Modular forms modulo p and p-adic modular forms

FRANCESC GISPERT

Montréal, 12th November 2020

Abstract

These are the notes for a one-and-a-half-hour talk given in an informal seminar[1] to prepare for a workshop on higher Coleman theory at the Centre de Recherches Mathématiques. I present the theory of (classical) modular forms modulo a fixed prime number p and introduce the notion of p-adic modular forms using their power series expansions. I tried to present these objects in the most elementary possible form thinking of the variety of backgrounds amongst the audience. The notes follow almost verbatim Serre and Swinnerton-Dyer's original work in the early 70's, published in the articles [2, 5, 4]. At the end, there is a brief review of p-adic Banach theory, following Serre's article [3], which was meant to set the ground for Giovanni Rosso's talk that followed mine. No originality is claimed.

1 Modular forms over $\mathbb{C}$

We begin by quickly recalling the basic definitions and results of the theory of modular forms. Let $\mathbb{H} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$.

Definition 1.

(1) A *modular form* of *weight* $k \in \mathbb{Z}$ (and *level*[2] 1) is a holomorphic function $f\colon \mathbb{H} \to \mathbb{P}^1(\mathbb{C})$ with the property that

$$f\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^k \cdot f(z) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and all } z \in \mathbb{H}$$

[1] I thank Adrian Iovita for organizing the seminar and thinking of me to give this talk.

[2] The notion of *level* will appear in Giovanni's talk on Katz's definitions of modular forms. I will focus on the simplest case.

and admitting a *q–expansion*

$$f(z) = \sum_{n \geq 0} a_n(f) q^n, \quad \text{where } q = e^{2\pi i z}.$$

We identify f with its q–expansion (i.e., we view it as an element of $\mathbb{C}[\![q]\!]$).

(2) Let A be a subring of $\mathbb{C}$. We say that f is *defined over A* if $f \in A[\![q]\!]$.[3]

(3) Let $M_k(A)$ denote the set of modular forms of weight k defined over A. (It is, in fact, an A–module.)

(4) Set

$$M(A) = \bigoplus_{k \in \mathbb{Z}} M_k(A).$$

(It is a graded A–algebra.)

Example 2. The first examples of modular forms are the (normalized) *Eisenstein series*

$$E_{2k} = 1 - 2 \cdot \frac{2k}{B_{2k}} \cdot \sum_{n \geq 1} \sigma_{2k-1}(n) q^n \in M_{2k}(\mathbb{Q}) \text{ for } k \geq 2,$$

where B_{2k} is the $2k$–th Bernoulli number and

$$\sigma_{2k-1}(n) = \sum_{0 < d \mid n} d^{2k-1}.$$

In particular, we will mostly be interested in the following series:

$$P = E_2 = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n \notin M_2,^4$$
$$Q = E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n \in M_4,$$
$$R = E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n \in M_6.$$

From these, we can also construct a modular form whose q–expansion has trivial constant coefficient, the (normalized) *modular discriminant*

$$\Delta = \frac{Q^3 - R^2}{1728} = \cdots = q \prod_{n \geq 1} (1 - q^n)^{24} \in M_{12}.$$

Theorem 3. *There is a canonical isomorphism of graded $\mathbb{C}$–algebras*

$$\mathbb{C}[X, Y] \cong \mathbb{C}[Q, R] = M(\mathbb{C})$$
$$X \mapsto Q$$
$$Y \mapsto R$$

[3]This definition of being *defined over a certain ring* will agree with Katz's one, which is more natural, thanks to a result known as the *q–expansion principle*.

[4]This is not a mistake. The Eisenstein series of weight 2 is not a modular form in the sense of definition 1, but "almost": it is a p–adic modular form and even a modular form of level $\Gamma_0(p)$.

(where X and Y are independent variables of weights 4 and 6, respectively).

