P-ADIC MODULAR FORMS

ASVIN GOTHANDARAMAN

CONTENTS

1. INTRODUCTION

This note covers the basic theory of p-adic modular forms. I will define the notion of a p-adic modular form, define a corresponding weight and use these ideas to construct the Kubto-Leopoldt p-adic zeta function.

First however, I will need to cover the basic theory of modular forms with Fourier coefficients in $\mathbb{F}_p$. I will also prove some congruences as an application and show a connection to the moduli theoretic interpretation of modular forms.

To get off the ground, I will need to recall some classical results about modular forms in characteristic 0. There will be no proofs in this section:

2. MODULAR FORMS OVER $\mathbb{C}$

Recall that modular forms are functions from the upper half plane to the complex numbers $f : \mathbb{H} \longrightarrow \mathbb{C}$ that satisfy a functional equation:

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z), \quad ad-bc = 1, a, b, c, d \in \mathbb{Z}.$$

Date:

The k is called the weight of f and is an even non-negative integer. They also satisfy a growth condition that can be phrased in the following way:

Note that $f(z+1) = f(z)$ and therefore, setting $q = e^{2\pi iz}$, there is a Fourier expansion $f = \sum_n a_n q^n$. We will demand that $q \geq 0$. This is equivalent to saying the function has a well defined value as we go to infinity along the imaginary axis.

From the definition, it immediately follows that the space of modular forms of weight k is a vector space over $\mathbb{C}$. It is denoted by M_k. It is also clear that the product of modular forms of weight k, l produces a modular form of weight $k+l$. Thus, we can define a graded algebra:

$$M = \bigoplus_{k \geq 0} M_k.$$

Using the Riemann-Roch and an interpretation of modular forms as sections of a line bundle on a curve, one can prove that M_k is finite dimensional. Now, let us see some examples of modular forms. Our first example is a sequence of modular forms called Eisenstein series indexed by the weight $k \geq 4$ and even:

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n).$$

The B_k are Bernoulli numbers defined by the following generating function:

$$\frac{t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}$$

and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ is the standard divisor sum function.

We will see soon that while E_2 is not a modular form, it satisfies a similar functional equation and will be important soon. We will make particular use of the following three functions:

$$P = E_2 = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n$$

$$Q = E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$

$$R = E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n$$

We will sometimes think of Q, R as transcendental variables and other times as the modular forms. This is not too bad an abuse of notation since E_4, E_6 are algebraically independent even over $\mathbb{C}$. Hopefully, it will be clear from the context.

Our second example of a modular form is the modular discriminant function:

$$\Delta = q[\prod_{n \geq 1} (1 - q^n)]^{24} = \sum_{n \geq 0} \tau(n) q^n.$$

Note that $\tau(0) = 0, \tau(1) = 1$. By calculating the dimension of the space of modular forms of weight 12, one can prove that $1728\Delta = E_4^3 - E_6^2$.

Since the leading non-zero term is 1 and E_4, E_6, Δ have fourier coefficients in $\mathbb{Z}$, one can prove that any modular form f can be written as a polynomial $F(E_4, E_6, \Delta)$ and further, if $f \in S[[q]]$ for some ring $S \subset \mathbb{C}$, then F is also a polynomial with coefficients in S.

Let us define M_S to be the subring of M consisting of the modular forms that have coefficients in S. Then, the above shows that we have an isomorphism

$$S[Q, R, \Delta]/(1728\Delta = Q^3 - R^2) \longrightarrow M_S$$

where the map is the obvious one. We also see that if 6 is invertible in S, then the polynomial ring on the left is simply $S[Q, R]$.

Finally, we will need to define a derivation on the space of modular forms. First, we define an operator $\theta(f) = qf'(q)$ where we differentiate formally with respect to q. In other words, it sends the Fourier coefficients a_n to na_n.

This is clearly a derivation but unfortunately, $\theta(f)$ will usually not be a modular form. We modify it so that we do get a modular form in the following way:

$$\partial(f) = 12\theta(f) - kPf.$$

It is a simple computation to prove that ∂ is a derivation. Showing that is a modular form turns out to be equivalent to proving the functional equation for $P = E_2$. The easiest way to figure this out is to show first that P is the logarithmic derivative of Δ (using the product representation for Δ) and use the functional equation of Δ to derive the corresponding one for P.

3. Modular forms with coefficients in $\mathbb{F}_p$

Let $S = \mathbb{Z}_{(p)}$ and for the moment, assume that $p \geq 5$. Then, in the first section, we showed that $S[Q, R] \cong M_S$ since Δ is an integral combination of Q, R in $\mathbb{F}_p$. Let us now define $\overline{M}$ to be the subring of $\mathbb{F}_p$ consisting of power series that are the reduction of elements in M_S. We can consider the following commutative diagram:

$$\begin{array}{ccc} Z_{(p)}[Q, R] & \xrightarrow{\cong} & M_S \\ \downarrow & & \downarrow \\ \mathbb{F}_p[Q, R] & \dashrightarrow & \overline{M} \end{array}$$

The top vertical map corresponds to reduction maps while the horizontal maps evaluate Q, R to E_4, E_6. The bottom vertical map is induced by the rest of the diagram. That is, it sends $Q, R \longrightarrow \overline{Q}, \overline{R} \in \overline{M} \subset \mathbb{F}_p[[q]]$.

