Modular forms modulo p

FRANCESC GISPERT

Montréal, 11th November 2019

Abstract

These are the notes for a talk given in the graduate students seminar[1] at Concordia University. I present the theory of (classical) modular forms modulo a fixed prime number p using their power series expansions. The notes follow almost verbatim Serre and Swinnerton-Dyer's original work in the early 70's, published in two articles [2, 3]. The exposition should hopefully be accessible to graduate students in all areas of mathematics. No originality is claimed.

1 The classical theory

We begin by recalling the basic definitions and facts of the theory of modular forms. Consider the upper half-plane $\mathbb{H} = \{ z \in \mathbb{C} : \mathrm{Im}(z) > 0 \}$ with the left action of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Definition 1. A *weakly modular form of weight* $k \in \mathbb{Z}$ is a meromorphic function $f \colon \mathbb{H} \to \mathbb{P}^1(\mathbb{C})$ with the property that

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

Remark. The transformation rule above for the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

is that $f(z+1) = f(z)$ for all $z \in \mathbb{H}$. That is, a weakly modular form must be periodic (with respect to the real axis) of period 1. Therefore, and as it is also

[1] I thank Kenzy Abdel Malek for organizing the seminar.

meromorphic, f admits a Fourier series of the form

$$f(z) = \sum_{n \in \mathbb{Z}} a_n(f) q^n, \quad \text{where } q = e^{2\pi i z},$$

its *q–expansion*.

Definition 2. A *modular form of weight* $k \in \mathbb{Z}$ is a weakly modular form $f : \mathbb{H} \to \mathbb{C}$ of weight k that is holomorphic on $\mathbb{H}$ and at ∞ (in the sense that its q–expansion is of the form

$$f(z) = \sum_{n \geq 0} a_n(f) q^n$$

with no negative powers of q).

Remark. We identify a modular form f with its q–expansion and so view $f \in \mathbb{C}[\![q]\!]$.

Our objective in this talk is not to study modular forms individually, but to understand the algebraic structure of some spaces of modular forms.

Definition 3.

(1) Let M_k denote the $\mathbb{C}$–vector space of modular forms of weight $k \in \mathbb{Z}$.
(2) The *algebra of modular forms* is the graded $\mathbb{C}$–algebra

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

Spaces of modular forms have "nice" algebraic structures (vector spaces, algebras…), as this talk will emphasize. What makes them interesting to number theorists, however, is not the "linear algebra" but that the q–expansions are often generating functions of invariants of arithmetic objects (class numbers, rational points in curves,…).

Example 4. The first examples of modular forms are the (normalized) *Eisenstein series*

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

where B_j is the j–th Bernoulli number and

$$\sigma_t(n) = \sum_{0 < d \mid n} d^t.$$

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

$$P = E_2 = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n \notin M_2,^2$$
$$Q = E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n \in M_4,$$
$$R = E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n \in M_6.$$

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

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

(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 6. *Let k be an even integer ≥ 4 and let $d = \dim_{\mathbb{C}} M_k - 1$. 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 $0 \leq j \leq d$, $g_j = \Delta^j Q^\alpha R^{2(d-j)+\beta}$. Every $f \in M_k \cap \mathbb{Z}[\![q]\!]$ can be expressed uniquely as a $\mathbb{Z}$–linear combination of $g_0, g_1, \ldots, g_d$.

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.

Proof. From the formulae in example 4, it is clear that $Q, R, \Delta \in \mathbb{Z}[\![q]\!]$ and that the first non-zero coefficient of each of them is equal to 1. Therefore,

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

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

Looking at the coefficients of $1, q, \ldots, q^d$, it is now clear that the g_j, $0 \leq j \leq d$, are linearly independent and so form a $\mathbb{C}$–basis of M_k by the definition of d.

