

Drinfeld modular forms of level T

Gunther Cornelissen¹

21.04.97

This paper should be seen as a companion to [2], giving an introduction to the results contained therein by working out an easy example: we will give a presentation for the ring of Drinfeld modular forms for the principal congruence group of level T , $\Gamma(T)$ over $\mathbf{F}_q[T]$ by generators and relations. In our example, the modular curve $\bar{M}_{\Gamma(T)}$ is of genus zero, which greatly simplifies the arguments. It will be our policy to always indicate what becomes more difficult or remains unproven for modular curves of general genus. Our notations will be compatible with [3] in this volume. Apart from this, the paper is written in a self-contained way, in particular, independent of [2].

To simplify notations, we will fix once and for all a level $N \in \mathbf{F}_q[T]$, and let $\Gamma := \Gamma(N)$.

(1.1) Example By $\bar{M}_{\Gamma(T)}$ we will mean the C -projective curve which is the compactification of $\Gamma(T)\backslash\Omega$. It has $q + 1$ cusps and genus zero. This curve (and its K -structure) is also studied in the instructional lectures 8 and 9. We will represent the cusps by $\{\infty = (1 : 0), (\alpha : 1), \alpha \in \mathbf{F}_q\} \in \Gamma(T)\backslash\mathbf{P}^1(\mathbf{F}_q(T)) = \mathbf{P}^1(\mathbf{F}_q)$. As prototypical modular forms of weight one for $\Gamma(T)$ we have the Eisenstein series ([3], (1.5.5)):

$$E_u(\omega) := \sum_{(a_1, a_2) \equiv u \pmod{T}} \frac{1}{a_1\omega + a_2},$$

for different $u \in \mathbf{F}_q[T]^2 - \{(0, 0)\}$. There are $q^2 - 1$ different such functions, one for each class modulo T in $\mathbf{F}_q[T]^2$; choose e.g. as representatives $u \in \mathbf{F}_q^* \times U$ with $U := \{\infty = (0, 1), (1, \beta), \beta \in \mathbf{F}_q\}$. (Note that one can make a different choice of representatives for the cusps and the indices U . We have chosen them in the above “dual” way, because this simplifies some formulae.) There exist C -linear relations between these functions, namely $E_{\lambda u} = \lambda^{-1}E_u$ for all $\lambda \in \mathbf{F}_q^*$, but these are the only ones, i.e. if we choose only representatives in U (having “sign one”), we get linearly independent functions, as can be seen by calculating the order of these functions at the cusps: it is clear that the function E_u can only be non-zero at the cusp ∞ if $a_1 = 0$ for all a_1 occurring in the sum, so $u = (0, 1)$. If one is at a different cusp $s = (s_1, s_2) = \gamma \cdot \infty$, and $\gamma \in \Gamma(1)$, then $\text{ord}_s E_u = \text{ord}_\infty E_{u \cdot \gamma} = 0$ only if $u_1 s_1 + u_2 s_2 = 0$. So we see that there is a bijection between the cusps and U , given by associating to any cusp the unique Eisenstein series that doesn’t vanish at that cusp. This suffices to see that they are linearly independent: any relation $\sum a_u E_u$ can be evaluated at all cusps to find $a_u = 0, \forall u$. To simplify future notations, we will write E_β for $E_{(1, \beta)}$.

On the other hand, If \mathcal{M} is the divisor of germs of modular forms of weight one on $\bar{M}_{\Gamma(T)}$, we have $\text{deg } \mathcal{M} = q$, and application of the Riemann-Roch theorem gives

$$\dim M_1(\Gamma(T)) = \dim H^0(\bar{M}_{\Gamma(T)}, \mathcal{M}) = \text{deg}(\mathcal{M}) + 1 = q + 1,$$

¹supported as “aspirant” by the Belgian National Fund for Scientific Research (NFWO)

using the fact that $\bar{M}_{\Gamma(T)}$ has genus zero. Hence $\{E_u : u \in U\}$ form a basis for $M_1(\Gamma(T))$. Note that since $\bar{M}_{\Gamma(T)} = \mathbf{P}^1$, a bundle is uniquely determined up to isomorphism by its degree, so $\mathcal{M} \cong \mathcal{O}(q)$, cf. the notation of lecture 9.

