing in the factorization for u_n, we get $H(\zeta_{p^{1+m}} - 1) = \mathrm{Tr}_{k_n/k_m}(u_n)$ for $0\le m\le n$. Put

$$F(x) = \left(\prod_{\delta\in\Delta}\frac{(1+x)^{\delta}\chi(\gamma) - 1}{(1+x)^{\delta} - 1}\right)^{e_n}\frac{H((1+x)^{\chi(\gamma)} - 1)}{H(x)}.$$

$G(x)$ and $F(x)$ coincide when $x = \zeta_{p^{1+m}} - 1$ for $m\in\{0,\dots,n\}$, consequently we have

$$G(x) \equiv F(x) \mod \frac{(1+x)^{p^{1+n}} - 1}{x}.$$

By putting $x = 0$ in the above congruence and taking (p-adic) logarithm we get the desired congruence. ♣

Chapter 6

The Coleman map for the Tate elliptic curve

In this section we consider the Tate elliptic curve over the cyclotomic $\mathbb{Z}_p$- extension of $\mathbb{Q}_p$. First fix a tate curve

$$E = E_q \colon y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where $q = q_E \in \mathbb{Q}_p^\times$ satisfying $\mid q \mid_p < 1$.
By Tate's uniformization (Theorem 2.1) one has

$$\phi \colon \overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}} \xrightarrow{\cong} E_q(\overline{\mathbb{Q}}_p), \quad \phi(u) = (X(u,q), Y(u,q)).$$

Calculating $X(u,q)/Y(u,q)$ gives a power series in $\mathbb{Q}_p[[q,u]]$ and since $\mathbb{Q}_p[[q]] = \mathbb{Q}_p$, $X(u,q)/Y(u,q)$ is a power series in $\mathbb{Q}_p[[u]]$. Considering the quantities just formally ϕ induces an isomorphism $\widehat{\phi}$ over $\mathbb{Q}_p$ of formal groups $\widehat{E}$ and the formal multiplicative group $\widehat{\mathbb{G}}_m$. Expicitly, $\widehat{\phi}$ equals the power series $\exp_{\widehat{E}} \circ \ln(1+x) - 1 \in \mathbb{Z}_p[[x]]$, where $\exp_{\widehat{E}}$ is the exponential map of the formal group $\widehat{E}$:

$$\widehat{E} \xrightarrow[\cong]{\exp_{\widehat{E}}} \widehat{\mathbb{G}}_a.$$

With the isomorphism $\widehat{\phi}$ from now onwards we identify $\widehat{E}$ with $\widehat{\mathbb{G}}_m$.
The cup product in Galois cohomology gives a non-degenerate bilinear pairing

$$(\ ,\ )_{E,n} : H^1(k_n, T) \times H^1(k_n, T^*(1)) \longrightarrow H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

The isomorphism $H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ can be seen as follows: Let k be any finite extension of $\mathbb{Q}_p$. We will show that $H^2(k, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$.

Lemma 0.7.

$$H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$$

Let n be any natural number. We have the Kummer sequence for the field k.

$$1 \to \mu_n(\overline{k}^\times) \xrightarrow{i} \overline{k}^\times \xrightarrow{x \rightsquigarrow x^n} \overline{k}^\times \to 1$$

where i is the inclusion map.
We derive the long exact sequence from it:

$$\ldots \to H^1(k, \overline{k}^\times) \xrightarrow{\delta} H^2(k, \mu_n(\overline{k}^\times)) \xrightarrow{i} H^2(k, \overline{k}^\times) \xrightarrow{[n]} H^2(k, \overline{k}^\times) \to \ldots$$

By Hilbert's theorem 90, the group $H^1(k, \overline{k}^\times)$ is trivial. Hence we have

$$H^2(k, \mu_n(\overline{k}^\times)) = \ker(H^2(k, \overline{k}^\times) \xrightarrow{[n]} H^2(k, \overline{k}^\times)).$$

From local class field theory $H^2(k, \overline{k}^\times) = \mathbb{Q}/\mathbb{Z}$ (Theorem 19.6 of [11]).
So

$$H^2(k, \mu_n(\overline{k}^\times)) = \ker([n]) = \frac{\mathbb{Z}}{n}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