Let $f \in M_k \cap \mathbb{Z}[\![q]\!]$ and write

$$f = \sum_{j=0}^{d} \lambda_j \cdot g_j \quad \text{with } \lambda_0, \ldots, \lambda_d \in \mathbb{C}.$$

Again looking at the coefficients of $1, q, \ldots, q^d$, we obtain a system of equations

$$\begin{pmatrix} 1 & & & & \\ * & 1 & & & \\ * & * & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ * & * & * & \ldots & 1 \end{pmatrix} \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_d \end{pmatrix} = \begin{pmatrix} a_0(f) \\ a_1(f) \\ a_2(f) \\ \vdots \\ a_d(f) \end{pmatrix}$$

(where $*$ represents any integer entry). But this lower triangular matrix admits an inverse with integer entries. Thus, $\lambda_0, \ldots, \lambda_d \in \mathbb{Z}$ if $a_0(f), \ldots, a_d(f) \in \mathbb{Z}$. □

Theorem 6 gives an explicit basis $g_0, g_1, \ldots, g_d$ of the $\mathbb{C}$–vector space M_k with a very interesting "algebraicity" property: the (infinitely many) coefficients appearing in the q–expansion of a modular form f lie in the same ring where the coefficients $\lambda_0, \lambda_1, \ldots, \lambda_d$ of the linear combination

$$f = \sum_{j=0}^{d} \lambda_j \cdot g_j$$

are defined.

2 The theory modulo p

Fix a prime number p and consider the p–adic valuation $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ given by

$$v_p\Big(p^n \cdot \frac{a}{b}\Big) = n \quad \text{if } p \nmid ab \text{ and } n \in \mathbb{Z} \qquad \text{and} \qquad v_p(0) = \infty.$$

Let $\mathbb{Z}_{(p)} = \{\, x \in \mathbb{Q} : v_p(x) \geq 0 \,\}$ and write $\widetilde{\cdot} \colon \mathbb{Z}_{(p)} \twoheadrightarrow \mathbb{F}_p$ for the reduction modulo p. (The ring $\mathbb{Z}_{(p)}$ might look strange at first sight, but it is just the set of rational numbers that can be reduced modulo p.)

Definition 7.

(1) Let $M_k^p = M_k \cap \mathbb{Z}_{(p)}[\![q]\!]$ denote the $\mathbb{Z}_{(p)}$–module of p–integral modular forms of weight $k \in \mathbb{Z}$.

(2) The *algebra of p–integral modular forms* is the graded $\mathbb{Z}_{(p)}$–algebra

$$M^p = \bigoplus_{k\in\mathbb{Z}} M_k^p.$$

Given any power series

$$f = \sum_{n\geq 0} a_n q^n \in \mathbb{Z}_{(p)}[\![q]\!],$$

we write

$$\widetilde{f} = \sum_{n\geq 0} \widetilde{a}_n q^n \in \mathbb{F}_p[\![q]\!]$$

for its reduction modulo p. This construction provides a natural notion of "reductions of modular forms modulo p".

Definition 8.

(1) Let

$$\widetilde{M}_k^p = \{\, \widetilde{f} \in \mathbb{F}_p[\![q]\!] : f \in M_k^p \,\}$$

be the $\mathbb{F}_p$–vector space of modular forms of weight $k \in \mathbb{Z}$ reduced modulo p.

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

$$\widetilde{M}^p = \sum_{k\in\mathbb{Z}} \widetilde{M}_k^p.$$

Remark. In this case, we do not necessarily have a direct sum because modular forms of different weights might have equivalent q–expansions modulo p. Therefore, $\widetilde{M}^p$ is not graded by the integer degrees.

Our main objective is to determine the (algebraic) structure of $\widetilde{M}^p$. By theorem 6, we can express $M^p = \mathbb{Z}_{(p)}[Q, R, \Delta]$ with $1728\Delta = Q^3 - R^2$. Thus, we only need to find the relations that $\widetilde{Q}$, $\widetilde{R}$ and $\widetilde{\Delta}$ satisfy in $\mathbb{F}_p[\![q]\!]$.

Theorem 9. *If $p = 2$ or 3, then $\widetilde{P} = \widetilde{Q} = \widetilde{R} = 1$ and $\widetilde{M}^p = \mathbb{F}_p[\widetilde{\Delta}] \cong \mathbb{F}_p[T]$ (where T is a formal variable with no relations).*

Proof. It is immediate from the formulae in example 4, as 24, 240 and 504 are all divisible by p and the coefficient of q in Δ is 1. □

