Iwasawa theory of elliptic curves with complex multiplication

Cambridge, Lent 2010.

1. Introduction. $[F:\mathbb{Q}] < \infty$, E/F - an elliptic curve.

We say E has complex multiplication (= CM) if $\mathrm{End}_{\mathbb{Q}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \neq \mathbb{Q}$ (it is then true that $K = \mathrm{End}_{\mathbb{Q}}(E) \otimes_{\mathbb{Z}}$ is an imaginary quadratic field K).

Classical examples

(i) $y^2 = x^3 - Dx$, $D \neq 0$ in F, $(x,y) \longmapsto (-x, iy)$; $K = \mathbb{Q}(i$

(ii) $y^2 = x^3 + D$, $D \neq 0$ in F, $(x,y) \longmapsto (\rho x, y)$, $\rho^3 = 1$, $K = \mathbb{Q}$

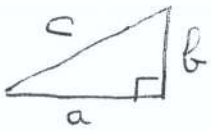
We shall be interested in the arithmetic of these curves (not questions like Kronecker's jugendtraum...). These are the most ancient unsolved major problems on diophantine equations, and probably the whole of number theory. Attempting to solve these problems remains one of the major challenges of number theory today. Here is one of the most important examples:-

Congruent number problem.

D - an integer ≥ 1.

Defn. D is a congruent number if there exists a right-angled triangle, all of whose sides have rational length, of area D.

e.g. $D = 5, 6, \text{or } 7$



$(a, b, c) = \left(\frac{40}{6}, \frac{9}{6}, \frac{41}{6}\right), (3, 4, 5), \left(\frac{288}{60}, \frac{175}{60}, \frac{337}{60}\right)$.

10 th century Arab manuscript of Al Kazin lists as congruent:-

$$5, 6, 14, 15, 21, 30, 34, 65, \ldots, 10374.$$

Two major unsolved problems:-

<u>Problem 1</u>. Prove the existence of an algorithm for deciding in a finite number of steps whether or not a given D is congruent.

<u>Problem 2</u>. Prove that every integer $\equiv 5, 6, 7 \bmod 8$ is congruent.

Problem 2 was noticed classically, but can only be explained by the connexion with L-functions. Solutions of either of these problems remains one of the great challenges to number theory.

Why are these problems about the arithmetic of CM elliptic curves?

<u>Lemma</u>. Let D be an integer ≥ 1. Then D is congruent $\iff$ there exists a point (x, y), with x, y in $\mathbb{Q}$, & $y \neq 0$ on the curve

$$E_D : y^2 = x^3 - D^2 x.$$

<u>Proof</u>

$\longmapsto \quad x = \dfrac{D(a+c)}{b}, \; y = \dfrac{2D^2(a+c)}{b^2}$

is a point on E_D with $y \neq 0$.

Point (x, y) on E_D with $y \neq 0 \longmapsto$

$$a = \left|\frac{D^2 - x^2}{y}\right|, \quad b = \left|\frac{2Dx}{y}\right|, \quad c = \left|\frac{D^2 + x^2}{y}\right|.$$

<u>Remark</u>. Fermat's proof that 1 is not congruent started the whole modern theory of the arithmetic of elliptic curves.

<u>Nature of the course</u>.

<u>Part I</u>. Automorphic nature of CM elliptic curves. Complex L-functions (Deuring-Weil...). This is surprisingly easy.

<u>Part II</u>. Will cover some aspects of the p-adic theory. We know much less about p-adic L-functions but in some cases we can relate the p-adic L-functions to the arithmetic of the curve (Iwasawa theory).

I. Complex Automorphic Theory.

Here is a typical example of the problem we want to solve.

$E: \; y^2 = x^3 - x$, good reduction outside 2

$[F:\mathbb{Q}] < \infty$, $L(E/F, s) = \prod_{v \text{ good}} \left(1 - a_v (Nv)^{-s} + (Nv)^{1-2s}\right)^{-1}$

where $\#(\tilde{E}_v(k_v)) = Nv + 1 - a_v$, k_v = res. field of v, $Nv = \#(k_v)$.

How do we analytically continue $L(E/F, s)$ and prove its functional equation. We relate it to a Hecke L-function, where we know analytic continuation.

<u>Remark</u>. There are no $E/\mathbb{Q}$ without CM for which we know the analytic continuation and functional equation for all $F/\mathbb{Q}$ with $[F:\mathbb{Q}]$ finite.

<u>Need</u>. Local and global class field theory (Cassels-Frohlich)

We also assume basic knowledge of elliptic curves (see Part III course).

1 Commutants in endomorphisms rings of elliptic curves

k - any field, k^{sep} = separable closure, $G_k = Gal(k^{sep}/k)$

$End_k(A)$ = ring of endomorphisms of A defined over k.

<u>Hypothesis C</u>. We are given an injection

$$i : K \longrightarrow End_k(A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where K is an imaginary quadratic field.

We assume Hypothesis C is valid for this discussion.

$p \neq \text{char. } k$, $A_{p^n} = \operatorname{Ker}\left(A(k^{sep}) \xrightarrow{p^n} A(k^{sep})\right)$.

<u>Defn</u>. $T_p(A) = \varprojlim A_{p^n}$, $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

$V_p(A)$ has dimension 2 over $\mathbb{Q}_p$.

$\operatorname{End}_k(A)$ operates on $V_p(A)$

<u>Fact</u> (See Silverman):

$$j : \operatorname{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \operatorname{End}_{\mathbb{Q}_p}(V_p(A))$$

is injective.

<u>Identify</u>: K with $i(K)$, $\operatorname{End}_k(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with its image under

<u>Defn</u>. $R = K \cap \operatorname{End}_k(A)$.

Then R is an order in K.

<u>Defn</u>. $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p = R \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

<u>Theorem</u>. Assume Hypothesis C is valid. Then $V_p(A)$ is a free K_p-module of rank 1. Moreover, an element φ of K_p maps $T_p(A)$ into itself if and only if φ belongs to R_p.

<u>Proof</u>. Both K_p and $V_p(A)$ have dimension 2 over $\mathbb{Q}_p$.

K_p a field $\Rightarrow$ $V_p(A)$ must have dimension 1 over K

K_p not a field $\Rightarrow$ $K_p = \mathbb{Q}_p \times \mathbb{Q}_p$.

K_p operates faithfully on $V_p(A)$.

$e_1 = (1,0)$, $e_2 = (0,1)$. $e_i V_p(A) \neq 0$.

$V_p(A) = e_1 V_p(A) \oplus e_2 V_p(A) \Rightarrow e_i V_p(A)$ has dim. 1 over $\mathbb{Q}_p$

$\alpha_i = \mathbb{Q}_p$-basis of $e_i V_p(A)$.

Take $\beta = \alpha_1 + \alpha_2$, $V_p(A) = K_p \beta$.

This proves first assertion.

Given φ in K_p such that $\varphi(T_p(A)) \subset T_p(A)$.

Then $p^n \varphi \in R_p$ for some $n \geq 0$.

We can ψ in R such that $p^n \varphi \equiv \psi \bmod p^n R_p$.

Now $\varphi(T_p(A)) \subset T_p(A) \Rightarrow \psi(T_p(A)) \subset p^n T_p(A)$.

$\Rightarrow \psi(A_{p^n}) = 0$. By a standard result (see Silverman) $\Rightarrow \psi = p^n \rho$ for some $\rho \in \mathrm{End}_k(A)$

$\Rightarrow \rho \in R = K \cap \mathrm{End}_k(A) \Rightarrow \varphi \in R_p$ (which is a free $\mathbb{Z}_p$-module).

<u>Corollary</u>. Assume Hypothesis C is valid. Then the commutant of R in (i) $\mathrm{End}(V_p(A))$ is K_p, (ii) $\mathrm{End}(T_p(A))$ is R_p, (iii) $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is K, and (iv) $\mathrm{End}_k(A)$ is R.

<u>Proof</u>. (i) α commutes with $R \Rightarrow \alpha$ commutes with $K_p = R \otimes_{\mathbb{Z}} \mathbb{Q}_p \Rightarrow \alpha$ lies in K_p.

ii). $R_p = K_p \cap \mathrm{End}(T_p(A))$ by previous theorem.

(iii). j injective $\Rightarrow$ dimension over $\mathbb{Q}$ of the commutant of R in $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is at most $[K_p : \mathbb{Q}_p] = 2$.

(iv). Follows because $R = K \cap \mathrm{End}_k(A)$.

<u>Corollary</u>. Assume that Hypothesis C is valid, and let $\rho_p : G_k \longrightarrow \mathrm{Aut}(T_p(A))$ be the p-adic Galois representation attached to A. Then $\rho_p(G_k) \subset R_p^\times$. In particular, $\rho_p(G_k)$ is abelian.

<u>Proof</u>. If σ is in G_k, $\rho_p(\sigma)$ commutes with $\mathrm{End}_k(A)$, and so with R. Hence it commutes with $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, whence $\rho_p(\sigma) \in R_p$ q.e.d.

<u>Lifting Frobenius Endomorphisms</u>

$[F : \mathbb{Q}] < \infty$, E/F.

S - finite set of places where E has bad reduction.

$v \notin S$, k_v = residue field of v, $\tilde{E}_v/k_v$ - reduced curve.

$\mathrm{End}_{k_v}(\tilde{E}_v)$, $N_v = \#(k_v)$.

$\varphi_v \in \mathrm{End}_{k_v}(\tilde{E}_v)$, we have defined by $\varphi_v(x, y) = (x^{N_v}, y^{N_v})$

<u>Lemma</u>. For each $v \notin S$, φ_v lies in the centre of $\mathrm{End}_{k_v}(\tilde{E}_v)$.

Note we have, for $v \notin S$, a reduction map

$$i_v : \mathrm{End}_F(E) \longrightarrow \mathrm{End}_{k_v}(\tilde{E}_v)$$

which is <u>injective</u>. This gives a canonical injection

$$i_v : \mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}_{k_v}(\tilde{E}_v) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

<u>Question</u>. When will there exist $\pi_v \in \mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $i_v(\pi_v) = \varphi_v$?
There is no hope (e.g. just in terms of degrees) if $\mathrm{End}_F(E) = \mathbb{Z}$.

<u>Theorem</u>. Assume $\mathrm{End}_F(E) \neq \mathbb{Z}$. For each $v \notin S$, there exists a unique π_v in K such that $i_v(\pi_v) = \varphi_v$

<u>Proof</u>. Put $K = \mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then K is an imaginary quadratic field, and i_v gives an injection

$$i_v : K \longrightarrow \mathrm{End}_{k_v}(\tilde{E}_v) \otimes_{\mathbb{Z}} \mathbb{Q}$$

In other words, Hypothesis (C) holds for $\tilde{E}_v / k_v$. φ_v lies in the centre of $\mathrm{End}_{k_v}(\tilde{E}_v)$. Hence by our theorem, we have that $\exists !$

$$\pi_v \in i_v(K) \cap \mathrm{End}_{k_v}(\tilde{E}_v)$$

such that $i_v(\pi_v) = \varphi_v$.

<u>Note</u>. It is <u>not</u> necessarily true that $i_v(\mathrm{End}_F(E)) = i_v(K) \cap \mathrm{End}_{k_v}(\tilde{E}_v)$.

<u>ex</u>. (Rubin & Silverberg)

$K = \mathbb{Q}(\sqrt{-11})$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\beta$, $\beta = \dfrac{1+\sqrt{-11}}{2}$.

$\mathcal{O} = \mathbb{Z} + 3\,\mathcal{O}_K$ — order of conductor 3

$$F = K(\sqrt{-3}) = K(\sqrt{33}) = K(j(\mathcal{O}))$$

$$j(\mathcal{O}) = -1880803047833 6 - 3274057859072\sqrt{33}$$

$$E: \; y^2 + y = x^3 + ax^2 + bx + c$$

$$a = -\frac{(7+\sqrt{33})}{2}, \quad b = -\frac{(2487+433\sqrt{33})}{2}, \quad c = -(21416+3728\sqrt{33})$$

$$j(E) = j(\mathcal{O})$$

$\Delta(E) = -23 - 4\sqrt{33}$ – a unit $\Rightarrow$ E has good reduction everywhere and $S = \phi$.

$3 = \beta\bar{\beta}$, $\mathfrak{p} = \beta\mathcal{O}_K$, $\mathfrak{P}$ a prime of F above $\mathfrak{p}$.

We have to have $\pi_{\mathfrak{P}}\mathcal{O}_K = \beta\mathcal{O}_K \Rightarrow \pi_{\mathfrak{P}} = \pm\beta \notin \mathcal{O}$.

<u>Factorization of Frobenius elements</u>.

We assume that E/F has $\mathrm{End}_F(E) \neq \mathbb{Z}$. Put

$$K = \mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

$\Omega(E/F)$ = space of holomorphic differentials on E/F

$$= F\omega, \quad \omega = \frac{dx}{2y + a_1x + a_3}$$

$$E/F: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Action of $\mathrm{End}_F(E)$ on $\Omega(E/F)$ gives an embedding $\mathrm{End}_F(E) \hookrightarrow F$ and so an embedding $K \hookrightarrow F$.

We let $N_{F/K}$ denote the norm map from F to K.

$\mathcal{O}_K$ = ring of integers of K, $\mathrm{End}_F(E)$ is a subring of $\mathcal{O}_K$ of finite index.

<u>Theorem</u>. Assume $\mathrm{End}_F(E) \neq \mathbb{Z}$. For each prime v of F such that (i) v is not in S, and (ii) the characteristic of k_v is prime to $[\mathcal{O}_K : \mathrm{End}_F(E)]$, we have

$$(\pi_v) = N_{F/K}\, v.$$

We begin with a lemma:-

<u>Lemma</u>. For each $v \notin S$, we have

$$N_{K/\mathbb{Q}}\, \pi_v = Nv, \quad \mathrm{Tr}_{K/\mathbb{Q}}\, \pi_v = Nv + 1 - \#(\tilde{E}_v(k_v)).$$

<u>Proof</u>. It use the l-adic rep. ($l \neq$ res. fold char.). Reduction modulo v defines an isomorphism

$$V_l(E) \xrightarrow{\sim} V_l(\tilde{E}_v).$$

Thus we have a commutative diagram

$$\begin{tikzcd} K \arrow[r, "e_l"] \arrow[d, "i_v"'] & \mathrm{End}_{\mathbb{Q}_l}(V_l(E)) \arrow[d, "\wr"] \\ \mathrm{End}_k(\tilde{E}_v) \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r, "e_{v,l}"] & \mathrm{End}_{\mathbb{Q}_l}(V_l(\tilde{E}_v)) \end{tikzcd}$$

$\alpha \in K$, trace and determinant of $e_l(\alpha)$ are $\mathrm{Tr}_{K/\mathbb{Q}}\, \alpha$ & $N_{K/\mathbb{Q}}\, \alpha$.

$\beta \in \mathrm{End}_{k_v}(\tilde{E}_v) \otimes_{\mathbb{Z}} \mathbb{Q}$, $\hat{\beta}$ its transpose

trace and determinant of $e_{v,l}(\beta)$ is equal to $\beta + \hat{\beta}$, $\beta \circ \hat{\beta}$.

Take $\beta = \varphi_v$, we know in this case (see Silverman) that the trace and determinant are equal to $N_v + 1 - \#(\tilde{E}_v(k_v))$ and N_v q.e.d.

<u>Conclusion</u>. π_v $(v \notin S)$ are algebraic integers in K.

<u>Note</u>: We immediately get our result if there is a unique prime of K above p_v = res. char. of k_v. But we need something more to handle the case when p_v splits in

<u>Lemma</u>. Assume that $v \notin S$, and that the characteristic of k_v is prime to $[\mathcal{O}_K : \mathrm{End}_F(E)]$. Then $\mathrm{ord}_w(\pi_v) > 0$, where $w = v|K$.

<u>Proof</u>. F has a generalized Weierstrass equation for E over F with good reduction at v.

$$\omega = \frac{dx}{2y + a_1 x + a_3} \quad \text{— basis of } F\text{-vector space of hol. diff.}$$

$\omega \circ \alpha = \alpha \omega$ for $\alpha \in \mathrm{End}_F(E)$, thanks to our choice of $K \hookrightarrow F$.

Pick a positive integer n, prime to char. of k_v, such that $n\pi_v$ is in $\mathrm{End}_F(E)$ (possible because of our hypothesis that char. of k_v does not divide $[\mathcal{O}_K : \mathrm{End}_F(E)]$. Then

$$\omega \circ n\pi_v = n\pi_v \, \omega .$$

We now reduce modulo v, and get

$$\tilde{\omega} \circ n\tilde{\pi}_v = n\tilde{\pi}_v \, \tilde{\omega} .$$

But $n\tilde{\pi}_v = n\varphi_v$, and so is purely inseparable.

Hence $n\tilde{\pi}_v = 0 \Rightarrow \tilde{\pi}_v = 0$ q.e.d.

We can now prove our theorem.

p_v = res. char. of v

(i). unique prime w of K above p_v: $(\pi_v) = w^a$, where $a = [k_v : k_w]$.

(ii). Two primes w, w^* of K above p_v.

$(\pi_v) = w^a w^{*b}$, where $a > 0$ by previous lemma.

Hence we must show that $b = 0$.

Assume the contrary, i.e. $b > 0$.

$\Rightarrow$ p_v divides $\pi_v^n + \pi_v^{*n}$ for all $n \geq 1$.

$k_{v,n}$ – unique extension of k_v of degree n. Then

$$\#\left(\widetilde{E}_v(k_{v,n})\right) = (Nv)^n + 1 - \left(\pi_v^n + \pi_v^{*n}\right).$$

$\Rightarrow$ $\widetilde{E}_v(k_{v,n})(p_v) = 0$. $\square$

(formal groups $\Rightarrow$ w^* torsion (which is p-torsion) injects into $\widehat{E}_v$.