Recall that in M, E_4 and E_6 have weight 4 and 6 respectively. We will define a grading on the polynomial rings so that Q, R have weights $4, 6$ respectively. Then, in characteristic 0, modular forms correspond precisely to homogeneous polynomials in Q, R and the maps are maps of graded algebras that preserve the grading.

We would like to understand the bottom horizontal arrow better but first, let us establish some notation. Let $F(Q, R)$ be the polynomial corresponding to a modular form f in characteristic 0. Then, by $\overline{F}(Q, R)$, we denote the reduction of the polynomial F in $\mathbb{F}_p[Q, R]$ and by $\overline{F}(\overline{Q}, \overline{R})$, we mean the corresponding modular form in $\overline{M}$.

Now, we define $A(Q, R)$ to be the polynomial that maps to E_{p-1} and $B(Q, R)$ to be the polynomial mapping to E_{p+1}. These are polynomials in characteristic 0 and they are homogeneous of weight $p - 1$ and $p + 1$ respectively.

3.1. **Computing a presentation of $\overline{M}$:** Since the dotted arrow is surjective, it simply remains to find the kernel. Let this kernel be the ideal $I \subset \mathbb{F}_p[Q,R]$. Note that since the image of the dotted map is an integral domain, I has to be a prime ideal.

Let us now guess an element in the kernel. The main tool we use will be the congruences of Von Staudt-Clausen and Kummer regarding Bernoulli numbers.

Theorem 1 (Von-Staudt, Clausen and Kummer)**.** *Let p be a prime number. Then the following statements hold:*

- *if $p-1|r$, then $pB_r/2r$ is a p-adic integer.*
- *if $p-1 \nmid r$, then $B_r/2r$ is a p-adic integer and modulo p, it depends only on $r \pmod{p-1}$.*

Corollary 2. *Thus, we see that in $\overline{M}$:*

$$\overline{A}(\overline{Q},\overline{R}) = \overline{E}_{p-1} \equiv 1 \pmod{p}$$

and furthermore

$$\overline{B}(\overline{Q},\overline{R}) \equiv \overline{P} \pmod{p}.$$

In particular, P is a modular form mod p! This will be crucial in the theory. Also, $A(Q,R)-1$ is in I.

Since $p \geq 5$, one can see that one of $\overline{Q}, \overline{R} \notin \mathbb{F}_p$ and so the image is not a field. This shows that I is a prime ideal of height exactly 1.

Therefore, if we can show that $\overline{A}-1$ is irreducible, we will have shown that $I = (\overline{A}-1)$. This is what we now proceed to do:

Theorem 3. *For $\overline{A}, \overline{B}$, elements of $\mathbb{F}_p[Q,R]$ as defined above:*

(1) $\partial\overline{A} = B$ and $\partial\overline{B} = -\overline{QA}$.
(2) $\overline{A}$ has no repeated factors and is co-prime to $\overline{B}$.
(3) $\overline{A}-1$ is absolutely irreducible.

Proof. This theorem is a statement purely about $\mathbb{F}_p[Q,R]$ as an abstract algebra and the proof is mostly commutative algebra. The only input from modular form theory will be in proving the first step:

(1) By the above corollary, we see that $\theta\overline{A}(\overline{Q},\overline{R}) = 0$ in $\overline{M}$. Now, consider $F = \partial\overline{A} - (p-1)\overline{B}$ in $\mathbb{F}_p[Q,R]$. This is homogeneous of weight $p+1$. Under the dotted arrow, F maps to $\partial\overline{A} - k\overline{B}$ which is equal to $\partial\overline{A}(\overline{Q},\overline{R}) - k\overline{PA}(\overline{Q},\overline{R}) = \theta\overline{E}_{p-1} = 0$ by the corollary.

That is, we have shown that $\partial A(Q,R) - (p-1)B(Q,R) = \partial E_{p-1} - E_{p+1}$ is a p-integral modular form of weight $p+1$ that reduces to 0 mod p. As such, it must be a polynomial of Q,R with coefficients in $p\mathbb{Z}_{(p)}$ and hence $F = 0$ in $\mathbb{F}_p[Q,R]$. That is, $\partial\overline{A} = \overline{B}$ as required.

The second part of (1) follows exactly the same proof by considering $F = \partial\overline{B} - \overline{QA}$ in $\mathbb{F}_p[Q,R]$ and using that $\partial P = Q$ in characteristic 0.

