Preliminary version
May 15, 2018

II Università degli
Studi di Roma

TOR VERGATA

Modular forms invariant under non-split Cartan subgroups

Pietro Mercuri

René Schoof

Dipartimento di Matematica
2ª Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: mercuri.ptr@gmail.com
schoof.rene@gmail.com

Abstract. In this paper we describe a method for computing a basis for the space of weight 2 cusp forms invariant under a non-split Cartan subgroup of prime level p. As an application we compute, for certain small values of p, explicit equations over $\mathbf{Q}$ for the canonical embeddings of the associated modular curves.

1. Introduction.

It is well known how to compute bases for the spaces of cusp forms that are invariant under the modular groups $\Gamma_0(N)$ or $\Gamma_1(N)$. Indeed, efficient algorithms to compute q-expansions of eigenforms exist [17, 22] and extensive tables are available online [7, 18, 25]. For other congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ the situation is different. While for some groups, like *split* Cartan subgroups, there are efficient algorithms [22] and it is easy to obtain q-expansions from the existing tables for $\Gamma_0(N)$, for other subgroups this is not so immediate [3, 4].

In this paper we describe a method to compute q-expansions of a basis for the space $S_2(\Gamma_{\mathrm{ns}}(p))$ of weight 2 cusp forms invariant under a *non-split* Cartan subgroup $\Gamma_{\mathrm{ns}}(p)$ of prime level p. As in the computation for $p = 13$ by B. Baran [5], we obtain a basis of $S_2(\Gamma_{\mathrm{ns}}(p))$ by applying trace maps to certain normalized eigenforms in $S_2(\Gamma_0(p^2))$ and $S_2(\Gamma_1(p))$. In Baran's computation for $p = 13$ this involves, only one eigenform. It generates a cuspidal $\mathrm{GL}_2(\mathbf{F}_p)$-representation. For larger primes p, several non-isomorphic irreducible representations, both cuspidal and principal series, are involved. This complicates matters, since in each case the trace map is different. Our main results are the formulas of Propositions 4.4 and 5.2.

As an application we are able to compute explicit equations for the canonical embeddings of the modular curves $X_{\mathrm{ns}}(p)$ associated to the non-split Cartan subgroups and the curves $X_{\mathrm{ns}}^{+}(p)$ associated to their normalizers. Since our method allows us to compute a basis that is defined over $\mathbf{Q}$, the equations that we compute have coefficients in $\mathbf{Q}$. We work this out for the modular curves $X_{\mathrm{ns}}^{+}(p)$ for $p = 17$, 19 and 23.

In the remainder of this introduction, we provide some context for our computational results. The curves $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^{+}(p)$ are defined over $\mathbf{Q}$. Their genera grow rapidly with p. See [4]. This may explain why thus far not many computations have been done with these curves.

The curves $X_{\mathrm{ns}}(p)$ have no real and hence no rational points. For $p \leq 5$ the genus of $X_{\mathrm{ns}}(p)$ is zero. The curve $X_{\mathrm{ns}}(7)$ has genus 1 and, for the record, is given by the equation $-y^2 = 2x^4 - 14x^3 + 21x^2 + 28x + 7$. Equations for the genus 4 curve $X_{\mathrm{ns}}(11)$ are given in [11]. Using the methods explained in this paper, equations for the genus 8 curve $X_{\mathrm{ns}}(13)$ are determined in [13]. No explicit equations have been computed for the curves $X_{\mathrm{ns}}(p)$ for primes $p > 13$.

The curves $X_{\mathrm{ns}}^{+}(p)$ are quotients of $X_{\mathrm{ns}}(p)$ by a modular involution. The rational points of the curves $X_{\mathrm{ns}}^{+}(p)$ are relevant in connection with Serre's Uniformity Conjecture [24]. Indeed, after Mazur's 1978 result [19] and the 2010 paper by Bilu, Parent and Rebolledo [6], the conjecture would follow, if for sufficiently large primes p, the only rational points of the curves $X_{\mathrm{ns}}^{+}(p)$ are CM-points.

For $p \leq 7$ the curves $X_{\mathrm{ns}}^{+}(p)$ have genus zero and have infinitely many rational points. For $p = 11$ the genus is 1 and there are also infinitely many rational points. An explicit equation was computed in 1976 by Ligozat [16]. For $p > 11$ the genus exceeds 2 and hence there are only finitely many rational points. An equation for the genus 3 curve $X_{\mathrm{ns}}^{+}(13)$ was computed in 2014 by B. Baran [5]. In this paper we present equations for $X_{\mathrm{ns}}^{+}(p)$ for the primes $p = 17, 19$ and 23. Recently Balakrishnan and her coauthors [2] used the Chabauty-Kim method to show that the curve $X_{\mathrm{ns}}^{+}(13)$ has precisely seven rational points. All these points are CM-points. For $p > 13$ it is at present not known whether or not $X_{\mathrm{ns}}^{+}(p)$ admits any rational points that are not CM. For $p = 17, 19$ and 23 a quick computer calculation shows that these curves do not admit any non-CM rational points that have small coordinates in our models. There may very well not be any. See sections 6, 7 and 8.