Putting p^m in place of n and taking inverse limit over m, one obtains

$$\varprojlim_m H^2(k, \mu_{p^m}(\overline{k}^\times)) \cong H^2(k, \varprojlim_m \mu_{p^m}(\overline{k}^\times)) = H^2(k, \mathbb{Z}_p(1)) \cong \varprojlim_m \mathbb{Z}/p^m\mathbb{Z} = \mathbb{Z}_p$$

♣

The multiplication by n homomorphism is surjective on $E(\overline{k})$. There is a Kummer sequence for the elliptic curve

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

which induces the long exact sequence:

$$0 \to E(\overline{k})[n]^{G(\overline{k}/k)} \to E(\overline{k})^{G(\overline{k}/k)} \xrightarrow{[n]} E(\overline{k})^{G(\overline{k}/k)} \xrightarrow{\delta} H^1(k, E(\overline{k})[n])$$
$$\to H^1(k, E(\overline{k})) \xrightarrow{[n]} H^1(k, E(\overline{k})) \to \ldots$$

from which we derive the inclusion

$$E(k)/nE(k) \hookrightarrow H^1(k, E(\overline{k})[n]).$$

Replacing n with p^m and taking inverse limit gives

$$\varprojlim_m E(k)/p^m E(k) \hookrightarrow \varprojlim_m H^1(k, E(\overline{k})[p^m])$$

Interchanging inverse limits with cohomology groups we have

$$\varprojlim_m H^1(k, E(\overline{k})[p^m]) \cong H^1(k, \varprojlim_m E(\overline{k})[p^m]) \cong H^1(k, T)$$

. We have

$$E(k) \cong k^\times / q^{\mathbb{Z}},$$

and $k^\times / q^{\mathbb{Z}}$, by Proposition 5.7 [7] admits the decomposition

$$k^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(p^b - 1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[k\colon \mathbb{Q}_p]}$$

for some non-negative integers a, b. From this decomposition we can see directly the isomorphism

$$\varprojlim_n E(k)/p^n E(k) \cong \varprojlim_n E(k) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \cong E(k) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

We have the map $\iota\colon \widehat{E}(\mathcal{M}) \rightarrowtail E(k)$. The group $\widehat{E}(\wp)$ sits inside $E(k)$ injectively. The group $\widehat{E}(\wp)$ no prime-to-p torsion (Chapter 4, Proposition 3.2 of [10]), and hence sits injectively inside the tensor product $E(k) \otimes \mathbb{Z}_p$. We shall regard $\widehat{E}(\mathcal{M})$ as a subgroup of $H^1(k, T)$. We shall return to the cup product pairing described above. We put $k = k_n$ and by fixing the sequence of elements $c_n \in \wp_n \hookrightarrow H^1(k_n, T)$ described in the previous section, we define at each level n, the map

Definition 6.1.

$$\mathrm{Col}_n\colon H^1(k_n, T^*(1)) \to \mathbb{Z}_p[[\Gamma_n]], \quad \mathrm{Col}_n(z) := \sum_{\sigma \in \Gamma_n} (\sigma(c_n), z)_{E,n}\sigma.$$

The group $G_{k_{1+n}}$ is a finite index subgroup of G_{k_n} hence there exists corestriction map $H^1(k_{1+n}, T^*(1)) \xrightarrow{Cor} H^1(k_n, T^*(1))$. The following diagram commutes for every n:

$$\begin{tikzcd}
H^1(k_{1+n}, T^*(1)) \arrow[r, "\mathrm{Col}_{1+n}"] \arrow[d, "\mathrm{Cor}"'] & \mathbb{Z}_p[\Gamma_{1+n}] \arrow[d, "\mathrm{proj}"] \\
H^1(k_n, T^*(1)) \arrow[r, "\mathrm{Col}_n"] & \mathbb{Z}_P[\Gamma_n]
\end{tikzcd}$$

where *proj* is induced by the natural projection $\Gamma_{1+n} \to \Gamma_n$. So we can give the following definition:

Definition 6.2. Because the above diagram commutes, we can form the inverse limit of the maps Col$_n$ to get a map

$$\text{Col} : \varprojlim_n H^1(k_n, T^*(1)) \to \Lambda = \mathbb{Z}_p[[\Gamma]]$$

and the map Col is called the Coleman map.