Idea of the proof. This classical result can be proved using contour integration and studying the possible poles of modular forms to compare dimensions at each degree. □

Theorem 4. *Let k be an even integer ≥ 4 and let $d = \dim_{\mathbb{C}}(M_k(\mathbb{C})) - 1$. Choose $\alpha, \beta \geq 0$ such that*

(i) $4\alpha + 6\beta \equiv k \bmod 12$ *and*

(ii) $4\alpha + 6\beta \leq 14$.

Define, for $0 \leq j \leq d$, $g_j = \Delta^j Q^\alpha R^{2(d-j)+\beta}$. The elements $g_0, g_1, \ldots, g_d$ form an integral basis of $M_k(\mathbb{C})$. That is,

$$M_k(A) = \bigoplus_{j=0}^{d} A \cdot g_j$$

for every subring $A \subseteq \mathbb{C}$.

Remark. In the way this theorem is stated, it is unclear even if $g_j \in M_k$. What happens is that one can compute d, which happens to be approximately $\frac{k}{12}$. Then α and β are chosen to compensate the difference between $12d$ and k.

Idea of the proof. There are the right number of elements g_j, $0 \leq j \leq d$, and by construction

$$g_j = q^j + O(q^{j+1}) \in \mathbb{Z}[\![q]\!]$$

(cf. the formulae in example 2). The theorem follows by looking at the coefficients of $1, q, \ldots, q^d$. □

In particular, $M(A) = A[Q, R, \Delta]$ with the relation $1728\Delta = Q^3 - R^2$.

2 Modular forms modulo p (Serre–Swinnerton-Dyer)

This section is mostly a rewriting of some of the work of Serre and Swinnerton-Dyer, which they published in the articles [2] and [5]. Since most of the proofs are quite short and elementary, I tried to include at least the main ideas.

Fix a prime number p and let $\bar{\cdot}$ denote reduction modulo p.

Definition 5.

(1) For $k \in \mathbb{Z}$, let $M_k(\mathbb{F}_p) = \{ \bar{f} \in \mathbb{F}_p[\![q]\!] : f \in M_k(\mathbb{Z}_{(p)}) \}$.

(2) The *algebra of modular forms modulo p* is the $\mathbb{F}_p$–algebra

$$M(\mathbb{F}_p) = \sum_{k \in \mathbb{Z}} M_k(\mathbb{F}_p).$$

Remark. The last sum is not direct (i.e., a power series in $\mathbb{F}_p[\![q]\!]$ may appear as the reduction of two modular forms with different weights).

If $p = 2$ or 3, $M(\mathbb{F}_p) = \mathbb{F}_p[\overline{\Delta}] \cong \mathbb{F}_p[T]$ (where T is an independent variable) because $\overline{Q} = \overline{R} = 1$. From now on, assume that $p \geq 5$. Then $p \nmid 1728$ and so $M(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}[Q, R]$. We have surjections

$$\begin{array}{ccccccc} M(\mathbb{Z}_{(p)}) & \cong & \mathbb{Z}_{(p)}[X,Y] & \twoheadrightarrow & \mathbb{F}_p[X,Y] & \twoheadrightarrow & M(\mathbb{F}_p) \\ \phi(Q,R) & \longmapsto & \phi(X,Y) & \longmapsto & \overline{\phi}(X,Y) & \longmapsto & \overline{\phi}(\overline{Q},\overline{R}) \end{array}$$

and just need to describe $\mathrm{Ker}\big(\mathbb{F}_p[X,Y] \twoheadrightarrow M(\mathbb{F}_p)\big)$. To do so, we will use Serre's differential operator

$$\theta = q\frac{d}{dq}.$$

Theorem 6 (Ramanujan).

(1) *Let* $k \in \mathbb{Z}$. *If* $f \in M_k(\mathbb{C})$, *then* $(12\theta - kP)f \in M_{k+2}(\mathbb{C})$.