We have $w^{*\tau} = (\beta)$ for some $\beta \in \mathcal{O}_K$.

Choose n with $(n, p_v) = 1$ such that $\lambda = n\beta \in \mathrm{End}_F(E)$

$E_\lambda(p_v) \neq 0$ – for example it contains $E_{w^{*\tau}}$, which is cyclic of order p_v^τ.

$\widehat{E}$ – formal group of E at v.

<u>Claim</u>. $\widehat{E}_\lambda \cap \widehat{E} = 0$.

$:= -[x, y]$

$$\frac{[\lambda](t)}{t} = \lambda + \sum_{n=2}^{\infty} b_n t^{n-1} \quad b_n \in \mathcal{O}_{F_v}.$$

But λ is a unit at $w \Rightarrow \frac{[\lambda](t)}{t}$ has no zeroes in max. ideal of ring of [illegible]

of the algebraic closure of F_v. Hence $\widetilde{E}_\lambda$ is isomorphic to E_λ, and so we get $\widetilde{E}_v(k_{v,n})(p_v) \neq 0$ for $n >> 0$.

<u>Existence of the Grossencharacter</u>.

E/F, S, as before, I_S - free abelian group on $v \notin S$.

<u>Defn</u>: $\psi_{E/F} : I_S \longrightarrow K^\times$

$\psi_{E/F}(v) = \pi_v$ and extend by multiplicativity.

<u>Note</u>: By factorization theorem, π_v is <u>never</u> a root of unity.

<u>Theorem</u>. There exists an integral ideal $\mathfrak{g}$ of F, divisible by at least by all v in S, such that, for all $\alpha \in K^\times$ with $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g})$ for all $v \mid \mathfrak{g}$, we have

$$\psi_{E/F}((\alpha)) = N_{F/K}(\alpha).$$

<u>Remark</u>. Shows $\psi_{E/F}$ is a Grossencharacter of F in the sense of Hecke.

<u>Proof</u> $S' = S \cup$ places of F whose residue characteristic divides $[\mathcal{O}_K : \mathrm{End}_F(E)]$.

<u>Claim</u>. $\alpha \in F^\times$, prime to S', we have

$$(\psi_{E/F}((\alpha))) = (N_{F/K}\alpha)$$

Follows immediately from $(\pi_v) = N_{F/K}v$ for $v \notin S'$.

$$\Rightarrow \quad \psi_{E/F}((\alpha)) = \zeta_\alpha N_{F/K}\alpha, \quad \zeta_\alpha \in \mu_K.$$

Hence we must show we can find a $\mathfrak{g}$ such that $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g}) \Rightarrow \zeta_\alpha = 1$.

We have to use Artin's global reciprocity law.

<u>Strategy</u>. To find $\mathfrak{g}$ such that $\mathrm{ord}_v(\alpha-1) \geq \mathrm{ord}_v(\mathfrak{g})$ for all $v \mid \mathfrak{g} \Rightarrow \mathcal{S}_\alpha \equiv 1 \bmod w$ for some prime w of K which does not divide $\#(\mu_K)$.

This implies $\mathcal{S}_\alpha = 1$.

Artin's law applies to <u>abelian</u> extensions of F. How do we get one?

ℓ - any prime number: $\rho_\ell : G_F \longrightarrow \mathrm{Aut}(T_\ell(E))$.

We know $\rho_\ell(G_F) \subset R_\ell^\times$ and so is abelian.

Hence $F(E_{\ell^\infty})/F$ is abelian $\Rightarrow F(E_\ell)/F$ is abelian.

We will apply Artin's law to this abelian extension.

<u>Lemma</u>. $F(E_\ell)/F$ is unramified outside S and the primes dividing ℓ.

<u>Proof</u>. Assume $v \notin S$ and $v \nmid \ell$. Then reduction modulo v is injective on E_ℓ.

<u>Frobenius automorphism</u>: $v \notin S$ & $v \nmid \ell$

$$\begin{array}{ccc} F(E_\ell) & & w \\ | & & | \\ F & & v \\ | & & \\ K & & \end{array}$$

$\sigma_v \in \mathrm{Gal}(F(E_\ell)$: Frobenius aut. of v

$\sigma_v \alpha \equiv \alpha^{Nv} \bmod w$ for all $\alpha \in \mathcal{O}_{F(E_\ell)}$

$Nv = \#(k_v)$.

<u>Question</u> : What is $\sigma_{\mathfrak{v}}(P)$ for $P \in E_\ell$.

By definition : $\widetilde{\sigma_{\mathfrak{v}}(P)} = \varphi_{\mathfrak{v}}(\widetilde{P})$, where $\sim$ denotes reduc mod $\mathfrak{v}$.

We want to lift this to a statement in char. 0.

~~Lemma~~
<u>Assumption</u> : ℓ does not divide $[\mathcal{O}_K : \mathrm{End}_F(E)]$.

$\Rightarrow \quad \mathrm{End}_F(E)/\ell\,\mathrm{End}_F(E) = \mathcal{O}_K/\ell\mathcal{O}_K$.

$\Rightarrow$ $\pi_{\mathfrak{v}}$ can be viewed as an element of $\mathrm{End}_F(E)/\ell\mathrm{End}_F$ provided we assume $\mathfrak{v} \notin S$.

<u>Lemma</u>. Assume $\mathfrak{v} \notin S$ and $\mathfrak{v} \nmid \ell$, and that $(\ell, [\mathcal{O}_K : \mathrm{End}_F(E)]) = 1$.

Then

$$\sigma_{\mathfrak{v}}(P) = \psi_{E/F}(\mathfrak{v})(P) \quad \forall\, P \in E_\ell.$$

Hence, if $\mathfrak{a}$ is an ideal of F prime to S and ℓ, we have

$$\sigma_{\mathfrak{a}}(P) = \psi_{E/F}(\mathfrak{a})(P).$$

<u>Proof</u>. We check that $\widetilde{\sigma_{\mathfrak{v}}(P)} = \widetilde{\psi_{E/F}(\mathfrak{v})(P)} = \varphi_{\mathfrak{v}}(\widetilde{P})$.

We now apply Artin's reciprocity law to the abelian extension $F(E_\ell)/F \Rightarrow$ there exists a conductor for this extension. Hence there exists an ideal $\mathfrak{g}$, divisible by all primes in S and all primes dividing ℓ, such that

$$\mathrm{ord}_{\mathfrak{v}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{v}}(\mathfrak{g}) \text{ for all } \mathfrak{v} \text{ dividing } \mathfrak{g}$$

$\Rightarrow \quad \sigma_{(\alpha)} = 1.$

Hence

$$\psi_{E|F}((\alpha))(P) = P \qquad \text{for all} \quad P \in E_\ell .$$

Hence

$$\psi_{E/F}((\alpha)) \equiv 1 \bmod \ell .$$

But we can assume that $\mathfrak{g}$ is also divisible by all places v of F whose residue characteristic divides $[\mathcal{O}_K : \mathrm{End}_F(E)]$. Hence

$$\psi_{E/F}((\alpha)) = S_\alpha N_{E/F}\alpha .$$

But $\alpha \equiv 1 \bmod v$ for all $v | \ell \Rightarrow N_{E/F}\alpha \equiv 1 \bmod u$, where $u = v|K \Rightarrow S_\alpha \equiv 1 \bmod u$.

<u>Final choice</u>. Choose ℓ so that $(\ell, \#(\mu_K)) = 1$.
Hence $S_\alpha \equiv 1 \bmod u \Rightarrow S_\alpha = 1$ q.e.d.

<u>Serre-Tate homomorphism</u>.

From the above argument, it is not clear what ~~is~~ are the primes dividing the conductor of $\psi_{E/F}$. Important for questions of good reduction.

<u>Idea</u>. Switch to an idèle-theoretic point of view. Formulated nicely by Serre-Tate.

$\mathcal{I}_F$ = idèle group of F.

T - finite set of places of F containing infinite ones

<u>Defn</u>: $\mathcal{I}_F^T = \{(x_v) \in \mathcal{I}_F : x_v = 1 \text{ for } v \in T\}$.

26. Put the usual topology on $\mathcal{I}_F$, and discrete topology on $K^\times$.

Theorem (Serre - Tate). There exists a unique homomorphism

$$\varepsilon_{E/F} : \mathcal{I}_F \longrightarrow K^\times$$

such that :- (i) $\varepsilon_{E/F}$ is continuous ($\Leftrightarrow$ Ker $\varepsilon_{E/F}$ is open in $\mathcal{I}_F$); (ii). for all $\alpha \in F^\times$, we have $\varepsilon_{E/F}(\alpha) = N_{F/K}\alpha$; and (iii) there exists a finite set T of places of F, containing S and the infinite places, such that

(*) $\varepsilon_{E/F}(x) = \prod_{v \notin T} \pi_v^{\mathrm{ord}_v(x_v)}$ for all $x = (x_v)$ in $\mathcal{I}_F^T$.

Proof. Let T be any finite set of places of F, containing the infinite places, and let W be any open subgroup of $\mathcal{I}_F$ containing the infinite places. Then the weak approximation theorem shows that $\mathcal{I}_F = F^\times W$. (see Tate's article).

Immediately implies uniqueness : (i) & (iii) show that (*) must hold on some open subgroup of $\mathcal{I}_F$ containing $\mathcal{I}_F^T$.

Existence. Take $W = \{(x_v) : \mathrm{ord}_v(x_v - 1) \geqslant \mathrm{ord}_v(\mathfrak{q})$ for all $v \mid \mathfrak{q}\}$. W is open. We define T to be the set consisting of all primes dividing $\mathfrak{q}$, together with the infinite primes. For $x \in W$, define $\varepsilon_{E/F}(x)$ by (*). For $x \in F^\times$, define $\varepsilon_{E/F}(x) = N_{F/K}(x)$. They agree on $W \cap F^\times$ by our previous theorem and so we can define $\varepsilon_{E/F}$ on the whole of $\mathcal{I}_F = F^\times W$.

Complex Grossencharacters

$x \in \mathcal{I}_F$, define $x_\infty \in \mathcal{I}_F$ to be the idèle with the same components as x at the infinite places, and 1's elsewhere. Obviously $N_{F/K}(x_\infty^{-1}) \in (K \otimes \mathbb{R})^\times = K_\infty^\times$

<u>Defn</u>. Define $\eta_{E/F,\infty} : \mathcal{I}_F \longrightarrow K_\infty^\times$ by

$$\eta_{E/F,\infty}(x) = \varepsilon_{E/F}(x)\, N_{F/K}(x_\infty^{-1}).$$

<u>Clear</u>: $\eta_{E/F,\infty}$ is continuous and $\eta_{E/F,\infty}(F^\times) = 1$

Now $K_\infty^\times \xrightarrow{\sim} \mathbb{C}^\times$. Let us fix some isomorphism $i_\infty : K_\infty^\times \xrightarrow{\sim} \mathbb{C}^\times$. A second isomorphism is given by composi with complex conjugati

<u>Defn</u>. $\rho_{E/F,\infty} : \mathcal{I}_F \longrightarrow \mathbb{C}^\times$ by $\rho_{E/F,\infty}(x) = i_\infty \circ \eta_{E/F,\infty}(x)$

This is a <u>grossencharacter</u> in the sense of Hecke, i.e. we have $\rho_{E/F,\infty}$ is continuous and $\rho_{E/F,\infty}(F^\times) = 1$. We can also compose it with complex conjugation on $\mathbb{C}$, to get $\overline{\rho_{E/F,\infty}}$ defined by $\overline{\rho_{E/F,\infty}}(x) = \overline{\rho_{E/F,\infty}(x)}$.

<u>Ramified primes</u>. Let v be any finite place of F. We have

$$U_{F_v} \hookrightarrow F_v^\times \quad \text{where } U_{F_v} = \text{group of units of } \mathcal{O}_{F_v}.$$

We can embed $F_v^\times \hookrightarrow \mathcal{I}_v$ by mapping $a \mapsto (1,\dots,1,\underset{v\text{-th place}}{a},1,\dots)$

<u>Defn</u>. We say $\rho_{E/F,\infty}$ is <u>unramified</u> at v if

$\rho_{E/F,\infty}(U_{F_v}) = 1$.

<u>Defn</u>. If $\rho_{E/F,\infty}$ is unramified at v, we can define

$$\rho_{E/F,\infty}(v) = \rho_{E/F,\infty}(\lambda_v),$$

where λ_v is any local parameter at v.

We then follow Hecke in defining:-

<u>Defn</u>. $$L(\rho_{E/F,\infty}, s) = \prod_{v \text{ unramified}} \left(1 - \frac{\rho_{E/F,\infty}(v)}{(Nv)^s}\right)^{-1}.$$

Hecke - Tate: we know the analytic continuation and functional equation for this L-function.

T - finite set of primes occurring in earlier theorem. If $v \notin T$, it is clear that $\rho_{E/F,\infty}$ is unramified at v. Moreover

<u>Lemma</u>. $$\rho_{E/F,\infty}(v) = \pi_v.$$

But we know that $\pi_v + \overline{\pi_v} = Nv + 1 - \#(\tilde{E}_v(k_v))$, $Nv = \pi_v \cdot \overline{\pi_v}$.

<u>Corollary</u>. For $v \notin T$, we have

$$\left(1 - \frac{\rho_{E/F,\infty}(v)}{(Nv)^s}\right)\left(1 - \frac{\overline{\rho_{E/F,\infty}(v)}}{(Nv)^s}\right)$$

$$= \left(1 - (\pi_v + \overline{\pi_v})(Nv)^{-s} + (Nv)^{1-2s}\right)$$

RHS is the E-factor at v of complex L-function of E/F

<u>L7</u>. E/K, $K = \mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, $K \hookrightarrow F$, $K \hookrightarrow \mathbb{C}$.

$\rho_{E/F,\infty} : \mathcal{J}_F \longrightarrow \mathbb{C}^\times$

$$\rho_{E/F,\infty}(x) = \varepsilon_{E/F}(x)\, N_{F/K}(x_\infty^{-1}).$$

Recall that

$$L(E/F, s) = \prod_{v \notin S} \left(1 - (\pi_v + \overline{\pi}_v)(Nv)^{-s} + (Nv)^{1-2s}\right)^{-1}.$$

Last time we saw that, up to a finite number of factors, this coincided with $L(\rho_{E/F,\infty}, s)\, L(\overline{\rho_{E/F,\infty}}, s)$.

<u>Key Question</u>. What are the ramified primes for $\rho_{E/F,\infty}$?

<u>Recall</u>. v a finite place of F, $F_v^\times \hookrightarrow \mathcal{J}_F$. We say $\rho_{E/F,\infty}$ is unramified at v if $\rho_{E/F,\infty}(U_v) = 1$, where U_v is the group of units of $\mathcal{O}_{F_v}$.

<u>Theorem</u> (Deuring). $\rho_{E/F,\infty}$ is unramified at v $\iff$ E has good reduction at v.

<u>Corollary</u>. $L(E/F, s) = L(\rho_{E/F,\infty}, s)\, L(\overline{\rho_{E/F,\infty}}, s)$.

<u>How do we prove this theorem</u>. I_v = inertial subgroup of $G_v = \mathrm{Gal}(\overline{F_v}/F_v)$. ℓ a prime number.

$$\rho_\ell : G_F \longrightarrow \mathrm{Aut}(V_\ell(E)) \qquad (\ell \text{ - a prime number}).$$

<u>Criterion</u> (Néron - Ogg - Shafarevich). Let v be any finite place of F, and let ℓ be any prime number distinct from the characteristic of k_v. Then

E has good reduction at $v \iff \rho_\ell(I_v) = 1$, where I_v is the inertial subgroup of v in G_F.

Remarkable criterion which we just accept (see Silverman). It is true whether or not E has complex multiplication.

<u>Return now</u> to our curve E/F with $\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$.
We have $V_\ell(E)$ is free of rank 1 over $K_\ell = K \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$.
Hence $\mathrm{Aut}(V_\ell(E)) = K_\ell^\times$ & $\rho_\ell(G_F)$ is abelian.
In other words, ρ_ℓ factors through

$$G_F^{ab} = \mathrm{Gal}(F^{ab}/F),$$

where F^{ab} is the maximal abelian extension of F.
Hence, in this situation, we can regard

$$\rho_\ell : G_F^{ab} \longrightarrow K_\ell^\times.$$

But now we invoke the full force of global class field theory, which tells us that we have a canonical surjection

$$\xi_F : \mathcal{J}_F \longrightarrow G_F^{ab}.$$

Recall also that $F_v^\times \hookrightarrow \mathcal{J}_F$, and let U_v be the group of units of $\mathcal{O}_{F_v}$.

<u>Fact</u> : $\xi_F(U_v) = I_v^{ab}$ = inertia subgroup of v in G_F^{ab}.

<u>Defn</u>. $\eta_{E/F,\ell} : \mathcal{J}_F \longrightarrow (K \otimes \mathbb{Q}_\ell)^\times = K_\ell^\times$ by $\eta_{E/F,\ell} = p_\ell \circ \xi_F$.

Putting this together with the criterion of Neron-Ogg-Shafarevi we obtain

<u>Proposition</u>. Let v be a finite place of F, and ℓ a prime distinct from the residue characteristic of k_v. Then E has good reduction at v iff $\eta_{E/F,\ell}(U_v) = 1$.