From now on, assume that $p \geq 5$. Then $p \nmid 1728$ and so $M^p = \mathbb{Z}_{(p)}[Q, R]$. That is, we can even forget about Δ. By construction and theorems 5 and 6, we can express $\widetilde{M}^p$ as a quotient via the composition

$$\begin{array}{ccccc} M^p \cong \mathbb{Z}_{(p)}[X,Y] & \twoheadrightarrow & \mathbb{F}_p[X,Y] & \twoheadrightarrow & \widetilde{M}^p \subset \mathbb{F}_p[\![q]\!] \\ \Phi(X,Y) & \longmapsto & \widetilde{\Phi}(X,Y) & \longmapsto & \widetilde{\Phi}(\widetilde{Q},\widetilde{R}) \end{array}$$

and we need to describe $\mathrm{Ker}\big(\mathbb{F}_p[X,Y] \twoheadrightarrow \widetilde{M}^p\big)$, which is to say the relations between $\widetilde{Q}$ and $\widetilde{R}$. To do so, we will use Serre's differential operator

$$\theta = q\frac{d}{dq} = \left(\sum_{n\geq 0} a_n q^n \mapsto \sum_{n\geq 0} n a_n q^n\right).$$

Theorem 10 (Ramanujan).

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

(2) We have the following identities:

$$\begin{aligned}(12\theta - P)P &= -Q,^3\\ (12\theta - 4P)Q &= -4R,\\ (12\theta - 6P)R &= -6Q^2,\\ (12\theta - 12P)\Delta &= 0.\end{aligned}$$

Idea of the proof. For the proof of (1), one can express θ in terms of $\frac{d}{dz}$ and use implicit differentiation on the modularity condition.

For the proof of (2), it suffices to compare the first (i.e., constant) coefficients of the q–expansions on the left-hand and right-hand sides of each equality because M_4, M_6 and M_8 are 1–dimensional. □

Definition 11. Let ∂ be the *graded derivation* on M given by

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

Remarks.

(1) Since $\partial Q = -4R$ and $\partial R = -6Q^2$, we see that ∂ acts on $M^p = \mathbb{Z}_{(p)}[Q,R]$. Define ∂ on $\mathbb{Z}_{(p)}[X,Y]$ (resp. on $\mathbb{F}_p[X,Y]$) by $\partial X = -4Y$ and $\partial Y = -6X^2$.

(2) For $f \in M_k^p$, we define $\partial\widetilde{f} = \partial f \bmod p \in \widetilde{M}^p_{k+2}$. Thus $\partial\widetilde{f} = (12\theta - k\widetilde{P})\widetilde{f}$ in $\mathbb{F}_p[\![q]\!]$. There is an abuse of notation here, as $\widetilde{k} \in \mathbb{F}_p$ depends on the choice of the representative f, not only on $\widetilde{f}$. (We also write 12 and k for their images in $\mathbb{F}_p$; it should be clear from the context.)

Next, we want to focus on some congruences between Eisenstein series, which are the first building block of the algebras of modular forms. Recall from example 4 that in the definition of E_{2k} appears the Bernoulli number B_{2k}. Therefore, we need to recall some classical congruences between Bernoulli numbers first.

Theorem 12. *Let $k \in \mathbb{Z}_{\geq 1}$.*

[3] I did not forget a $k = 2$ before the first P; as mentioned earlier, P is somewhat special. We will see that this coefficient before P has to be $\equiv p+1 \bmod p$ for every $p \geq 5$, so it really must be 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 13.

(1) $E_{p-1} \in M^p_{p-1}$ *and* $\widetilde{E}_{p-1} = 1$.

(2) $E_{p+1} \in M^p_{p+1}$ *and* $\widetilde{E}_{p+1} = \widetilde{P}$.

Proof. Items (1) and (2) follow from the explicit formulae for the Eisenstein series E_{p-1} and E_{p+1} and from items (1) and (2) of theorem 12, respectively. (The proof of (2) also uses Fermat's little theorem.) □

Corollary 14. *The subalgebra* $\widetilde{M}^p$ *of* $\mathbb{F}_p[\![q]\!]$ *is stable under the action of* θ.