(2) *We have the following identities:*

$$\begin{aligned} (12\theta - P)P &= -Q,^{5} \\ (12\theta - 4P)Q &= -4R, \\ (12\theta - 6P)R &= -6Q^2, \\ (12\theta - 12P)\Delta &= 0. \end{aligned}$$

Idea of the proof. Since all these forms live in 1–dimensional $\mathbb{C}$–vector spaces, it suffices to compare the first coefficients of the q–expansions in each equality. □

Definition 7.

(1) Let ∂ be the *graded derivation* on $M(\mathbb{C})$ given by

$$\partial|_{M_k(\mathbb{C})} = 12\theta - kP \quad \text{for every } k \in \mathbb{Z}.$$

(2) On $\mathbb{Z}_{(p)}[X,Y]$ (resp. $\mathbb{F}_p[X,Y]$), define ∂ by $\partial X = -4Y$ and $\partial Y = -6X^2$.

(3) Let $k \in \mathbb{Z}$. For $f \in M_k(\mathbb{Z}_{(p)})$, write $\partial\overline{f} = \overline{\partial f} \in M_{k+2}(\mathbb{F}_p)$.

Next, we want to find congruences between Eisenstein series, but there are Bernoulli numbers in their q–expansions (see example 2).

[5] I did not forget a $k = 2$ before the first P; as mentioned earlier, P is somewhat special.

Theorem 8. *Let $k \in \mathbb{Z}_{\geq 1}$.*

(1) *If $p-1 \mid 2k$, then $pB_{2k} \in \mathbb{Z}_{(p)}$ and*

$$pB_{2k} \equiv -1 \mod p \qquad \textit{(Clausen–von Staudt congruence).}$$

In particular, $v_p(B_{2k}) = -1$.

(2) *If $p-1 \nmid 2k$, then $B_{2k} \,/\, 2k \in \mathbb{Z}_{(p)}$ and*

$$\frac{B_{2k}}{2k} \equiv \frac{B_{2k+m(p-1)}}{2k+m(p-1)} \mod p \quad \textit{for every } m \in \mathbb{Z} \qquad \textit{(Kummer congruence).}$$

That is, the class of $B_{2k} \,/\, 2k \bmod p$ depends only on $2k \bmod p-1$.

Corollary 9.

(1) $\overline{E}_{p-1} = 1$.

(2) $\overline{E}_{p+1} = \overline{P}$.

Definition 10. We define $A, B \in \mathbb{Z}_{(p)}[X,Y]$ to be the polynomials determined by the equations

$$A(Q,R) = E_{p-1} \quad \text{and} \quad B(Q,R) = E_{p+1}.$$

Lemma 11.

(1) $\partial\overline{A} = \overline{B}$ *and* $\partial\overline{B} = -X\overline{A}$ *in* $\mathbb{F}_p[X,Y]$.

(2) *The polynomial $\overline{A}$ has no repeated factors in $\overline{\mathbb{F}}_p[X,Y]$.*

Idea of the proof.

(1) These equalities follow from a simple calculation.

(2) Using (1), one can argue by contradiction. □

Theorem 12. *We have an isomorphism of rings*

$$M(\mathbb{F}_p) \cong \mathbb{F}_p[X,Y] \,/\, (\overline{A}-1).$$

Idea of the proof. We know that $\dim(\mathbb{F}_p[X,Y]) = 2$ and one can check that the ideal $\mathfrak{a} = \mathrm{Ker}\big(\varphi(X,Y) \mapsto \varphi(\overline{Q},\overline{R})\colon \mathbb{F}_p[X,Y] \to M(\mathbb{F}_p)\big)$ is prime of height 1 and contains $(\overline{A}-1)$. By lemma 11, the ideal $(\overline{A}-1)$ is also prime. Therefore, $\mathfrak{a} = (\overline{A}-1)$. □

In particular, congruences between modular forms are only possible when the weights are congruent modulo $p-1$.

3 p–adic modular forms (Serre)

The next two sections are my attempt to summarize Serre's article [4]. The original in this case is much longer and contains many more interesting results that I had to omit due to the time constraints.