(2) Recall that $\overline{A}$ is homogeneous of degree $p-1$ in Q,R. Therefore, any factor of it (over $\overline{\mathbb{F}_p}$) is of the form $(Q^3 - cR^2)$ for some $c \in \overline{\mathbb{F}_p}$. Note that $c \neq 1$ since under the dotted arrow, $\overline{A}$ has an expansion with non zero constant term while $Q^3 - R^2$ has no constant term. Let us now assume for contradiction that:

$$\overline{A}(Q.R) = (Q^3 - cR^2)^n X$$

where $n \geq 2$ and X is coprime to $(Q^3 - cR^2)$. The standard way one gains information about repeated factors is by comparing a polynomial to it's derivatives but here, it is more

useful to use the derivation ∂. A simple computation shows us that:

$$\overline{B} = \partial\overline{A} = (Q^3 - cR^2)^{n-1}Y \text{and } -Q\overline{A} = \partial^2\overline{A} = (Q^3 - cR^2)^{n-2}Z$$

where Y, Z are coprime to $(Q^3 - cR^2)$ (since $c \neq 1$). However, this is clearly a contradiction and so $n = 1$. This also shows that $\overline{A}$ is coprime to $\overline{B}$.

(3) Assume for contradiction that $\overline{A} - 1$ is reducible (over $\overline{\mathbb{F}_p}$) and we have a non trivial absolutely irreducible factor of $\overline{A} - 1$:

$$\varphi(Q, R) = \varphi_n(Q, R) + \varphi_{n-1}(Q, R) + \dots$$

where the φ_k are the degree k homogeneous pieces. Let c be a primitive root of $p - 1$ in $\mathbb{F}_p$. Observe that $\overline{A}(c^4Q, c^6R) = c^{p-1}\overline{A}(Q, R) = \overline{A}(Q, R)$ by homogeneity.

Therefore, $\varphi(c^4Q, c^6R)$ is also a factor of $\overline{A} - 1$. Since $Q \longrightarrow c^4Q, R \longrightarrow c^6R$ is an automorphism of $\mathbb{F}_p[Q, R]$ and $\varphi(Q, R)$ is absolutely irreducible, we see that the same is true of $\varphi(c^4Q, c^4R)$ and $\varphi(Q, R)\varphi(c^4Q, c^6R)$ divides $\overline{A} - 1$. On comparing the highest weight pieces, we see that $\varphi_n(Q, R)\varphi_n(c^4Q, c^6R) = c^n\varphi_n^2(Q, R)$ divides $\overline{A}$. However, this contradicts part (2).

□

Thus, we have shown that $I = (\overline{A} - 1)$ and $\overline{M} \cong \mathbb{F}_p[Q, R]/(\overline{A} - 1)$ as $\mathbb{F}_p-$algebras. In fact there is an induced grading by the group $\mathbb{Z}/(p - 1)$ on the algebras such that the modular forms mod p are precisely the homogeneous elements.

3.2. $\overline{M}$ **as a graded algebra:** Consider M_k to be the space of modular forms of weight k as a submodule of $\mathbb{Z}_{(p)}[Q, R]$. Then, denote by $\overline{M}_k$ the reduction to $\mathbb{F}_p[Q, R]$.

Note that multiplication by $\overline{A}(Q, R)$ is an injective map from $\overline{M}_k \longrightarrow \overline{M}_{k+p-1}$. We will think of this as an inclusion and define:

$$\overline{M}_\alpha = \bigcup_{k\in\alpha} \overline{M}_k \text{ for } \alpha \in \mathbb{Z}/(p - 1).$$

Clearly, $\mathbb{F}_p[Q, R] = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)} \overline{M}_\alpha$. In fact, I claim that they are disjoint even after we take the quotient:

Theorem 4. *We have the decomposition into homogeneous pieces:*

$$\mathbb{F}_p[Q, R]/(\overline{A} - 1) = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)} \overline{M}_\alpha.$$

Proof. Suppose not. Then there exist f, g such that $f(Q, R) = g(Q, R) \pmod{\overline{A} - 1}$ where $f \in \overline{M}_\alpha$ and $g \in \overline{M}_\beta$ and $\alpha \neq \beta$. By multiplying f, g by $\overline{A}$, we can further assume that f, g are homogeneous of weight k, l.

That is, $f(Q, R) = g(Q, R) + (\overline{A} - 1)h(Q, R)$ for some $h(Q, R) \in \mathbb{F}_p[Q, R]$. Let $h(Q, R) = \sum_{\gamma\in\mathbb{Z}/(p-1)} h_\gamma(Q, R)$ where $h_\gamma(Q, R)$ is a sum of polynomials in $\overline{M}_\gamma$.

From the direct sum decomposition of $\mathbb{F}_p[Q, R]$, we see immediately that $(\overline{A} - 1)h_\alpha = f$, $(\overline{A} - 1)h_\beta = g$ and $h_\gamma = 0$ otherwise but this clearly contradicts the assumption that f, g are homogeneous.

□

This theorem is particularly interesting because it lets us assign weights to modular forms with coefficients in $\mathbb{F}_p$ (by pushing the grading through the isomorphism established in the previous section: $\overline{M} \cong \mathbb{F}_p[Q,R]/(\overline{A}-1)$. The modular forms in $\overline{M}$ are precisely the homogeneous elements, exactly as i characteristic 0.

In fact, by defining a slightly finer invariant, we will see that our work so far immediately gives us several congruences on the coefficients of modular forms.

