BASIC NOTIONS IN MODULAR FORMS ON GL_2

EYAL GOREN (MCGILL UNIVERSITY)

Séminaire de Mathématiques Supérieures
"Automorphic forms and L-functions: computational aspects".
June 22- July 3, 2009, CRM, Montreal.

1

1.1. **The Upper 1/2 plane.** Let

$$\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\},$$

be the upper half plane. It is a (non-compact) Riemann surface and its automorphism group as a Riemann surface is

$$\mathrm{Aut}(\mathfrak{H}) = \mathrm{PGL}_2(\mathbb{R})^+ = \mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I_2\},$$

where the plus sign denotes matrices with positive determinant. A fundamental result of Riemann states that every simply connected connected Riemann surface is isomorphic to $\mathbb{C}, \mathbb{P}^1(\mathbb{C})$ or $\mathfrak{H}$. In fact, any punctured Riemann surface, R (namely $R \subseteq \overline{R}$ with $\overline{R}$ a compact Riemann surface and $\overline{R} - R$ a finite set of points), which is hyperbolic, that is,

$$2 - 2 \cdot \mathrm{genus}(R) - \sharp \text{ punctures} < 0,$$

has $\mathfrak{H}$ as a universal covering space.

1.2. The group $SL_2(\mathbb{R})$ acts transitively on $\mathfrak{H}$. The stabilizer of i is

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1 \right\} \cong \mathrm{SO}_2(\mathbb{R}).$$

We therefore have an identification:

$$\mathfrak{H} \cong \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}).$$

The involution $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ has i as an isolated fixed point. One concludes that $\mathfrak{H}$ is a hermitian symmetric space.

1.3. Lattices. Consider lattices $L \subseteq \mathbb{C}$. By choosing a basis, we may write

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

and, without loss of generality, $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$. We would like to classify lattices up to rescaling. The quantity $\tau = \frac{\omega_1}{\omega_2}$ doesn't change under rescaling, but depends on the choice of basis. Given another choice of basis $a\omega_1 + b\omega_2, c\omega_1 + d\omega_2$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, such that $\frac{a\omega_1+b\omega_2}{c\omega_1+d\omega_2} \in \mathfrak{H}$, then in fact $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and

$$\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d}.$$

One concludes that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ classified lattices up to rescaling. (The inverse map is of course $\tau \mapsto L_\tau := \mathbb{Z}\tau \oplus \mathbb{Z}$.) The Riemann surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ is isomorphic to $\mathbb{C}$; one such isomorphism is provided by the modular function j, $j(\tau) = \frac{1}{q} + 744 + 196884q + \ldots$, $q = e^{2\pi i\tau}$.

1.4. Elliptic curves. An elliptic curve over $\mathbb{C}$ is isomorphic as a complex analytic manifold to $\mathbb{C}/L$, where $L \subset \mathbb{C}$ is a lattice, and vice-versa. The lattice L is uniquely determined up to rescaling. One concludes that there is a bijection:

$$\{\text{Elliptic curves}/\mathbb{C}\}/\cong \quad \longleftrightarrow \quad \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}.$$

Given a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index, one can ask if the complex manifold $\Gamma\backslash\mathfrak{H}$ has also an interpretation as a parameter space. The answer is always yes, but it's easier to explain the objects being parameterized in the case of the following subgroups. Let $N \geq 1$ be an integer and let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N|c \right\},$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N|c, N|(a-1), N|(c-1) \right\}.$$

We then have

$$Y_0(N) := \Gamma_0(N)\backslash\mathfrak{H} \quad \longleftrightarrow \quad \{(E, H) : E/\mathbb{C} \text{ ell. curve}, H \subset E \text{ cyclic gp of order} N\}/\cong,$$

and

$$Y_1(N) := \Gamma_1(N)\backslash\mathfrak{H} \quad \longleftrightarrow \quad \{(E, P) : E/\mathbb{C} \text{ ell. curve}, P \in E \text{ of exact order} N\}/\cong .$$

(One says that $(E_1, H_1) \cong (E_2, H_2)$ if there is an isomorphism $\varphi : E_1 \to E_2$ such that $\varphi(H_1) = H_2$; similarly for points of order N.) The maps in one direction are $\tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau, \langle\frac{1}{N}\rangle)$ and $\tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau, \frac{1}{N})$.

1.5. Integral models. There are (reduced) schemes over $\mathbb{Z}$, $\mathscr{Y}_0(N), \mathscr{Y}_1(N)$, with the following properties:

(1) $\mathscr{Y}_i(N) \to \mathrm{Spec}(\mathbb{Z})$ is a relative quasi-projective curve with connected geometric fibers.
(2) $\mathscr{Y}_i(N) \otimes_{\mathbb{Z}} \mathbb{C} \cong Y_i(N)$ as complex manifolds.

(3) For every algebraically closed field k there is a natural bijection between $\mathscr{Y}_i(N)(k)$ and isomorphism classes of pairs $(E, *)$ (where $*$ is either a cyclic subgroup of order N, or a point of exact order N) defined over k. One says that $\mathscr{Y}_i(N)$ are coarse moduli schemes.
(4) $\mathscr{Y}_i(N) \to \mathrm{Spec}(\mathbb{Z}[1/N])$ is smooth.

The notion of a cyclic group H of order N when $\mathrm{char}(k)|N$ just means that H doesn't contain $E[m]$ for any $m > 1$; the notion of a point of exact order N is more subtle and one needs the notion of Drinfeld level structures as in Katz-Mazur.

For $N \geq 3$, $\mathscr{Y}_1(N)$ is a fine moduli scheme, which means that in property (3) above one can replace k by any scheme.

Let p be a prime and N_1 a positive integer such that $p \nmid N_1$. Let $N = pN_1$. The fibre of $\mathscr{Y}_0(N)$ over $\mathbb{F}_p$, namely, the reduction of $\mathscr{Y}_0(N)$ modulo p, is a union of two copies of $\mathscr{Y}_0(N_1) \otimes \mathbb{F}_p$, crossing transversely at the supersingular points - the points corresponding to (E, H) where E is a supersingular elliptic curve. The morphism $\mathscr{Y}_0(N) \to \mathscr{Y}_0(N_1)$ (obtained by taking the "prime to p" part of the subgroup) is an isomorphism on one of the components of $\mathscr{Y}_0(N)$ and purely inseparable of degree p on the other component. Given a point $(E, H) \in \mathscr{Y}_0(N_1)(\overline{\mathbb{F}}_p)$ its two preimages in $\mathscr{Y}_0(N)$ are $(E, H \times \mathrm{Ker}(\mathrm{Fr}))$ and $(E, H \times \mathrm{Ker}(\mathrm{Ver}))$, where $\mathrm{Fr} : E \to E^{(p)}$ is the Frobenius morphism and $\mathrm{Ver} : E \to E^{(1/p)}$ is the verschiebung morphism. We note that E is supersingular if and only if $\mathrm{Ker}(\mathrm{Fr}) = \mathrm{Ker}(\mathrm{Ver})$ and that explains why the two components intersect exactly above the supersingular points.