Fix $p \geq 3$ (for simplicity). For $f \in \mathbb{Q}_p[\![q]\!]$, write

$$v_p(f) = \inf_{n \geq 0} \{ v_p(a_n(f)) \}.$$

Theorem 13. *Let $f \in M_k(\mathbb{Q})$ and $\widetilde{f} \in M_{\widetilde{k}}(\mathbb{Q})$. Suppose that $f \neq 0$. Let $m \in \mathbb{Z}_{\geq 0}$. If $v_p(f - \widetilde{f}) \geq v_p(f) + m$, then*

$$\widetilde{k} \equiv k \mod (p-1)p^{m-1}.$$

Idea of the proof. The theorem can be proved by induction on m. The base case follows from theorem 12. □

Intuitively, this theorem says that two modular forms can be *p–adically close* only if their weights are.

Definition 14. For $m \in \mathbb{Z}_{\geq 0}$, set

$$W_m = \big(\mathbb{Z} \,/\, (p-1)\mathbb{Z}\big) \times \big(\mathbb{Z} \,/\, p^{m-1}\mathbb{Z}\big) \cong \big(\mathbb{Z} \,/\, p^m\mathbb{Z}\big)^{\times}.$$

The *group of p–adic weights* is

$$W = \varprojlim_m W_m = \big(\mathbb{Z} \,/\, (p-1)\mathbb{Z}\big) \times \mathbb{Z}_p \cong \mathbb{Z}_p^{\times}.$$

Remark. One often identifies W with $\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p^{\times}, \mathbb{Z}_p^{\times})$ via $k \longmapsto \big(x \mapsto x^k\big)$.[6]

Definition 15.

1. A *p–adic modular form* is a formal power series $f \in \mathbb{Q}_p[\![q]\!]$ such that there exist $f_i \in M_{k_i}(\mathbb{Q})$ for $i \in \mathbb{Z}_{\geq 1}$ with the property that

   $$v_p(f - f_i) \xrightarrow[i \to \infty]{} +\infty.$$

   If $k = \lim_{i \to \infty} k_i \in W$ (i.e., this limit exists and is well-defined in W), we say that f has *weight k*.
2. Let $M_k(\mathbb{Q}_p)$ denote the set of p–adic modular forms of weight k. (It is, in fact, a Banach space over $\mathbb{Q}_p$.)
3. Set

   $$M(\mathbb{Q}_p) = \bigoplus_{k \in W} M_k(\mathbb{Q}_p).^{7}$$

   (It is a graded $\mathbb{Q}_p$–algebra.)

[6] We will see more of this and other interpretations of the weight space in future talks.

Remark. Since a p–adic modular form can be obtained as the limit of several sequences of modular forms, it might seem unclear whether weights are well-defined. Theorem 13 is what justifies this definition (with a little work that is left to the reader).

Example 16. If $p = 3$, then $Q \equiv 1 \bmod p$ and so we obtain

$$\frac{1}{Q} = \lim_{i\to\infty} \frac{Q^{p^i}}{Q} = \lim_{i\to\infty} Q^{p^i-1} \in M_{-4}(\mathbb{Q}_p).$$

Theorem 17. *Consider* $f_i \in M_{k_i}(\mathbb{Q}_p)$ *for* $i \in \mathbb{Z}_{\geq 1}$*. If*

(i) *each sequence* $\big(a_n(f_i)\big)_{i\geq 1}$ *for* $n \in \mathbb{Z}_{\geq 1}$ *has a limit* $a_n \in \mathbb{Q}_p$ *and*

(ii) *the sequence* $\big(k_i\big)_{i\geq 1}$ *has a limit* $k \in W$ *which is* $\neq 0$*,*

then the sequence $\big(a_0(f_i)\big)_{i\geq 1}$ *too admits a limit* $a_0 \in \mathbb{Q}_p$ *and*

$$f = \sum_{n\geq 0} a_n q^n \in M_k(\mathbb{Q}_p).$$

Idea of the proof. By theorem 13 applied to any $g \in M_k(\mathbb{Q}_p)$ and $\widetilde{g} = a_0(g)$ (i.e., a constant, which we view in $M_0(\mathbb{Q}_p)$), if we choose $m \gg 0$ such that $k \neq 0$ in W_{m+1}, then