3.3. **Congruences on the coefficients of modular forms:** Given $f \in \overline{M}_\alpha$, we know by the above that is the reduction of some characteristic 0 modular form g. In fact, there will be several such choices and all of them will differ by multiples of $A(Q,R) = E_{p-1}$ as can be easily verified. Thus, we can define for $f \in \overline{M}_\alpha$:

$$\omega(f) = \min\{\deg(g) : g \in M_S \text{ such that } \overline{g} = f\}.$$

Equivalently, it is the unique modular form in characteristic zero that reduces to f and is not divisible by $A(Q,R)$ (thinking of them as elements in $\mathbb{Z}_{(p)}[Q,R]$).

How is this useful? Well, take $p = 7$. Recall that the differential operator θ takes $\mathbb{F}_p$ modular forms to $\mathbb{F}_p$ modular forms. We would like to study how ω interacts with θ:

Theorem 5. *For $f \in \overline{M}_\alpha$, let $\omega(f) = k$. Recall that $k \pmod{p-1} = \alpha$. The following is true:*

$$\omega(\theta(f)) \leq \omega(f) + p + 1$$

and we have equality precisely when $\alpha \neq 0$ or equivalently, $k \neq 0 \pmod{p-1}$.

Proof. Let g be the characteristic 0 modular form of weight $\omega(f)$ such that $\overline{g} = f$. Then, by the definition of θ, we have:

$$\theta(f) = \overline{\theta(g)} = \overline{A\partial(g) + kBg}$$

since A, B reduce to $1, P$ respectively. However, $A\partial(g) + kBg$ is a modular form of weight $k+p+1$ and so, $\omega(\theta(f)) \leq k+p+1$.

Moreover, suppose $p|k$. Then $\theta(f) = \overline{A\partial(g)} = \overline{\partial(g)}$. This shows that $\omega(\theta(f)) \leq k+2$.

Conversely, if $\omega(f) < k+p+1$, then $A(Q,R)|A(Q,R)\partial(g) + kB(Q,R)g$. By assumption $A(Q,R)$ does not divide g and since $A(Q,R)$ is irreducible (by Theorem 3), we have that $A(Q,R)|B(Q,R)$. But this contradicts Theorem 3 and we are done. □

This immediately lets us prove congruences. Take $p = 5$. Consider $f = \overline{R} = \overline{E}_6$. Certainly, $\omega(f) = 6$ and since $5 \nmid 6$, we have $\omega(\theta(f)) = 6+5+1 = 12$.

That is, $\theta(f)$ is equal to the reduction of some modular form of weight 12. Since $\theta(f)$ is always a cusp form (ie, it has no constant term), we see that $\theta(f)$ is equal to the reduction of some *cusp* form. However, there the cusp forms of weight 12 are of dimension 1, generated by Δ and we have shown that $\theta(E_{p-1} = \lambda\Delta \pmod 5$. Comparing leading coefficients, we see that $\lambda = 1$ and we have shown the congruence:

$$n\sigma_5(n) \equiv \tau(n) \pmod 5.$$

where $\tau(n)$ is the Ramanujan tau function (the Fourier coefficients of Δ). Exactly along the same lines, we can also show that:

$$n\sigma_3(n) \equiv \tau(n) \pmod 7.$$

We will also find use for ω while studying p-adic modular forms. Also useful then will be the following section on the smoothness of $\overline{M}$ as a curve over $\mathbb{F}_p$.

3.4. $\overline{M}$ **as a smooth algebra:** It is clear from the description of $\overline{M} = \mathbb{F}_p[Q,R]/(\overline{A}(Q,R)-1)$ that it is a planar curve. Since $\overline{A}(Q,R)-1$ is a prime ideal, this is an irreducible curve. In fact, it is even smooth over $\mathbb{F}_p$. (Note that this is equivalent to being regular or normal for curves over a field).

The proof follows from general considerations of commutative algebra but will prove to be quite useful in the theory of p-adic modular forms. Since $\overline{A}(Q,R)$ is homogeneous of degree $p-1$ (where $\deg Q = 4, \deg R = 6$), the following lemma is clearly sufficient to show smoothness:

Lemma 6. *Let $S = k[x,y]/(f(x,y)-1)$ be a one dimensional algebra over the field k. Suppose that under the grading $\deg x = k, \deg y = l$, $f(x,y)$ is homogeneous of degree d. Then S is smooth over k.*

Proof. Suppose not. Then there exist points $\alpha, \beta \in \overline{k}$ such that $f(\alpha,\beta) = 1$ and $f_x(\alpha,\beta) = f_y(\alpha,\beta) = 0$. Here f_x, f_y stand for the partial derivatives of f with respect to x and y respectively. (This follows from the Jacobian criterion for smoothness).

Consider the operator on $k[x,y]$:

$$\partial(h(x,y)) = kxh_x + yh_y.$$

As a linear combination of derivations, it is a derivation on $k[x,y]$. Further, on homogeneous polynomials $g(x,y)$ of degree d, it acts by $\partial(g(x,y)) = dg(x,y)$. This can be verified on monomials of the form $x^a y^b$, $ka + lb = d$ quite easily. Then, simply note that all homogeneous polynomials are sums of monomials of this form.

Since ∂ is a linear combination of f_x, f_y, we know that $\partial(f)(\alpha,\beta) = 0$. However, by definition, $\partial(f) = df$ and this contradicts our assumption that $f(\alpha,\beta) = 1$ and completes the proof.