1.6. The modular polynomial. There is a morphism

$$Y_0(N) \to Y_0(1) \times Y_0(1), \qquad (E, C) \mapsto (E, E/C).$$

Consider the image of $Y_0(N)$ under this morphism. Since $Y_0(1)$ is the j-line, and the image is closed (extend the map to $X_0(N)$ and use properness), the image is given by a polynomial $\Phi_N(j, j')$, where we use j' for the coordinate on the second copy of $Y_0(1)$. There is a lot that can be said about this polynomial, using "pure thought". For example, the existence of dual isogeny implies it's symmetric. The existence of this whole set up over $\mathrm{Spec}(\mathbb{Z})$ implies that it is a polynomial with integer coefficients. For fixed j, the polynomial has degree $\psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$ in j' as there are $\psi(N)$ cyclic subgroups $\{C_i\}$ of degree N in an elliptic curve, and the coefficient of $j'^{\psi(N)}$ is ± 1 (because the same argument can be made in any characteristic). Since the $j(E/C_i)$ are typically distinct (consider the corresponding τ's in the upper half plane modulo $\Gamma_0(N)$ for example), the polynomial is reduced. Since $X_0(N)$ is irreducible, the polynomial is irreducible.

The actual computation of the modular polynomials is not an easy matter due to the huge size of the coefficients. For $N = 2$ one obtains

$$\begin{aligned}(1.6.1) \quad \Phi_2(x, j) = {} & x^3 + j^3 - x^2 * j^2 + 1488 * (x^2 * j + x * j^2) - 162000 * (x^2 + j^2) \\ & + 40773375 * x * j + 8748000000 * (x + j) - 157464000000000,\end{aligned}$$

while for $N = 3$, one obtains

$$\begin{aligned}(1.6.2)\quad \Phi_N(x,j) = {} & x^4 + j^4 - x^3 * j^3 + 2232 * (x^3 * j^2 + x^2 * j^3) - 1069956 * (x^3 * j + x * j^3) + 36864000 * (x^3 + j^3) \\ & + 2587918086 * x^2 * j^2 + 8900222976000 * (x^2 * j + x * j^2) + 452984832000000 * (x^2 + j^2) \\ & - 770845966336000000 * x * j + 1855425871872000000000 * (x + j).\end{aligned}$$

We remark that this plane model of $Y_0(N)$ is in general highly singular.

1.7. Further reading.

- Charles, D.; Lauter, K.: Computing modular polynomials. LMS J. Comput. Math. 8 (2005), 195–204 (electronic).
- Deligne, P.; Rapoport, M.: Les schémas de modules de courbes elliptiques. Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.
- Katz, N. M.; Mazur, B.: Arithmetic moduli of elliptic curves. Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.
- Lang, S.: Elliptic functions. With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.
- Silverman, J. H.: The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992.
- Silverman, J. H.: Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

2

2.1. Complex modular forms. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be either $\Gamma_0(N)$ or $\Gamma_1(N)$, although much of the discussion will work for any congruence subgroup Γ. A modular form of level Γ and weight k is a holomorphic function

$$f : \mathfrak{H} \to \mathbb{C},$$

such that

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Define a function $j : \Gamma \times \mathfrak{H} \to \mathbb{C}$ by

$$j(\gamma, \tau) = c\tau + d.$$

For any integer k, $j(\gamma,\tau)^k$ is a cocycle in $Z^1(\Gamma, \mathcal{O}_{\mathfrak{H}}^\times)$, also called a factor of automorphy. This means that $j(\gamma,\tau)^k$ never vanishes and it satisfies the identities

$$j(\gamma_1\gamma_2, \tau)^k = j(\gamma_1, \gamma_2\tau)^k \cdot j(\gamma_2, \tau)^k, \qquad \gamma_1, \gamma_2 \in \Gamma.$$

2.2. A factor of automorphy allows us to define a line bundle on $\Gamma\backslash\mathfrak{H}$. We take the trivial line bundle $T = \mathfrak{H} \times \mathbb{C}$ over $\mathfrak{H}$ and glue (τ, α) to $(\gamma\tau, j(\gamma, \tau) \cdot \alpha)$. The cocycle relation guarantees that this glueing process is consistent. If Γ is torsion free (which is the case for $\Gamma_1(N)$ for $N > 3$), one obtains a line-bundle $\mathbb{E}$ on $\Gamma\backslash\mathfrak{H}$. The sections of $\mathbb{E}^k$ are modular forms of weight k.

In fact, the line bundle $\mathbb{E}$ is directly connected to the family of elliptic curves over $\Gamma\backslash\mathfrak{H}$. Recall that to $\tau \in \mathfrak{H}$ we have associated the elliptic curve $E_\tau = \mathbb{C}/L_\tau$, where $L_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$. Therefore, the line bundle T is naturally identified with the relative tangent space of the family of elliptic curves $\mathscr{E} \to \mathfrak{H}$ (a family whose fiber at τ is E_τ). If $\gamma \in \Gamma$ and $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ then $E_{\gamma\tau} = \mathbb{C}/\frac{1}{c\tau+d}(\mathbb{Z} \oplus \mathbb{Z}\tau)$ and there is an isomorphism $E_{\gamma\tau} \to E_\tau$ induced by multiplication by $j(\gamma, \tau)$. It follows that the relative tangent space at the origin of the family

$$\Gamma\backslash\mathscr{E} \to \Gamma\backslash\mathfrak{H}$$

is defined by the factor of automorphy $j(\gamma, \tau)^{-1}$. And so $\mathbb{E}$ is the relative contangent bundle of that family; it is sometimes called the Hodge bundle.

Suppose that $N > 3$. The scheme $\mathscr{Y}_1(N)$ then is a fine moduli scheme and so carries a universal family of elliptic curves $\pi : \mathscr{E} \to \mathscr{Y}_1(N)$. Let $\mathbb{E} = \pi_*\Omega^1_{\mathscr{E}/\mathscr{Y}_1(N)}$ be the Hodge bundle. We can then say that for any scheme R the modular forms of weight k and level $\Gamma_1(N)$ are the sections $H^0(\mathscr{Y}_1(N) \otimes_{\mathbb{Z}} R, \mathbb{E}^{\otimes k})$. This gives our previous definition over $\mathbb{C}$.