What is the connexion with the homomorphism $\varepsilon_{E/F} : \mathcal{J}_F \longrightarrow K^\times$. Let x_ℓ be the component of $x \in \mathcal{J}_F$ lying inside $K_\ell^\times \hookrightarrow \mathcal{J}_F$ (same components as x for $v \mid \ell$, 1 elsewhere)

<u>Theorem</u>. For all $x \in \mathcal{J}_F$, we have

$$(*) \quad \eta_{E/F,\ell}(x) = \varepsilon_{E/F}(x)\, N_{F/K}(x_\ell)^{-1}.$$

<u>Note</u> analogy with $\eta_{E/F,\infty}(x) = \varepsilon_{E/F}(x) \cdot N_{F/K}(x_\infty)^{-1}$.

Granted this, the next corollary is immediate:-

<u>Corollary</u>. Let v be a finite place of F, and ℓ a prime distinct from the characteristic of k_v. Then E has good reduction at $v \iff \varepsilon_{E/F}(U_v) = 1$.

Corollary follows from criterion of Neron - Ogg - Shafarevich since local class field theory shows that

$$\eta_{E/F,\ell}(U_v) = \rho_\ell(I_v^{ab}) = \varepsilon_{E/F}(U_v)$$

by the theorem.

<u>Proof of Theorem</u>.

Both maps are continuous, and so it suffices to show they coincide on dense subset of $\mathcal{I}_F$.

Let $T = \{v : \mathrm{ord}_v(\mathfrak{g}) > 0\}$ in the earlier theorem proving $\varepsilon_{E/F}$ exists.

Define $T' = T \cup \{v : v | \ell\}$.

<u>Fact</u>. $F^\times \mathcal{I}_F^{T'}$ is dense in $\mathcal{I}_F$.

Now right and left hand side of $(*)$ coincide on $F^\times$, since $\varepsilon_{E/F}(\alpha) = N_{F/K}\alpha = N_{F/K}((\alpha)_\ell)$ for $\alpha \in F^\times$.

We now show that both coincide on $\mathcal{I}_F^{T'}$.

Pick $v \notin T'$ a finite place. Let τ_v be a local parameter at v. Then $\varepsilon_{E/F}(\tau_v) = \pi_v$ by Serre-Tate theorem. Also $N_{F/K}((\tau_v)_\ell) = 1$ because $v \nmid \ell$. Hence right hand side of $(*)$ is π_v when evaluated at τ_v. What about left hand side of $(*)$.

<u>Fact</u> : $V_\ell(E) \xrightarrow{\sim} V_\ell(\tilde{E}_v)$ since $v \nmid \ell$ and E has good reduction.

<u>Fact</u> : $\eta_{E/F,\ell}(\tau_v)$ is the element of $K_\ell^\times$ which reduces mod v to the Frobenius endomorphism of $\tilde{E}_v/k_v$.

Thus $\eta_{E/F,\ell}(\tau_v) = \pi_v$ q.e.d.

28.

<u>Example</u>: $E : y^2 = x^3 - x$, $F = K = \mathbb{Q}(i)$

$S = \{\mathfrak{p}_2\}$, $\mathfrak{p}_2 = (1+i)$, $\mathfrak{f}$ = conductor of $\psi_{E/K}$

(return now to the ideal theoretic viewpoint).

$\mathfrak{f} = \mathfrak{p}_2^a$ for some $a \geq 1$.

<u>Note</u>: if $\alpha \equiv 1 \bmod \mathfrak{f} \Rightarrow \psi_{E/K}((\alpha)) = \alpha$.

Hence we must have $a \geq 3$ since $-1 \equiv 1 \bmod \mathfrak{p}_2^2$.

In fact: $a = 3$. Two ways of seeing this (apply Tate's algorithm, or use knowledge of conductor over $\mathbb{Q}$).

<u>Applications</u>:

1. Conductor of E/F.

<u>Theorem</u>. The conductor of E/F is the square of the conductor of $\psi_{E/F}$.

See Serre - Tate for the proof.

2. <u>Good reduction everywhere</u>.

<u>Theorem</u>. Let p be a prime number satisfying:-

(i) $(p, [\mathcal{O}_K : \mathrm{End}_F(E)]) = 1$, (ii) $p > 2$, (iii) $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, $\mathfrak{p} \neq \mathfrak{p}^*$,

and (iv). E has good reduction at all primes of F above p.

Then E has good reduction everywhere over $F(E_{\mathfrak{p}})$.

<u>Defn</u>: $E_{\mathfrak{a}} = \bigcap_{\substack{\lambda \in \mathfrak{a} \\ \lambda \neq 0}} E_\lambda$, where $\mathfrak{a}$ is any ideal in $\mathrm{End}_F(E)$

We will need the following

<u>Lemma</u>. Assume F'/F is a finite extension. Then

$$\varepsilon_{E/F'} = \varepsilon_{E/F} \circ N_{F'/F}.$$

<u>Proof</u>. We show that the right hand side has the desired properties.

(i) $\alpha' \in F'$: $\quad \varepsilon_{E/F}\left(N_{F'/F}\alpha\right) = N_{F/K}\left(N_{F'/F}\alpha\right) = N_{F'/K}\alpha.$

(ii). T' – primes of F above T together with primes of F' which are ramified in F'/F.

$$\begin{array}{ccc} F' & w & k_w \\ | & | & | \\ F & v & k_v \end{array} \qquad w \notin T', \ \tau_w = \text{local par. at } w.$$

We we have $\varphi_w = \varphi_v^{[k_w : k_v]} \implies \pi_w(E/F') = \pi_v(E/F)^{[k_w : k_v]}$.

$$\varepsilon_{E/F} \circ N_{F'/F}(\tau_w) = \varepsilon_{E/F}\left(N_{F_w'/F_v}\tau_w\right) = \pi_v^{\operatorname{ord}_v\left(N_{F_w'/F_v}\tau_w\right)}.$$

But, as w/v is unramified, we have $\operatorname{ord}_v\left(N_{F_w'/F_v}\tau_w\right) = [k_w : k_v]$

Hence RHS is $\pi_v^{[k_w : k_v]} = \pi_w$ q.e.d.

<u>Proof of Theorem</u>. Put $F' = F(E_{\mathfrak{p}})$

$$\varepsilon_{E/F'} : \mathcal{J}_{F'} \longrightarrow K^\times.$$

After criterion of earlier, it suffices to show that, for each place w of F', we have

<u>Eg</u>

Assume $\left(p, \left[\mathcal{O}_K : \mathrm{End}_F(E)\right]\right) = 1 \Rightarrow$

$$\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p .$$

Assume that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, with $\mathfrak{p} \neq \mathfrak{p}^*$. Then

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p \times \mathbb{Z}_p \quad (\text{corresponding to } \mathcal{O}_K \hookrightarrow \mathbb{Z}_p)$$

Hence our Galois representation

$$\rho_p : G_F \longrightarrow \mathrm{Aut}(V_p(E))$$

has values in $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$. Suppose first factor corresponds to the embedding $\mathcal{O}_K \hookrightarrow \mathbb{Z}_p$ inducing $\mathfrak{p}$.

<u>Defn</u>: $\rho_{\mathfrak{p}} : G_F \longrightarrow \mathbb{Z}_p^\times$ is given by $pr_{\mathfrak{p}} \circ \rho_p$.

<u>Defn</u>. $E_{\mathfrak{p}^\infty} = \bigcup_{n \geq 1} E_{\mathfrak{p}^n}$

<u>Fact</u>: $\rho_{\mathfrak{p}}$ is the character giving the action of G_F on $E_{\mathfrak{p}^\infty}$.

Take $F' = F(E_{\mathfrak{p}})$. Then $\sigma \in G_F$ fixes $E_{\mathfrak{p}}$ and so fixes $F' \Longleftrightarrow \rho_{\mathfrak{p}}(\sigma) \equiv 1 \bmod \mathfrak{p}$

(because $\sigma \longmapsto \rho_{\mathfrak{p}} \bmod \mathfrak{p}$ is character giving action on $E_{\mathfrak{p}}$)

We now switch to idèles, using the map

$$\xi_F : \mathcal{I}_F \longrightarrow G_F^{ab}.$$

<u>Defn</u> : $\eta_{E/F,\wp} = \xi_F \circ \rho_\wp \quad : \mathcal{I}_F \longrightarrow \mathbb{Z}_p^\times$

$\Theta_\wp = \xi_F \circ (\rho_\wp \bmod \wp) \quad : \mathcal{I}_F \longrightarrow \mathbb{F}_p^\times$.

<u>Note</u> : $\eta_{E/F,\wp}$ is the map $\eta_{E/F,p}$ composed with the $\wp$-projection on $\mathbb{Z}_p^\times$.

<u>Remark</u>. Ker $\Theta_\wp$ is the subgroup of $\mathcal{I}_F$ corresponding to the abelian extension $F'/F \Longleftrightarrow$

$$\operatorname{Ker} \Theta_\wp = F^\times N_{F'/F} \mathcal{I}_{F'}.$$

<u>Key Lemma</u>. Let v be any place of F not dividing p. Then, if $x \in U_v \cap \operatorname{Ker} \Theta_\wp$, $\varepsilon_{E/F}(x) = 1$.

<u>Corollary</u>. Let w be any place of F not dividing p. Then $\varepsilon_{E'/F'}(U_w) = 1$ and hence E has good reduction at w

<u>Proof of Corollary</u>. $\varepsilon_{E/F'}(U_w) = \varepsilon_{E/F}(N_{F'_w/F_v} U_w) = 1$, as $N_{F'_w/F_w} U_w \in U_v \cap \operatorname{Ker} \Theta_\wp$.

<u>Proof of Key Lemma</u>.

Note that $\xi_F(U_v) = I_v^{ab}$ by local class field theory & its link with global class field theory.

Now E has potential good reduction at v.

Since $v \nmid p$, the criterion of Néron - Ogg - Shafarevich

$\Longrightarrow \rho_p(I_v^{ab})$ finite $\Longrightarrow \eta_{E/F,p}(U_v)$ finite $\Longrightarrow \eta_{E/F,\wp}(U_v)$

Since $v \nmid \mathfrak{p}$, we have $\eta_{E/F,\mathfrak{p}}(U_v) = \varepsilon_{E/F}(U_v)$.

Suppose now that $x \in U_v \cap \operatorname{Ker} \Theta_{\mathfrak{p}}$.

<u>Claim</u>. $\eta_{E/F,\mathfrak{p}}(x) = 1$.

Since $x \in \operatorname{Ker} \Theta_{\mathfrak{p}}$, $\eta_{E/F,\mathfrak{p}}(x) \equiv 1 \bmod \mathfrak{p} \Rightarrow$ it must be a p-power root of unity in K. But this is impossible since $p > 2$ and $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, unless it is 1. Hence the claim.

This completes the proof.

<u>Example</u>. $E : y^2 = x^3 - x$, $F = K = \mathbb{Q}(i)$.

$p = 5$, $5 = (1+2i)(1-2i)$, $F' = K(E_{1+2i}) = K(\sqrt[4]{1-2i})$.

E/F' has good reduction everywhere. Above 2 :—

$$x = \frac{1-2iX}{(1-2i)^{1/2}}, \quad y = \frac{1+i}{(1-2i)^{3/4}}\left(1-(1-i)X+2Y\right).$$

<u>Ray class fields of K</u>.

Important abelian extensions of K.

$\mathfrak{g}$ - an integral ideal of K.

<u>Assumption</u>. If ζ in μ_K satisfies $\zeta \equiv 1 \bmod \mathfrak{g}$, then $\zeta = 1$.

$R_{\mathfrak{g}}$ - ray class field mod $\mathfrak{g}$.

It is a certain abelian extension of K.

K

$$0 \to (\mathcal{O}_K/\mathfrak{g})^\times \to \operatorname{Gal}(R_{\mathfrak{g}}/K) \to C_K \to 0$$

C_K = ideal class group of K.

<u>210</u>. Classical theory of complex multiplication explains how we can explicitly construct the ray class field of K mod $\mathfrak{g}$.

Pick <u>any</u> E/F, $\mathrm{End}_F(E) \xrightarrow{\sim} \mathcal{O}_K$, F/K finite

<u>Fact</u>. $R_{\mathfrak{g}} \subset F(E_F)$ (essentially field generated by the x-coordinate of a primitive F-division point).

Now return to our special case when $F = K$, and we have E/K with $\mathrm{End}_K(E) = \mathcal{O}_K$.

$\psi_{E/K} : I_S \longrightarrow K^\times$ – Grossencharacter of E/K.

<u>Defn</u>: $\mathfrak{f}$ = conductor of $\psi_{E/K}$.

We have proven that the prime factors of $\mathfrak{f}$ are precisely the elements of S = set of bad primes for E/K.

<u>Theorem</u>. Let $\mathfrak{g}$ be any integral ideal of K such that $\mathfrak{f}$ = conductor of $\psi_{E/K}$, divides $\mathfrak{g}$. Then $R_{\mathfrak{g}} = K(E_{\mathfrak{g}})$. In particular, $[K(E_{\mathfrak{g}}) : K] = \#(\mathcal{O}_K/\mathfrak{g})^\times / \#(\mu_K)$.

<u>Ex</u>. $E : y^2 = x^3 - x$, $K = \mathbb{Q}(i)$, $\mathfrak{f} = \mathfrak{p}_2^3$.

$\#\left(\left(\mathbb{Z}[i]/\mathfrak{p}_2^3\right)^\times\right) = 4$, $\#(\mu_K) = 4$

$\Rightarrow K(E_{\mathfrak{p}_2^3}) = K$, i.e. $\mathfrak{p}_2^3$-division points are rational over K.

<u>Ex</u>. $E : y^2 + xy = x^3 - x^2 - 2x - 1$, $K = \mathbb{Q}(\sqrt{-7})$

$N_{E/\mathbb{Q}} = 49 \Rightarrow F = (\sqrt{-7})$.

$\mathcal{O}/F)^\times$ has order 6, and μ_K has order 2.

Hence $[K(E_F) : K] = 3$, not 6!

<u>Ex</u>: $y^2 = x^3 - Dx$, $D \in \mathbb{Z}$ fourth power free. Δ = product of primes dividing D.
$F = \mathfrak{p}_2^3 \cdot \Delta\, \mathbb{Z}[i]$ when $D \equiv 1 \bmod 4$, $F = \mathfrak{p}_2^4 \Delta\, \mathbb{Z}[i]$ when $D \not\equiv 1 \bmod 4$.

<u>Proof of Theorem</u>. We have the tower of fields

$$K(E_{\mathfrak{g}}) \supset R_{\mathfrak{g}} \supset K.$$

All three are abelian extensions of K, unramified outside set of primes dividing $\mathfrak{g}$ (since every prime in S divides $\mathfrak{g}$). We invoke global class field theory. We must show that every $\sigma \in \mathrm{Gal}(K(E_{\mathfrak{g}})/K)$ that fixes $R_{\mathfrak{g}}$ (also fixes $K(E_F)$) by Galois theory. Now we know that, by the surjectivity of the Artin map, we have

$$\sigma = (\mathfrak{a}, K(E_{\mathfrak{g}})/K)$$

for some integral ideal $\mathfrak{a}$ of K prime to $\mathfrak{g}$.

<u>Fact</u>: $\sigma(P) = \psi_E(\mathfrak{a})(P)$ for all P in $E_{\mathfrak{g}}$.

Now assume σ fixes $R_{\mathfrak{g}}$. Hence $\mathfrak{a} = (\alpha)$ with $\alpha \equiv 1 \bmod \mathfrak{g}$. But

$$\psi_E(\mathfrak{a}) = \alpha \quad \text{because } \alpha \equiv 1 \bmod F \text{ since } F \mid \mathfrak{g}.$$

Hence

$$\sigma(P) = \alpha(P) = P \text{ since } \alpha \equiv 1 \bmod \mathfrak{g}.$$

q.e.d.

Final fact.

Theorem. Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\mathbb{Q}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$ an imaginary quadratic field. Let F be the conductor of $\psi_{E/K}$. Then $N(E/\mathbb{Q})$ (= conductor of $E/\mathbb{Q}$) $= (N_{K/\mathbb{Q}} F) . d_K$, where d_K is the absolute value of the discriminant of K over $\mathbb{Q}$.

L-functions.

These are the objects which are mysteriously linked to $E(F)$ and $Ш(E/F)$ conjecturally via the conjecture of Birch and Swinnerton-Dyer.

Complex L-functions. E/F, $\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$, an imaginary quadratic field. $K \hookrightarrow \mathbb{C}$

Hecke proved the analytic continuation of $L(\psi_{E/F}, s)$ and $L(\overline{\psi}_{E/F}, s)$, and hence also $L(E/F, s)$.

Tate gave a very beautiful adelic proof, which was then vastly generalized to the automorphic theory - Russian school + Jacquet Langlands.

We will only discuss the special case $F = K$, where in fact the analytic continuation goes back to Eisenstein and Kronecker - and it works for the p-adic theory.

Eisenstein - Kronecker series

L - any lattice in complex plane

$z, s \in \mathbb{C}$, k an integer ≥ 1.

<u>Defn</u>. $$H_k(z, s, L) = \sum_{\omega \in L}^{*} \frac{(\bar{z} + \bar{\omega})^k}{|z + \omega|^{2s}} \qquad R(s) > 1 + \frac{k}{2}.$$

Here $\sum^*$ means sum over all $\omega \in L$ except $-z$ if $z \in L$.

<u>Theorem</u>. $\Gamma(s) H_k(z, s, L)$ has a holomorphic continuation over the whole complex plane, and satisfies a functional equation.

See Weil: Chapter VIII, §14 - but his functional equation seems to be wrong! ((32) cannot be right if $x_0 = 0$!)
Kronecker - his work must have inspired Hecke.
We shall use our own analytic continuation, due essentially to Eisenstein.