□

4. Moduli theoretic interpretation of $\mathbb{F}_p$ modular forms.

Characteristic modular forms (over $\mathbb{C}$ for instance) have moduli theoretic interpretations in terms of function on Elliptic curves. There is a corresponding interpretation for $\mathbb{F}_p$ modular forms and in fact, we can provide a concrete interpretation of $\overline{A}(Q,R)$ as above. To begin with, let us recall the classical moduli theoretic story:

4.1. **Modular forms as functions on Elliptic Curves.** :

Recall that modular forms over $\mathbb{C}$ are functions on the upper half plane satisfying certain functorial and growth criterion. However, this definition does not generalize well.

Instead, we use that points of the upper half plane parametrize pairs (E,ω) up to isomorphism where E is an Elliptic curve over $\mathbb{C}$ and ω is a differential form on E. Explicitly, the correspondence is as follows:

$$\tau \in \mathbb{H} \longleftrightarrow (\mathbb{C}/(2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}), dz)$$

where z is the parameter on $\mathbb{C}$. The $2\pi i$ is simply for cosmetic reasons. We can then define modular forms as functions to $\mathbb{C}$ on pairs (E,ω) (up to isomorphism) as above subject to certain conditions:

One can verify quite easily that if τ corresponds to E,ω, then $(a\tau+b)/(c\tau+d)$ corresponds to $E, \omega/c\tau+d$. Therefore, the functional equation of a modular forms of weight k translates

to the following:

$$f(E, \lambda\omega) = \lambda^{-k} f(E, \omega).$$

Similarly, we require also some conditions on the "growth of f in families" corresponding to holomorphicity. Since we will not need it, I will not define it here.

This interpretation of modular forms are called as Katz' modular forms. Note that the above definition of a modular form is truly independent of $\mathbb{C}$ and we will make the same definition for any ring R. In particular, for $R = F_p$, modular forms are functions (to $\overline{\mathbb{F}_p}$) on pairs (E, ω) of an elliptic curve over $\overline{\mathbb{F}_p}$ and a differential form ω on it (up to isomorphism).

4.2. q **- expansions of Katz' modular forms:** One might naturally wonder whether we can interpret the Fourier series of modular forms in this setting. This is possible but is highly technical and I will only provide a sketch of how to do it. A rigorous treatment involves techniques from rigid geometry but we can go quite far taking a few things on faith.

A natural approach would be try and uniformize curves as one might do over $\mathbb{C}$. However, the standard set up does not generalize easily. Instead, we do the following:

First, let us treat the complex case. Usually, one uniformizes an elliptic curve $E_\tau/\mathbb{C}$ by means of a lattice $\Lambda = (2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}) \subset \mathbb{C}$ such that there is an analytic isomorphism $\mathbb{C}/\Lambda \longrightarrow E_\tau$. However, we can also uniformize E by $\mathbb{C}^\times$ by exponentiating first.

We note that the exponential map induces an isomorphism $\mathbb{C}/2\pi iz \longrightarrow \mathbb{C}^\times$. Let z be the co-ordinate on $\mathbb{C}$ and $t = e^z$ the coordinate on $\mathbb{C}^\times$. Then we have an induced isomorphism $\mathbb{C}^\times/q^{\mathbb{Z}} \cong E_\tau$ where $q = e^{2\pi i\tau}$. Also, we see that the differential dz maps to dt/t.

We can replicate this approach over any base in the following way. Suppose we want to consider elliptic curves over a base field k (equivalently, modular forms with values in k). Then, we define the tate curve to be an elliptic curve over $k((q))$ by the equation $y^2 + xy = x^3 + a_4x + a_6$ where

$$-a_4 = 5\sum_n \frac{n^3q^n}{1-q^n} = 5q + 45q^2 + 140q^3 + \cdots$$

and

$$-a_6 = \sum_n \frac{7n^5 + 5n^3}{12} \times \frac{q^n}{1-q^n} = q + 23q^2 + 154q^3 + \cdots$$

are power series with integer coefficients. Similarly, one has an explicit description of the differential.

One way to make sense of this is to note that over $\mathbb{C}$, the uniformization gives us a Weierstrass equation for E_τ with coefficients being modular forms. This definition is a slight variant of that equation.

At any rate, this explicit description will not be so useful for us. However, one can define the Tate curve to be $\mathbb{G}_m/q^{\mathbb{Z}}$ in an appropriate geometric category (that of rigid analytic objects). The differential is correspondingly dt/t.

One can show that evaluating a modular f on the tate curve along with the above differential will give us the q-expansion of the modular form over k. This provides a very geometric interpretation of modular forms over $\mathbb{F}_p$.