2.3. Katz's definition. Katz defines a modular form f of weight k and level Γ over a ring R to be a rule associating to a triple $(E, *, \omega)$ over an R-algebra S (where $*$ is either a point of order N, or a cyclic subgroup of order N) an element $f(E, *, \omega) \in S$ that depends only on the isomorphism class of $(E, *, \omega)$, commutes with base-change and satisfies

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

(The idea is that we use $\omega^{\otimes k}$ to trivialize $\mathbb{E}^{\otimes k}$.)

This definition has several advantages:

(1) It works also when Γ is not torsion free and allows us a very general notion of a modular form, in particular, a modular form over a finite field.
(2) It allows us to define algebraically the notion of q-expansion (see below).
(3) It allows us to construct certain modular forms, notably, the Hasse invariant.

Consider the situation over the complex numbers. Given a lattice L we can associate to it an elliptic curve and a differential $(\mathbb{C}/L, 2\pi i \cdot dz)$. The lattice is determined by the isomorphism class of E only up to a scalar. However, if we change the lattice L to the lattice λL then, under the isomorphism $\mathbb{C}/L \to \mathbb{C}/\lambda L$ the differential dz on $\mathbb{C}/L$ is identified with the differential $\lambda^{-1}dz$ on $\mathbb{C}/\lambda L$. We conclude that to give a complex elliptic curve with a differential (E, ω) is the same as to give a lattice in $\mathbb{C}$. Therefore, a modular form in the sense of Katz becomes a function on lattices

$$L \mapsto f(L) := f(\mathbb{C}/L, 2\pi i \cdot dz).$$

We then have $f(\lambda L)=f(\mathbb{C}/\lambda L, 2\pi i\cdot dz)=f(\mathbb{C}/L,\lambda\cdot 2\pi i\cdot dz)=\lambda^{-k}f(\mathbb{C}/L,2\pi i\cdot dz)=\lambda^{-k}f(L)$. We conclude that as a function on lattices a (Katz) modular form of weight k satisfies

$$f(\lambda L)=\lambda^{-k}f(L).$$

Conversely, given a homogenous function of lattices f of weight k, put

$$f(\tau)=f(\langle 1,\tau\rangle),\qquad \tau\in\mathfrak{H}.$$

Then, for $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z})$ we have, $f(\tau)=f(\langle 1,\tau\rangle)=f(\langle c\tau+d,a\tau+b\rangle)=f((c\tau+d)\langle 1,\gamma\tau\rangle)=(c\tau+d)^{-k}f(\gamma\tau)$ and so

$$f(\gamma\tau)=(c\tau+d)^k f(\tau).$$

This gives a more direct way to connect between Katz's definition of modular forms and modular forms as certain functions on the upper half plane. The more precise connection is through viewing modular forms as sections of the k-th power of the contangent bundle and realizing the Katz's definition is nothing but writing it down explicitly by choosing a trivialization of that bundle (the ω in the definition).

2.4. q-expansion. If $\Gamma=\Gamma_0(N)$ or $\Gamma_1(N)$ then $\gamma=\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\in\Gamma$, $\gamma\tau=\tau+1$, and we conclude that a modular form of weight k satisfies:

$$f(\tau+1)=f(\tau).$$

Therefore, f has an expansion

$$f(\tau)=\sum_{n\in\mathbb{Z}}a_n(f)q^n,\qquad q=e^{2\pi i\tau}.$$

Let $\mathfrak{H}^*=\mathfrak{H}\cup\mathbb{P}^1(\mathbb{Q})$. There is a way to extend the topology of $\mathfrak{H}$ to $\mathfrak{H}^*$ such that the quotient $X_0(\Gamma)$ (or $X_1(\Gamma)$) is a compact Riemann surface. The points $X_i(\Gamma)-Y_i(\Gamma)$ are finite in number and are called cusps. For example, a basis of open neighborhoods at ∞ are $\{\mathrm{Im}(z)>N\}$. Under this construction, the q-expansion given above is nothing else then the Laurent expansion of a function in a neighborhood of the point at infinity. Such a Laurent expansion exists at every cusp. One says that f is a holomorphic modular form if at every cusp the Laurent expansion is a Taylor expansion, namely, there are no negative powers of the parameter. In particular, at infinity, $f(\tau)=\sum_{n\geq 0}a_n(f)q^n$. This complex vector space is denoted $M_k(\Gamma)$. One says that f is a cusp form if it is holomorphic and at every cusp there is no constant term in the Taylor expansion, and in particular, at infinity, $f(\tau)=\sum_{n>0}a_n(f)q^n$. This complex vector space is denoted $S_k(\Gamma)$.

2.5. Tate curve. The q-expansion, initially an analytic concept, is in fact an algebraic concept. The family of elliptic curves $E_\tau,\tau\in\mathfrak{H}$, $E_\tau=\mathbb{C}/L_\tau, L_\tau=\mathbb{Z}\oplus\tau\mathbb{Z}$ can be "exponentiated". Via the exponential map, $z\mapsto e^{2\pi iz}$ the lattice L_τ is mapped to the multiplicative group $\langle q\rangle$, where $q=e^{2\pi i\tau}$ and $E_\tau\cong\mathbb{C}^\times/\langle q\rangle$. We now have a family of elliptic curves $\mathbb{C}^\times/\langle q\rangle$, parameterized by q such that $0<|q|<1$. We get a relative elliptic curve, defined by coefficients that are power series in q, and in fact, are in $\mathbb{Z}[\![q]\!]$ - a fact one proves by a long calculation. This curve is called

the Tate curve E_{Tate}. This "odd" coincidence of getting a family of elliptic curves, initially over the unit disc, but in fact over power series ring, was one of the motivating reasons for Tate to develop his theory of rigid analytic spaces! On this elliptic curve the relative differential $2\pi i \cdot dz$ on the family of elliptic curves E_τ becomes the differential $\frac{dt}{t}$, $t = e^{2\pi i z}$, which is algebraic. Given a modular form f defined over a ring R, we are then perfectly entitled to evaluate it at the elliptic curve $(E_{\mathrm{Tate}} \otimes R, \frac{dt}{t})$ and get a value lying in $R \otimes \mathbb{Z}(\!(q)\!) \subseteq R(\!(q)\!)$. The fundamental fact is that when R is the complex numbers, this is precisely the q-expansion of the modular form f. Thus, the construction of the Tate curve, in conjunction with Katz's point of view, allows us to define q-expansions algebraically, and in particular, over a field of positive characteristic. It makes then perfect sense to define a modular form defined over some ring R to be holomorphic if the q-expansions obtained by evaluating at the Tate curves, with all possible level structures, give elements of $R[\![q^{1/N}]\!]$ and not just $R(\!(q^{1/N})\!)$ (the definition of level structures on the Tate curve may necessitate passing to a larger ring where we adjoin $q^{1/N}$).