There is an isomorphism between Λ and $\mathbb{Z}_p[[x]]$ and the image of Col(z) in $\mathbb{Z}_p[[x]]$ shall be denoted by $C_z(x) = C(x)$. We want to compute $C'(0)$.
For each n, let tan(E/k_n) denote the tangent space of $E(k_n)$ at the identity. There exists an exponential map

$$\exp_{E,n} : \text{tan}(E/k_n) \to E(k_n) \otimes \mathbb{Q}_p$$

The dual of the above map, $\exp^*_{E,n}$ satisfies the property

$$(x, z)_{E,n} = Tr_{k_n/\mathbb{Q}_p}(\log_{\widehat{E}}(x) \exp^*_{E,n}(z)) \tag{6.1}$$

for every $x \in \widehat{E}(\wp_n)$ and $z \in H^1(k_n, V^*(1))$.

Chapter 7

Computing $C_z'(0)$ and the MTT conjecture

7.1 First derivative of the coleman at 0

In this section we will find the value of $C_z'(0)$.

Theorem 7.1. *For $z \in H^1(k_n, T^*(1))$, Col$(z)(x) \in \mathbb{Z}_p[[x]]$ satisfies*

$$C_z'(0) = \frac{d}{dx}\big(\textit{Col}(z)(x)\big)\Big|_{x=0} = \frac{p}{(p-1)\log_p(\chi(\gamma))}\frac{\log_p(q_E)}{\nu_p(q_E)}\exp^*_{\omega_E}(z).$$

By Tate's uniformization we have the following short exact sequence

$$0 \to T_1 \to T \to T_2 \to 0$$

where $T_1 \cong \mathbb{Z}_p(1)$ and hence $T_2 = T/T_1 \cong \mathbb{Z}_p$. The cup product again induces a non-degenerate pairing

$$H^1(k_n, T_1) \times H^1(k_n, T_1^*(1)) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

Since T_1 is isomorphic to $\mathbb{Z}_p(1)$, the above pairing takes the form:

$$H^1(k_n, \mathbb{Z}_p(1)) \times H^1(k_n, \mathbb{Z}_p) \to \mathbb{Z}_p$$

which we denote by $(\ ,\ )_{\mathbb{G}_m,n}$ or sometimes just $(\ ,\ )_{\mathbb{G}_m}$. The $\mathbb{Z}_p$-module T_1 is a direct summand of T and hence there exists a natural map $T^* \to T_1^*$ which induces $T^*(1) \to T_1^*(1)$ which further induces the map $H^1(k_n, T^*(1)) \xrightarrow{\pi} H^1(k_n, T_1^*(1))$. The element c_n in T_1 becomes $1 + c_n = d_n$ in the group $\mathbb{G}_m(k_n)$ so for $c_n \in \widehat{E}(\wp_n)$ and $z \in H^1(k_n, T^*(1))$ we have the equation

$$(\sigma(c_n), z)_{E,n} = (\sigma(d_n), \pi(z))_{\mathbb{G}_m,n}.$$

Lemma 0.8.

$$C'(0) = \mathit{Col}(z)'(0) = -\frac{p}{(p-1)\log_p \chi(\gamma)}(p, \pi(z))_{\mathbb{G}_m}. \tag{7.1}$$

We have, the n-th Coleman map given by

$$\text{Col}_n(z) = \sum_{\sigma \in \Gamma_n} (\sigma(c_n),\ z)_{E,n}\sigma = \sum_{\sigma \in \Gamma_n} (\sigma(d_n),\ \pi(z))_{\mathbb{G}_m,n}\sigma.$$