We will not need much more than the above definitions to prove that modular form $\overline{A}(Q, R)$ in $\overline{M}$ is to the Hasse invariant:

4.3. **The Hasse Invariant.** Elliptic curves over a finite field $\mathbb{F}_p$ come in two flavours: ordinary and supersingular. There are many ways of defining these terms but we will use the following:

Let $E/\overline{\mathbb{F}_p}$ be an elliptic curve and ω some non zero differential. Recall that there is a Frobenius map $F : E \longrightarrow E^{(p)}$ of degree p. It is an isomorphism on the underlying topological space and acts on the co-ordinate ring by raising to the p-th power. In other words, if a local equation for E is

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

then the corresponding equation for $E^{(p)}$ is

$$y^2 + a_1^p xy + a_3^p y = x^3 + a_2^p x^2 + a_4^p x + a_6^p$$

and the isogeny is given by $(x, y \longrightarrow (x^p, y^p))$. Similarly, if ω is given by $dx/(2y + a_1x + a_3)$, then $\omega^{(p)} = dx/(2y + a_1^p x + a_3^p)$.

However, we can also consider the dual isogeny $F^\vee : E^{(p)} \longrightarrow E$ and pull back ω along this map to get $F^{\vee *}(\omega)$. Since the space of differential forms is one dimensional, there exists some constant $A(E, \omega) \in \overline{\mathbb{F}_p}$ such that $F^{\vee *}(\omega) = A(E, \omega)\omega^{(p)}$.

$A(E, \omega)$ is known as the Hasse invariant and is zero precisely when E is supersingular. This notation is no coincidence. $A(E, \omega)$ will turn out to be a modular form of weight $p-1$ (with coefficients in $\overline{\mathbb{F}_p}$) and in fact, equal to our $\overline{A}(\overline{Q}, \overline{R}) = \overline{E_{p-1}}$ from before.

4.4. **The Hasse Invariant is a modular form.** I will only prove that it satisfies the functional equation of a modular form. We need to compute $A(E, \lambda\omega)$. It is clear from the local description of $\omega^{(p)}$ that $(\lambda\omega)^{(p)} = \lambda^{p-1}\omega^{(p)}$. Also, pullbacks commute with scalars and therefore, we have:

$$F^{\vee *}(\lambda\omega) = A(E, \lambda\omega)(\lambda\omega)^{(p)} \implies A(E, \lambda\omega) = \lambda^{p-1}A(E, \omega).$$

Therefore, $A(E, \omega)$ transfers as a modular form.

4.5. **The q-expansion of the Hasse invariant.** Since $A(E, \omega)$ is (the reduction of) a modular form of weight $p - 1$, to show that it is equal to $\overline{E_{p-1}}$, we simply need to compute the q-expansion and show it is equal to 1. This section will be *very* sketchy.

As discussed before, computing the q-expansion is equivalent to evaluation the modular form on the Tate curve with the differential dt/t. We will do this by considering the rigid analytic model $E_{\text{Tate}} = \mathbb{G}_m/q^{\mathbb{Z}}$ of the Tate curve:

Since $\mathbb{G}_m$ is defined over $\mathbb{F}_p$, the Frobenius leaves it invariant. Therefore, in computing $E^{(p)}_{\text{Tate}}$, we only have to raise q to the p-th power. (Recall that q is an element of our base $\overline{\mathbb{F}_p}((q))$ while t is the co-ordinate on it. The Frobenius changes the coefficients but leaves the co-ordinates invariant).

That is, $E^{(p)}_{\text{Tate}} = \mathbb{G}_m/q^{p\mathbb{Z}}$. For the same reason, $\omega^p = dt/t$. Further, one can verify that the dual to the Frobenius is simply the natural quotient map $F^\vee : \mathbb{G}_m/q^{p\mathbb{Z}} \longrightarrow \mathbb{G}_m/q^{\mathbb{Z}}$.

Therefore, $F^{\vee *}(\omega) = dt/t$ and thus, $A(E_{\text{Tate}}, dt/t) = 1$ which completes the proof.

5. P-ADIC MODULAR FORMS

We can finally start talking about modular forms with p-adic coefficients. The goal here is to find a subalgera M_p of $\mathbb{Q}_p[[q]]$ that provides us with a reasonable notion of p-adic modular forms.

Certainly, classical modular forms with coefficients in $S = \mathbb{Z}_{(p)}$ should be included in M_p. Equally clearly, we would in fact like to also allow $\mathbb{Q}_p$ linear combinations of these classical modular forms. That is, we would like to have:

$$M_S \otimes_{\mathbb{Z}} \mathbb{Q}_p \subset M_p.$$

We would also like to exploit the analytic nature of $\mathbb{Q}_p$ and allow (p-adic) limits of classical modular forms in M_S. That is, given a sequence

$$f_m = \sum_{n \geq 0} a_n q^n$$

of modular forms with coefficients $a_{mn} \in S = \mathbb{Z}_{(p)}$, we would like to define a p-adic modular form:

$$f = \lim_{m \longrightarrow \infty} f_m = \sum_{n \geq 1} a_n q^n$$

provided that the a_{nm} converge uniformly in n to a_n as m goes to infinity. The convergence is of course in the p-adic topology. This almost works except for a complication arising due to the weights of f_n.

In fact, if we require that the weights k_n of f_n are constant, then we will not get anything new outside $M_S \otimes \mathbb{Q}_p$. To get anything interesting, we are forced to let the weights k_n vary. We will see that this is in fact a feature and is responsible for the richness of the theory.

First, we would like to say that the weights converge p-adically provided that the series f_n converge uniformly (as above). As evidence for this, we have the following theorem that follows immediately from the Von Staudt-Clausen and Kummer congruences of section 3.1.