Besides this achievement, one obvious corollary of this method is that the Fourier coefficients of a modular form f defined over $\mathbb{Q}$ (say) are bounded. Indeed, the q-expansion lies in $\mathbb{Z}(\!(q)\!) \otimes_{\mathbb{Z}} \mathbb{Q}$.

2.6. Dimension formulas. There is yet another geometric interpretation for modular forms. To simplify the exposition we just deal with even weight modular forms and assume that $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a torsion free subgroup of finite index, $X_\Gamma = \Gamma \backslash \mathfrak{H}^*$. Let f be a modular form of weight 2 and level Γ. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ we have

$$d(\gamma\tau) = \frac{\det(\gamma)}{(c\tau + d)^2} \cdot d\tau,$$

and it follows that the holomorphic differential $f(\tau)d\tau$ is Γ-invariant. Since Γ is torsion free we may identify the holomorphic Γ-invariants differentials on $\mathfrak{H}$ with holomorphic differentials on $\Gamma \backslash \mathfrak{H}$. Consider the situation at infinity. We have $q = e^{2\pi i \tau}$ and so $d\tau = \frac{1}{2\pi i} \cdot \frac{dq}{q}$. So, locally,

$$f(\tau)d\tau = \left(\frac{1}{2\pi i} \sum_{n \in \mathbb{Z}} a_n(f) q^n \right) \frac{dq}{q}.$$

We conclude that holomorphic modular forms of weight 2 correspond to sections of $\Omega^1_{X_\Gamma}(\mathrm{cusps})$ (the sheaf meromorphic differentials with, at most, simple poles that are supported on the cusps), and that cusp forms of weight 2 correspond to sections of $\Omega^1_{X_\Gamma}$ (the sheaf of holomorphic differentials). Generalizing these considerations we find that

$$M_{2k}(\Gamma) = H^0(X_\Gamma, \Omega^{\otimes k}_{X_\Gamma}(k \cdot P_\Gamma)),$$

where P_Γ is the divisor which is the sum of the cusps (each with multiplicity 1), and

$$S_{2k}(\Gamma) = H^0(X_\Gamma, \Omega^{\otimes k}_{X_\Gamma}((k-1) \cdot P_\Gamma)).$$

Applying the Riemann-Roch formula, one finds the dimension formulas.

Theorem 2.6.1. *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a torsion-free, finite index subgroup. Let $\epsilon_\infty = \deg(P_\Gamma)$ be the number of cusps of Γ and g the genus of X_Γ. Then,*

$$\dim(M_{2k}(\Gamma)) = \begin{cases} (2k-1)(g-1) + k\cdot\epsilon_\infty & k \geq 1, \\ 1 & k = 0, \\ 0 & k < 0, \end{cases}$$

and

$$\dim(S_{2k}(\Gamma)) = \begin{cases} (2k-1)(g-1) + (k-1)\cdot\epsilon_\infty & k \geq 2, \\ g & k = 1, \\ 0 & k \leq 0. \end{cases}$$

We remark that there are closed formula for the genus. For example, for $p = 2, 3$, $X_0(p)$ has genus 0 and for a prime $p > 3$,

$$g(X_0(p)) = \frac{p+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{p}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{p}\right)\right)$$

(Legendre symbols). The group $\Gamma_0(p)$ is usually not torsion free, but we further remark that these considerations can be extended to provide closed dimension formulas for any weight $k \geq 2$ and any Γ.

2.7. Hecke operators. Consider the case of $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Thinking about a complex modular form f of level Γ in Katz's language, we may define for every prime $\ell \not| N$,

$$(T_\ell f)(E, C, \omega) = \frac{1}{\ell}\sum_H f(E/H, C + H/H, \omega_H),$$

where the summation is over all subgroups of order ℓ of E and ω_H is the differential on E/H that pulls back to ω under the projection map $E \mapsto E/H$. The definition is a little problematic in the sense that the subgroups need not be defined over the same base as E, but the argument that it works is not hard. On the other hand, it has the advantage that it extends to modular forms over any base ring R easily, as long as ℓ is invertible in R. A quick calculation over the complex numbers gives

$$(T_\ell f)(\tau) = \ell^{k-1} f(\ell\tau) + \frac{1}{\ell}\sum_{a=0}^{\ell-1} f\left(\frac{\tau + a}{\ell}\right).$$

Suppose that $f = \sum_n a_n q^n$ is of level $\Gamma_0(N)$ then, using the last formula, one calculates that

$$T_\ell f(q) = \sum_n a_{\ell n} q^n + \ell^{k-1}\sum_n a_n q^{\ell n}, \qquad (\ell \nmid N).$$

The formula is correct for modular forms over any base in which ℓ is invertible and is proven through Tate curves. In addition, one may also define Hecke operators for $\ell | N$, by

$$(T_\ell f)(E, C, \omega) = \frac{1}{\ell}\sum_H f(E/H, \omega_H),$$

where the sum now is over subgroups H such that $H \cap C = \{0\}$. The effect on q-expansion is now

$$(T_\ell f)(q) = \sum_n a_{\ell n} q^n, \qquad (\ell | N).$$

These operators are usually called U operators and denoted U_ℓ instead of T_ℓ. The family of operators U_ℓ for all ℓ (including $\ell | N$) form a commutative algebra. The operators $T_\ell, \ell \nmid N$ are semi-simple and can be simultaneously diagonalized.

2.8. Modular forms as functions on adele groups. Let $Z_\infty = \mathbb{R}^\times$ embedded diagonally in $\mathrm{GL}_2(\mathbb{R})^+$ and $K_\infty^+ = SO_2(\mathbb{R}) = \left\{k_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right) : \theta \in [0, 2\pi)\right\}$. The group $\mathrm{GL}_2(\mathbb{R})^+$ acts transitively on the upper half plane $\mathfrak{H}$ and the stabilizer of i is $Z_\infty K_\infty^+$. We find that

$$\mathfrak{H} = \mathrm{SL}_2(\mathbb{R})/K_\infty^+ = \mathrm{GL}_2(\mathbb{R})^+/Z_\infty K_\infty^+.$$

Let $f \in M_k(\Gamma)$, where $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is congruence subgroup. We define a function

$$\phi_f : \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C},$$

by

$$\phi_f(g_\infty) = j(g_\infty, i)^{-k} f(g_\infty(i)).$$

Note that f can be recovered from ϕ_f and so we get an injective linear map of $M_k(\Gamma)$ into the space of complex valued functions on $\mathrm{GL}_2(\mathbb{R})^+$.