Suppose we are now given our E/K, $\mathrm{End}_K(E) = \mathcal{O}_K$, $K \hookrightarrow \mathbb{C}$.
write ψ_E for $\psi_{E/K}$ since K is now fixed.

$\psi_E^n \quad (n = 1, 2, \ldots) : I_S \longrightarrow K^\times$

<u>But</u> the conductor of ψ_E^n may be a proper divisor of conductor F of ψ_E.

<u>Defn</u>. $$L_F(\psi_E^n, s) = \prod_{(\mathfrak{v}, F) = 1} \left(1 - \frac{\psi_E^n(\mathfrak{v})}{(N\mathfrak{v})^s}\right)^{-1}, \text{ similarly } L_F(\bar{\psi}_E^n,$$

This may be an imprimitive L-function. Note

$$L_F(\overline{\psi}_E^{\,n}, s) = \sum_{(\mathfrak{a},F)=1} \frac{\overline{\psi}_E^{\,n}(\mathfrak{a})}{(N\mathfrak{a})^s}.$$

How do we express this in terms of the Kronecker-Eisenstein function?

Pick a generator for F, say $F = f\mathcal{O}_K$.
We have fixed a global minimal ~~eq~~ Weierstrass equation for E over $\mathcal{O}_K$:-

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_i \in \mathcal{O}_K)$$

We let $\mathcal{L}$ = period lattice of the Néron differential

$$\omega = \frac{dx}{2y + a_1 x + a_3}.$$

$\mathcal{L}$ is an $\mathcal{O}_K$-module of rank 1, which must be free. Hence we can find Ω_∞ in $\mathcal{L}$ such that $\mathcal{L} = \Omega_\infty \mathcal{O}_K$, since $\mathcal{O}_K$ is principal. Here Ω_∞ is uniquely determined up to multiplication by a root of unity in K. We have the associated Weierstrass map

$$\Phi(z, \mathcal{L}) : \mathbb{C}/\mathcal{L} \xrightarrow{\sim} E(\mathbb{C})$$

given by

$$\Phi(z,\mathcal{L}) = \left(\wp(z,\mathcal{L}) - \frac{a_1^2+4a_2}{12}, \frac{1}{2}\left(\wp'(z,\mathcal{L}) - \cancel{\frac{a_1^2+4a_2}{12}}\right.\right.$$
$$\left.\left. - a_1\left(\wp(z,\mathcal{L}) - \frac{a_1^2+4a_2}{12}\right) - a_3\right)\right).$$

<u>Choice of a primitive $\mathfrak{f}$-division point</u>. We could choose any primitive $\mathfrak{f}$-division point on E, but the notation is lightest if we choose:–

<u>Defn</u>. $\varphi = \Phi\left(\frac{\Omega_\infty}{\mathfrak{f}}, \mathcal{L}\right)$.

We shall now establish:–

~~Theorem~~

<u>Defn</u>. $\mathcal{B}$ = set of integral ideals of K, prime to $\mathfrak{f}$, such that

$$\mathrm{Gal}\left(K(E_{\mathfrak{f}})/K\right) = \left\{\sigma_{\mathfrak{r}} : \mathfrak{r} \in \mathcal{B}\right\},$$

where $\sigma_{\mathfrak{r}} = \left(\mathfrak{r}, K(E_{\mathfrak{f}})/K\right)$ is the Artin symbol of $\mathfrak{r}$.

<u>Theorem</u>. For all integers $n \geqslant 1$, we have

$$L_{\mathfrak{f}}\left(\overline{\psi}_E^{\,n}, s\right) = \frac{|\Omega_\infty/\mathfrak{f}|^{2s}}{\left(\frac{\pi}{\Omega_\infty/\mathfrak{f}}\right)^n} \sum_{\mathfrak{r} \in \mathcal{B}} H_n\left(\psi_E(\mathfrak{r})\frac{\Omega_\infty}{\mathfrak{f}}, s, \mathcal{L}\right).$$

<u>Proof</u>. We have

$$L_{\mathfrak{f}}\left(\overline{\psi}_E^{\,n}, s\right) = \sum_{(\mathfrak{a}, \mathfrak{f})=1} \frac{\overline{\psi}_E^{\,n}(\mathfrak{a})}{(N\mathfrak{a})^s}.$$

$$\left.\begin{array}{c} K(E_{\mathfrak{f}}) = R_{\mathfrak{f}} \\ | \\ K \end{array}\right) \quad \text{Galois group isomorphic to } (\mathcal{O}/\mathfrak{f})^\times / \widetilde{\mu}_K.$$

<u>Key Observation</u>. As $\mathfrak{r}$ runs over $\mathcal{B}$ and c runs over $\mathfrak{f}$, the ideals $(\psi_E(\mathfrak{r})+c)$ run over all integral ideals of K, prime to $\mathfrak{f}$, precisely once.

<u>Note</u> $\{\psi_E(\mathfrak{r})\}_{\mathfrak{r}\in\mathcal{B}}$ are a set of representatives of $(\mathcal{O}/\mathfrak{f})^\times/\tilde{\mu}_K$.

Hence

$$L_{\mathfrak{f}}(\overline{\psi}_E^{\,n}, s) = \sum_{\mathfrak{r}\in\mathcal{B}}\sum_{c\in\mathfrak{f}} \frac{\overline{\psi}_E^{\,n}\left((\psi_E(\mathfrak{r})+c)\right)}{|\psi_E(\mathfrak{r})+c|^{2s}}$$

$$(\psi_E(\mathfrak{r})+c) = (\psi_E(\mathfrak{r}))\left(1+\frac{c}{\psi_E(\mathfrak{r})}\right) = \mathfrak{r}\left(1+\frac{c}{\psi_E(\mathfrak{r})}\right).$$

But $1+\dfrac{c}{\psi_E(\mathfrak{r})} \equiv 1^\times \bmod \mathfrak{f}$ since $c\in\mathfrak{f}$.

Hence

$$\overline{\psi}_E^{\,n}\left((\psi_E(\mathfrak{r})+c)\right) = \overline{\psi}_E^{\,n}(\mathfrak{r})\overline{\left(1+\frac{c}{\psi_E(\mathfrak{r})}\right)}^{\,n} = \overline{(\psi_E(\mathfrak{r})+c)}^{\,n}.$$

Thus

$$L_{\mathfrak{f}}(\overline{\psi}_E^{\,n}, s) = \sum_{\mathfrak{r}\in\mathcal{B}}\sum_{c\in\mathfrak{f}} \frac{\overline{(\psi_E(\mathfrak{r})+c)}^{\,n}}{|\psi_E(\mathfrak{r})+c|^{2s}}$$

$$= \frac{|\Omega_\infty/\mathfrak{f}|^{2s}}{\left(\overline{\Omega_\infty/\mathfrak{f}}\right)^n}\sum_{\mathfrak{r}\in\mathcal{B}}\sum_{c\in\mathfrak{f}} \frac{\overline{\left(\frac{\psi_E(\mathfrak{r})\Omega_\infty}{\mathfrak{f}}+\frac{c\Omega_\infty}{\mathfrak{f}}\right)}^{\,n}}{\left|\frac{\psi_E(\mathfrak{r})\Omega_\infty}{\mathfrak{f}}+\frac{c\Omega_\infty}{\mathfrak{f}}\right|^{2s}}$$

$\mathcal{L} = \Omega_\infty \mathcal{O}_K \Rightarrow c\,\frac{\Omega_\infty}{f}$ runs over $\mathcal{L}$ as c runs over $F = (f)$

$$= \frac{|\Omega_\infty / f|^{2s}}{\overline{(\Omega_\infty / f)}^{\,n}} \sum_{\nu \in \mathcal{B}} H_n\left(\frac{\psi_E(\nu)\Omega_\infty}{f}, s, \mathcal{L}\right).$$

We can immediately draw some important consequences.

<u>Case $n \geqslant 3$</u>. $\Rightarrow n > 1 + \frac{n}{2} \Rightarrow$ RHS converges and

$$H_n(z, n, \mathcal{L}) = \sum_{\omega \in \mathcal{L}} \frac{1}{(z+\omega)^n} = \frac{(-1)^n}{(n-1)!}\wp^{(n-2)}(z, \mathcal{L})$$

where $\wp(z, \mathcal{L})$ is the Weierstrass $\wp$-function of $\mathcal{L}$.

<u>Also</u>: $$\wp'\left(\frac{\psi_E(\nu)}{f}\Omega_\infty, \mathcal{L}\right) = \wp\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)^{\sigma_\nu}$$

$$\wp'\left(\frac{\psi_E(\nu)}{f}\Omega_\infty, \mathcal{L}\right) = \wp'\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)^{\sigma_\nu}.$$

Hence we have proven :-

<u>Theorem</u>. Assume $n \geqslant 3$. Then

$$L_F(\overline{\psi}_E^{\,n}, n) = \left(\frac{\Omega_\infty}{f}\right)^n \frac{(-1)^n}{(n-1)!}\, T_{r_{K(E_F)/K}}\left(\wp^{(n-2)}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right).$$

Also $L_F(\overline{\psi}_E^{\,n}, n) \neq 0$ when $n \geqslant 3$ (since the Euler product converges). It is not at all obvious when you look at RHS!

<u>§12</u> E/K, $\mathrm{End}_K(E) = \mathcal{O}_K$, $K \hookrightarrow \mathbb{C}$, ψ_E, $\mathcal{L} = \Omega_\infty \mathcal{O}_K$.

$\mathfrak{f}$ = conductor of ψ_E; $\mathfrak{f} = (f)$.

<u>Last time</u>. For $n \geqslant 3$, define

$$E_n^*(z, \mathcal{L}) = \sum_{\omega \in \mathcal{L}} \frac{1}{(z+\omega)^n} = \frac{(-1)^n}{(n-1)!} \wp^{(n-2)}(z, \mathcal{L}).$$

Here

$$\wp(z, \mathcal{L}) = \frac{1}{z^2} + \sum_{\substack{\omega \in \mathcal{L} \\ \omega \neq 0}} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$$

is the Weierstrass $\wp$-function of $\mathcal{L}$.

<u>Theorem</u>. $$L_{\mathfrak{f}}(\overline{\psi}_E^{\,n}, n) = \left(\frac{\Omega_\infty}{f}\right)^n \cdot \cancel{\frac{(-1)^n}{(n-1)!}} \, T_{K(E_{\mathfrak{f}})/K}\left(E_n^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right)$$

$(n \geqslant 3)$.

What about the all important cases $n = 1$ and 2?

<u>Defn</u>. $E_n^*(z, \mathcal{L}) = H_n(z, n, \mathcal{L})$ for all $n \geqslant 1$.

Makes perfectly good sense if you accept the analytic continuation of $\Gamma(s) H_n(z, s, \mathcal{L})$ (for $n = 1, 2$, we have $n \leqslant 1 + \frac{n}{2}$).

<u>Goal</u>. To prove that $E_n^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) \in K(E_{\mathfrak{f}})$ for all $n \geqslant 1$, and that we still have

$$L_{\mathfrak{f}}(\overline{\psi}_E^{\,n}, n) = \left(\frac{\Omega_\infty}{f}\right)^n \cdot \cancel{\frac{(-1)^n}{(n-1)!}} \, T_{K(E_{\mathfrak{f}})/K}\left(E_n^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right)$$

for all $n \geqslant 1$.

We have to recall more about elliptic functions.

L - any lattice in $\mathbb{C}$.

<u>Defn</u>. $$\sigma(z, L) = z \prod_{\substack{\omega \in L \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right).$$

<u>Defn</u>. $$\zeta(z, L) = \frac{d}{dz} \log \sigma(z, L) = \frac{1}{z} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

<u>Defn</u> $$\wp(z, L) = -\frac{d}{dz} \zeta(z, L).$$

<u>Note</u>: No analogue of $\sigma(z, L)$ is known for higher dimensional abelian varieties.

We need two other invariants of L :-

<u>Defn</u> $$s_2(L) = \lim_{\substack{s \to 0 \\ s > 0}} \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-2} |\omega|^{-2s}.$$

<u>Defn</u>. Pick a basis u, v of L such that $\Im(v/u) > 0$

$$A(L) = \frac{\bar{u} v - \bar{v} u}{2\pi i} = \pi^{-1} \cdot \text{Area of } (L).$$

It depends only on L and is > 0.

<u>Theorem</u>. For $z \in \mathbb{C} \setminus L$, we have

$$E_1^*(z, L) = \zeta(z, L) - z\, s_2(L) - \bar{z}/A(L).$$

$$E_2^*(z, L) = \wp(z, L) + s_2(L).$$

<u>Remarks</u> (i). $E_1^*(z, L)$ is not a holomorphic function of z (it was first introduced by Eisenstein).

(ii). Arithmetic nature of $s_2(L)$ is not clear or known in general.

<u>Proof</u>.

<u>Defn</u>. $$\Phi(z, s, L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left\{ \frac{\bar{z} + \bar{\omega}}{|z+\omega|^{2s}} - \frac{\bar{\omega}}{|\omega|^{2s}} \left(1 - \frac{sz}{\omega} - \frac{(s-1)\bar{z}}{\bar{\omega}} \right) \right\}$$

This converges for $s \in \mathbb{R}$ & $s > \frac{1}{2}$; also any s with $R(s) > \frac{1}{2}$.

Now when $s > \frac{3}{2}$, we have the identity

$$\Phi(z, s, L) = H_1(z, s, L) + sz \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-2} |\omega|^{2-2s} + (s-1)\bar{z} \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^{2s}}.$$

Here we have used the fact that

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} |\omega|^{-2s} \cdot \bar{\omega} = 0.$$

But

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-2} |\omega|^{2-2s}, \left(\sum_{\omega \neq 0} \frac{1}{|\omega|^{2s}} \right)(s-1)$$

are both holomorphic for $R(s) \geq 1/2$. Hence we get the analytic continuation of $H_1(z, s, L)$ to region $R(s) > \frac{1}{2}$. Also we see immediately that

$$\Phi(z, 1, L) = S(z, L).$$

<u>Additional Facts</u>.

$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^{2s}}$ has a simple pole at $s=1$ with residue $A(L)^{-1}$.

The conclusion of the theorem is now clear.

<u>Corollary</u>. For all integers $n \geq 1$, we have

$$L_f(\overline{\psi}_E^{\,n}, n) = \left(\frac{\Omega_\infty}{f}\right)^n \cdot \sum_{\mathfrak{r} \in \mathcal{B}} E_n^*\left(\frac{\psi_E(\mathfrak{r})\Omega_\infty}{f}, \mathcal{L}\right).$$

But for $n = 1, 2$, it is in no way clear that $E_n^*\left(\frac{\psi_E(\mathfrak{r})\Omega_\infty}{f}, \mathcal{L}\right) \in K(E_f)$, let alone that the right hand side is the trace. We now prove that this is true, but it requires new ideas.

<u>First ingredient</u>. Θ-function, essentially σ-function.

<u>Defn</u>. Let $L \subset \mathbb{C}$ be any lattice. Then

$$\Theta(z, L) = \exp\left(-s_2(L)\frac{z^2}{2}\right)\sigma(z, L).$$

<u>Theorem</u>. For all $\rho \in \mathbb{C} \setminus L$, we have

$$(*) \quad \frac{d}{dz}\log\Theta(z+\rho, L) = \frac{\overline{\rho}}{A(L)} + \sum_{k=1}^{\infty}(-1)^{k-1} E_k^*(\rho, L) z^{k-1}.$$

<u>Proof</u> $\frac{d}{dz}\log\Theta(z+\rho, L) = -s_2(L)(z+\rho) + \zeta(z+\rho, L)$.

Use the above formula, and put $z=0$ to get constant term of $(*)$. One keeps on differentiating to get higher terms.

<u>§13</u>. How close is $\Theta(z, L)$ to being periodic with respect to L

<u>Theorem</u>. For $\omega \in L$, we have

$$\Theta(z+\omega, L) = \pm\, \Theta(z, L) \exp\left(\bar{\omega}\left(z+\frac{\omega}{2}\right) / A(L)\right)$$

where $+$ or $-$ occurs according as $\omega \in 2L$ & $\omega \notin 2L$.

<u>Corollary</u>: For all $\lambda \neq 0$ in $\mathrm{End}(\mathbb{C}/L)$, we have

$$\Theta^2(z, L)^{\lambda\bar{\lambda}} / \Theta^2(z, \lambda^{-1}L).$$

is periodic with respect to L.

<u>Proof</u>. Since $\zeta(z+\omega, L) - \zeta(z, L)$ has derivative 0, there exists a constant $\eta(\omega, L)$ such that

$$\eta(\omega, L) = \zeta(z+\omega, L) - \zeta(z, L).$$

Since $E_1^*(z+\omega, L) = E_1^*(z, L)$, we have

$$\eta(\omega, L) = \omega s_2(L) + \bar{\omega} / A(L).$$

We next note that we have

$$(*) \quad \frac{\sigma(z+\omega, L)}{\sigma(z, L)} = \pm \exp\left(\eta(\omega, L)\left(z+\frac{\omega}{2}\right)\right),$$

where the $\pm$ occurs according as $\omega \in 2L$ & $\omega \notin 2L$.

Indeed

$$\frac{d}{dz} \log\left(\frac{\sigma(z+\omega, L)}{\sigma(z, L)}\right) = \eta(\omega)$$

$$\Rightarrow \quad \frac{\sigma(z+\omega, L)}{\sigma(z, L)} = \exp\left(\eta(\omega, L) z + c(\omega)\right).$$

So what is $c(\omega)$?

We can rewrite this as

$$\frac{\sigma(z+\omega, L)}{\sigma(z, L)} = \psi(\omega)\exp\left(\eta(\omega, L)\left(z+\frac{\omega}{2}\right)\right)$$

Note also that $\sigma(z, L) = -\sigma(-z, L)$ (clear from product expression for $\sigma(z, L)$).