(1.2) Generalizations For a level N with $\deg N > 1$, the modular curve \bar{M}_Γ is no longer of genus zero. Also, the linear relations between the different Eisenstein series are not so easy to find, but there is a trick due to Hecke [8], which roughly goes as follows: choose only *primitive* representatives $u = (u_1, u_2)$, which means that u_1, u_2, N have no common divisor. Change the definition of E_u by adding the condition in the sum that a_1, a_2 have no common divisor. Then there is again a one-one correspondence between cusps and primitive altered series

$$\sum_{\substack{(a_1, a_2) \equiv u \pmod{T} \\ (a_1, a_2) = 1}} \frac{1}{a_1\omega + a_2},$$

not vanishing at that cusp, so the different altered functions span a space of dimension $= \#S$, the number of cusps. One then uses Moebius-inversion to show that the original and altered functions can be linearly expressed in one another, and that the non-primitive functions can be expressed by primitive ones. In conclusion, the $\{E_u\}$ span a space of dimension $\#S$, and a linearly independent set is given by choosing only primitive u .

For the dimension of the space of modular forms of weight one, the Riemann-Roch theorem only gives

$$\dim M_1(\Gamma) = \#S + H^1(\bar{M}_\Gamma, \mathcal{M}),$$

but E.-U. Gekeler has shown that the H^1 vanishes (see [3], (6.9.1) — use duality to interpret H^1 as a space of double cusp forms of weight one, and calculate, following Teitelbaum [12], the “periods” of its q -th power). In conclusion, we still find that the primitive Eisenstein series span $M_1(\Gamma)$.

Please note that this conclusion is very different from the case of classical modular forms, where e.g. the square of the Dedekind eta-function $\eta^2 = e^{\frac{\pi iz}{6}} \prod (1 - e^{2\pi inz})^2$ is a cusp form of weight one for $\Gamma(12)$.

(2.1) Example The next question that arises is whether the Eisenstein series of weight one generate the whole algebra of modular forms, i.e. whether any modular form of level T is a polynomial in the $\{E_u\}$. One has:

$$\dim M_k(\Gamma(T)) = kq + 1.$$

For instance, $M_2(\Gamma(T))$ has dimension $2q + 1$; for any fixed $v \in U$, $\{E_u^2 : u \in U\} \cup \{E_v \cdot E_u : u \in U - \{v\}\}$ are linearly independent (same argument as before), hence form a basis for $M_2(\Gamma(T))$. Similarly, the $3q + 1$ -dimensional $M_3(\Gamma(T))$ is spanned, for fixed $v, w \in U$ by

$$\{E_u^3 : u \in U\} \cup \{E_v^2 E_u : u \in U - \{v\}\} \cup \{E_v E_u^2 \text{ some } u \neq v\} \cup \{E_u E_v E_w : u \in U - \{v, w\}\}.$$

This follows by a refinement of the independence argument in (1.1), now not only locating the zeroes, but also calculating their order. A calculation (e.g. following the product expansion by Gekeler in [5], (2.1)) shows that the series development of E_β in the parameter t at the cusp ∞ is

$$(2.1.1) \quad (T\pi)^{-1}E_\beta(\infty) = t + a_\beta t^2 + a_\beta^2 t^3 + \dots - (T-1)T^{q-1}t^q + o(t^{q+1}),$$

where $a_\beta = -Te_{\pi\mathbf{F}_q[T]}(T^{-1}\pi\beta)$ is a $q-1$ -th root of $-T$.

(2.1.2) *Remark* A suitable multiple of E_β admits a series development defined over K , namely if we let ζ be such that $\zeta^{q-1} = -T$, and we choose as parameter at ∞ , $s := \zeta Tt$, then

$$\frac{\beta\zeta}{\pi}E_\beta(\infty) = \beta s + \beta^2 s^2 + \beta^3 s^3 + \dots + \left(1 - \frac{1}{T}\right)\beta s^q + o(s^{q+1}) \in K[[s]].$$

From the point of view of rationality questions (i.e. the K -structure on $M_{\Gamma(T)}$), this approach seems to be more suitable.