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

Thus, the convergence of the $a_0(\cdot)$ coefficients is forced by that of the $a_n(\cdot)$ for $n \geq 1$.[8] □

Example 18. Take a sequence $k_i \in 2\mathbb{Z}_{\geq 2}$ such that

(i) $k_i \to k \in 2W$ and

(ii) $|k_i| \to \infty$ (in $\mathbb{R}$, where $|\cdot|$ is the usual archimedean absolute value).

Then

$$\sigma_{k_i-1}(n) = \sum_{d|n} d^{k_i-1} \xrightarrow[i\to\infty]{|\cdot|_p} \sum_{p\nmid d|n} d^{k-1} = \sigma^*_{k-1}(n),$$

where the last sum skips any p factors because condition (ii) makes them tend to 0 p–adically. Hence, we obtain a limit of Eisenstein series

$$\frac{B_{k_i}}{2k_i} E_{k_i} = \frac{B_{k_i}}{2k_i} + \sum_{n\geq 1} \sigma_{k_i-1}(n) q^n \xrightarrow[i\to\infty]{|\cdot|_p} \text{“}\frac{B_k}{2k}\text{''} + \sum_{n\geq 1} \sigma^*_{k-1}(n) q^n = E^*_k \in M_k(\mathbb{Q}_p).$$

[7] The notation I use here is not compatible with that of the previous sections. It is important to note that *p–adic modular forms* are not the same as *modular forms defined over* $\mathbb{Q}_p$. However, I believe there is little chance of confusion at the level of this talk.

[8] Here I did my best to give a bit of intuition, but the explanation is admittedly not enough to see how the proof would proceed. There is at least another key idea in the proof that I decided to omit because of the time constraints.

(The factors $B_{k_i}\,/\,2k_i$ occur as special values of the Riemann zeta function; likewise, the limit factor "$B_k\,/\,2k$" occurs as a special value of its p–adic counterpart, known as the Kubota–Leopoldt p–adic L–function.)

4 Hecke operators

Definition 19. Let

$$f = \sum_{n\geq 0} a_n(f) q^n \in \mathbb{Q}_p[\![q]\!].$$

We define

$$\begin{aligned} f|\,\mathrm{U}_p &= \sum_{n\geq 0} a_{np}(f) q^n, \\ f|\,\mathrm{V}_p &= \sum_{n\geq 0} a_n(f) q^{np}, \\ f|_k\,\mathrm{T}_\ell &= \sum_{n\geq 0} a_{n\ell}(f) q^n + \ell^{k-1} \sum_{n\geq 0} a_n(f) q^{n\ell} \end{aligned}$$

(for any prime number ℓ and any $k \in W$).

Theorem 20.

(1) *The operators T_ℓ, for ℓ prime, act on $M_k(\mathbb{Z}_{(p)})$ for every $k \in \mathbb{Z}$.*

(2) *The operators U_p, V_p and T_ℓ for $\ell \neq p$ act on $M_k(\mathbb{Q}_p)$ for every $k \in W$.*

(3) *The operators T_ℓ, for ℓ prime, commute among themselves and with U_p and V_p.*

We are usually interested in simultaneous eigenvectors for these operators (i.e., *eigenforms*). We also consider the operator $\theta = q\frac{d}{dq}$, which increases weights by 2.

Since $\mathrm{T}_p \equiv \mathrm{U}_p \mod p$, we get an action of U_p on $M(\mathbb{F}_p)$ with the following *contracting* property:

Theorem 21.