<u>Case 1</u>. $\omega \in 2L \Rightarrow \omega/2 \notin L \Rightarrow$ we can take $z = -\omega/2$.

$$\psi(\omega) = \sigma\left(\frac{\omega}{2}, L\right) \Big/ \sigma\left(-\frac{\omega}{2}, L\right) = -1.$$

<u>Case 2</u>.

$$\frac{\sigma(z+2\omega, L)}{\sigma(z, L)} = \frac{\sigma(z+2\omega, L)}{\sigma(z+\omega, L)} \cdot \frac{\sigma(z+\omega, L)}{\sigma(z, L)}.$$

We apply the equation twice and get

$$\psi(2\omega) = \psi(\omega)^2.$$

We keep dividing ω by 2 until it is not in L, and we easily deduce the above formula.

<u>Consequence</u>. $\theta^2(z, L)^{\lambda\bar{\lambda}} / \theta^2(z, \lambda^{-1}L)$ must be a rational function in $\wp(z, L)$ & $\wp'(z, L)$.

What is this rational function?

<u>Theorem</u>.

$$\theta^2(z, L)^{\lambda\bar{\lambda}} \Big/ \theta^2(z, \lambda^{-1}L) = \prod_{\substack{\alpha \in \frac{1}{\lambda}L/L \\ \alpha \neq 0}} \left(\wp(z, L) - \wp(\alpha, L)\right)^{-1}.$$

<u>Proof</u>. Both sides have same zeroes and poles, and constant term of z expansion is the same.

<u>Corollary</u>. We now return to our elliptic curve E/K with $\mathrm{End}_K(E) = \mathcal{O}_K$.

$$\Phi(z, \mathcal{L}) : \mathbb{C}/\mathcal{L} \xrightarrow{\sim} E(\mathbb{C}).$$

<u>Corollary</u>. Let $\mathfrak{g}$ be any integral ideal of K, and let $\rho \in \mathbb{C}$ such that $\Phi(\rho, \mathcal{L}) \in E_{\mathfrak{g}}$ & $\Phi(\rho, \mathcal{L})$ is non-zero in $E_{\mathfrak{g}}$. Then, for all $n \geq 1$,

$$E_n^*(\rho, \mathcal{L}) \in K(E_{\mathfrak{g}})$$

and, for all ideals $\mathfrak{r}$ of K, prime to $\mathfrak{g}$ and to S, we have

$$E_n^*(\rho, \mathcal{L})^{\sigma_{\mathfrak{r}}} = E_n^*(\psi_E(\mathfrak{r})\rho, \mathcal{L}),$$

where $\sigma_{\mathfrak{r}} = (\mathfrak{r}, K(E_{\mathfrak{g}})/K)$.

Put $\Theta_\lambda(z, \mathcal{L}) = \theta^2(z, \mathcal{L})^{\lambda\bar{\lambda}} / \theta^2(z, \lambda^{-1}\mathcal{L})$.

$\Theta_\lambda(z, \mathcal{L})$ is a rational function in $\wp(z, \mathcal{L})$ with coefficients in K.

$\Theta_\lambda(z+\rho, \mathcal{L})$ is a rational function in $\wp(z, \mathcal{L})$ & $\wp'(z, \mathcal{L})$ with coefficients in $K(E_{\mathfrak{g}})$. Hence the same is true for the coefficients of the z-expansion of $\Theta_\lambda(z+\rho, \mathcal{L})$.

and so also of the z-expansion of

$$\frac{d}{dz} \log \Theta_\lambda(z+\rho, \mathcal{L}) = 2 \sum_{k=1}^{\infty} a_k z^{k-1}$$

But these coefficients are given explicitly by

$$a_1 = \lambda\bar{\lambda}\left\{E_1^*(\rho,\mathcal{L}) + \bar{\rho}/A(\mathcal{L})\right\} - E_1^*(\rho,\lambda^{-1}\mathcal{L}) - \bar{\rho}\, A(\lambda^{-1}L)$$

$$a_k = (-1)^{k-1}\left\{\lambda\bar{\lambda}\, E_k^*(\rho,\mathcal{L}) - E_k^*(\rho,\lambda^{-1}\mathcal{L})\right\} \quad (k \geq 2).$$

But $E_k^*(\gamma z, \gamma L) = \gamma^{-k} E_k^*(z, L)$ for any $\gamma \in \mathbb{C}^\times$.
Hence we get finally :-

$$a_k = (-1)^{k-1}\left\{\lambda\bar{\lambda}\, E_k^*(\rho,\mathcal{L}) - \lambda^k E_k^*(\lambda\rho,\mathcal{L})\right\}$$

$(k = 1, 2, \ldots)$.

Now choose $\lambda \in \mathcal{O}_K \setminus \mathbb{Z}$ such that $\lambda \equiv 1 \bmod \mathfrak{q}$.
Then $E_k^*(\lambda\rho, \mathcal{L}) = E_k^*(\rho, \mathcal{L})$, and so

$$a_k = (-1)^{k-1}(\lambda\bar{\lambda} - \lambda^k)\, E_k^*(\rho, \mathcal{L}).$$

As $\lambda\bar{\lambda} - \lambda^k \neq 0$, it follows that $E_k^*(\rho, \mathcal{L}) \in K(E_{\mathfrak{q}})$
To get the last part, we simply note that

$$\Theta_\lambda(z+\rho, \mathcal{L})^{\sigma_\tau} = \Theta_\lambda(z + \psi_E(\tau)\rho, \mathcal{L}).$$

<u>Corollary</u>. $s_2(\mathcal{L}) \in K(E_{\mathfrak{q}})$ for all $\mathfrak{q} \neq 1$
$(\Rightarrow s_2(\mathcal{L}) \in K)$.

We have now proven our earlier formula :-

$$L_F(\overline{\psi}_E^{\,n}, n) = \left(\frac{\Omega_\infty}{f}\right)^n \mathrm{Trace}_{K(E_F)/K}\left(E_n^*\left(\psi_E(\mathfrak{b})\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right).$$

for all $n \geq 1$. But the seemingly strange proof turns out to be fundamental for the development of the p-adic theory.

<u>Defn</u>. Put $\mathfrak{B}$ as before.

$$\Theta_{\lambda,F}(z, \mathcal{L}) = \prod_{\mathfrak{b}\in\mathfrak{B}} \Theta_\lambda\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{f} + z, \mathcal{L}\right).$$

<u>Lemma</u>: $\Theta_{\lambda,F}(z, \mathcal{L})$ is a rational function in $\wp(z, \mathcal{L})$ and $\wp'(z, \mathcal{L})$ with coefficients in K, and does not depend on the particular choice of $\mathfrak{B}$.

<u>Theorem</u>. Assume $(\lambda, S) = 1$. Then, for all $n \geq 1$, we have

$$\left(\frac{d}{dz}\right)^n \log \Theta_{\lambda,F}(z, \mathcal{L})\Big|_{z=0} = 2\,(n-1)!\,(-1)^{n-1} f^n \Omega_\infty^{-n} \left(N\lambda - \psi_E((\lambda))^n\right) L_F(\overline{\psi}_E^{\,n}, n)$$

<u>Proof</u>. We compute $\frac{d}{dz}\log \Theta_\lambda\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{f} + z, \mathcal{L}\right)$. We have

$$\frac{d}{dz}\log \Theta_\lambda\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{f} + z, \mathcal{L}\right)$$

$$= \lambda\overline{\lambda}\cdot\frac{d}{dz}\log\Theta\left(z + \frac{\psi_E(\mathfrak{b})\Omega_\infty}{f}, \mathcal{L}\right) - \frac{d}{dz}\log\Theta\left(z + \frac{\psi_E(\mathfrak{b})\Omega_\infty}{f}, \lambda^{-1}\mathcal{L}\right).$$

We use the earlier expansion, noting that the terms involving $A(\mathcal{L})$ and $A(\lambda^{-1}\mathcal{L})$ cancel out. We obtain

$$= 2\sum_{k=1}^{\infty}(-1)^{k-1}z^{k-1}\left(N\lambda\, E_k^*\left(\psi_E(\mathfrak{r})\frac{\Omega_\infty}{f},\mathcal{L}\right) - E_k^*\left(\psi_E(\mathfrak{r})\frac{\Omega_\infty}{f},\lambda^{-1}\mathcal{L}\right)\right).$$

Now use the fact that $(\lambda, F)=1$. Hence $\psi_E((\lambda))$ is defined, and $\psi_E((\lambda)) = \mathfrak{S}_\lambda\lambda$, where $\mathfrak{S}_\lambda \in K$. Thus

$$\lambda^{-1}\mathcal{L} = \psi_E((\lambda))^{-1}.\,\mathcal{L}$$

But $E_k^*(\alpha z, \alpha\mathcal{L}) = \alpha^{-k}E_k^*(z,\mathcal{L})$. Hence our expression is

$$= 2\sum_{k=1}^{\infty}(-1)^{k-1}z^{k-1}\left(N\lambda\, E_k^*\left(\frac{\Omega_\infty}{f},\mathcal{L}\right)^{\sigma_{\mathfrak{r}}} - \psi_E((\lambda))^k E_k^*\left(\frac{\Omega_\infty}{f},\mathcal{L}\right)^{\sigma_{\mathfrak{r}}(\lambda)}\right)$$

But

$$\sum_{\mathfrak{r}\in\mathfrak{B}} E_k^*\left(\frac{\Omega_\infty}{f},\mathcal{L}\right)^{\sigma_{\mathfrak{r}}} = \sum_{\mathfrak{r}\in\mathfrak{B}} E_k^*\left(\frac{\Omega_\infty}{f},\mathcal{L}\right)^{\sigma_{\mathfrak{r}}(\lambda)} = \left(\frac{f}{\Omega_\infty}\right)^k L_F(\overline{\psi}_E^k, k), \quad (k=1,2,\ldots$$

This proves our desired formula.

<u>Remark</u>. We would get exactly the same theorem if we multiplied $\Theta_\lambda(z,\mathcal{L})$ by any non-zero element of $\mathbb{C}$.

$$\left(c_E(\lambda)/c_E'(\lambda)\right)^{N\alpha-1} = 1$$

for all α with $(\alpha, \lambda) = 1$. Take $\alpha = 2$ and $\alpha = 3$. This is possible because $(\lambda, 6) = 1$. Then

$$\left(c_E(\lambda)/c_E'(\lambda)\right)^3 = \left(c_E(\lambda)/c_E'(\lambda)\right)^8 = 1.$$

<u>Existence</u>. Define $\omega_\lambda(\alpha)$ by the right hand side above.

<u>Claim</u>. Take α_1, α_2 with $(\alpha_1, \lambda) = (\alpha_2, \lambda) = 1$. Then

$$\omega_\lambda(\alpha_1\alpha_2) = \omega_\lambda(\alpha_1)^{N\alpha_2} \cdot \omega_\lambda(\alpha_2).$$

But $\mathcal{O}_K$ is commutative, hence

$$\omega_\lambda(\alpha_1)^{N\alpha_2-1} = \omega_\lambda(\alpha_2)^{N\alpha_1-1}.$$

Take $\alpha_1 = 2$ & $\alpha_2 = 3$. Now

$$3.(N\alpha_1 - 1) - (N\alpha_2 - 1) = 1.$$

Hence

$$\omega_\lambda(\alpha) = \omega_\lambda(\alpha)^{3(N\alpha_1-1)} \Big/ \omega_\lambda(\alpha)^{N\alpha_2-1}$$

$$= \left(\omega_\lambda(\alpha_1)^3 / \omega_\lambda(\alpha_2)\right)^{N\alpha-1}$$

q.e.d.

<u>Final fact</u>: $c_E(\lambda)^{12} = \dfrac{\Delta(E)^{N\lambda-1}}{\lambda^{12}}$.

Not so easy to prove.

<u>Final Definition</u>. $R_\lambda(P) = c_E(\lambda)\, r_\lambda(P)$.

Recall that $\varphi = \Phi\left(\frac{\Omega_\infty}{f}, \mathfrak{L}\right)$ – a primitive f-division point

We can now make:-

<u>Key Definition</u>. $\mathcal{R}_\lambda(P) = \prod_{\tau \in Gal(K(E_f)/K)} R_\lambda(P \oplus \varphi^\tau)$.

<u>Theorem</u>. Assume $(\lambda, 6) = 1$. Then $\mathcal{R}_\lambda(P)$ is a rational function on E with coefficients in K. Moreover, for each integral ideal $\mathfrak{a}$ of K with $(\mathfrak{a}, f) = 1$, we have $(\mathfrak{a}, \lambda) = 1$,

$$\mathcal{R}_\lambda(\psi_E(\mathfrak{a})(P)) = \prod_{V \in E_{\mathfrak{a}}} \mathcal{R}_\lambda(P \oplus V).$$

<u>Proof</u>. The first assertion is clear. To prove the second, we note that, if $\alpha = \psi_E(\mathfrak{a})$, we have

$$\alpha(\varphi^\tau) = (\varphi^{\tau\sigma_{\mathfrak{a}}})$$

where $\sigma_{\mathfrak{a}} = (\mathfrak{a}, K(E_f)/K)$. Hence

$\alpha(Q^{\tau})$

Sums over the same set

$$\mathcal{R}_\lambda(\alpha(P)) = \prod_{\tau \in Gal(K(E_f)/K)} R_\lambda(\alpha(P) \oplus (\varphi^\tau))$$

$$= \prod_{\tau \in Gal(K(E_f)/K)} R_\lambda(\alpha(P \oplus \varphi^\tau))$$

$$= \prod_{\tau \in Gal(K(E_f)/K)} \prod_{V \in E_{\mathfrak{a}}} R_\lambda(P \oplus \varphi^\tau \oplus V)$$

$$= \prod_{V \in E_{\mathfrak{a}}} \mathcal{R}_\lambda(P \oplus V) \qquad \text{q.e.d.}$$

Normalization of the function $\Theta_\lambda(z, \mathcal{L})$.

This turns out to be crucially important for the definition of elliptic units and for the p-adic theory.

$$\Theta_\lambda(z, \mathcal{L}) = \prod_{\substack{\alpha \in \frac{1}{\lambda} L/L \\ \alpha \neq 0}} \left(\wp(z, L) - \wp(\alpha, L)\right)^{-1}.$$

Classically the normalization was done analytically, and required rather elaborate arguments. We shall use simple algebraic arguments instead.

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_i \in \mathcal{O}_K)$$

$P = (x, y)$ – general point on E.

<u>Assumption</u>. We assume from now on that $\lambda \in \mathcal{O}_K$ and $(\lambda, 6) = 1$ and $\lambda \notin \mu_K$.

<u>Defn</u>. We define $\tau_\lambda(P) \in K(E)$ by

$$\tau_\lambda(P) = \prod_{R \in V_\lambda} \left(x(P) - x(R)\right)^{-1}$$

where V_λ denotes a set of representatives of $\overset{E_\lambda}{\overset{\shortparallel}{\mathrm{Ker}\,\lambda}} \setminus \{0\}$ modulo ± 1. This is well defined because $x(\ominus P) = x(P)$. It is also clear that $\tau_\lambda(P)$ is fixed by $\mathrm{Gal}(K(E_\lambda)/K)$ and so lies in $K(E)$.

<u>Note</u> $\Phi(z, \mathcal{L}) : \mathbb{C}/\mathcal{L} \xrightarrow{\sim} E(\mathbb{C})$.

<u>Clear</u>: $\Theta_\lambda(z, \mathcal{L}) = \tau_\lambda(\Phi(z, \mathcal{L}))^2$.

<u>Example</u>: $y^2 = x^3 - Dx$, take $\lambda = 2+i$, $K = \mathbb{Q}(i)$

<u>Ray class field of K mod λ</u>.

(i). By theory of complex multiplication, the ray class field of K mod λ is given <u>explicitly</u> by $K(x(V)^2)$, where V is a primitive λ-division point on E.

(ii). By class field theory, the Galois group of the ray class field of K mod λ is $(\mathbb{Z}[i]/\lambda)^\times/\tilde{\mu}_4$, which has order 1.

<u>Conclusion</u>: $K(x(V)^2) = K$. $x(V)^2 = \dfrac{D}{1+2i}$.

$$\tau_\lambda(P) = \left(x^2 - x(V)^2\right)^{-1}.$$

<u>Proposition</u>. There exists a unique $c_E(\lambda) \in K^\times$ such that, for all $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, with $(\alpha, \lambda) = 1$, we have

$$\frac{\tau_\lambda(\alpha(P))}{\prod_{U \in E_\alpha} \tau_\lambda(P \oplus U)} = c_E(\lambda)^{N\alpha - 1}.$$

<u>Proof</u>. We note that $\tau_\lambda(\alpha(P))$ & $\prod_{U \in E_\alpha} \tau_\lambda(P \oplus U)$ have the same divisor. Hence the ratio is a constant.

(i). <u>Uniqueness</u>. Suppose that we have two such constants $c_E(\lambda)$ and $c'_E(\lambda)$. Then

Now

$$\Theta_{\lambda,\mathfrak{f}}(z,\mathcal{L}) \cdot c_E(\lambda)^{2\varphi(F)/\#(\mu_K)} = \mathcal{R}_\lambda\left(\Phi(z,\mathcal{L})\right)^2.$$

Hence we immediately obtain the following :-

<u>Theorem</u>. Assume that $(\lambda, G) = (\lambda, F) = 1$. Then, for all integers $n \geq 1$, we have

$$\left(\frac{d}{dz}\right)^n \log \mathcal{R}_\lambda\left(\Phi(z,\mathcal{L})\right)\Big|_{z=0} = (-1)^{n-1}(n-1)!\, f^n \Omega_\infty^{-n}\left(N\lambda - \psi_E((\lambda))^n\right) \times$$
$$\times\, L_F(\overline{\psi}_E^n, n).$$

So far all these computations, L-functions etc. have been taking place in the complex world via our embedding $K \hookrightarrow \mathbb{C}$. How can we interpret them in the p-adic world?