From the definition $\text{Col} = \varprojlim \text{Col}_n$ we get the following

$$\begin{aligned}
\text{Col}(z) &\equiv \text{Col}_n(z) \mod \mathbb{Z}_p[\Gamma_n] \\
&= \sum_{\sigma \in \Gamma_n} (\sigma(c_n), z)_{E,n}\sigma \\
&= \sum_{\sigma \in \Gamma_n} (\sigma(d_n), \pi(z))_{\mathbb{G}_m,n}\sigma \\
&= \sum_{\sigma \in \Gamma_n} (\sigma(\gamma(x_n)/x_n), \pi(z))_{\mathbb{G}_m,n}\sigma \\
&= \sum_{\sigma \in \Gamma_n} (\sigma\gamma(x_n)/\sigma(x_n), \pi(z))_{\mathbb{G}_m,n}\sigma
\end{aligned}$$

Since the cup product is bilinear one gets

$$\begin{aligned}
&= \sum_{\sigma \in \Gamma_n} (\sigma(\gamma(x_n)), \pi(z))_{\mathbb{G}_m,n}\sigma - \sum_{\sigma \in \Gamma_n} (\sigma(x_n), \pi(z))_{\mathbb{G}_m,n}\sigma \\
&= \gamma^{-1} \sum_{\sigma \in \Gamma_n} (\sigma(\gamma(x_n)), \pi(z))_{\mathbb{G}_m,n}\sigma\gamma - \sum_{\sigma \in \Gamma_n} (\sigma(x_n), \pi(z))_{\mathbb{G}_m,n}\sigma
\end{aligned}$$

As γ acts as a generator for each Γ_n, we get

$$= (\gamma^{-1} - 1) \sum_{\sigma \in \Gamma_n} (\sigma(x_n), \pi(z))_{\mathbb{G}_m,n}\sigma.$$

The ring $\mathbb{Z}_p[[\Gamma]]$ is isomorphic to the ring $\mathbb{Z}_p[[x]]$ by the isomorphism $\gamma \rightsquigarrow 1+x$ and for each n the ring $\mathbb{Z}_p[\Gamma_n]$ is isomorphic to $\mathbb{Z}_p[x]/((1+x)^{p^n}-1)$ by the map $\gamma \mod \Gamma_n \rightsquigarrow 1+x \mod ((1+x)^{p^n}-1)$ (section 7.1,[12]). We shall use these identifications to get a power series for Col(z).

Let the image of Col$_n(z)$ in $\mathbb{Z}_p[x]/((1+x)^{p^n}-1)$ be $C_n(x)$ and let $C(x)$ denote the image of Col(z) in $\mathbb{Z}_p[[x]]$.

$$C(x) \equiv (\frac{1}{1+x}-1)\sum_{j=0}^{p^n-1}(\sigma_j(x_n),\pi(z))_{\widehat{\mathbb{G}}_m,n}(1+x)^j \mod ((1+x)^{p^n}-1)$$

$$\frac{C(x)-C(0)}{x} \equiv -\frac{x}{1+x}\sum_{j=0}^{p^n-1}(\sigma_j(x_n),\pi(z))_{\widehat{\mathbb{G}}_m,n}(1+x)^j \mod \frac{(1+x)^{p^n}-1}{x}$$

By taking the limit as $x \to 0$ we have the following equation.

$$C'(0) \equiv -\sum_{j=0}^{p^n-1}(\sigma_j(x_n),\pi(z))_{\widehat{\mathbb{G}}_m,n} \mod p^n.$$

By the linearity of the cup product in the first variable we get

$$C'(0) = \mathbf{Col}(z)'(0) \equiv -(\mathrm{N}_{n/0}(x_n),\pi(z))_{\mathbb{G}_m,0} \mod p^n$$

It remains to calculate $(\mathrm{N}_{n/0}(x_n),\pi(z))_{\mathbb{G}_m,0}$. We know that $x_n = \pi_n^{e_n}u_n$ where $u_n \in (\mathcal{U}_n^1)^{\mathrm{N}=1}$. Therefore by item 2 $\mathrm{N}_{n/0}(x_n) = p^{e_n}$.

$$\begin{aligned}(\mathrm{N}_{n/0}(x_n),\pi(z))_{\mathbb{G}_m,0} &= (p^{e_n},\pi(z))_{\mathbb{G}_m,0}\\ &= e_n(p,\pi(z))_{\mathbb{G}_m,0}\\ &\equiv \frac{p}{(p-1)\log_p\chi(\gamma)}(p,\pi(z))_{\mathbb{G}_m,0} \mod p^n\end{aligned}$$