(1) *Let $k \in \mathbb{Z}$. If $k > p+1$, then U_p maps $M_k(\mathbb{F}_p)$ into $M_{\widetilde{k}}(\mathbb{F}_p)$ for some $\widetilde{k} < k$.*

(2) *The operator U_p acts on $M_{p-1}(\mathbb{F}_p)$ bijectively.*

Corollary 22. *Assume that $p \geq 5$. Let $[a] \in \big(2\mathbb{Z}\,/\,(p-1)\mathbb{Z}\big)$ and define*

$$M_{[a]}(\mathbb{F}_p) = \bigcup_{k\in[a]} M_k(\mathbb{F}_p).$$

(1) *There exists a unique decomposition $M_{[a]}(\mathbb{F}_p) = S \oplus N$ with the property that U_p acts invertibly on S and acts nilpotently on N.*

(2) *If $k \in [a]$ and $4 \leq k \leq p+1$, then $S \subset M_k(\mathbb{F}_p)$.*

(3) *If $[a] = [0]$, then $S = M_{p-1}(\mathbb{F}_p)$.*

It is natural to wonder if there are similar decompositions for p–adic modular forms, as that would allow us to study smaller spaces of modular forms by means of the U_p–action. To go in that direction, we need functional analysis.

5 Compact operators on Banach spaces

This last section (which one might think of as an appendix) is a very brief summary of the results that we will need from Serre's article [3].

Definition 23. A $\mathbb{Q}_p$–Banach space X is called *orthonormalizable* if there exists a family $(e_i)_{i\in I} \subset\in X$ (an *orthonormal basis*) with the property that each $x \in X$ admits a unique expression as a linear combination

$$x = \sum_{i\in I} x_i e_i, \quad x_i \in \mathbb{Q}_p \text{ for all } i \in I,$$

with

(i) $x_i \xrightarrow[i\to\infty]{} 0$ (i.e., for every $\epsilon > 0$, $|x_i|_p < \epsilon$ for all but finitely many $i \in I$) and

(ii) $|x| = \sup_{i\in I} \{ \, |x_i|_p \, \}$.

From now on, fix an orthonormalizable $\mathbb{Q}_p$–Banach space X and write $\mathscr{L}(X)$ for the space of continuous $\mathbb{Q}_p$–linear maps $U\colon X \to X$ endowed with the supremum norm

$$\|U\| = \sup_{\substack{x\in X \\ x\neq 0}} \frac{|Ux|}{|x|}.$$

Definition 24.

(1) An operator $U \in \mathscr{L}(X)$ is *compact* if it is the limit of a sequence of maps of finite rank in $\mathscr{L}(X)$.

(2) Let $\mathscr{C}(X)$ denote the Banach algebra of compact operators on X.

Given $U \in \mathscr{C}(X)$, we can construct what is known as the *Fredholm determinant*, $\det(1 - tU) \in \mathbb{Q}_p[\![t]\!]$, as follows:

- Up to scaling, we may assume that $\|U\| \leq 1$ and so that U acts on the unit ball $X_0 = \{ \, x \in X : |x| \leq 1 \, \}$.
- By the definition of compact, for each $n \in \mathbb{Z}_{\geq 1}$, the image of $U|_{(X_0 \,/\, p^n X_0)}$ is contained in a finite free $\left(\mathbb{Z} \,/\, p^n\mathbb{Z}\right)$–module Y_n; then there is a well-defined

$$\det\left(1 - tU|_{Y_n}\right) \in \left(\mathbb{Z} \,/\, p^n\mathbb{Z}\right)[t].$$

- Take projective limits of the previous polynomials over $n \in \mathbb{Z}_{\geq 1}$ to obtain

$$\det(1 - tU) \in \mathbb{Z}_p[\![t]\!].$$

(The assumption in the first step forces coefficients to lie in $\mathbb{Z}_p$, but for general U we get an element of $\mathbb{Q}_p[\![t]\!]$.)