In section 2 we fix our notation and recall some of the basic properties of representations of $\mathrm{GL}_2(\mathbf{F}_p)$. In section 3 we do the same for the various modular curves that play a role. In section 4 we determine our trace map for the principal series and the twisted Steinberg representations. In section 5 we do the same for the cuspidal representations. In section 6 we describe in some detail the actual computations for the curve $X_{\mathrm{ns}}^{+}(17)$. In sections 7 and 8 we present the numerical results for $X_{\mathrm{ns}}^{+}(19)$ and $X_{\mathrm{ns}}^{+}(23)$.

2. Representations of $\mathrm{GL}_2(\mathbf{F}_p)$.

Let $p > 2$ be a prime. In this section we fix notation and recall the basic properties of the representation theory of the group $G = \mathrm{GL}_2(\mathbf{F}_p)$, on which our computations are based.

The group G acts on the $p+1$ points of the projective line $\mathbf{P}_1(\mathbf{F}_p)$ via linear fractional transformations. A *Borel subgroup* is the stabilizer of a point. It is conjugate to the subgroup B of upper triangular matrices and has order $p(p-1)^2$. A *split Cartan subgroup* of G is the stabilizer of two points. It is conjugate to the subgroup T of diagonal matrices. It has order $(p-1)^2$ and index 2 in its normalizer N. The group G also acts on the p^2+1 points of $\mathbf{P}_1(\mathbf{F}_{p^2})$. A *non-split Cartan subgroup* of G is the stabilizer of two points of $\mathbf{P}_1(\mathbf{F}_{p^2})$ that are conjugate over $\mathbf{F}_p$. Any such group is conjugate to the subgroup T' of matrices that fixes the points $\pm\sqrt{u}$, where u denotes a non-square in $\mathbf{F}_p$. Explicitly, we have

$$T' = \{\begin{pmatrix} a & bu \\ b & a \end{pmatrix} \in G : a, b \in \mathbf{F}_p \text{ with } a^2 - ub^2 \neq 0\}.$$

The group T' is cyclic of order $p^2 - 1$ and has index 2 in its normalizer N'.

In this paper we mostly deal with representations V of G for which the subgroup of scalar matrices Z act trivially. These are representations of $G/Z = \mathrm{PGL}_2(\mathbf{F}_p)$. The complex irreducible representations of $\mathrm{PGL}_2(\mathbf{F}_p)$ come in *four types* [8, 14]. There are two 1-dimensional representations: the trivial character and a quadratic character ω. Both factor through the determinant. There are also two irreducible p-dimensional representations. To define them, we consider the natural action of $\mathrm{PGL}_2(\mathbf{F}_p)$ on the ring A of functions $\phi : \mathbf{P}_1(\mathbf{F}_p) \longrightarrow \mathbf{C}$ given by $\sigma\phi(P) = \phi(\sigma^{-1}(P))$ for $P \in \mathbf{P}_1(\mathbf{F}_p)$. Since the subspace $\mathbf{C}$ of constant functions is preserved by this action, $\mathrm{PGL}_2(\mathbf{F}_p)$ acts on the p-dimensional quotient space $V_{\mathrm{st}} = A/\mathbf{C}$. This representation is irreducible, has dimension p and is called the *Steinberg representation* V_{st}. Its twist by ω is denoted by V_ω.

The irreducible representations of the third type are the *principal series* representations V_μ. These are the inductions of characters $\mu : B/Z \longrightarrow \mathbf{C}^*$ for which $\mu^2 \neq 1$. Since the characters μ are trivial on the unipotent subgroup

$$U = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbf{F}_p\},$$

they can be viewed as characters of the cyclic group T/Z. The representations V_μ have dimension $p+1$. Two representations V_μ and $V_{\mu'}$ are isomorphic if and only if $\mu' = \mu^{\pm 1}$. There are $(p-3)/2$ mutually non-isomorphic representations of this type. The irreducible representations of the fourth type are the *cuspidal* ones. They are associated to characters $\theta : T'/Z \longrightarrow \mathbf{C}^*$ for which $\theta^2 \neq 1$. These representations have dimension $p-1$ and are denoted by V_θ. Two representations V_θ and $V_{\theta'}$ are isomorphic if and only if $\theta' = \theta^{\pm 1}$. There are $(p-1)/2$ mutually non-isomorphic representations of the this type. See [8, 14] for all this. In section 5 we describe explicit models for the representations V_θ.