Taking the limit as $n \to \infty$,

$$C'(0) = \mathbf{Col}(z)'(0) = -\frac{p}{(p-1)\log_p\chi(\gamma)}(p,\pi(z))_{\mathbb{G}_m}.$$

♣

The exact sequence

$$0 \to T_1 \to T \to T_2 \to 0$$

is split exact and hence on taking dual and tensoring with $\mathbb{Z}_p(1)$ produces

$$0 \to T_2^*(1) \to T^*(1) \xrightarrow{\pi} T_1^*(1) \to 0.$$

We get the following exact sequence from the long exact sequence of the above sequence:

$$H^1(\mathbb{Q}_p, T^*(1)) \xrightarrow{\pi} H^1(\mathbb{Q}_p, T_1^*(1)) \xrightarrow{\delta} H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

We have the following diagram coming from Galois cohomology [6].

$$\begin{tikzcd}
H^1(\mathbb{Q}_p, T_1) & \times & H^1(\mathbb{Q}_p, T^*_1(1)) \arrow[dd, "\delta_2"] \arrow[dr, "(\,.\,)_{G_m}"] & \\
 & & & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p \\
H^0(\mathbb{Q}_p, T_2) \arrow[uu, "\delta_1"] & \times & H^2(\mathbb{Q}_p, T^*_2(1)) \arrow[ur, "(\,.\,)_{G_m}"'] &
\end{tikzcd}$$

It is easy to calculate the map δ_1 from $H^0(\mathbb{Q}_p, T_2) = \mathbb{Z}_p$ to $H^1(\mathbb{Q}_p, T_1)$.

Theorem 7.2. *The image of* $1 \in T_2$ *under the map*

$$H^0(\mathbb{Q}_p, T_2) = \mathbb{Z}_p \xrightarrow{\delta_1} H^1(\mathbb{Q}_p, T_1) \xrightarrow{\cong} \mathbb{Q}_p^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

is given by $q_E \otimes 1$.

Proof. The $G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules T_2 and $\mathbb{Z}_p$ are isomorphic, so $H^0(\mathbb{Q}_p, T_2) = \mathbb{Z}_p$. The element 1 in $\mathbb{Z}_p$ which actually is $\bar{f}$ in $T_2 = T/T_1$ is sent to the the element $\sigma \rightsquigarrow c(\sigma)$ since for any $\sigma \in G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ we have

$$\sigma \cdot f - f = c(\sigma)e.$$

But we also have

$$H^1(\mathbb{Q}_p, T_1) = H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \varprojlim H^1(\mathbb{Q}_p, \mu_{p^n}(\overline{\mathbb{Q}}_p^\times)).$$

Under this isomorphism the element $c : \ \sigma \rightsquigarrow c(\sigma)e$ can be thought of as the compatible sequence

$$(c_n : \ \sigma \rightsquigarrow c_n(\sigma)e_n)$$

where $c_n(\sigma)$ is $c(\sigma) \mod p^n$ and e_n is the n-th component of e. The term $c_n e_n$ is the additive notation for the element $\varepsilon^{(n)^{c_n}}$ from $H^1(\mathbb{Q}_p, \mu_{p^n}(\overline{\mathbb{Q}}_p^{\times}))$. The element $\varepsilon^{(n)^{c_n}}$ corresponds to the class of $q^{(n)}$ in $\mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times p^n}$ since we have

$$\sigma \cdot q^{(n)}/q^{(n)} = \varepsilon^{(n)^{c_n}}.$$

The image of $q^{(n)}$ in $\mathbb{Q}_p^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}$ is $q^{(n)} \otimes 1$ which under inverse limit is $q \otimes 1 = q_E \otimes 1$. ♣

If $w \in H^1(\mathbb{Q}_p, T^*(1))$, the commutative diagram above gives

$$(q \otimes 1,\, w)_{\mathbb{G}_m} = (\delta_1(1),\, w)_{\widehat{\mathbb{G}}_m} = (1,\, \delta_2(w))_{\mathbb{G}_m}.$$