Proof. Given $\widetilde{f} \in \widetilde{M}^p_k$, we can express

$$12\theta\widetilde{f} = k\widetilde{P}\widetilde{f} + \partial\widetilde{f} = k\widetilde{E}_{p+1}\widetilde{f} + \widetilde{E}_{p-1}\partial\widetilde{f}.$$

Since the terms appearing in the right-hand side are reductions of actual modular forms (cf. part (1) of theorem 10), we can see looking at the weights that

$$\widetilde{E}_{p+1}\widetilde{f} \in \widetilde{M}^p_{k+p+1} \quad \text{and} \quad \widetilde{E}_{p-1}\partial\widetilde{f} \in \widetilde{M}^p_{k+p+1}.$$

Therefore, $\theta\widetilde{f} \in \widetilde{M}^p_{k+p+1}$. □

We have almost all the tools required to give an explicit algebraic description of $\widetilde{M}^p$. Recall that we have surjective homomorphisms

$$\begin{array}{ccccc} M^p \cong \mathbb{Z}_{(p)}[X,Y] & \twoheadrightarrow & \mathbb{F}_p[X,Y] & \twoheadrightarrow & \widetilde{M}^p \subset \mathbb{F}_p[\![q]\!] \\ \Phi(X,Y) & \longmapsto & \widetilde{\Phi}(X,Y) & \longmapsto & \widetilde{\Phi}(\widetilde{Q},\widetilde{R}) \end{array}$$

and it is now apparent that both Eisenstein series E_{p-1} and E_{p+1} play some role in determining the structure of $\widetilde{M}^p$. Indeed,

- the congruence $\widetilde{E}_{p-1} = 1$ yields a non-trivial element of the kernel of the reduction map $M^p \twoheadrightarrow \widetilde{M}^p$ and
- the congruence $\widetilde{E}_{p+1} = \widetilde{P}$ allows us to replace any occurrence of P (usually coming from the definition of ∂) by the modular form E_{p+1}.

Definition 15. We define $A, B \in \mathbb{Z}_{(p)}[X, Y]$ to be the polynomials uniquely characterized by the equations

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

Lemma 16. *The reductions modulo p of A and B satisfy that*

$$\partial \widetilde{A} = \widetilde{B} \quad \textit{and} \quad \partial \widetilde{B} = -X\widetilde{A} \quad \textit{in } \mathbb{F}_p[X, Y].$$

Proof. First observe that, since $\widetilde{E}_{p-1} = 1$, we can express

$$\partial \widetilde{E}_{p-1} = 12\theta \widetilde{E}_{p-1} + \widetilde{P}\widetilde{E}_{p-1} = \widetilde{P}\widetilde{E}_{p-1} = \widetilde{E}_{p+1}.$$

This is only possible if $\partial A(Q, R) - B(Q, R) \in pM^p_{p+1}$ or, equivalently under the isomorphism $M^p \cong \mathbb{Z}_{(p)}[X, Y]$, $\partial A - B \in p\mathbb{Z}_{(p)}[X, Y]$. Therefore, $\partial \widetilde{A} - \widetilde{B} = 0$ in $\mathbb{F}_p[X, Y]$.

Similarly, for the second identity, we express

$$\partial \widetilde{E}_{p+1} = (12\theta - \widetilde{P})\widetilde{E}_{p+1} = (12\theta - \widetilde{P})\widetilde{P} = -\widetilde{Q} = -\widetilde{Q}\widetilde{E}_{p-1},$$

where in the second-to-last equality we used theorem 10. But this is only possible if $\partial B(Q, R) + QA(Q, R) \in pM^p_{p+3}$ or, equivalently, $\partial B + XA \in p\mathbb{Z}_{(p)}[X, Y]$. Hence, $\partial \widetilde{B} + X\widetilde{A} = 0$ in $\mathbb{F}_p[X, Y]$. □

Lemma 17. *The polynomial $\widetilde{A}$ has no repeated factors in $\overline{\mathbb{F}}_p[X, Y]$ and is prime to $\widetilde{B}$.*

Proof. Recall that X and Y have weights 4 and 6, respectively. Since $\widetilde{A}$ is isobaric (of weight $p - 1$), its factors must be of the form $X^3 - cY^2$ with $c \in \overline{\mathbb{F}}_p^\times$ or X or Y.