A character $\mu : T/Z \longrightarrow \mathbf{C}^*$ is called even or odd, depending on whether it is 1 on the unique element of order 2 in T/Z or not. Similarly, a character $\theta : T'/Z \longrightarrow \mathbf{C}^*$ is called even or odd, depending on whether it is 1 on the unique element of order 2 in T'/Z

or not. Note that the restriction of the quadratic character ω to T/Z is even if and only if its restriction to T'/Z is odd. This happens if and only if $p \equiv 1 \pmod 4$.

The following proposition gives the dimensions of the T-invariant and T'-invariant subspaces V^T and $V^{T'}$ of irreducible representations V of $\mathrm{PGL}_2(\mathbf{F}_p)$.

Proposition 2.1. *Let V be an irreducible complex representation of $\mathrm{PGL}_2(\mathbf{F}_p)$ that is not 1-dimensional. If $V = V_{st}$, then*

$$\dim V^T \,=\, 2, \quad \dim V^N \,=\, 1, \quad \text{and} \quad \dim V^{T'} = \dim V^{N'} \,=\, 0.$$

In all other cases we have

$$\dim V^T \,=\, \dim V^{T'} \,=\, 1, \quad \text{and} \quad \dim V^N \,=\, \dim V^{N'} \,\le\, 1.$$

Moreover, we have

$$\dim V^N = \dim V^{N'} = 1, \quad \text{if and only if} \quad \begin{cases} V = V_\mu, & \text{with } \mu \text{ even}, \\ V = V_\theta, & \text{with } \theta \text{ odd}, \\ V = V_\omega, & \text{and } p \equiv 1 \pmod 4). \end{cases}$$

Proof. We recall the remarkable isomorphisms of rational G-representations

$$\mathbf{Q}[G/T] \,\cong\, \mathbf{Q}[G/T'] \times V_{\mathrm{st}} \times V_{\mathrm{st}}, \quad \text{and} \quad \mathbf{Q}[G/N] \,\cong\, \mathbf{Q}[G/N'] \times V_{\mathrm{st}},$$

described by De Smit and Edixhoven in [10].

When $V \neq V_{st}$, the fact that the vector spaces V^H and $\mathrm{Hom}_G(\mathbf{Q}[G/H], V)$ are naturally isomorphic for every subgroup H of G, implies that $\dim V^T = \dim V^{T'}$ and $\dim V^N = \dim V^{N'}$. To show that $\dim V^T = 1$, we observe that $\dim V^T$ is equal to the scalar product $\langle \mathrm{Res}_T(\chi_V), 1_T \rangle_T$. Here χ_V denotes the character of V and 1_T is the trivial character on T. A standard character computation shows this to be equal to 1 in all cases. A similar computation shows that $\langle \mathrm{Res}_N(\chi_V), 1_N \rangle_N$ is 0 or 1 depending on the parity of the relevant character μ, θ or ω. These computations are particularly straightforward when $V = V_\mu$ or V_ω. For the cuspidal representations $V = V_\theta$, everything can be computed using the description of V_θ as a virtual representation as in [8, 14]. Alternatively, one may use the explicit models for V_μ and V_θ given in sections 4 and 5.

For the Steinberg representation V_{st}, an explicit calculation shows that $\dim V_{st}^T = 2$ and $\dim V_{st}^N = 1$. The result by De Smit and Edixhoven implies therefore that $V_{st}^{T'}$ and $V_{st}^{N'}$ vanish.

This proves the proposition.

In the next sections we construct T'-invariant elements in G-representations V by applying the T'-trace

$$\sum_{t \in T'} t \;=\; \sum_{a,b \in \mathbf{F}_p,\, a^2 - ub^2 \neq 0} \begin{pmatrix} a & bu \\ b & a \end{pmatrix} \quad \text{in} \quad \mathbf{Q}[G]$$

to suitable vectors $v \in V$. Since we have the Bruhat decomposition $G = B \cup BwB$, where

$$w \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

every non-scalar element in T' can be written as an element in BwB. This leads to the following formula for a projective version of the T'-trace.