If w is of the form $\pi(z)$ for some $z \in H^1(\mathbb{Q}_p, T^*(1))$ then

$$(q \otimes 1,\, \pi(z))_{\mathbb{G}_m} = (1,\, \delta_2 \circ \pi(z))_{\mathbb{G}_m} = (1,\, 0)_{\mathbb{G}_m} = 0 \tag{7.2}$$

since $\delta_2 \circ \pi = 0$. Factorising q in $\mathbb{Q}_p$ as $q = p^{\nu_p(q)}\omega u$ where $\omega \in \mu_{p-1}$ and $u \in \Gamma$, we have

$$\begin{aligned}(q \otimes 1,\, w)_{\mathbb{G}_m} &= \nu_p(q)(p,\, w)_{\mathbb{G}_m} + (u,\, w)_{\mathbb{G}_m} & (7.3)\\ &= \nu_p(q)(p,\, w)_{\mathbb{G}_m} + \log_p(u)\exp^*_{\omega_{\mathbb{G}_m}}(w). & (7.4)\end{aligned}$$

Using Equation 7.2 and Equation 7.3 we have

$$\begin{aligned}(p,\, \pi(z))_{\mathbb{G}_m} &= -\frac{\log_p(u)}{\nu_p(q)}\exp^*_{\omega_{\mathbb{G}_m}}(\pi(z)) & (7.5)\\ &= -\frac{\log_p(q)}{\nu_p(q)}\exp^*_{\omega_E}(z). & (7.6)\end{aligned}$$

Combining Equation 7.1 and Equation 7.5 we obtain the following

$$\frac{d}{dx}\big(\mathrm{Col}(z)(x)\big)\bigg|_{x=0} = \frac{p}{(p-1)\log_p(\chi(\gamma))}\frac{\log_p(q_E)}{\nu_p(q_E)}\exp^*_{\omega_E}(z). \tag{7.7}$$

The Mazur-Tate-teitelbaum conjecture

We have the equation:

$$\mathrm{Col}_n(z) = \sum_{\sigma \in \Gamma_n} (\sigma(c_n),\, z)_{E,n}\sigma.$$

From the equation Equation 6.1, we have

$$\begin{aligned}
\mathrm{Col}_n(z) &= \sum_{\sigma\in\Gamma_n} \mathrm{Tr}_{\mathrm{k_n/\mathbb{Q}_p}}\big(\mathrm{\log_p(\sigma(d_n))\exp^*_{\omega_E}(z)}\big)\sigma \\
&= \sum_{\sigma\in\Gamma_n}\Big[\sum_{\sigma_1\in\Gamma_n}\sigma_1\big(\log_p(\sigma(d_n))\big)\exp^*_{\omega_E}(z)\Big]\sigma \\
&= \sum_{\sigma,\sigma_1\in\Gamma_n}\log_p\big(\sigma_1\sigma(d_n)\big)\exp^*_{\omega_E}(z^{\sigma_1})\sigma \\
&= \sum_{\sigma_1}\exp^*_{\omega_E}(z^{\sigma_1})\sum_{\sigma}\log_p(\sigma_1\sigma(d_n)) \\
&= \big(\sum_{\sigma_1}\exp^*_{\omega_E}(z^{\sigma_1})\sigma_1^{-1}\big)\big(\sum_{\sigma}\log_p(\sigma_1\sigma(d_n)\sigma)\big).
\end{aligned}$$

Kato showed that there exists an element $z^{Kato}\in\varprojlim_n H^1(k_n,T^*(1))$ such that

$$\sum_{\sigma}\exp^*_{\omega_E}\big(\sigma(z^{Kato})\big)\chi(\sigma)^{-1} = e_p(\overline{\chi})\frac{L(E,\overline{\chi},1)}{\Omega_E^+},$$

where

$$e_p(\chi)=\begin{cases}1 & \chi \text{ is not trivial}\\ 1-\frac{1}{p} & \chi \text{ is trivial}\end{cases}$$

and Ω_E^+ is the real period of the elliptic curve.