Two cases for a rational prime p :-

(i). potentially ordinary : p splits in K, $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, $\mathfrak{p} \neq \mathfrak{p}^* \Longleftrightarrow$ we can embed $K \xhookrightarrow{i_\mathfrak{p}} \mathbb{Q}_p$ & there is a second embedding which is given by $i_\mathfrak{p} \circ c$, c = complex conjugation.

(ii) potentially supersingular : $p\mathcal{O}_K = \mathfrak{p}$ or $\mathfrak{p}^2$.

<u>Reality</u>. We know exactly what to do in case (i). In case (ii), we do not know how to carry out the p-adic theory – just small fragments of it.

<u>p-adic theory</u>.

How are we going to define a p-adic L-function? Neither Euler products nor Dirichlet series make sense in the p-adic world.

$\mathfrak{p}$ – any finite prime of K.

We fix an embedding $i_{\mathfrak{p}} : K \hookrightarrow \mathbb{C}_p$ which determines $\mathfrak{p}$.

<u>Defn</u>. $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$.

$$E_{\mathfrak{p}^\infty} = \bigcup_{n \geq 1} E_{\mathfrak{p}^n} \qquad \mathcal{O}_{\mathfrak{p}} = \overline{i_{\mathfrak{p}}(\mathcal{O}_K)}.$$

<u>Defn</u>. $F_\infty = K(E_{\mathfrak{p}^\infty})$, $G = \mathrm{Gal}(F_\infty / K)$.

What is G? Well G acts on $E_{\mathfrak{p}}$ and action commutes with action of $\mathcal{O}_K$. Now $\mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(E_{\mathfrak{p}^\infty}) = \mathcal{O}_{\mathfrak{p}}^\times$

Hence we get a character

$$\chi_{\mathfrak{p}} : G \hookrightarrow \mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(E_{\mathfrak{p}^\infty}) = \mathcal{O}_{\mathfrak{p}}^\times.$$

<u>Fact</u>. $\mathrm{Im}\, \chi_{\mathfrak{p}}$ is open in $\mathcal{O}_{\mathfrak{p}}^\times$.

<u>Basic idea</u>. Our $\mathfrak{p}$-adic L-function will be a p-adic valued measure on G.

We want to integrate functions $f : G \longrightarrow \mathbb{C}_p$ like $\chi_{\mathfrak{p}}^n$ $(n \in \mathbb{Z})$.

We want to consider a special class of measures

<u>L16</u>. <u>p-adic measure theory</u>. $C_p = \widehat{\overline{\mathbb{Q}}}_p$, completion w.r.t. $|\,|_p$.

$\mathbb{Q}_p^{nr}$ = max. unramified extension of $\mathbb{Q}_p$, $\widehat{\mathbb{Q}_p^{nr}}$ completion w.r.t. $|\,|_p$

<u>Defn</u>. $\mathcal{I}$ = ring of integers of $\widehat{\mathbb{Q}_p^{nr}}$.

We have to define what we mean by an $\mathcal{I}$-valued measure on G. We recall that $G = \mathrm{Gal}(F_\infty/K)$, $F_\infty = K(E_{\mathfrak{p}^\infty})$, $\mathcal{O}_{\mathfrak{p}}$ = ring of integers of K completed at $\mathfrak{p}$. Then the character $\chi_{\mathfrak{p}}$ giving the action of G on $E_{\mathfrak{p}^\infty}$ gives an embedding $\chi_{\mathfrak{p}} : G \hookrightarrow \mathcal{O}_{\mathfrak{p}}^\times$ with open image. For the moment, $\mathfrak{p}$ is any finite prime of K above p.

<u>Naive approach</u>.

<u>Defn</u>. $C(G, \mathbb{C}_p) = \{f : G \to \mathbb{C}_p\}$ & f continuous.

<u>Defn</u>. $$\|f\| = \sup_{g \in G} |f(g)|_p.$$

This norm makes $C(G, \mathbb{C}_p)$ into a $\mathbb{C}_p$-Banach space.

<u>Defn</u>. An $\mathcal{I}$-valued measure on G is a continuous linear map $L : C(G, \mathbb{C}_p) \to \mathbb{C}_p$ such that

(i). $|L(g)|_p \leqslant \|g\|$ for all g in $C(G, \mathbb{C}_p)$;

(ii). $L(g) \in \widehat{\mathbb{Q}_p^{nr}}$ whenever $g(G) \subset \widehat{\mathbb{Q}_p^{nr}}$.

Let $M_{\mathcal{I}}(G)$ be the set of all such $\mathcal{I}$-valued measures. Clearly $M_{\mathcal{I}}(G)$ is an $\mathcal{I}$-module. We can even make it into an $\mathcal{I}$-algebra by

introducing convolutions.

<u>Iwasawa algebras</u>.

If U is an open subgroup of G, G/U is a finite group, and we write $\mathcal{I}[G/U]$ for the group ring of G/U with coefficients in $\mathcal{I}$. We endow it with the p-adic topology.

<u>Fundamental definition</u>.

$$\Lambda_{\mathcal{I}}(G) = \varprojlim_{U} \mathcal{I}[G/U]$$

This is called the Iwasawa algebra of $\mathcal{I}$ with coefficients in G. It is clearly an $\mathcal{I}$-algebra.

<u>Theorem</u>. We have a canonical $\mathcal{I}$-module isomorphism

$$c : \Lambda_{\mathcal{I}}(G) \xrightarrow{\sim} M_{\mathcal{I}}(G).$$

<u>Remark</u>. In fact, it is an isomorphism of $\mathcal{I}$-algebras if we endow $M_{\mathcal{I}}(G)$ with the product given by convolution.

<u>Proof</u>. We define the map c. For each U, let

$$\pi_U : \Lambda_{\mathcal{I}}(G) \longrightarrow \mathcal{I}[G/U]$$

be the projection map. Suppose we are given $\mu \in \Lambda_{\mathcal{I}}(G)$. We have

$$\pi_U(\mu) = \sum_{x \in G/U} a_{\mu,U}(x)\, x \quad , \quad a_{\mu,U} \in \mathcal{I}.$$

We want to define $c(\mu)$ on $C(G, \mathbb{C}_p)$. In fact, every f in $C(G, \mathbb{C}_p)$ is a limit of locally constant $f : G \longrightarrow \mathbb{C}_p$. Moreover, locally constant

means that f factors through G/U for some open subgroup U of G. Supposing f factors through G/U, we define

$$c(\mu)(f) = \sum_{x \in G/U} a_{\mu,U}(x) f(x).$$

One checks immediately that, as $\mu \in \Lambda_{\mathcal{J}}(G)$, this definition does not depend on μ. Since $|a_{\mu,U}(x)|_p \leq 1$, we clearly have

$$|c(\mu)(f)|_p \leq \|f\|.$$

Also, it is obvious that $c(\mu)(f) \in \widehat{\mathcal{O}}_p^{nr}$ whenever $_U(G) \subset \widehat{\mathcal{O}}_p^{nr}$. Conversely, given any L in $M_I(G)$, we can define μ_L in $\Lambda_{\mathcal{J}}(G)$ as follows. If U is any open subgroup of G, and $x \in G/U$, let $f_{x,U}$ be the locally constant function on G/U which satisfies $f_{x,U}(x) = 1$ and $f_{x,U}(y) = 0$ for $y \neq x$. We then define μ by giving, for any open subgroup U of G,

$$\pi_U(\mu) = \sum_{x \in G/U} L(f_{x,U})\, x.$$

One sees immediately that $\pi_U(\mu)$ belongs to $\mathcal{J}[G/U]$, and defines, as U varies, and element μ of $\Lambda_{\mathcal{J}}(G)$.

<u>Question</u>. How we get a canonical element of $\Lambda_{\mathcal{J}}(G)$?

We only know the answer when $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_p$, i.e. p splits in K, say $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$.

For simplicity, we assume that $(\mathfrak{p}, F) = 1$.

<u>Lemma</u> (Proven later). If $(\mathfrak{p}, F) = 1$, the character $\chi_{\mathfrak{p}} : G \longrightarrow \mathcal{O}_{\mathfrak{p}}^{\times}$ is <u>surjective</u> (hence an isomorphism

Hence we are now in the case when $G \xrightarrow[\sim]{\chi_p} \mathcal{O}_p^\times = \mathbb{Z}_p^\times$.

The method of construction of a canonical element of $\Lambda_{\mathcal{G}}(\mathbb{Z}_p^\times)$ is to first look at $\Lambda_{\mathcal{G}}(\mathbb{Z}_p)$.

<u>Note</u>: The group-theoretic structure on $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$ is totally different! One is multiplicative, the other is additive.

<u>Mahler's Theorem</u> (see). Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be any continuous function. Then f has a unique expansion of the form

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n},$$

where $a_n \in \mathbb{C}_p$ and $a_n \to 0$ in $\mathbb{C}_p$ as $n \to \infty$.

<u>Remarks</u>. $\left|\binom{x}{n}\right|_p \leq 1$ for $x \in \mathbb{Z}_p$. Hence every series of the above form converges uniformly to a continuous function $f : \mathbb{Z}_p \to \mathbb{C}_p$. Also $a_n = (\nabla^n f)(0)$, where $(\nabla f)(x) = f(x+1) - f(x)$. Thus the uniqueness of the expansion is obvious. What is <u>not</u> obvious is the existence.

<u>Lemma</u>. In the Mahler expansion, we have

$$\|f\| = \sup_{n \geq 0} |a_n|_p.$$

<u>Proof</u>. $\left|\binom{x}{n}\right|_p \leq 1 \Rightarrow |f(x)|_p \leq \sup_{n \geq 0} |a_n|_p$.

But $a_n = (\nabla^n f)(0) \Rightarrow |a_n|_p \leq \|f\|_p$ for all $n \geq 0$.

<u>L17</u>. Given $\mu \in \Lambda_{\mathfrak{g}}(\mathbb{Z}_p)$, we define

$$c_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu \quad (n \geqslant 0).$$

Thus $c_n(\mu)$ is in $\mathfrak{g}$ because $\left|\binom{x}{n}\right|_p \leqslant 1$ for $x \in \mathbb{Z}_p$.

<u>Defn</u>. $\mathfrak{M} : \Lambda_{\mathfrak{g}}(\mathbb{Z}_p) \xrightarrow{\sim} \mathfrak{g}[[W]]$

$$\mathfrak{M}(\mu) = \sum_{n=0}^{\infty} c_n(\mu) W^n.$$

This is an isomorphism because of Mahler's theorem.

<u>Passage to $\Lambda_{\mathfrak{g}}(\mathbb{Z}_p^\times)$.</u>

Note that $\mathbb{Z}_p^\times$ is an open and closed subgroup of $\mathbb{Z}_p$.

<u>Lemma</u>. We have a canonical inclusion

$$i : \Lambda_{\mathfrak{g}}(\mathbb{Z}_p^\times) \hookrightarrow \Lambda_{\mathfrak{g}}(\mathbb{Z}_p).$$

<u>Proof</u>. We define i by

$$\int_{\mathbb{Z}_p} f \, d\, i(\eta) = \int_{\mathbb{Z}_p^\times} f\big|_{\mathbb{Z}_p^\times} d\eta \quad \text{for } \eta \in \Lambda_{\mathfrak{g}}(\mathbb{Z}_p^\times),\ f : \mathbb{Z}_p \to \mathbb{C}_p.$$

This is clearly an $\mathfrak{g}$-linear map; since every continuous function $g : \mathbb{Z}_p^\times \to \mathbb{C}_p$ can be extended by 0 to a continuous function $\tilde{g} : \mathbb{Z}_p \to \mathbb{C}_p$, we see immediately that $i(\eta) = 0$ implies that $\eta = 0$.

<u>Question</u>. What is the subset of $\mathfrak{g}[[W]]$ given by $\mathfrak{M}(i(\Lambda_{\mathfrak{g}}(\mathbb{Z}_p^\times)))$?

<u>Defn</u> of $\# : \Lambda_{\mathcal{G}}(\mathbb{Z}_p) \longrightarrow \Lambda_{\mathcal{G}}(\mathbb{Z}_p)$.

Let $\varepsilon : \mathbb{Z}_p \longrightarrow \{0,1\}$ be defined by $\varepsilon(x) = 1$ if x is in $\mathbb{Z}_p^\times$, and $\varepsilon(x) = 0$ if x is in $p\mathbb{Z}_p$. This is continuous since $\mathbb{Z}_p^\times$ is open and closed in $\mathbb{Z}_p$. Given μ in $\Lambda_{\mathcal{G}}(\mathbb{Z}_p)$, we have the linear functional $L : C(G, \mathbb{C}_p) \longrightarrow \mathbb{C}_p$ defined by

$$L(f) = \int_{\mathbb{Z}_p} f \varepsilon \, d\mu .$$

It satisfies all the desired properties, and hence must correspond to some element $\#(\mu)$ of $\Lambda_{\mathcal{G}}(G)$.

<u>Remark</u>. $\mu \in i\left(\Lambda(\mathbb{Z}_p^\times)\right) \Longleftrightarrow \#(\mu) = \mu$.

How can we compute $\mathcal{M}(\#(\mu))$ from $\mathcal{M}(\mu)$?

<u>Defn</u>. $S : \mathcal{G}[[W]] \longrightarrow \mathcal{G}[[W]]$ is defined by

$$S(f)(W) = f(W) - \frac{1}{p} \sum_{\zeta \in \mu_p} f(\zeta(1+W) - 1).$$

<u>Lemma</u>. $\mathcal{M}(\#(\mu)) = S(\mathcal{M}(\mu))$. In particular, $\#(\mu) = \mu$ if and only if $S(\mathcal{M}(\mu)) = \mathcal{M}(\mu)$, or equivalently

$$\sum_{\zeta \in \mu_p} \mathcal{M}(\mu)(\zeta(1+W) - 1) = 0.$$

<u>Proof</u>. For each $n \geqslant 0$, let

$$pr_n : \Lambda_{\mathcal{G}}(\mathbb{Z}_p) \longrightarrow \mathcal{G}\left[\mathbb{Z}_p / p^n \mathbb{Z}_p\right]$$

be the projection map. Suppose

$$pr_n(\mu) = \sum_{k=0}^{p^n - 1} e_n(k)\left(k + p^n \mathbb{Z}_p\right).$$

We recall that

$$e_n(k) = \int_{\mathbb{Z}_p} \varepsilon_{k+p^n\mathbb{Z}_p}\, d\mu,$$

where $\varepsilon_{k+p^n\mathbb{Z}_p}$ is the characteristic function of $k+p^n\mathbb{Z}_p$. It is then clear that $\#(\mu)$ is the unique element of $\Lambda_{\mathcal{G}}(\mathbb{Z}_p)$ defined by

$$pr_n(\#(\mu)) = \sum_{\substack{k=0\\(k,p)=1}}^{p^n-1} e_n(k)\,(k+p^n\mathbb{Z}_p).$$

$\mathcal{L}$ – $\omega_n(T) = (1+W)^{p^n}-1$. Then, if $R = \mathcal{G}[[W]]$,

$$\mathcal{G}[W]/\omega_n\mathcal{G}[W] \xrightarrow{\sim} R/\omega_n R$$

by the Weierstrass Preparation Theorem. But $R = \varprojlim R/\omega_n R$.

Hence we have projection maps

$$pr_n' : R \longrightarrow \mathcal{G}[W]/\omega_n\mathcal{G}[W].$$

<u>Claim</u> : $\mathcal{M}(1_{\mathbb{Z}_p}) = 1+W$. Put $\mu = 1_{\mathbb{Z}_p}$

$$\mathcal{M}(\mu) = \sum_{n=0}^{\infty} c_n(\mu)W^n, \quad \text{where } c_n(\mu) = \int_{\mathbb{Z}_p}\binom{x}{n}d\mu = \binom{1}{n}_{\text{gen.}}$$

Hence, returning to the general case,

$$pr_n'(\mathcal{M}(\mu)) = \sum_{k=0}^{p^n-1} e_n(k)(1+W)^k \bmod \omega_n\mathbb{Z}_p[W].$$

$$pr_n'(\mathcal{M}(\#\mu)) = \sum_{\substack{k=0\\(k,p)=1}}^{p^n-1} e_n(k)(1+W)^k \bmod \omega_n\mathbb{Z}_p[W].$$

But

$$S\left(\sum_{k=0}^{p^n-1} e_n(k)(1+W)^k\right) = \sum_{\substack{k=0\\(k,p)=1}}^{p^n-1} e_n(k)(1+W)^k,$$

and the assertion follows.

<u>An additional property</u>.

<u>Lemma</u>. For all μ in $\Lambda_{\mathcal{G}}(\mathbb{Z}_p)$, and all integers $k \geq 0$, we have

$$\int_{\mathbb{Z}_p} x^k \, d\mu = \left(D^k \mathcal{M}(\mu)(W)\right)_{W=0},$$

where $D = (1+W)\frac{d}{dW}$.