Proposition 25. *For every $U \in \mathscr{C}(X)$, the Fredholm determinant $\det(1 - tU)$ is entire (i.e., has an infinite radius of convergence).*

Theorem 26 (Riesz decomposition). *Let $a \in \mathbb{Q}_p^\times$ be a zero of order h of $\det(1 - tU)$. There exists a unique decomposition as a direct sum of closed subspaces $X = S(a) \oplus N(a)$ with the property that $1 - aU$ acts invertibly on $S(a)$ and acts nilpotently on $N(a)$. Moreover, $\dim_{\mathbb{Q}_p}(N(a)) = h$.*

Remark. $N(a) = \mathrm{Ker}\big((1 - aU)^h\big)$ is the U–eigenspace of eigenvalue a^{-1}; its elements are *generalized U–eigenvectors* of *slope $\alpha = -v_p(a)$*, which is one of the slopes of the Newton polygon of $\det(1 - tU)$.

Idea of the proof. One can use Fredholm's resolvent $\det(1 - tU) \,/\, (1 - tU)$ and divided differences to obtain several identities and then evaluate them at $t = a$ to explicitly find projectors for the decomposition $X = S(a) \oplus N(a)$. □

Corollary 27. *Let $Q(t)$ be an irreducible polynomial of $\mathbb{Q}_p[t]$ with $Q(0) = 1$. There exists a unique decomposition as a direct sum of closed subspaces $X = S(Q) \oplus N(Q)$ such that the operator $Q(U)$ acts invertibly on $S(Q)$ and acts nilpotently on $N(Q)$. Moreover, $\dim_{\mathbb{Q}_p}(N(Q)) < \infty$.*

Proof. Write $Q(U) = 1 - \widetilde{U}$ and apply theorem 26 to $\widetilde{U}$ and $a = 1$. □

Fix $h \in \mathbb{R}$. By an analogue of Weierstrass's preparation theorem, there are only finitely many Q as in corollary 27 with slope

$$v_p(Q) = v_p(\text{“root of } Q\text{''}) \leq h.$$

Defining

$$X^{(\leq h)} = \bigoplus_{v_p(Q) \leq h} N(Q),$$

we obtain a unique *slope $\leq h$ decomposition* $X = X^{(\leq h)} \oplus X^{(>h)}$ and the first part is even finite-dimensional.

Fact. The space $M_k(\mathbb{Q}_p)$ of p–adic modular forms of weight $k \in W$ is a $\mathbb{Q}_p$–Banach space. However, the operator U_p acting on $M_k(\mathbb{Q}_p)$ is not compact.

The reason why we cannot apply this theory to the operator U_p is that the space $M_k(\mathbb{Q}_p)$ is *too large*. As we will see in the next talk, Katz's solution to this problem was to work with subspaces of *overconvergent modular forms*.

References

[1] Ramanujan, S. "On certain arithmetical functions". In: *Trans. Cambridge Phil. Soc.* 22.9 (1916), pp. 159–184.

[2] Serre, J.-P. "Congruences et formes modulaires". In: *Séminaire Bourbaki. Vol. 1971/72. Exposés 400–417*. Ed. by Dold, A. and Eckmann, B. Lecture notes in mathematics 317. Berlin, Germany: Springer-Verlag, 1973, pp. 319–338.

[3] Serre, J.-P. "Endomorphismes complètement continus des espaces de Banach p-adiques". In: *Publ. Math. IHÉS* 12 (1962), pp. 69–85.

[4] Serre, J.-P. "Formes modulaires et fonctions zêta p-adiques". In: *Modular functions of one variable III*. Ed. by Serre, J.-P. and Kuijk, W. Lecture notes in mathematics 350. Berlin, Germany: Sprinver-Verlag, 1973, pp. 191–268.

[5] Swinnerton-Dyer, H. P. F. "On ℓ-adic representations and congruences for coefficients of modular forms". In: *Modular functions of one variable III*. Ed. by Serre, J.-P. and Kuijk, W. Lecture notes in mathematics 350. Berlin, Germany: Springer-Verlag, 1973, pp. 1–55.