Proposition 2.2. *The T'-trace element $\sum_{M\in T'/Z} M$ of the group ring $\mathbf{Q}[\mathrm{PGL}_2(\mathbf{F}_p)]$ is given by*

$$\mathrm{id} + \sum_{r\in\mathbf{F}_p} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & r \\ 0 & r^2-u \end{pmatrix}.$$

Proof. Representatives in T' of the quotient group T'/Z are the identity matrix and the matrices $\begin{pmatrix} r & u \\ 1 & r \end{pmatrix}$ with $r \in \mathbf{F}_p$. Since $\begin{pmatrix} r & u \\ 1 & r \end{pmatrix} = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & r \\ 0 & r^2-u \end{pmatrix}$, the result follows.

3. Modular curves.

Let $p > 2$ be prime and put $G = \mathrm{GL}_2(\mathbf{F}_p)$. The modular curve $X(p)$ is an algebraic curve over $\mathbf{Q}$ that parametrizes elliptic curves with full level p structure. The field of constants of its function field is the cyclotomic field $\mathbf{Q}(\zeta_p)$. The curve $X(p)$ admits a natural morphism to the j-line $X(1)$ over $\mathbf{Q}$. The Galois group of $X(p)$ over $X(1)$ is naturally isomorphic to $\mathrm{GL}_2(\mathbf{F}_p)/\{\pm\mathrm{id}\}$. Restriction of automorphisms in $\mathrm{Gal}(X(p)/X(1))$ to the Galois group of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ coincides with the determinant map $G/\{\pm\mathrm{id}\} \longrightarrow \mathbf{F}_p^*$.

For every subgroup H of G containing $\{\pm\mathrm{id}\}$ we write $X(p)_H$ for the quotient of $X(p)$ by H. The field of constants of its function field is the subfield of $\mathbf{Q}(\zeta_p)$ that is invariant under the subgroup $\det(H)$ of $\mathbf{F}_p^*$. We put

$$\Gamma_H \;=\; \{A \in \mathrm{SL}_2(\mathbf{Z}) : A \pmod{p} \in H\}.$$

Then the non-cuspidal complex points of any base change of $X(p)_H$ from its field of constants to $\mathbf{C}$, form the Riemann surface $\Gamma_H\backslash\mathbf{H}$.

Taking for H the subgroup Z of scalar matrices of G, we obtain the curve $X(p)_Z$. We denote it by $X(p)'$. Its field of constants is the quadratic subfield of $\mathbf{Q}(\zeta_p)$. This is $\mathbf{Q}(\sqrt{p})$ or $\mathbf{Q}(\sqrt{-p})$ depending on whether $p \equiv 1$ or $3 \pmod 4$. Since $Z \cap \mathrm{SL}_2(\mathbf{F}_p) = \{\pm\mathrm{id}\}$, the base change of $X(p)'$ from $\mathbf{Q}(\sqrt{\pm p})$ to $\mathbf{Q}(\zeta_p)$ is the curve $X(p)$. The curves $X(p)_T$ and $X(p)_N$ associated to the split Cartan subgroup T and its normalizer N and the curves $X(p)_{T'}$ and $X(p)_{N'}$ associated to the non-split Cartan subgroup T' and its normalizer N' are quotients of $X(p)'$. These are the curves $X_{\mathrm{s}}(p)$, $X_{\mathrm{s}}^+(p)$, $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$ respectively, that were mentioned in the introduction. Since the determinant maps from the subgroups T, N, T' and N' to $\mathbf{F}_p^*$ are all surjective, the curves are all defined over $\mathbf{Q}$, in the sense that their fields of constants are equal to $\mathbf{Q}$.

The group $G = \mathrm{GL}_2(\mathbf{F}_p)$ acts naturally and linearly on the $\mathbf{Q}$-vector space $\Omega^1(X(p))$ of Kähler differentials. Therefore its quotient $G/Z = \mathrm{PGL}_2(\mathbf{F}_p)$ acts on the $\mathbf{Q}$-vector space $\Omega^1(X(p))^Z$ of Z-invariants. On the other hand, the index 2 subgroup $\mathrm{PSL}_2(\mathbf{F}_p)$ of $\mathrm{PGL}_2(\mathbf{F}_p)$ is isomorphic to the quotient group $\mathrm{SL}_2(\mathbf{Z})/\Gamma_Z$. Therefore it acts naturally on the complex vector space $S_2(\Gamma_Z)$ of weight 2 cusp forms for the congruence subgroup Γ_Z. The two actions are related by the fact that $\Omega^1(X(p)')\otimes_{\mathbf{Q}}\mathbf{C}$ is isomorphic to the induction from $\mathrm{PSL}_2(\mathbf{F}_p)$ to $\mathrm{PGL}_2(\mathbf{F}_p)$ of $S_2(\Gamma_Z)$. See [5, p.279]. So we can write $\Omega^1(X(p)')\otimes_{\mathbf{Q}}\mathbf{C} = S_2(\Gamma_Z) + [R]S_2(\Gamma_Z)$ for some fixed respresentative R of the non-trivial coset of the normal subgroup $\mathrm{PSL}_2(\mathbf{F}_p)$ of $\mathrm{PGL}_2(\mathbf{F}_p)$. Following [5], we call the first coordinate f_1 of an element $f_1 + [R]f_2$ of $S_2(\Gamma_Z) + [R]S_2(\Gamma_Z)$, its *classical coordinate.*