<u>Proof</u>. We consider the linear functional $L : C(\mathbb{Z}_p, \mathbb{C}_p) \to \mathbb{C}_p$ defined by

$$L(f) = \int_{\mathbb{Z}_p} x f(x) \, d\mu .$$

We again clearly have $|L(f)|_p \leq \|f\|$, and so $L \Longleftrightarrow \lambda$ in $\Lambda_{\mathcal{G}}(\mathbb{Z}_p)$, i.e.

$$\int_{\mathbb{Z}_p} x f(x) \, d\mu = \int_{\mathbb{Z}_p} f(x) \, d\lambda .$$

We first claim that $\mathcal{M}(\lambda)(W) = D\mathcal{M}(\mu)(W)$.
Suppose $\mathcal{M}(\mu)(W) = \sum_{n=0}^{\infty} c_n W^n$. Then

$$D\mathcal{M}(\mu)(W) = \sum_{n=0}^{\infty} \left(n c_n + (n+1) c_{n+1}\right) W^n. \text{ But}$$

$$c_n(\lambda) = \int_{\mathbb{Z}_p} x \binom{x}{n} d\mu .$$

But we have the identity

$$x \binom{x}{n} = (n+1)\binom{x}{n+1} + n \binom{x}{n} .$$

Hence $c_n(\lambda) = n c_n + (n+1) c_{n+1}$ as required.

It follows by induction on k that, for all integers $k \geqslant 0$, we have

$$\int_{\mathbb{Z}_p} x^k f(x)\, d\mu = \int_{\mathbb{Z}_p} f(x)\, d\lambda_k ,$$

where $\mathcal{M}(\lambda_k) = D^k \mathcal{M}(\mu)$. The theorem follows on recalling that

$$\int_{\mathbb{Z}_p} d\mu = \mathcal{M}(\mu)(0).$$

This finishes the general measure theory, and we return to our CM elliptic curve E/K with $\mathrm{End}_K(E) = \mathcal{O}_K$.

<u>Question</u>: $(\wp, F) = 1$, $\chi_\wp : G \xrightarrow{\sim} \mathbb{Z}_p^\times$. $\mathcal{O}_\wp = \mathbb{Z}_p$.

How do we find a canonical $g(W) \in \mathcal{I}[[W]]$ such that $\sum_{\zeta \in \mu_p} g(\zeta(1+W)-1) = 0$?

This is in no way obvious!

We return to our canonical rational function $\mathcal{R}_\lambda(P)$ on E/K, where $(\lambda, 6) = (\lambda, F) = 1$. It has two basic properties:–

(i). If $(\sigma, F) = (\sigma, \lambda) = 1$, we have

$$\mathcal{R}_\lambda\left(\psi_E(\sigma)(P)\right) = \prod_{V \in E_\sigma} \mathcal{R}_\lambda(P \oplus V).$$

(ii). $$\left(\frac{d}{dz}\right)^n \log \mathcal{R}_\lambda\left(\Phi(z, \mathcal{L})\right)\Big|_{z=0} = (-1)^{n-1}(n-1)!\, F^n \Omega_\infty^{-n} \left(N\lambda - \psi_E((\lambda))^n\right) \times L_F(\overline{\psi}_E^n, n).$$

How do we make such a g out of $\mathcal{R}_\lambda(P)$?

Two vague ideas :–

(a). Expand this in terms of the local parameter $t = -x/y$ of the formal group of E at $\mathfrak{p}$;

(b). Take logarithms.

But remember that we must end up with a series in $\mathcal{I}[[t]]$. We assume that $(\lambda, 6f) = 1$ & $(\mathfrak{p}, \lambda f) = 1$.

<u>Defn</u>. $\Phi_\lambda(P) = \mathcal{R}_\lambda(P)^h \big/ \mathcal{R}_\lambda(\psi_E(\mathfrak{p})(P))$.

<u>Lemma</u>. $\prod_{R \in E_{\mathfrak{p}}} \Phi_\lambda(P \oplus R) = 1$.

<u>Proof</u>. Use (i) with $(\mathfrak{p} = \mathfrak{v})$.

<u>Lemma</u>. The t-expansion of $\mathcal{R}_\lambda(P)$ is a unit in $\mathcal{O}_{\mathfrak{p}}[[t]]$.

<u>Corollary</u>. The t-expansion of $\Phi_\lambda(P)$ belongs to $1 + \psi_E(\mathfrak{p})\mathcal{O}_{\mathfrak{p}}[[t]]$.

<u>Proof of Corollary</u> (assuming the lemma). Let $g(t) = \sum_{n=0}^{\infty} g_n t^n$ be the t-expansion of $\mathcal{R}_\lambda(P)$. Thus, by the previous lemma, g_n belongs to $\mathcal{O}_{\mathfrak{p}}$ for all $n \geq 0$, and g_0 is a unit in $\mathcal{O}_{\mathfrak{p}}$.

Let $\hat{E}^{\mathfrak{p}}$ denote the formal group of E at $\mathfrak{p}$. It has endomorphism ring $\mathcal{O}_{\mathfrak{p}}$. If $\alpha \in \mathcal{O}_{\mathfrak{p}}$, we write $[\alpha](t)$ for the corresponding endomorphism of $\hat{E}^{\mathfrak{p}}$. It

is a power series in $\mathcal{O}_{\mathfrak{p}}[[t]]$, which starts off $[\alpha](t) \equiv \alpha t + \dots$. Now, putting $\pi = \psi_E(\mathfrak{p})$, we see that $\Phi_\lambda(P)$ has power series expansion

$$g(t)^p / g([\pi](t)).$$

<u>Key claim</u>. $[\pi](t) \bmod \mathfrak{p} = t^p$, i.e. $[\pi](t) \equiv t^p \bmod \mathfrak{p}$.

<u>Proof of key claim</u>. $\widetilde{[\pi](t)}$ = image of $\pi[t]$ in $\mathbb{F}_p[[t]]$ is the endomorphism of $\tilde{E}$ (= reduction of $E \bmod \mathfrak{p}$), which is given by $\pi \bmod \mathfrak{p}$. But this is the Frobenius endomorphism! Hence $\widetilde{[\pi](t)} = -x^p/y^p = \left(\frac{-x}{y}\right)^p$ in $\mathbb{F}_{p^{q^e}}$

Using the key claim we see that

$$g([\pi](t)) = \sum_{n=0}^{\infty} g_n ([\pi](t))^n \equiv \sum_{n=0}^{\infty} g_n t^{np} \bmod \mathfrak{p}.$$

But

$$g(t)^p \equiv \sum_{n=0}^{\infty} g_n^p t^{np} \equiv \sum_{n=0}^{\infty} g_n t^{np} \bmod \mathfrak{p}.$$

Now it is clear that the t-expansion of $\Phi_\lambda(P)$ lies in $\mathcal{O}_{\mathfrak{p}}[[t]]$, and the above argument shows that it is $\equiv 1 \bmod \mathfrak{p}$. q.e.d.

<u>Proof of Lemma</u>. We have to look at the explicit expression for $\mathcal{R}_\lambda(P)$, namely:–

$$\mathcal{R}_\lambda(P) = c_E(\lambda)^{\tau} \prod_{\tau \in \mathrm{Gal}(K(E_f)/K)} \mathcal{R}_\lambda(P \oplus Q^{\tau})$$

$$\mathcal{R}_\lambda(P) = \prod_{U \in V_\lambda} (x(P) - x(R))^{-1}.$$

<u>Fact</u>. $c_E(\lambda) \in \mathcal{O}_\mathfrak{p}^\times$ because $c_E(\lambda) = \dfrac{\Delta(E)^{N\lambda-1}}{\lambda^{12}}$ and by hypothesis $(\mathfrak{p}, \Delta(E)) = (\mathfrak{p}, \lambda) = 1$. Hence it suffices to show that the t-expansion of

$$x(P \oplus \varphi^\tau) - x(R),$$

where R is any non-zero element of E_λ, is a unit in $\mathcal{O}_\mathfrak{p}[[t]]$. Now neither φ^τ nor R lies on the formal group of E at $\mathfrak{p}$, since $(\mathfrak{p}, F) = (\mathfrak{p}, \lambda) = 1$. Hence all of the coordinates $x(\varphi^\tau), y(\varphi^\tau), x(R), y(R)$ are integers in $\overline{K}_\mathfrak{p}$. Hence

$$x(P) - x(\varphi^\tau) = t^{-2}\left(1 + \sum_{n=1}^{\infty} \alpha_n t^n\right),$$

where the α_n belong to $\overline{\mathcal{O}}_\mathfrak{p}$ = ring of integers of $\overline{K}_\mathfrak{p}$. Now $y = -x/t$. It follows that

$$\frac{y(P) - y(\varphi^\tau)}{x(P) - x(\varphi^\tau)} = -t^{-1}\left(1 + \sum_{n=1}^{\infty} \beta_n t^n\right),$$

where all of the coefficients β_n lie in $\overline{\mathcal{O}}_\mathfrak{p}$. By the explicit addition law on E, we have

$$x(P \oplus \varphi^\tau) - x(R) = \left(\frac{y(P) - y(\varphi^\tau)}{x(P) - x(\varphi^\tau)}\right)^2 + a_1\left(\frac{y(P) - y(\varphi^\tau)}{x(P) - x(\varphi^\tau)}\right)$$

$$- a_2 - x(P) - x(\varphi^\tau) - x(R).$$

Hence we get a power series in $\overline{\mathcal{O}}_\mathfrak{p}[[t]]$ (note that the negative powers of t must cancel out!). The constant term is $x(\varphi^\tau) - x(R)$. Suppose it

was not a unit in $\overline{\mathcal{O}}_{\mathfrak{p}}$. Writing $a \longmapsto \tilde{a}$ for reduction modulo the maximal ideal of $\overline{\mathcal{O}}_{\mathfrak{p}}$, we would have $x(\widetilde{Q^\tau}) = x(\tilde{R}) \Rightarrow \tilde{R} = \pm \widetilde{Q^\tau}$. Hence $R \pm Q^\tau$ would belong to the formal group of E at $\mathfrak{p}$, which is impossible since they are points of finite order prime to $\mathfrak{p}$. Hence $x(Q^\tau) - x(R)$ is a unit in $\overline{\mathcal{O}}_{\mathfrak{p}}$, and the proof of the lemma is complete.

We continue to assume that $\mathfrak{p}\mathfrak{p}^* = p\mathcal{O}_K$, $\mathfrak{p} \neq \mathfrak{p}^*$. $(\mathfrak{p}, F) = 1$ & $p > 2$. We also have chosen $\lambda \in \mathcal{O}_K$ with $(\lambda, 6F) = 1$ & $(\lambda, \mathfrak{p}) = 1$.

<u>Defn</u>. $A_\lambda(t) = t$-expansion of $\Phi_\lambda(P) = \mathcal{R}_\lambda(P)^p / \mathcal{R}_\lambda(\psi_E(\mathfrak{p}))$

We know that $A_\lambda(t) \in \mathcal{O}_{\mathfrak{p}}[[t]]$, and $A_\lambda(t) \equiv 1 \bmod \mathfrak{p}$.

<u>Defn</u>. $$B_\lambda(t) = \frac{1}{p} \log A_\lambda(t) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(A_\lambda(t) - 1)^n}{pn}.$$

<u>Key remark</u>. Since $p > 2$, $n > 1 + \mathrm{ord}_p(n)$ and so we see that $B_\lambda(t) \in \mathcal{O}_{\mathfrak{p}}[[t]]$.

<u>Lemma</u>. $$\sum_{R \in E_{\mathfrak{p}}} B_\lambda(t \oplus t_R) = 0. \quad \left(\text{because } \prod_{x \in E_{\mathfrak{p}}} \Phi_\lambda(P \oplus R) = 1\right)$$

This is still not what we want! We want a power series $g(W)$ in $\mathcal{I}[[W]]$ such that

$$\sum_{\zeta \in \mu_p} g(\zeta(1 + W) - 1) = 0.$$

Re-interpretation in terms of formal groups.

Formal multiplicative group $\hat{\mathbb{G}}_m$

$\hat{\mathbb{G}}_m$: group law $(1+W_1)(1+W_2)-1 = W_1+W_2+W_1W_2$

We can view this as a group law defined over $\mathcal{O}_{\mathfrak{p}}$.

$$\zeta(1+W)-1 = (\zeta-1)\underset{\hat{\mathbb{G}}_m}{\oplus} W$$

Hence above equation can be written as

$$\sum_{\zeta\in\mu_p} g\left((\zeta-1)\underset{\hat{\mathbb{G}}_m}{\oplus} W\right) = 0.$$

As ζ runs over μ_p, $\zeta-1$ runs over $\hat{\mathbb{G}}_{m,p}$ = p-torsion of $\hat{\mathbb{G}}_m(\overline{\mathfrak{m}})$, where $\overline{\mathfrak{m}}$ = maximal ideal of ring of integers of $\overline{K}_{\mathfrak{p}}$.

Formal group $\hat{E}^{\mathfrak{p}}$.

Recall that $\hat{E}^{\mathfrak{p}}$ is the formal group of E at $\mathfrak{p}$. The formal group law cannot be written down in simple finite terms

$$t_{P_1\oplus P_2} = F(t_{P_1}, t_{P_2}).$$

It is a formal group also defined $\mathcal{O}_{\mathfrak{p}}$.

Facts: 1. $E_1(\overline{K}_{\mathfrak{p}})$ = kernel of reduction mod $\mathfrak{p}$ on $E(\overline{K}_{\mathfrak{p}})$.

$$E_1(\overline{K}_{\mathfrak{p}}) \xrightarrow{\sim} \hat{E}^{\mathfrak{p}}(\overline{\mathfrak{m}}) \quad (x,y)\longmapsto t=-x/y.$$

2. Under this isomorphism, $E_{\mathfrak{p}\infty}$ is mapped onto $\hat{E}^{\mathfrak{p}}(\overline{\mathfrak{m}})(p)$. Hence $\hat{E}^{\mathfrak{p}}(\overline{\mathfrak{m}})(p) = \mathbb{Q}_p/\mathbb{Z}_p$.

In other words, $\hat{E}^{\mathfrak{p}}$ is a formal group of height 1 defined over $\mathcal{O}_{\mathfrak{p}}$. In fact, it is a Lubin-Tate group over $\mathcal{O}_{\mathfrak{p}}$

How can we compare $\hat{E}^{\mathfrak{p}}$ and $\widehat{\mathbb{G}_m}$?

<u>Theorem</u>. There exists an isomorphism

$$\delta : \widehat{\mathbb{G}_m} \xrightarrow{\sim} \hat{E}^{\mathfrak{p}}$$

defined over $\mathcal{I}$. This isomorphism is given explicitly by a power series $t = \delta(W)$ in $\mathcal{I}[[W]]$, which starts off $\delta(W) = \Omega_{\mathfrak{p}} W + \dots$, for some $\Omega_{\mathfrak{p}} \in \mathcal{I}^{\times}$.

<u>Proof</u>. Here it is true because both are Lubin-Tate groups over $\mathcal{O}_{\mathfrak{p}}$ for local parameters p and $\psi_E(\mathfrak{p})$.

<u>Remark</u>. A theorem of Tate shows that δ is already defined over the completion of the ring of integers of $K_{\mathfrak{p}}(E_{\mathfrak{p}^{*\infty}})$.

<u>Corollary</u>. Define $J_\lambda(W) = B_\lambda(\delta(W))$. Then $B_\lambda(\delta(W)) \in \mathcal{I}[[W]]$ and satisfies

$$\sum_{\zeta \in \mu_p} J_\lambda(\zeta(1+W)-1) = 0.$$

<u>Proof</u>. $\psi_E(\mathfrak{p}) = p \cdot$ unit in $\mathcal{O}_{\mathfrak{p}}$.

Hence δ maps $\widehat{\mathbb{G}_m}, p$ isomorphically to $\hat{E}^{\mathfrak{p}}_p = E_{\mathfrak{p}}$.

<u>Defn</u>. μ_λ = measure in $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^{\times})$ determined by $J_\lambda(W)$.

From our earlier theory, we know that, writing also μ_λ for the corresponding measure on $\Lambda_{\mathcal{I}}(G)$, we have

$$\int_G \chi_{\mathfrak{p}}(\sigma)^n d\mu_\lambda = \int_{\mathbb{Z}_p} x^n d\mu_\lambda = D^n J_\lambda(W)\Big|_{W=0} \quad (n=0,1,2,\dots)$$

Computation of $D^n J_\lambda(W)\big|_{W=0}$.

z = parameter of $\hat{\mathbb{G}}_a$.

Exponential map on $\hat{\mathbb{G}}_m$: $W = e^z - 1$ $\quad \hat{\mathbb{G}}_a \xrightarrow{\sim} \hat{\mathbb{G}}_m$ over $\mathbb{Q}$.

Here we see immediately that $D = (1+W)\frac{d}{dW} = \frac{d}{dz}$.

Hence

$$D^n J_\lambda(W)\Big|_{W=0} = \left(\frac{d}{dz}\right)^n J_\lambda\left(e^z - 1\right)\Big|_{z=0}.$$

<u>Lemma</u>. If $t = \delta(W)$ as above, then

$$t = \delta\left(e^{\Omega_\wp^{-1} z} - 1\right) = \nu(z),$$

where $t = \nu(z) = -x(z)/y(z) = \dfrac{\frac{a_1^2+4a_2}{12} - \wp(z,\mathcal{L})}{\frac{1}{2}\left(\wp'(z,\mathcal{L}) - a_1\left(\wp(z,\mathcal{L}) - \frac{a_1^2+4a_2}{12}\right) - a_3\right)}$.