Since $\bar{M}_{\Gamma(T)} \cong \mathbf{P}^1$, we have $\mathcal{M} \cong \mathcal{O}(q)$, and, one can see immediately that $M(\Gamma(T)) \cong \Gamma_*(\mathcal{O}(q))$ is generated by the Eisenstein series of weight one $M_1 = H^0(\bar{M}_{\Gamma(T)}, \mathcal{O}(1))$.

(2.2) Generalizations Since $M(\Gamma)$ is a finitely generated algebra, there must be some bound b , such that the elements of weight $\leq b$ generate $M(\Gamma)$. It is no longer immediate that $b = 1$ (as for positive bundles on the projective line). There is a general theory attacking this question, due to Castelnuovo and Mumford (C.I.M.E.-course [10]). They study conditions under which the natural map $M_k(\Gamma) \otimes M_l(\Gamma) \rightarrow M_{k+l}(\Gamma)$, reinterpreted as

$$H^0(\bar{M}_\Gamma, \mathcal{M}^{\otimes k}) \otimes H^0(\bar{M}_\Gamma, \mathcal{M}^{\otimes l}) \rightarrow H^0(\bar{M}_\Gamma, \mathcal{M}^{\otimes k+l})$$

is surjective. One of their results says that this map is surjective if $\min\{k, l\} \cdot \deg \mathcal{M} > 2g + 1$. It has been remarked by D. Goss that this implies $M(\Gamma)$ is generated in weight ≤ 3 . Actually, a refinement shows that weight ≤ 2 suffices ([2]). I don't see how the proof can be adapted to show that weight one suffices; the bundle \mathcal{M} is in general approximately half-canonical and non-special.

If $M(\Gamma)$ is generated in weight one, then certainly \mathcal{M} has to be very ample (see *loc. cit.*). We can first address the weaker question of whether this holds in general. So consider the map induced by \mathcal{M}

$$i : \bar{M}_\Gamma \rightarrow \mathbf{P}^n : \omega \mapsto (E_i(\omega)),$$

where we have chosen an ordering E_1, \dots, E_n on the *different* Eisenstein series E_u . (Note that although the values of E_u are not well defined for $z \in \bar{M}_{\Gamma(T)}$, their ratios are). It turns out that this is an embedding in general, so \mathcal{M} is very ample. The homogeneous coordinate ring of $\text{im}(i)$ is exactly the ring $E(\Gamma)$, defined as the subring of $M(\Gamma)$ generated by the Eisenstein series of weight one. Hence the closed points of $\text{Proj}(E(\Gamma))$ are isomorphic to \bar{M}_Γ .

If R is a graded domain, let $R_{((0))}$ denote the ring consisting of quotients of homogeneous elements of the same degree in R . Since the function field of \bar{M}_Γ is the field of modular

functions $M(\Gamma)_{((0))}$, and the function field of $\text{Proj}(E(\Gamma))$ is $E(\Gamma)_{((0))}$, we find that these are equal. But let $f \in M_k(\Gamma)$ be a modular form of weight k , then fE_u^{-k} is a modular function, hence belongs to $E(\Gamma)_{((0))}$ by the above. It follows that the quotient fields of $E(\Gamma)$ and $M(\Gamma)$ are equal. But what is more, all rings of modular forms for arithmetic groups are normal (i.e. integrally closed in their quotient field); this is classically due to Igusa ([9] III.5 – basically, one puts a grading on the integral closure, and then shows that homogeneous integral elements satisfy the correct transformation equation for a modular form. Finally, holomorphy is preserved for integral elements everywhere locally, as follows from Weierstrass’ lemma). In conclusion, we see that $M(\Gamma)$ is the integral closure of $E(\Gamma)$.

In this way, the question whether $E(\Gamma) = M(\Gamma)$ turns out to be equivalent to the normality of $E(\Gamma)$, or combining the fact that $\text{Proj } E(\Gamma)$ is smooth with Serre’s criterium for normality ([4], 11.5), it is equivalent to the fact that $E(\Gamma)$ is Cohen-Macaulay. The latter can be interpreted by saying that $E(\Gamma)$ is free as a $C[g, \Delta]$ -module. An affirmative answer to this question is not known, except when $\deg N = 1$ or $(q, \deg N) = (2, 2)$ (the latter since the embedding via \mathcal{M} turns out to be an extremal curve w.r.t. Castelnuovo’s bound — see e.g. [1], p. 116).