Lemma 2.8.1. *The function $\phi = \phi_f$ has the following properties:*

(1) *ϕ is a smooth (i.e., C^∞) function on $\mathrm{GL}_2(\mathbb{R})^+$.*
(2) *$\phi(\gamma g_\infty) = \phi(g_\infty), \forall \gamma \in \Gamma$.*
(3) *$\phi(g_\infty k_\theta) = e^{-i\theta k}\phi(g_\infty)$, $k_\theta \in K_\infty^+$.*
(4) *$\phi(g_\infty z) = \phi(g_\infty)\,\mathrm{sgn}(z)^k$, $z \in Z_\infty$.*
(5) *If f is a cusp form then ϕ is* cuspidal*: for every $g_\infty \in \mathrm{GL}_2(\mathbb{R})^+$ we have*

$$\int_0^1 \phi_f\left(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) g_\infty\right) dx = 0.$$

(6) *ϕ satisfies a certain "slow-growth" condition.*

2.9.

Theorem 2.9.1. *(A special case of the* Strong Approximation Theorem*) Let G be a simply connected semi-simple algebraic group over $\mathbb{Q}$ such that $G(\mathbb{R})$ is non-compact. Then $G(\mathbb{Q})G(\mathbb{R})$ is dense in $G(\mathbb{A})$.*

The group SL_n is semi-simple, so, in particular, for every compact open subgroup $K_f \subset \mathrm{SL}_n(\mathbb{A}_f)$, one finds that

$$\mathrm{SL}_n(\mathbb{A}) = \mathrm{SL}_n(\mathbb{Q})\mathrm{SL}_n(\mathbb{R})K_f.$$

We remark that for a general reductive group G over a number field F the number of double cosets $G(F)\backslash G(\mathbb{A}_F)/G(\mathbb{A}_{F,S_\infty})$ is finite. One can prove that for the group GL_n the number of double cosets $\mathrm{GL}_n(F)\backslash \mathrm{GL}_n(\mathbb{A}_F)/\mathrm{GL}_n(\mathbb{A}_{F,S_\infty})$ is equal to the class number of F and so strong

approximation in its simplest form fails. On the other hand, the strong approximation theorem allows the following conclusion. Let $K_f \subset \mathrm{GL}_n(\mathbb{A}_f)$ be a compact open subgroup such that $\det(K_f) = \widehat{\mathbb{Z}}^\times$. Then

$$\mathrm{GL}_n(\mathbb{A}) = \mathrm{GL}_n(\mathbb{Q})\mathrm{GL}_n(\mathbb{R})^+ K_f.$$

Furthermore,

$$\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A})/K_f \cong \Gamma_{K_f}\backslash\mathrm{GL}_n(\mathbb{R})^+, \quad \Gamma_{K_f} = \mathrm{GL}_n(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{R})^+ K_f.$$

Let $n = 2$. Define the subgroups $K(N), K_1(N)$ and $K_0(N)$ of $\mathrm{GL}_2(\mathbb{A}_f)$ as the subgroups of elements $(M_p)_p$ such that we have $M_p \in \mathrm{GL}_2(\mathbb{Z}_p)$ and if $p^a||N$, $a > 0$, then also M_p is congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$, respectively. Note that only $K_0(N)$ satisfies the requirement on the determinant.

Suppose that $n = 2$ and K_f satisfies the determinant condition. It is easy to see that Γ_{K_f} is a congruence subgroup. Suppose that f is a modular form of weight k and level Γ_{K_f}. Then the function $\phi_f : \Gamma_{K_f}\backslash\mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$ we have previously defined may be transported to a function, still denoted ϕ_f, on $\mathrm{GL}_2(\mathbb{A})$ as follows:

$$\phi_f(\gamma g_\infty k) = \phi_f(g_\infty) = j(g_\infty, i)^{-k} f(g_\infty(i)),$$

where $\gamma \in \mathrm{GL}_2(\mathbb{Q}), g_\infty \in \mathrm{GL}_2(\mathbb{R})^+, k \in K_f$.

The function $\phi = \phi_f : \mathrm{GL}_2(\mathbb{A}) \to \mathbb{C}$ is well defined. Indeed, one checks that if $\gamma_1 g_1 k_1 = \gamma_2 g_2 k_2$ then $g_2 = \gamma_2^{-1}\gamma_1 g_1$ where in the right hand side we mean the projection on the infinite component and $\gamma_2^{-1}\gamma_1 = (g_2 g_1^{-1})(k_2 k_1^{-1})$ and so is in Γ_{K_f}. It follows that $\phi_f(g_2) = \phi_f(\gamma_2^{-1}\gamma_1 g_1) = \phi_f(g_1)$.

Lemma 2.9.2. *The function ϕ_f has the following properties.*

1. $\phi(\gamma g) = \phi(g), \forall \gamma \in \mathrm{GL}_2(\mathbb{Q})$.
2. $\phi(g k_f) = \phi(g), \forall k_f \in K_f$.
3. $\phi(g k_\theta) = e^{-ik\theta}\phi(g), \forall k_\theta \in K_\infty^+$.
4. *ϕ is invariant under Z_∞^+.*
5. *ϕ satisfies a slow growth condition.*
6. *If f is a cusp form then ϕ is cuspidal: for all $g \in \mathrm{GL}_2(\mathbb{A})$ we have*
$$\int_{\mathbb{Q}\backslash\mathbb{A}} \phi\left(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) g\right) dx = 0.$$
7. *$\Omega\phi = -\frac{k}{2}(\frac{k}{2} - 1)\phi$, where Ω is the suitably normalized Casimir operator.*

2.10. The case of $\Gamma_1(N)$. Modular forms on the group $\Gamma_0(N)$ with a character χ are of great interest. The problem is that such modular forms are actually modular forms on $\Gamma_1(N)$ but the group $K_1(N)$ doesn't satisfy the determinant condition and so we can not transfer them in the same way to $\mathrm{GL}_2(\mathbb{A})$. We thus modify our definitions slightly.