<u>Proof</u>. This follows from the uniqueness of the exponential map for $\hat{E}^\wp$, since

$$t = \delta\left(e^{\Omega_\wp^{-1} z} - 1\right) = z + \dots \quad \text{as } \delta(W) = \Omega_\wp W + \dots.$$

<u>Conclusion</u>

$$\left(\frac{d}{dz}\right)^n J_\lambda\left(e^z - 1\right)\Big|_{z=0} = \Omega_\wp^n \left(\frac{d}{dz}\right)^n J_\lambda\left(e^{\Omega_\wp^{-1} z} - 1\right)\Big|_{z=0}$$

$$= \Omega_\wp^n \left(\frac{d}{dz}\right)^n B_\lambda(\nu(z))\Big|_{z=0}$$

$$= \frac{1}{p}\Omega_\wp^n \left(\frac{d}{dz}\right)^n \log\left(\mathcal{R}_\lambda(\Phi(z,\mathcal{L}))^p \Big/ \mathcal{R}_\lambda(\Phi(\psi_E(\wp)z,\mathcal{L}))\right)\Big|_{z=0}$$

$$= \Omega_{\mathfrak{p}}^{n}\left(1-\frac{\psi_E(\mathfrak{p})^n}{N\mathfrak{p}}\right)\left(\frac{d}{dz}\right)^n \log \mathcal{R}_\lambda\left(\Phi(z,\mathcal{L})\right)\Big|_{z=0}.$$

$$= \Omega_{\mathfrak{p}}^{n}\left(1-\frac{\psi_E(\mathfrak{p})^n}{N\mathfrak{p}}\right)(-1)^{n-1}(n-1)!\, f^n \Omega_\infty^{-n}\left(N\lambda-\psi_E((\lambda))^n\right) L_F(\overline{\psi}_E^{\,n}, n) \quad (n \geqslant 1).$$

Hence we have proven:–

<u>Theorem</u>. Assume $\lambda \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ and $(\lambda, 6F\mathfrak{p}) = (F, \mathfrak{p}\mathfrak{p}^*) = 1$ and $p > 2$. Then, for all integers $n \geqslant 1$, we have

$$\mathfrak{p}^n \int_G \chi_{\mathfrak{p}}^n \, d\mu_\lambda = (-1)^{n-1}(n-1)!\, f^n \Omega_\infty^{-n}\left(N\lambda-\psi_E((\lambda))^n\right)\left(1-\frac{\psi_E(\mathfrak{p})^n}{N\mathfrak{p}}\right) L_F(\overline{\psi}_E^{\,n}, n).$$

<u>Getting rid of extraneous terms</u>. $p > 2$

$\chi_{\mathfrak{p}} : G \xrightarrow{\sim} \mathbb{Z}_p^\times \qquad \mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$.

So we have the corresponding decomposition $G = \Delta \times \Gamma$.

$\theta_{\mathfrak{p}} = \chi_{\mathfrak{p}} \circ \mathrm{pr}_\Delta$, $\kappa_{\mathfrak{p}} = \chi_{\mathfrak{p}} \circ \mathrm{pr}_\Gamma$.

$$e_{\theta_{\mathfrak{p}}^i} = \frac{1}{p-1}\sum_{\delta \in \Delta} \theta_{\mathfrak{p}}^{-i}(\delta)\delta \in \qquad \theta e_{\theta^i} =$$

Then we have:–

(i) $\Lambda_{\mathcal{G}}(G) = \bigoplus_{i=0}^{p-2} e_{\theta_{\mathfrak{p}}^i}\Lambda_{\mathcal{G}}(G) \xrightarrow{\sim} \bigoplus_{i=0}^{p-2} \Lambda_{\mathcal{G}}(\Gamma)$

(ii). $\xi \in \Lambda_{\mathcal{G}}(G)$ is a unit in $\Lambda_{\mathcal{G}}(G) \iff \chi_{\mathfrak{p}}^n(\xi) \in \mathcal{G}^\times$ for all $n \geqslant 1$. Assume $(F, \mathfrak{p}\mathfrak{p}^*) = 1$.

<u>Lemma</u>. There exists λ in $\mathcal{O}_K \setminus \mathcal{O}_K^\times$ with $(\lambda, 6F\mathfrak{p}) = 1$ such that there exists $\alpha_\lambda \in \Lambda_{\mathcal{G}}(G)^\times$ such that

$$\int \chi_{\mathfrak{p}}^n \, d\alpha_\lambda = (-1)^{n-1} f^n \left(N\lambda - \psi_E((\lambda))^n\right) \text{ for all } n \geqslant 1.$$

<u>Proof</u>. For $z \in \mathcal{O}_{\mathfrak{p}}^{\times}$, let σ_z be the unique element of G such that $\chi_{\mathfrak{p}}(\sigma_z) = z$. Choose λ in $\mathcal{O}_K \setminus \mathcal{O}_K^{\times}$ such that

$$\lambda \equiv 1 \bmod 2F, \quad \lambda \equiv 1 \bmod \mathfrak{p}, \quad \lambda \equiv 2 \bmod \mathfrak{p}^*$$

and also $(\lambda, 3) = 1$. We then define

$$\alpha_\lambda = -\sigma_{-f}(N\lambda - \sigma_\lambda).$$

We then note that, when $n \geqslant 1$, we have

$$*) \int_G \chi_{\mathfrak{p}}^n \, d\alpha_\lambda = (-1)^{n-1} f^n (N\lambda - \lambda^n).$$

But $\psi_E((\lambda)) = \lambda^n$ since $\lambda \equiv 1 \bmod F$. Hence the last thing we have to check that $(*)$ is a unit in $\mathcal{O}_{\mathfrak{p}}$ for all $n \geqslant 0$. But this is clear, since $(F, \mathfrak{p}) = 1$, and also $N\lambda - \lambda^n = \lambda(\bar{\lambda} - \lambda^{n-1})$. But $\bar{\lambda} \equiv 2 \bmod \mathfrak{p}$, and $\lambda^{n-1} \equiv 1 \bmod \mathfrak{p}$, so that the right hand side of $(*)$ is a unit for all $n \geqslant 1$.

<u>Conclusion</u>. Assume $(F, \mathfrak{p}\mathfrak{p}^*) = 1$ and $p > 2$. Then there exists a measure β_E on G such that, for all $n \geqslant 1$, we have

$$\Omega_{\mathfrak{p}}^{-n} \int_G \chi_{\mathfrak{p}}^n \, d\beta_E = (n-1)! \, \Omega_\infty^{-n} \left(1 - \frac{\psi_E(\mathfrak{p})^n}{N\mathfrak{p}}\right) \cdot L_F(\psi_E^{-n}, n).$$

<u>Proof</u>. Take $\beta_E = \mu_\lambda / \alpha_\lambda$.

<u>Remark</u>. If $(n, w) = 1$, where $w = \#(\mu_K)$, then $\overline{\psi}_E^{\,n}$ has conductor exactly n. When w divides n, $\overline{\psi}_E^{\,n}$ has conductor 1. In general we have to modify the measure β_E to get primitive L-values, and this leads one to a pseudo-measure

<u>Branches of a measure</u>. Take any $\mu \in \Lambda_{\mathcal{I}}(G)$. For each $i \bmod (p-1)$, we define

<u>Defn</u>. $$L_{\mu,i}(s) = \int_G \kappa_{\mathfrak{p}}^{s}\, \Theta_{\mathfrak{p}}^{i}\, d\mu \qquad (s \in \mathbb{Z}_p).$$

These $p-1$ functions of s are the branches of the measure μ

<u>Remark</u>. If $n \in \mathbb{Z}$ and $n \equiv i \bmod (p-1)$, we have

$$L_{\mu,i}(n) = \int_G \chi_{\mathfrak{p}}^{n}\, d\mu.$$

<u>Lemma</u>. For each $i \bmod (p-1)$, there exists $G_{\mu,i}(T)$ in $\mathcal{I}[[T]]$ such that

$$L_{\mu,i}(s) = G_{\mu,i}(u^s - 1);$$

here u is any fixed topological generator of $1 + p\mathbb{Z}_p$, e.g. $u = 1 + p$.

<u>Proof</u>. $\kappa_{\mathfrak{p}} : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$. Pick a topological generator γ of $\Gamma \iff u = \kappa_{\mathfrak{p}}(\gamma)$ is a topological generator of $1 + p\mathbb{Z}_p$

Define $\tau(\sigma) : G \longrightarrow \mathbb{Z}_p$ by $\mu\tau_\Gamma(\sigma) = \gamma^{\tau(\sigma)}$

Hence

$$\kappa_{\mathfrak{p}}(\sigma)^s = \kappa_{\mathfrak{p}}\left(\gamma^{s\tau(\sigma)}\right) = u^{s\tau(\sigma)}. \quad \text{Hence}$$

$$L_{\mu,i}(s) = \int_G u^{s\tau(\sigma)}\, \Theta_{\mathfrak{p}}^{i}\, d\mu$$

But now we have the expansion :–

$$u^{s\tau(\sigma)} = \left(u^s - 1 + 1\right)^{\tau(\sigma)} = \sum_{n=0}^{\infty} \left(u^s - 1\right)^n \binom{\tau(\sigma)}{n}.$$

Hence, as the convergence is uniform, we get

$$L_{\mu,i}(s) = \sum_{n=0}^{\infty} \left(u^s - 1\right)^n \int_G \Theta_{\mathfrak{p}}^i(\sigma) \binom{\tau(\sigma)}{n} d\mu .$$

Also $\left| \int_G \Theta_{\mathfrak{p}}^i(\sigma) \binom{\tau(\sigma)}{n} d\mu \right|_p \leqslant \left\| \Theta_{\mathfrak{p}}^i(\sigma) \binom{\tau(\sigma)}{n} \right\| \leqslant 1.$

Hence we define $G_{\mu,i}(T) = \sum_{n=0}^{\infty} a_n T^n$, where $a_n = \int_G \Theta_{\mathfrak{p}}^i(\sigma) \binom{\tau(\sigma)}{n} d\mu$

<u>Corollary</u>. Assume Ω_∞ and $\Omega_{\mathfrak{p}}$ are fixed. Then there exists a unique power series $H_{\mathfrak{p}}(T)$ in $\mathcal{I}[[T]]$ such that, for all integers $n \geqslant 1$ with $n \equiv 1 \bmod (p-1)$, we have

$$\Omega_{\mathfrak{p}}^{-n} H_{\mathfrak{p}}\left(\left(1+p\right)^n - 1\right) = \Omega_\infty^{-n} (n-1)!\, L(\overline{\psi}_E^n, n) \left(1 - \frac{\psi_E^n(\mathfrak{p})}{N\mathfrak{p}}\right).$$

<u>Proof</u>. Take the branch with $i = 1$ for the measure β_E, to get existence. Uniqueness follows from Weierstrass prep. theorem.

<u>Ex</u>. $E : y^2 = x^3 - 82x$, $F = 8.41\,\mathbb{Z}[i]$.
Conductor $N(E) = 2^8 \cdot 41^2$, $g_E = 3$, $Ш(E/\mathbb{Q}) = (0)$ by BSD
$E(\mathbb{Q})$ mod torsion is generated by $(-1, 9)$, $(-8, 12)$, $(-9, 3)$.
$L(E/\mathbb{Q}, s)$ has a zero at $s = 1$ of order 3 by Gross-Zagier.
$p \equiv 1 \bmod 4$ & $p \neq 41$.

$$L_{\mathfrak{p}}(E, s) = L_{\beta_E, 1}(s) = H_{\mathfrak{p}}\left(\left(1+p\right)^s - 1\right).$$

<u>Theorem</u>. $L_{\mathfrak{p}}(E, s)$ has a zero at $s = 1$ of order $\geqslant 3$.

<u>Last time</u>. E/K, $\mathrm{End}_K(E) = \mathcal{O}_K$, $p > 2$,
$p\,\mathcal{O}_K = \wp\wp^*$, $\wp \neq \wp^*$, $(F, \wp\wp^*) = 1$.

We constructed the $\wp$-adic L-function of E/K:-

$$L_\wp(E, s) = L_{\beta_E, 1}(s) = H_\wp\left((1+p)^s - 1\right),$$

where $H_\wp(T) \in \mathcal{I}[[T]]$. We have the interpolation property: for all integers $n \geq 1$ with $n \equiv 1 \bmod (p-1)$

$$\Omega_\wp^{-n} H_\wp\left((1+p)^n - 1\right) = \Omega_\infty^{-n}\,(n-1)!\,L(\overline{\Psi}_E^n, n)\left(1 - \frac{\Psi_E^n(\wp)}{N\wp}\right).$$

So this gives values at $n = 1, p, 2p-1, \ldots$

<u>Connection with Galois cohomology</u>.

$F_\infty = K(E_{\wp^\infty})$, $G = \mathrm{Gal}(F_\infty/K) \xrightarrow{\sim} \mathcal{O}_\wp^\times$ and $G = \Delta \times \Gamma$.

<u>Selmer group</u>.

M - any algebraic extension of K, possibly infinite
w - a non-archimedean place of M.

<u>Defn</u>. M_w = union of completions at w of finite extension of K contained in M

<u>Remark</u>. This way M_w is an <u>algebraic</u> extension of K.

$E_{\wp^\infty}$ - $\mathrm{Gal}(\overline{K}/K)$-module

$E(\overline{M}_w) = K(\overline{K}_w)$ is a $\mathrm{Gal}(\overline{K}_w/K_w)$-module.

<u>Defn</u>.

$$\mathrm{Sel}_\wp(E/M) = \mathrm{Ker}\Big(H^1(\mathrm{Gal}(\overline{M}/M), E_{\wp^\infty}) \longrightarrow \prod_w H^1(\mathrm{Gal}(\overline{M}_w/M_w), E(\overline{M}_w))\Big).$$

Using Kummer theory on E, it is easy to see that we have an exact sequence

$$0 \to E(M) \otimes_{\mathcal{O}_K} K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}} \to \mathrm{Sel}_{\mathfrak{p}}(E/M) \to Ш(E/M)(\mathfrak{p}) \to 0.$$

<u>Key remark</u>. If M is Galois over K, then $\mathrm{Gal}(M/K)$ acts on $\mathrm{Sel}_{\mathfrak{p}}(E/M)$ (since it acts on ~~Gal(K∞)~~ $H^1(\mathrm{Gal}(\overline{M}/M), E_{\mathfrak{p}^\infty})$). This is a left action!

We also need its Pontrjagin dual :-

<u>Defn</u>. $X_{\mathfrak{p}}(E/M) = \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(\mathrm{Sel}_{\mathfrak{p}}(E/M), K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$.

We define an action of $\mathrm{Gal}(M/K)$ via :-

$(\sigma f)(x) = f(\sigma^{-1}x)$. This makes again a left action

<u>Underlying idea</u>. For certain infinite extensions M/K, the $\mathrm{Gal}(M/K)$-structure of $X_{\mathfrak{p}}(E/M)$ is related to special values of the complex L-functions.

How do we make this precise?

<u>Defn</u>. K_∞ = fixed field of Δ.

Thus $\mathrm{Gal}(K_\infty/K) = \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p$.

<u>Fact</u>. K_∞/K is the unique $\mathbb{Z}_p$-extension of K unramified outside S_0.

<u>Remark on $\Lambda(\mathcal{G})$-action</u>. Here $\mathcal{G} = \mathrm{Gal}(M/K)$. Let X be any compact left $\mathcal{G}$-module. Then

$$X = \varprojlim_{U} X_U ,$$

where U runs over the open normal subgroups of $\mathcal{G}$. Suppose now that X is also a $\mathbb{Z}_p$-module. Then X_U is a module over $\mathbb{Z}_p[\mathcal{G}/U]$. We define

Defn. $\Lambda(\mathcal{G}) = \varprojlim_{U} \mathbb{Z}_p[\mathcal{G}/U]$ = Iwasawa algebra of $\mathcal{G}$.

Then it is clear that X inherits a structure as a left $\Lambda(\mathcal{G})$-module.

Apply this to $X_{\mathfrak{p}}(E/K_\infty)$. It is then a module over $\Lambda(\Gamma)$. It is not difficult to see it is a finitely generated $\Lambda(\Gamma)$-module.

<u>Theorem</u>. $X_{\mathfrak{p}}(E/K_\infty)$ is a torsion $\Lambda(\Gamma)$-module.

This lies much deeper. Then we have, by the structure theory for finitely generated torsion $\Lambda(\Gamma)$-modules, an exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^{r} \Lambda(\Gamma)/f_i\Lambda(\Gamma) \longrightarrow X_{\mathfrak{p}}(E/K_\infty) \to D \to 0,$$

where D is some finite $\Lambda(\Gamma)$-module, and

$f_1, \dots, f_T$ are non-zero elements of $\Lambda(\Gamma)$. Let us define $g = \prod_{i=1}^{T} f_i$. Then $g\,\Lambda(\Gamma)$ is called the characteristic ideal of $X_{\mathfrak{p}}(E/K_\infty)$. Recall that γ is the unique topological generator of Γ such that $K_{\mathfrak{p}}(\gamma) = 1 + p$. We then have an isomorphism of rings

$$j : \Lambda(\Gamma) \xrightarrow{\sim} \mathbb{Z}_p[[T]]$$

defined by $j(\gamma) = 1 + T$.

<u>Defn</u>. $B_{\mathfrak{p}}(T) = j(g)$.

<u>Theorem</u> (One variable main conjecture).

$$H_{\mathfrak{p}}\big((1+p)(1+T)-1\big)\mathcal{O}[[T]] = B_{\mathfrak{p}}(T)\mathcal{O}[[T]].$$

Discuss consequences when there is time.

$H_{\mathfrak{p}}\big((1+p)(1+T)-1\big)$ has a zero at $T=0$ of order $\geqslant n_{E/K} + t_{E,\mathfrak{p}}$, where

$n_{E/K} = \mathcal{O}_K$-rank of $E(K)$

$t_{E,\mathfrak{p}} = \mathbb{Z}_p$-corank of $Ш(E/K)(\mathfrak{p})$.