(3.1) Example So far, we know that $M(\Gamma(T))$ is generated by $\{E_u\}$, so the next question is to find the algebraic relations between these functions. The degree of the embedding

$$i : \bar{M}_{\Gamma(T)} \rightarrow \mathbf{P}^q : \omega \mapsto (E_u(\omega) : u \in U)$$

(the number of points of intersection of $\text{im}(i)$ with a general plane in \mathbf{P}^q) equals the degree of \mathcal{M} as a line bundle = q . We also have that $\text{im}(i)$ is non-degenerate, by which we mean that it doesn’t belong to any hyperplane: the basis points $(1 : \dots : 0), \dots, (0 : \dots : 1)$ belong to it (they are the images of the cusps of $\bar{M}_{\Gamma(T)}$). But a smooth non-degenerate curve of degree q in \mathbf{P}^q is projectively isomorphic to the rational normal curve \mathcal{R}_q given by $\mathbf{P}^1 \rightarrow \mathbf{P}^q : (X : Y) \mapsto (X^q : X^{q-1}Y : \dots : XY^{q-1} : Y^q)$ ([7], 1.14).

From the fact that i embeds the modular curve as a rational normal curve, we know it is the intersection of quadrics. Let $x_\beta : \beta \in \mathbf{F}_q \cup \{\infty\}$ be $q+1$ variables, and define the “ideal of relations” I as the kernel of

$$R := C[x_\beta : \beta \in \mathbf{F}_q \cup \{\infty\}] \rightarrow E(\Gamma) : x_\beta \rightarrow E_\beta.$$

Then I can be generated by elements of degree two. We will now try to determine these.

(3.1.1) Here is an ad-hoc way of finding I : use the series expansions (2.1.1) to produce quadratic polynomials in E_β that have a zero of order ≥ 2 at all cusps, hence identically zero since there are no cusp forms of weight two. Make as many relations as required to let R/I have the same Hilbert function as $E(\Gamma)$.

(3.1.2) Second method: use the fact that $\text{im}(i)$ is projectively isomorphic to the standard rational normal curve \mathcal{R}_q in \mathbf{P}^q , which has equations

$$(3.1.3) \quad Z_i Z_j - Z_{i-1} Z_{j+1}, \quad (1 \leq i \leq j \leq q-1),$$

in terms of the coordinates Z_0, \dots, Z_q on \mathbf{P}^q ([7], 5.4). The curve \mathcal{R}_q passes through the $q+1$ points $(0 : \dots : 1), (1 : \alpha : \alpha^2 : \dots : \alpha^q), \alpha \in \mathbf{F}_q$, which are linearly independent (their determinant is Vandermonde). On the other hand, evaluating i at the different cusps of $\bar{M}_{\Gamma(T)}$, we see that $\text{im}(i)$ passes through the $q+1$ “base”-points $(0 : \dots : 1 : \dots : 0)$. Suppose we transform coordinates in \mathbf{P}^q via the transformation of these two bases of the underlying affine space \mathbf{A}^{q+1} :

$$T\pi \cdot Z_j = \sum_{\alpha \in \mathbf{F}_q} \alpha^j x_\alpha + \delta_{j,q} x_\infty, \quad j = 0, \dots, q \quad (\text{convention: } 0^0 = 1),$$

where δ is a Kronecker symbol. There is in general a unique rational normal curve through $q+3$ points, of which no $q+1$ lie in a hyperplane; so there is no immediate reason why the image of \mathcal{R}_q under this transformation would have to be $\text{im}(i)$. But we are lucky, because we will now show that the relations (3.1.3) are identically satisfied when substituting $x_\beta = E_\beta(\omega), \forall \omega \in \Omega$.