- Suppose that there exist $c \in \overline{\mathbb{F}}_p^\times$ and $n \in \mathbb{Z}_{\geq 2}$ such that $(X^3 - cY^2)^n$ divides $\widetilde{A}$ exactly. Since $\widetilde{A}(\widetilde{Q}, \widetilde{R}) = 1$ and $\widetilde{Q}^3 - \widetilde{R}^2 = 1728\widetilde{\Delta} \in q\mathbb{F}_p[\![q]\!]$, we see that $c \neq 1$. But then $\partial(X^3 - cY^2) = 12(c - 1)X^2Y$ is prime to $X^3 - cY^2$, which implies that $(X^3 - cY^2)^{n-1}$ divides $\partial \widetilde{A} = \widetilde{B}$ exactly and (repeating the argument) that $(X^3 - cY^2)^{n-2}$ divides $\partial \widetilde{B} = -X\widetilde{A}$ exactly. Thus, we obtain a contradiction (as $n - 2 < n$).
- Similar arguments show that it is impossible that X^n or Y^n for $n \in \mathbb{Z}_{\geq 2}$ divide $\widetilde{A}$ exactly.
- In conclusion, the factors of $\widetilde{A}$ have multiplicity $n = 1$ and so appear with multiplicity $n - 1 = 0$ in $\widetilde{B} = \partial \widetilde{A}$. □

We are finally in a position to state and proof the main theorem of this talk, which gives an explicit algebraic description of the algebra $\widetilde{M}^p$:

Theorem 18. *The algebra $\widetilde{M}^p$ of modular forms modulo p is isomorphic to the ring $\mathbb{F}_p[X, Y] \,/\, (\widetilde{A} - 1)$ via*

$$\Phi(Q, R) \longmapsto \widetilde{\Phi}(X, Y).$$

Proof. Let $\mathfrak{a}$ be the kernel of the morphism $\mathbb{F}_p[X,Y] \twoheadrightarrow \widetilde{M}^p \subset \mathbb{F}_p[\![q]\!]$ defined by

$$\varphi(X,Y) \longmapsto \varphi(\widetilde{Q},\widetilde{R}).$$

It is clear that the ideal $(\widetilde{A}-1)$ is contained in $\mathfrak{a}$; it remains to check that this inclusion is actually an equality.

Since $\mathbb{F}_p[\![q]\!]$ is a domain, we see that $\mathfrak{a}$ is a prime ideal of $\mathbb{F}_p[X,Y]$. But $\mathbb{F}_p[X,Y]$ has Krull dimension 2 and $\mathfrak{a}$ is not maximal because $\widetilde{M}^p \cong \mathbb{F}_p[X,Y]\,/\,\mathfrak{a}$ is not finite. Therefore, $\mathfrak{a}$ must have height 1. Since the ideal $(\widetilde{A}-1)$ has height 1 too, it suffices to prove that it is prime.

Suppose, for the sake of contradiction, that the polynomial $\widetilde{A}-1$ is not irreducible and let φ be one of its irreducible factors. Decompose

$$\varphi = \varphi_n + \varphi_{n-1} + \cdots + \varphi_0,$$

where φ_k is an isobaric polynomial of weight k for each $k \in \{\,0,1,\ldots,n\,\}$, and suppose that $\varphi_n \neq 0$. In particular, $n < p-1 = \deg(\widetilde{A})$. Let $\zeta \in \overline{\mathbb{F}}_p$ be a primitive $(p-1)$–th root of 1. Since

$$\widetilde{A}(\zeta^4 X, \zeta^6 Y) = \widetilde{A}(X,Y) \quad \text{but} \quad \varphi_n(\zeta^4 X, \zeta^6 Y) = \zeta^n \varphi_n(X,Y) \neq \varphi_n(X,Y),$$

we obtain another irreducible factor of $\widetilde{A}-1$ (distinct from φ): we can write

$$\widetilde{A}(X,Y) - 1 = \varphi(X,Y)\varphi(\zeta^4 X, \zeta^6 Y)\psi(X,Y) \quad \text{for some } \psi \in \mathbb{F}_p[X,Y]$$

and decompose $\psi = \psi_m + \psi_{m-1} + \cdots + \psi_0$, where ψ_k is an isobaric polynomial of weight k for each $k \in \{\,0,1,\ldots,m\,\}$ and $\psi_m \neq 0$. Comparing the terms of maximal weight in both sides of the previous equation, we conclude that

$$\widetilde{A}(X,Y) = \varphi_n(X,Y)\varphi_n(\zeta^4 X, \zeta^6 Y)\psi_m(X,Y) = \zeta^n \big(\varphi_n(X,Y)\big)^2 \psi_m(X,Y),$$

which contradicts lemma 17. □

After seeing these results, one may wonder about congruences modulo higher powers of p. Or even modulo *all* powers of p at the same time, which leads to the notion of what are known as *p–adic modular forms*. But the arguments in that direction start being less elementary.

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] 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.