Theorem 7. *The Eisenstein series E_k satisfy the following congruence:*

$$E_k \equiv 1 \pmod{p^r} \iff (p-1)p^{r-1} | k \qquad \text{for } p \geq 3$$

and

$$E_k \equiv 1 \pmod{p^r} \iff p^{r-2} | k \qquad \text{for } p = 2.$$

Note that the congruence is between modular forms of weights $(p-1)p^{r-1}$ and 0 and so the weights are p-adically close. This is not an isolated incidence as the following theorem shows. The p-adic valuation v_p is normalized so that $v_p(p) = 1$.

Theorem 8. *Suppose that*

$$f = \sum_{n \geq 0} a_n q^n \text{ and } f' = \sum_{n \geq 0} a'_n q^n$$

are two classical modular forms in M_S of weights k and k'. That is, $a_n, a'_n \in S = \mathbb{Z}_{(p)}$. If f, f' are p-adically close, that is:

$$v_p(f - f') \geq v_p(f) + r \qquad \text{for } r \geq 1$$

then the weights are p-adically close:

$$k \equiv k' \pmod{(p-1)p^{r-1}} \qquad \text{if } p \geq 3$$

and

$$k \equiv k' \pmod{p^{r-2}} \qquad \text{if } p = 2.$$

Proof. By dividing f by the highest power of p that divides it, we can assume that $v_p(f) = 0$ and that $f \equiv f' \pmod{p^r}$.

Note that, since f, f' are p-adically close, their reductions in $\overline{M}$ are equal. We thus see from section 3.2 that $k \equiv k' \pmod{p-1}$. We now need to show that k and k' are p-adically close.

We can make the following reductions without loss of generality. Assume that $k' \geq k$. In fact, letting $h = k' - k$, we can assume that $h \geq 4$ by replacing f' by $f' E_{(p-1)p^s}$ for s large enough. This follows from Theorem 7 on Eisenstein series.

For ease of notation, let $\lambda = r - 1$ if $p \geq 3$ or $\lambda = r - 2$ if $p = 2$. Thus, we need to show that $l = v_p(h) \geq \lambda$. Assume otherwise for contradiction, that is, $l < \lambda$ for the remainder of this proof.

Note that fE_h and f' are modular forms of the same weight k'. Therefore, $g = f' - fE_h$ is a modular form of weight k' and we see that:

$$f(1 - E_h) \equiv g \pmod{p^r}.$$

By theorem 7, $1 - E_h$ is divisible by p^λ and hence by p^{l+1}. Similarly, $g \equiv 0 \pmod{p^{l+1}}$ since $E_h \equiv 1 \pmod{p^\lambda}$.

By theorem 7:

$$\frac{1 - E_h}{p^l} = c\phi = c \sum_{n \geq 1} \sigma_h(n) q^n.$$

where $p \nmid c$. Similarly, $g' = g/p^l$ is a modular form mod p of weight $k' \pmod{p-1}$ and f is a *non-zero* modular form mod p of weight $k \equiv k' \pmod{p-1}$.

Therefore, dividing the above congruence by p^l, we get the following congruence:

$$\phi \equiv \frac{g'}{cf} \pmod{p}$$

where g'/f is also a mod p modular form of degree $0 \pmod{p-1}$. It is not clear whether ϕ is a modular form mod p, however, the above congruences shows us that it is indeed a modular form mod p of degree $0 \pmod{p-1}$.

However, this is sufficient to produce a contradiction as follows:

$$\psi = \phi - \phi^p = \sum_{\substack{n \geq 1 \\ p \nmid n}} \sigma_{h-1}(n) q^n = \frac{1}{24} \theta^{h-1}(E_2) \equiv \frac{1}{24} \theta^{p-2}(E_{p+1}) \pmod{p}.$$

Hence, θ satisfies an algebraic equation over $\overline{M}$. To conclude the proof, let us compute ω of both sides. This function was defined in section 3.3. From Theorem 5 in that section, recall that:

$$\omega(\theta^{p-2}(\overline{E_{p+1}})) = \omega(\overline{E_{p+1}}) + (p-2)(p+1) = p^2 - 1.$$

On the other hand, $\omega(\phi^p) = p\omega(\phi)$ and this dominates $\omega(\phi)$. Therefore, $p | \omega(\phi - \phi^p)$ while $p \nmid p^- 1$ which gives rise to the required contradiction.

□

The above theorem suggests the following definitions:

Define X_m to be:

$$X_m = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} & p \geq 3 \\ \mathbb{Z}/2^{m-2}\mathbb{Z} & p = 2 \end{cases}$$

and $X = \varprojlim X_m$.

We define p-adic modular forms to be formal series in $\mathbb{Q}_p[[q]]$, $f = \sum_{n \geq 0} a_n q^n$ such that $f = \lim f_i$ where the f_i are classical modular forms with rational coefficients.

Further, by the above theorem, the weights k_i of f_i converge to some element k in X that we call the weight of f. This weight is clearly independent of the sequence we choose.

Since classical forms are all of even weight, the same is true for p-adic modular forms. That is, the weight of a p-adic modular form is in $2X$ or equivalently, $(-1)^k = 1$ for k the weight of a p-adic modular form. We will define an Eisenstein series for each of these weights in the following way.