Proof. We will prove this by showing that the series expansions vanish at all cusps of order two. This will suffice to show that the relations hold identically, since setting $x_\beta = E_\beta$ will produce a modular form in $M_2^2(\Gamma(T)) = 0$. Let us therefore first of all expand the result from (2.1.1) to include all cusps. We will skip the calculation, and just state that for a non-zero constant $\zeta \in C^*$:

$$\begin{cases} (T\pi)^{-1} \cdot E_\infty(\infty) = \zeta + o(t^2) \\ (T\pi)^{-1} \cdot E_\beta(\infty) = t + o(t^2), \quad \beta \neq \infty \\ (T\pi)^{-1} \cdot E_\infty((\alpha : 1)) = t + o(t^2), \quad \alpha \neq \infty \\ (T\pi)^{-1} \cdot E_\beta((\alpha : 1)) = (\alpha + \beta)^{-1}t + o(t^2), \quad 0 \neq \alpha + \beta < \infty \\ (T\pi)^{-1} \cdot E_\beta(\alpha : 1) = \zeta + o(t^2), \quad \alpha + \beta = 0, \end{cases}$$

A little calculation using the transformation equations shows that

$$\begin{cases} Z_j(\infty) = o(t^2), \quad j < q-1 \\ Z_{q-1}(\infty) = -t + o(t^2) \\ Z_q(\infty) = \zeta + o(t^2) \\ Z_j((\alpha : 1)) = -\binom{q-2}{j-1} \alpha^{j-1} t + (-\alpha)^j \zeta + o(t^2), \quad \alpha \neq \infty, \quad j = 0 \dots q. \end{cases}$$

From this, it is immediately clear that (3.1.3) is satisfied at ∞ , up to t^2 . For the other cusps, one finds:

$$\begin{aligned} & (Z_i Z_j - Z_{i-1} Z_{j+1})(\alpha : 1) \\ &= \alpha^{i+j-1} [(-1)^{j+1} \left(\binom{q-2}{i-1} + \binom{q-2}{i-2} \right) + (-1)^{i+1} \left(\binom{q-2}{j-1} + \binom{q-2}{j} \right)] + o(t^2) \\ &= \alpha^{i+j-1} [(-1)^{j+1} \binom{q-1}{i-1} + (-1)^{i+1} \binom{q-1}{j}] + o(t^2) \\ &= \alpha^{i+j-1} [(-1)^{j+1} (-1)^{i-1} + (-1)^{i+1} (-1)^j] + o(t^2) \\ &= o(t^2), \end{aligned}$$

where we have used the fact that $\binom{q-1}{m} = (-1)^m \in \mathbf{F}_q$ (this follows inductively from $\binom{q}{m} = \binom{q-1}{m-1} + \binom{q-1}{m} = \delta_{m,0}$ for $m < q$). \square

We can put these results together in the following theorem:

Theorem *The ring of (Drinfeld) modular forms of level T is isomorphic to*

$$C[x_\beta : \beta \in \mathbf{F}_q \cup \{\infty\}] / \langle f_{i,j} : 1 \leq i \leq j \leq q-1 \rangle \cong M(\Gamma(T)),$$

where the isomorphism is given by sending $x_\beta \rightarrow E_\beta$, and the “relations” $f_{i,j}$ are given by

$$f_{i,j} := \sum_{\alpha, \beta \in \mathbf{F}_q} \alpha^{i-1} \beta^j (\alpha - \beta) x_\alpha x_\beta - \delta_{j,q-1} \cdot \sum_{\alpha \in \mathbf{F}_q} \alpha^{i-1} x_\alpha x_\infty,$$

where we again have adopted the convention that $0^0 = 1$.

(3.1.4) Here is one more way of finding the ideal of relations I : Since a general lattice function $e_\Lambda(\omega)$ is additive, its derivative $e'_\Lambda(\omega) = 1$. Hence by taking the logarithmic derivative of $e_\Lambda(\omega)$, we find that

$$\frac{1}{e_\Lambda(\omega)} = \sum_{\lambda \in \Lambda} \frac{1}{\omega - \lambda}, \quad \omega \notin \Lambda.$$

For our particular case, this implies that

$$E_u^{-1}(\omega) = T^{-1} e_{\Lambda_\omega} \left(\frac{u_1 \omega + u_2}{T} \right), \quad \Lambda_\omega = \omega A \oplus A$$

is almost the T -torsion of the Drinfeld module ϕ^{Λ_ω} = the roots of $\phi_T^{\Lambda_\omega}$ ([3], (1.5.5)). This means that

$$\phi_T^{\Lambda_\omega} = TX + g(\omega)X^q + \Delta(\omega)X^{q^2} = TX \prod_{\beta \in U} (X^{q-1} T^{1-q} E_\beta^{q-1}(\omega) - 1)$$

holds as a formal identity in X for all $\omega \in \Omega$.