Let f is a modular form of weight k and character χ on $\Gamma_0(N)$. We may view χ is a character on $K_0(N)$ and we let

$$\phi(\gamma g_\infty k) = \phi(g_\infty)\chi(k), \quad k \in K_0(N), \tag{2.10.1}$$

where $\phi(g_\infty) = j(g_\infty, i)^{-k} f(g_\infty(i))$ (a function on $\Gamma_1(N)\backslash \mathrm{GL}_2(\mathbb{R})^+$, transforming under χ with respect to $\Gamma_0(N)$.) One can then prove that $\phi = \phi_f$ satisfies:

$$\phi(zg) = \chi(z)\phi(g), \quad \forall z \in Z(\mathbb{A}) = \mathbb{A}_{\mathbb{Q}}^{\times},$$

where χ is interpreted as a unitary grossencharacter.

Proposition 2.10.1. *There is an isomorphism*

$$S_k(\Gamma_0(N), \chi) \cong \mathcal{A}_0(\mathrm{GL}_2)(hol, k, N, \chi),$$

where $\mathcal{A}_0(\mathrm{GL}_2)(hol, k, N, \chi)$ is the space of functions on $\mathrm{GL}_2(\mathbb{A})$ which satisfy the following conditions:

(1) $\phi(\gamma g) = \phi(g), \forall \gamma \in \mathrm{GL}_2(\mathbb{Q})$.
(2) $\phi(gk) = \chi(k)\phi(g), \forall k \in K_0(N)$.
(3) $\phi(gk_\theta) = e^{-ik\theta}\phi(g), \forall k_\theta \in K_\infty^+$.
(4) *ϕ is invariant under Z_∞^+.*
(5) *ϕ satisfies a slow growth condition.*
(6) *ϕ is cuspidal: for all $g \in \mathrm{GL}_2(\mathbb{A})$ we have*

$$\int_{\mathbb{Q}\backslash\mathbb{A}} \phi\left(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) g\right) dx = 0.$$

(7) *$\Omega\phi = -\frac{k}{2}(\frac{k}{2} - 1)\phi$, where Ω is the suitably normalized Casimir operator.*

Remark 2.10.2. One can show that these conditions imply that $|\phi|$ is in $L^2(Z(\mathbb{A})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}))$ and that for $z \in Z(\mathbb{A})$ we have

$$\phi(zx) = \chi(z)f(x),$$

where χ is viewed as a Hecke character (use the decomposition $\mathbb{A}_{\mathbb{Q}}^{\times} = \mathbb{Q}^{\times}\mathbb{R}^{\times,+}\widehat{\mathbb{Z}}^{\times}$). This gives two different choices to developing the theory of automorphic forms: (i) via L^2 theory; (ii) via a more intrinsic notion of extending the space $\mathcal{A}_0(\mathrm{GL}_2)(hol, k, N, \chi)$ just enough as to make it a $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-module.

2.11. Eisenstein Series. Let

$$\Gamma(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma \equiv I_2 \pmod{N} \right\}.$$

Let $k \geq 3$ be an integer and $c, d \in \mathbb{Z}$. Let

$$G_k(\tau; c, d; N) = \sum_{\substack{m \equiv c \pmod N \\ n \equiv d \pmod N}}{}' (m\tau + n)^{-k}.$$

(The prime indicates that $(m, n) = (0, 0)$ is omitted, if it occurs at all.) This Eisenstein series is a modular form of weight k for the group $\Gamma(N)$. It depends only on $(c, d) \pmod N$. In

fact, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ then $G_k(\tau;c,d;N)|_k\gamma := j(\gamma,\tau)^{-k}G_k(\gamma\tau;(c,d);N) = G_k(\tau;(c,d)\gamma;N)$. As a consequence, for any $\Gamma \supseteq \Gamma(N)$ (e.g., $\Gamma_0(N), \Gamma_1(N)$) the function

$$\sum_{\gamma\in\Gamma/\Gamma(N)} G_k(\tau;c,d;N)|_k\gamma$$

is a modular form of weight k on Γ (possibly zero).

2.12. Theta functions. Let B a positive definite symmetric bilinear form on $\mathbb{R}^n$, represented relative to the standard basis $e_1,\dots,e_n$, by a matrix A with integer entries and even diagonal entries. Write $A = {}^tMM$ and let L be the lattice in $\mathbb{R}^n$ generator by the columns of M. The matrix A is the called the Gram matrix of L. The dual lattice $L^\vee$ of L, namely $\{x \in \mathbb{R}^n : x\cdot\ell \in \mathbb{Z}, \forall \ell \in L\}$, has generator matrix ${}^tM^{-1}$ (here the dot refers to the usual inner product on $\mathbb{R}^n$).The Gram matrix of $L^\vee$ is then $A^{-1} = M^{-1}\cdot {}^tM^{-1}$; it's symmetric and positive definite. Note that L is an even lattice: for $\ell \in L$, $\ell\cdot\ell \in 2\mathbb{Z}$.

The associated theta function is

$$\Theta_L(q) = \sum_{\ell\in L} q^{\ell\cdot\ell/2}, \qquad q = e^{2\pi i\tau}.$$

Then

$$\Theta_L(q) = \Theta_A(q) := \sum_{a\in\mathbb{Z}^n} q^{\frac{1}{2}A[a]} = \sum_{n=0}^{\infty} r(n)q^n,$$

where $A[a] = {}^taAa$ and $r(n) = \sharp\,\{a \in \mathbb{Z}^n : \frac{1}{2}A[a] = n\}$. If we let $Q(a) = \frac{1}{2}A[a]$ then Q is an integer valued quadratic form on $\mathbb{Z}^n$, whose associated bilinear form $Q(x+y) - Q(x) - Q(y)$ is A, and $r(n) = \sharp\,\{a \in \mathbb{Z}^n : Q(a) = n\}$ are the representation numbers for the quadratic form Q.

For a matrix A as above, the minimal N such that NA^{-1} is integral (this is the exponent of the finite group $L^\vee/L$), is called the level of A (or L). Assume that also NA^{-1} has even integral entries and $n = 2k$ is an even integer. The main theorem is the following.

Theorem 2.12.1. *$\Theta_A(q)$ is a modular form on $\Gamma_0(N)$, of weight k and a quadratic character $\left(\frac{D}{\cdot}\right)$, where $D = (-1)^k\det(A)$. That means that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_0(N)$ we have*

$$f(\gamma\tau) = \left(\frac{D}{d}\right) j(\gamma,t)^k f(t).$$

(So, in particular, f is a modular form on $\Gamma_1(N)$).

2.13. Quaternion algebras. Let R be a maximal order in the quaternion algebra $B_{p,\infty}$ - "the" quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞. Choose a basis $e_1,\dots,e_4$ for R and consider the matrix

$$A = (\mathrm{Tr}(e_i\bar{e}_j))_{i,j},$$

where Tr is the reduced trace from $B_{p,\infty}$ to $\mathbb{Q}$ and $\bar{x} = \mathrm{Tr}(x) - x$. As is easily verified, the matrix A is a 4×4 symmetric positive definite matrix, with integral entries and even diagonal entries. Its determinant is p^2. The level of A is p and it turns out that pA^{-1} has again even diagonal entries.