6. P-adic Eisenstein Series

Let $k \in 2X$. Pick a sequence of even integers k_m such that $k_m \longrightarrow k$ in X and $k_m \longrightarrow \infty$ in the Euclidean topology. Then, define the p-adic Eisenstein series E_k^* by:

$$G_k^* = \lim_{m \longrightarrow \infty} G_{k_m} = \lim_{m \longrightarrow \infty} -\frac{B_{2k_m}}{2k_m} + \sum_{n \geq 1} \sigma_{k-1}^*(n) q^n$$

where $\sigma_{k-1}^*(n) = \lim_{m \longrightarrow \infty} \sigma_{k_m - 1}(n)$. For $p \nmid n$, this is well defined since n^x is p-adically continuous in x. On the other hand, for $p|n$, this is 0 since $k_m \longrightarrow \infty$. Clearly, σ_{k-1}^* is independent of the sequence k_m we choose.

However, it is still not clear that the constant term converges or that it is independent of our choice. We are in the position of having good control over non constant terms but having no control at all over the constant term. This is precisely what the next few theorems give us:

First, we can restate theorem 8 in the following way:

Theorem 9. *Suppose f, f' are non zero (p-adic) modular forms of weights k, k'. If:*

$$v_p(f - f') \geq v_p(f) + m$$

then k, k' have the same image in X_m.

Let $g = \sum_{n \geq 0} a_n q^n$ be a p-adic modular of non-zero weight $k \in X$. Applying the contrapositive of the above to $f = a_0$, $f' = g$, we obtain:

Corollary 10. *Suppose $k \neq 0$ in X_{m+1}. Then:*

$$\inf_{n \geq 1} v_p(a_n) = v_p(f - f') < v_p(f) + m + 1 \leq v_p(a_0) + m.$$

That is:

$$v_p(a_0) + m \geq \inf_{n \geq 1} v_p(a_n)$$

This let's us control the constant term as required.

Theorem 11. *Suppose that $f_m = \sum_{n \geq 0} a_{mn} q^n$ is a sequence of p-adic modular forms such that:*

- *The sequence in m a_{mn} tends to a_n uniformly (in n).*
- *The weights k_m of f_m converge to $k \neq 0$ in X.*

Then, a_{m0} has a unique limit a_0 and therefore $f = \sum_{n \geq 0} a_n$ is a p-adic modular form.

Proof. Since the a_{mn} tend uniformly to a_m, for any $t \geq 0$, we can find a M such that $v_p(a_{mn}) \geq t$ for $m \geq M$. Also, since $k \neq 0$, the k_n are all non zero in some X_{l+1} (dropping some initial terms if necessary). However, then the previous theorem tells us that $v_p(a_{m0}) \geq t - l$ for $m \geq M$. Thus, the a_{m0} lie in a compact subset of X and we can find a limit point a_0.

Picking a subsequence so that a_0 is an actual limit point, we see that f is a p-adic modular form. Further, if a_o', f' give rise to a different limit, then $f - f' = a_0 - a_0'$ is a modular form of weight both 0 and $k \neq 0$. This is a contradiction unless it is 0. $\square$

Applying this theorem to Eisenstein series shows us that G_k^* is well defined. Define $\zeta^*(k)$ by:

$$G_k^* = \frac{1}{2}\zeta^*(1-k) + \sum_{n\geq 1} \sigma_{k-1}^*(n)q^n.$$

It is defined for all even k and is a continuous function on the odd elements of X and in fact, this is the Kubota-Leopoldt p-adic zeta function. More precisely:

Theorem 12. *For $p \neq 2$, let $1 \neq k = (s,u)$ be an odd element of $X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. Then:*

$$\zeta^*(s,u) = L_p(s, \omega^{1-u}),$$

where L_p is the Kubota-Leopoldt zeta function and ω the Teichmuller character.

Proof. Define $\zeta'(s,u)$, a function on X, by:

$$\zeta'(s,u) = L_p(s, \omega^{1-u}).$$

For an integer $k = (s,u)$ in X, by the very definition of L_p, one has:

$$\zeta'(1-k) = (1-p^{k-1})\zeta(1-k).$$

If $k \in 2X$ and non zero with a sequence of integers $k_i \longrightarrow k$, then:

$$\zeta'(1-k) = \lim_{i \longrightarrow \infty} (1-p^{k_i-1})\zeta(1-k_i)$$

and moreover, if $k_i \longrightarrow \infty$ in the usual topology, then:

$$\zeta'(1-k) = \lim_{i \longrightarrow \infty} \zeta(1-k_i) = \zeta^*(1-k).$$

Thus, we have shown that $\zeta' = \zeta^*$. as the theorem required.

□

The p-adic Eisenstein series also satisfy the same congruences that the usual Eisenstein series did. In particular, if we let $E_k^* = 2G_k^*/\zeta^*(1-k)$, then the following is true:

$$k = 0 \in X_{m+1} \implies E_k^* \equiv 1 \pmod{p^m}.$$

This is a straightforward consequence of the usual congruences for Eisenstein series (Theorem 7).