The idea is that any set of functions satisfying such an identity cannot be far away from $\{E_u\}$. This is formalised as follows: let $J' \subseteq C[x_1, \dots, x_{q+1}, \gamma, \delta]$ be the ideal generated by the coefficients in the formal variable X of the identity

$$TX + \gamma X^q + \delta X^{q^2} = TX \prod_{\beta \in U} (X^{q-1} T^{1-q} x_\beta^{q-1} - 1).$$

Let $J \subseteq R$ be the ideal generated by the elements of J' , but where the variables γ, δ are eliminated. Then

$$J = \langle \sigma_2(x_\beta^{q-1}), \dots, \sigma_q(x_\beta^{q-1}) \rangle,$$

where σ_i is the symmetric function of weight i . This is certainly an ideal of relations between $E_\alpha(\omega), \forall \omega \in \Omega$, and it is not far away from I . As a matter of fact, for any

permutation $\sigma \in \text{Sym}\{\mathbf{F}_q \cup \{\infty\}\}$ and any vector $\lambda = (\lambda_i) \in (\mathbf{F}_q^*)^{q+1}$, let $I^{\sigma, \lambda}$ be the kernel of

$$R \rightarrow E(\Gamma(T)) : x_\beta \mapsto \lambda_\beta E_{\sigma(\beta)}.$$

Then:

$$\bigcap I^{\sigma, \lambda} = J.$$

Proof. The proof is given in [2]. Let Z indicates the zero set of a homogeneous ideal in \mathbf{P}^q . First of all, one checks that the zero sets of both ideals are equal. But the left ideal is radical, since $E(\Gamma(T))$ is reduced. On the other hand, R/J is a complete intersection ($\#$ equations = $\#$ variables - $\#$ relations). Hence it is reduced \iff the singularities of its zero locus have dimension zero ([4], 18.15). But one can find these singularities by calculating the Jacobian ideal of J . Via the formula for the Vandermonde determinant, one can even factor the Jacobian ideal, and one finds that all singularities belong to planes of the form $Z(x_\beta - \lambda x_{\beta'}), \beta \neq \beta', \lambda \in \mathbf{F}_q^*$. Hence there are only a finite number of singular points if the components of $Z(J)$ don't belong to such hyperplanes. But these components are $Z(I^{\sigma, \lambda})$, parametrized by $\bar{M}_{\Gamma(T)} \rightarrow \mathbf{P}^q : \omega \mapsto (\lambda_\beta E_{\sigma(\beta)}(\omega))$, and this never belongs to such a hyperplane, since otherwise $E_\beta(\omega) \equiv \lambda \lambda_{\beta'}^{-1} \lambda_{\beta'} E_{\beta'}(\omega)$ for all ω , a contradiction since we have constructed the E_β as linearly independent functions. \square

So to find I , it suffices to find one factor of the ideal J , which is explicitly given as a complete intersection. There exist algorithms for finding such factors, and one of them (Gianni, Trager, Zacharias [6]) was implemented by Hans Decker at Saarbrücken. Unfortunately, the complexity of the algorithm is rather bad, so we had to stick to the case $q = 3$, where a factor

$$I = \langle x_0x_1 + x_0x_2 + x_1x_2, x_0x_1 - x_0x_2 - x_1x_2, x_1x_2 + x_1x_\infty - x_2x_\infty \rangle$$

was found. This is compatible with the construction of I from (3.1.2).

(3.2) Generalizations The ad-hoc computation of (3.1.1) can of course always be made, within the limits of computation. The first case $q = 2, N = T(T + 1)$ has 9 indeterminates, the ideal of relations will have approximately 15 generators, and these numbers grow rapidly. The calculation in (3.1.2) was based specifically on the rational normal curve, and this definitely doesn't hold any more if the level increases. Finally, calculation (3.1.3) continues to hold in general. This then produces the relations between $\{E_u\}$ up to permutation.