Example. Let p be a prime congruent to 3 mod 4. Then

$$B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right).$$

Thus, $B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$, where

$$i^2 = -1, \quad j^2 = -p, \quad ij = -ji = k.$$

We have $\mathrm{Tr}(a + bi + cj + dk) = 2a$. A maximal order is given by $\mathbb{Z}[1, i, (i + j)/2, (1 + k)/2]$, and the Gram matrix relative to this basis is

$$A = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & (p+1)/2 & 0 \\ 1 & 0 & 0 & (p+1)/2 \end{pmatrix}.$$

One checks that

$$pA^{-1} = \begin{pmatrix} (p+1)/2 & 0 & 0 & -1 \\ 0 & (p+1)/2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 0 & 2 \end{pmatrix}.$$

In fact, the construction can be generalized even further. Let $\mathfrak{a}$ be a left ideal for a maximal order. Then the quadratic form

$$q_{\mathfrak{a}} : \mathfrak{a} \to \mathbb{Z}, \qquad q(x) = \mathrm{Norm}(\mathfrak{a})^{-1}\mathrm{Norm}(x),$$

is integer valued and the associated bilinear form is represented by a matrix A having integral entries, even diagonal entries, determinant p^2, level p, and pA^{-1} also has even diagonal entries. (We remark that $\mathrm{Norm}(x) = x\bar{x}$ and $\mathrm{Norm}(\mathfrak{a})$ is the $\mathbb{Z}$-module generated by all the norms of elements of $\mathfrak{a}$.) Running over all ideals $\mathfrak{a}$ for all maximal orders we get a collection of theta functions $\Theta_{q_{\mathfrak{a}}}$ that are modular forms of weight 2 and level $\Gamma_0(p)$. The positive solution to Eichler's basis problem says in this case that these theta series span $M_2(\Gamma_0(p))$.

The construction can be generalized to modular forms of higher weight by using harmonic polynomials, and at the same time to modular forms of higher level by using Eichler orders instead of maximal orders.

2.14. Further reading.

- Bump, D.: Automorphic forms and representations. Cambridge Studies in Advanced Mathematics, 55. Cambridge University Press, Cambridge, 1997.
- Bump, D.; Cogdell, J. W.; de Shalit, E.; Gaitsgory, D.; Kowalski, E.; Kudla, S. S.: An introduction to the Langlands program. Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001. Edited by Joseph Bernstein and Stephen Gelbart. Birkhuser Boston, Inc., Boston, MA, 2003.
- Diamond, F.; Shurman, J.: A first course in modular forms. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.
- Gelbart, S. S.: Automorphic forms on adèle groups. Annals of Mathematics Studies, No. 83. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

- Iwaniec, H.: Topics in classical automorphic forms. Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.
- Katz, N.: p-adic properties of modular schemes and modular forms. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 69–190. Lecture Notes in Mathematics, Vol. 350, Springer, Berlin, 1973.
- Ogg, A.: Modular forms and Dirichlet series. W. A. Benjamin, Inc., New York-Amsterdam 1969.
- Pizer, A.: An algorithm for computing modular forms on $\Gamma_0(N)$. J. Algebra 64 (1980), no. 2, 340–390.
- Serre, J.-P.: A course in arithmetic. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.
- Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kan Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.
- Silverman, J. H.: The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992.
- Silverman, J. H.: Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.
- Tate, J.: A review of non-Archimedean elliptic functions. Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 162–184, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

3

This section is concerned with presenting several ways in which modular forms modulo p, or the structure of modular curves modulo p, interact with characteristic zero phenomena.

3.1. La méthode des graphes. This method, utilized by Mestre and Oesterlé, makes use of the structure of quaternion algebras to quickly compute bases for modular forms on $S_k(\Gamma_0(pN_1))$, where N_1 is prime to p. To illustrate the idea, we shall assume that $k = 2$ and $N_1 = 1$ and $p > 2$. Recall that by the solution to Eichler's basis problem all modular forms of weight 2 and level $\Gamma_0(p)$ are spanned by theta series of ideals for maximal orders in the quaternion algebra $B_{p,\infty}$. The theta series are associated to the norm form on such an ideal $\mathfrak{a}$, scaled by $\mathrm{Norm}(\mathfrak{a})^{-1}$. It is thus clear that the theta series depend only on the $\lambda_1\mathfrak{a}\lambda_2$, where $\lambda_i \in B_{p,\infty}^\times$.

Let R_1 be a maximal order of $B_{p,\infty}^\times$. There is a supersingular elliptic curve E_1 over $\mathbb{F}_{p^2}$, such that $R_1 \cong \mathrm{End}(E_1)$. Consider left ideals $\mathfrak{a}$ of R_1, up to the equivalence $\mathfrak{a} \sim \mathfrak{a}\lambda$, where $\lambda \in B_{p,\infty}^\times$. The number of ideal classes is finite and is equal to the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, i.e., the number of supersingular j-invariants. Denote this number by $\hbar$ and let $E_1, \dots, E_\hbar$ be representatives for the supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Every supersingular elliptic curve E_i, furnishes us with a projective rank 1 left R_1-module, $\mathrm{Hom}(E_i, E_1)$, with a natural quadratic form – the degree of the isogeny. It turns out that the isomorphism classes of these quadratic modules are precisely the ideal classes for R_1 with the scaled norm form. Given such an ideal $\mathfrak{a}$, its right order is another maximal order, corresponding to $\mathrm{End}(E_i)$ under the interpretation above.

Fix representatives $I_1, \ldots, I_\hbar$ for the ideal classes of R_1. Let R_i be the right order of I_i. One can show that for every j the ideals $I_j^{-1} I_i$ are representatives for the ideal classes of R_j and we can think about them as coming from $\mathrm{Hom}(E_i, E_j)$ (j fixed).

Let $n \geq 1$ be an integer and form the n-th Brandt matrix $B(n) = (B(n)_{ij})$, whose ij entry is the number of isogenies in $\mathrm{Hom}(E_i, E_j)$ of degree n divided by $|R_j^\times|$. One can phrase that in terms of the ideals $I_j^{-1} I_i$. The fundamental fact is that the representation of the Brandt matrices on the vector space, which we can interpret as the vector space on the basis consisting of supersingular j-invariants, is isomorphic to the representation of the Hecke algebra on modular forms of weight 2 on $\Gamma_0(p)$, where the ℓ-th Hecke operator corresponds to $B(\ell)$. The method of graphs is concerned with quickly constructing the matrices $B(n)$.