The p-adic L-function of an elliptic curve $L_p(E,s)$ can be written as $\mathcal{L}_{p,\gamma}(E,\chi(\gamma)^{s-1}-1)$. It follows that

$$\mathrm{Col}(z^{Kato})(X)=\mathcal{L}_{p,\gamma}(E,X).$$

Combining the above with equation Equation 7.7, we get the following theorem, which is the **Mazur-Tate-teitelbaum conjecture**.

Corollary 7.2.1. *Let $\mathcal{L}_{p,\gamma}(E,X)$ be the power series in $\mathbb{Z}_p[[X]]$ such that*

$$L_p(E,s)=\mathcal{L}_{p,\gamma}(E,\chi(\gamma)^{s-1}-1).$$

Then, we have

$$\frac{d}{dX}\mathcal{L}_{p,\gamma}(E,X)\big|_{X=0}=\frac{1}{\log_p\chi(\gamma)}\frac{\log_p q_E}{\nu_p(q_E)}\frac{L(E,1)}{\Omega_E^+}$$

or,

$$L_p'(E,1)=\frac{\log_p q_E}{\nu_p(q_E)}\frac{L(E,1)}{\Omega_E^+}.$$

Bibliography

[1] BERGER, Laurent: An introduction to the theory of p-adic representations. In: *Geometric aspects of Dwork theory. Vol. I, II.* Walter de Gruyter GmbH & Co. KG, Berlin, 2004, S. 255–292

[2] COATES, J. ; SUJATHA, R.: *Cyclotomic fields and zeta values.* Springer-Verlag, Berlin, 2006 (Springer Monographs in Mathematics). – x+113 S. – ISBN 978-3-540-33068-4; 3-540-33068-2

[3] CONRAD, Keith: *p-ADIC INTERPOLATION.* – URL `http://www.math.uconn.edu/~kconrad/math5020f11/padicinterpolation.pdf`

[4] CRANCH, James: *Elliptic Curves.* 2005. – URL `http://homepages.warwick.ac.uk/~masiao/maths/lecturenotes/ellipticnotes.pdf`

[5] KOBAYASHI, Shin-ichi: Iwasawa theory for elliptic curves at supersingular primes. In: *Invent. Math.* 152 (2003), Nr. 1, S. 1–36. – URL `http://dx.doi.org/10.1007/s00222-002-0265-4`. – ISSN 0020-9910

[6] KOBAYASHI, Shinichi: An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves. In: *Doc. Math.* (2006), Nr. Extra Vol., S. 567–575. – ISSN 1431-0635

[7] NEUKIRCH, Jürgen: *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Bd. 322: *Algebraic number theory.* Springer-Verlag, Berlin, 1999. – xviii+571 S. – URL `http://dx.doi.org/10.1007/978-3-662-03983-0`. – Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. – ISBN 3-540-65399-6

[8] Shalit, Ehud de: *Perspectives in Mathematics*. Bd. 3: *Iwasawa theory of elliptic curves with complex multiplication*. Academic Press, Inc., Boston, MA, 1987. – x+154 S. – p-adic L functions. – ISBN 0-12-210255-X

[9] Silverman, Joseph H.: *Graduate Texts in Mathematics*. Bd. 151: *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994. – xiv+525 S. – URL http://dx.doi.org/10.1007/978-1-4612-0851-8. – ISBN 0-387-94328-5

[10] Silverman, Joseph H.: *Graduate Texts in Mathematics*. Bd. 106: *The arithmetic of elliptic curves*. Second. Springer, Dordrecht, 2009. – xx+513 S. – URL http://dx.doi.org/10.1007/978-0-387-09494-6. – ISBN 978-0-387-09493-9

[11] Stein, William: *A Short Course on Galois Cohomology*. Spring 2010. – URL http://wstein.org/edu/2010/582e/lectures/all/galois_cohomology.pdf

[12] Washington, Lawrence C.: *Graduate Texts in Mathematics*. Bd. 83: *Introduction to cyclotomic fields*. Springer-Verlag, New York, 1982. – xi+389 S. – URL http://dx.doi.org/10.1007/978-1-4684-0133-2. – ISBN 0-387-90622-3