(4.1) Example We can calculate the number M of irreducible components of $Z(J)$: it equals the quotient of the degree of $Z(J)$ by the degree of $Z(I)$. The latter is q , the former can be calculated using Stanley's formula for the Hilbert function of a complete intersection ([11], (3.3)). One finds:

$$M = q^{-1} \deg(Z(J)) = q^{-1} \lim_{t \rightarrow 1} \prod_{i=2}^q \frac{1 - t^{i(q-1)}}{1 - t} = (q-1)! \cdot (q-1)^{q-1}.$$

This is a very big number, which might explain the complexity of factoring.

In the example $q = 3$, the group D_8 of permutations of the variables generated by a 4-cycle and a transposition, acts simply transitive on the 8 components of $Z(J)$. This implies that the orbit space $D_8 \backslash Z(J)$ will be birational to one of the components $Z(I)$; in particular, the normalization of the cone over the orbit space will be isomorphic to $\text{Spec } M(\Gamma(T))$.

(4.2) Generalizations The calculation of the number of components immediately generalizes. If the genus of the modular curve is > 1 , this calculation has an application to estimating its number of automorphisms. Namely, any element $\{\sigma, \lambda\}$ acting on the components of an ideal similar to J , which stabilizes such a component, induces an automorphism on \bar{M}_Γ .

5. *Remark* It is clear that all results in this paper hold, not only for level T , but for any level $N = aT + b$, $a \in \mathbf{F}_q^*$, $b \in \mathbf{F}_q$ of degree one.

6. *Addendum* D. Zagier has observed that the relations $\{f_{ij} = 0\}$ of the main theorem in section (3.1.3) are equivalent to

$$\{(\alpha - \beta)x_\alpha x_\beta + (x_\alpha - x_\beta)x_\infty = 0, \forall \alpha, \beta \in \mathbf{F}_q\},$$

and that these can be shown to hold by the following observation: for all $\beta \in \mathbf{F}_q$, the \mathbf{F}_q -additivity of e_{Λ_ω} gives

$$E_\beta^{-1}(\omega) = e_{\Lambda_\omega}\left(\frac{\omega + \beta}{T}\right) = e_{\Lambda_\omega}\left(\frac{\omega}{T}\right) + \beta e_{\Lambda_\omega}\left(\frac{1}{T}\right) = E_0^{-1}(\omega) + \beta E_\infty^{-1}(\omega),$$

hence $E_\beta^{-1} - \beta E_\infty^{-1}$ is independent of β .

References

- [1] E. Arbarello, M. Cornalba, P.A. Griffiths, and J Harris, *Geometry of algebraic curves, volume 1*, Grundlehren der Math. Wiss., vol. 267, Springer, Berlin - Heidelberg - New York, 1985.
- [2] G. Cornelissen, *Drinfeld modular forms of weight one*, <http://cage.rug.ac.be/~gc/>, preprint 1996.
- [3] ———, *A survey of Drinfeld modular forms*, this volume.
- [4] D. Eisenbud, *Commutative algebra*, Graduate Texts in Math., vol. 150, Springer, Berlin - Heidelberg - New York, 1995.
- [5] E.-U. Gekeler, *Modulare Einheiten für Funktionenkörper*, J. Reine Angew. Math. **348** (1984), 94–115.
- [6] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, Computational aspects of Commutative Algebra (Robbiano, ed.), Academic Press, London - New York, 1988, pp. 15–33.
- [7] J. Harris, *Algebraic geometry - a first course*, Graduate Texts in Math., vol. 133, Springer, Berlin - Heidelberg - New York, 1992.
- [8] E. Hecke, *Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 199–224, = Werke, 461–486.
- [9] J. Igusa, *Theta functions*, Grundlehren der Math. Wiss., vol. 194, Springer, Berlin - Heidelberg - New York, 1972.

- [10] D. Mumford, *Varieties defined by quadratic equations*, Proceedings of the Centro Internazionale Matematico Estivo “Questions on algebraic varieties”, Edizioni Cremonese, Roma, 1969, pp. 31–100.
- [11] R. Stanley, *Hilbert functions of graded algebras*, Adv. in Math. **28** (1978), 57–83.
- [12] J. T. Teitelbaum, *The Poisson kernel for Drinfeld modular curves*, J. Amer. Math. Soc. **4** (1991), no. 3, 491–511.

University of Gent,
Dept. of Pure Mathematics and Computer Algebra,
Galglaan 2, B-9000 Gent, Belgium
e-mail `gc@cage.rug.ac.be`