Suppose one looks for eigenforms, i.e., eigenvectors for the Hecke algebra; these are of the utmost importance in connections with Galois representations and L-series. Such an eigenform is an eigenform also of the operator T_2, and, conversely, if it is an eigenform of the operator T_2 then it is an eigenform for every operator in $\mathbb{Z}[T_2]$ (a subring of the Hecke ring), and is thus likely to be an eigenform of the whole Hecke algebra. Thus, for many cases, it is enough to construct the operator T_2. Looking at $B(2)$, we notice that it is a matrix in which the sum of any row or columns is 3 (the number of subgroups of order 2 of an elliptic curve) and the entries are non-negative integers. We can think about $B(2)$ as providing an oriented graph structure on vertices corresponding to supersingular j-invariants. It turns out that this graph is Ramanujan – an excellent expander – which implies that by adjoining to a vertex its neighbors, and then to these neighbors their own neighbors, and so on, one exhausts the graph after about log of the number of vertices. Begin therefore with a supersingular j-invariant and calculate all the j-invariants that are 2-isogenous to it (one uses the modular polynomial $\Phi_2(j, j')$. The first step requires solving a cubic polynomial, but the rest of the steps require solving only quadratic polynomials as one of the edges "goes back") and so on. This way, very quickly, one calculates all the supersingular j-invariants and, at the same time, the matrix of $B(2)$.

3.2. Modular forms of weight 1. Modular forms of weight one that are eigenforms provide one with a finite image Galois representations. In that context we have the Artin conjecture saying that two dimensional complex Galois representations all arise from modular forms of weight 1; many cases are known.

It is thus an interesting problem to compute the space of modular forms of weight 1 and of a given level. Although this is a finite dimensional vector space there isn't a formula for its dimension. The extension of the Riemann-Roch technique to modular forms of weight 1 gives no information.

Using Katz's language we can define the following in characteristic p.

- Let k be a perfect field of characteristic p. Let $\sigma : k \to k, \sigma(x) = x^p$. Let $V : E \to E^{(1/p)}$ be the dual isogeny to the Frobenius isogeny $F : E^{(1/p)} \to E$. It induces a linear map

$$V^* : H^0(E, \Omega^1_{E^{(1/p)}/k}) \to H^0(E, \Omega^1_{E/k}),$$

and so, since $H^0(E,\Omega^1_{E^{(1/p)}/k}) = H^0(E,\Omega^1_{E^{(1/p)}/k}) \otimes_{k,\sigma^{-1}} k$, a σ^{-1}-linear map

$$H^0(E,\Omega^1_{E/k}) \to H^0(E,\Omega^1_{E/k}),$$

that we denote, by abuse of notation, also V.

We now define

$$h(E,\omega) = [V(\omega)/\omega]^p.$$

One proves that h is a modular form of weight $p-1$ called the Hasse invariant. For example, Note that $h(E,\lambda\omega) = [V(\lambda\omega)/\lambda\omega]^p = \lambda^{-(p-1)} \cdot [V(\omega)/\omega]^p$. Calculating the modular form on the reduction of the Tate curve modulo p, one calculates that $V(dq/q)$ is dq/q and one finds that h has q-expansion 1, though it's not the constant modular form 1. In fact, considering the q-expansion map on the graded ring of elliptic modular forms of level $\Gamma_0(N), (N,p)=1$, one finds that the kernel is the principal ideal $(h-1)$.

- Given a modular form f, let $F(f)$ be the modular form defined by

$$F(f)(E,\omega) = F(E^{(p)},\omega^{(p)})$$

(the base change of the object (E,ω)). If one considers the effect on this operation on the Tate curve one finds that if $f(q) = \sum_n a_n q^n$ then $F(f)(q) = \sum_n a_n q^{pn}$. Note that if f has weight k then $F(f)$ has weight pk (use that $(\lambda\omega)^{(p)} = \lambda^p \omega^{(p)}$).

Edixhoven provided an explicit constant B, in fact $B = \psi(N)/12$, such that if $g \in S_p(\Gamma_1(N),\mathbb{F}_p)$ is such that $a_n(g) = 0$ for all $n \le B$ not divisible by p, then $g = F(f)$ for some $f \in S_1(\Gamma_1(N),\mathbb{F}_p)$. This way, the computation of modular forms of weight 1, can be reduced to the computation of modular forms of weight p.

3.3. Hilbert modular forms. Almost everything mentioned so far has a generalization to Hilbert modular forms. Some initial references are given below.

3.4. Further reading.

- Andreatta, F.; Goren, E. Z.: Hilbert modular forms: mod p and p-adic aspects. Mem. Amer. Math. Soc. 173 (2005), no. 819.
- D. X. Charles, E. Z. Goren and K. E. Lauter: Families of Ramanujan graphs and quaternion algebras. To appear in special AMS-CRM volume "Groups and Symmetries" in honor of John McKay.
- Deligne, P.; Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. (4) 7 (1974), 507–530 (1975).
- Duke, W.: The dimension of the space of cusp forms of weight one. Internat. Math. Res. Notices 1995, no. 2, 99–109 (electronic).
- Edixhoven, B.: Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. With appendix A by Jean-Francois Mestre and appendix B by Gabor Wiese. J. Inst. Math. Jussieu 5 (2006), no. 1, 1–34.
- Freitag, E.: Hilbert modular forms. Springer-Verlag, Berlin, 1990.
- Garrett, P. B.: Holomorphic Hilbert modular forms. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1990.

- van der Geer, G.: Hilbert modular surfaces. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 16. Springer-Verlag, Berlin, 1988.
- Goren, E. Z.: Lectures on Hilbert modular varieties and modular forms. With the assistance of Marc-Hubert Nicole. CRM Monograph Series, 14. American Mathematical Society, Providence, RI, 2002.
- Mestre, J.-F.: La méthode des graphes. Exemples et applications. Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), 217–242, Nagoya Univ., Nagoya, 1986.
- Nicole, M.-H.: Superspecial abelian varieties and the Eichler basis problem for Hilbert modular forms. (English summary) J. Number Theory 128 (2008), no. 11, 2874–2889.
- Nicole, M.-H.: Superspecial abelian varieties, Theta series and the Jacquet-Langlands correspondence. (McGill Thesis, June 2005)
- Pizer, A.: An algorithm for computing modular forms on $\Gamma_0(N)$. J. Algebra 64 (1980), no. 2, 340–390.
- Wiese, G.: Thesis. Available from http://maths.pratum.net/