Proposition 3.1. *Let H be a subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ containing Z.*
(a) The natural maps

$$\Omega^1(X(p)_H) \xrightarrow{\cong} \Omega^1(X(p))^H = \Omega^1(X(p)')^{H'},$$

are isomorphisms. Here H' denotes the subgroup H/Z of $\mathrm{PGL}_2(\mathbf{F}_p)$.
(b) If H has the property that $\det(H) = \mathbf{F}_p^*$, then projection on the classical coordinate induces an isomorphism

$$\Omega^1(X(p)_H) \otimes_{\mathbf{Q}} \mathbf{C} \xrightarrow{\cong} S_2(\Gamma_H)$$

of $\mathrm{SL}_2(\mathbf{F}_p)$-representations.
(c) Let H be the standard Borel subgroup B. It acts on $\Omega^1(X_U) \otimes_{\mathbf{Q}} \mathbf{C}$ and for any character μ of B, projection on the classical coordinate induces an isomorphism

$$(\Omega^1(X_{ZU}) \otimes_{\mathbf{Q}} \mathbf{C})(\mu) \xrightarrow{\cong} S_2(\Gamma_1(p), \mu^2).$$

Here the left hand side denotes the subspace of $\Omega^1(X_{ZU}) \otimes_{\mathbf{Q}} \mathbf{C}$ on which B acts via the character μ. The right hand side is the subspace of $S_2(\Gamma_1(p))$ on which the diamond operators act through the character μ^2.

Proof. Part (a) is well known. Part (b) follows from the fact that H-invariant elements in $\Omega^1(X(p)') \otimes_{\mathbf{Q}} \mathbf{C} = S_2(\Gamma_Z) + [R]S_2(\Gamma_Z)$ are determined by their classical coordinates. Indeed, we may choose the representative R inside H. Then the two coordinates must be equal.

(c) The two coordinates of an element of $\Omega^1(X_{ZU})$ are cusp forms in $S_2(\Gamma_1(p))$. The diamond operators in $\Gamma_0(p)/\pm\Gamma_1(p)$ are congruent modulo p to matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \qquad \text{with } a \in \mathbf{F}_p^*.$$

It follows that, if $b \in B$ acts as multiplication by $\mu(b)$ on an element of $\Omega^1(X_{ZU})$, the two coordinates are in $S_2(\Gamma_1(p), \mu^2)$. The second coordinate is determined by the classical one. Indeed, we can choose $R \in B$ and then the second coordinate is equal to the first multiplied by $\mu^{-1}(R)$.

This proves the proposition

Of special interest is the standard split Cartan subgroup T of G. Since the subgroup Γ_T of $\mathrm{SL}_2(\mathbf{R})$ is conjugate to $\Gamma_0(p^2)$, there is a natural Hecke compatible isomorphism $S_2(\Gamma_0(p^2)) \longrightarrow S_2(\Gamma_T)$. In terms of q-expansions at infinity, the isomorphism is given by

$$\sum_{n\geq 1} a_n q^{pn} \mapsto \sum_{n\geq 1} a_n q^n,$$

where q denotes $\exp(2\pi i\tau/p)$ with $\tau \in \mathbf{H}$. Since, the Fourier coefficients of $\Gamma_0(p^2)$-invariant normalized eigenforms are totally real algebraic integers, so are those of T-invariant normalized eigenforms.

We denote the subspace of *newforms* of $S_2(\Gamma_0(p^2))$ by $S_2(\Gamma_0(p^2))^{\mathrm{new}}$. Abusing notation somewhat, we denote the corresponding subspace of $S_2(\Gamma_T)$ by $S_2(\Gamma_T)^{\mathrm{new}}$. Note however, that all forms in $S_2(\Gamma_T)$ are of level p. See [5, (3.4)]. By Prop. 3.1 (b) applied to $H = T$, we may identify $S_2(\Gamma_T)$ with the subspace of T-invariants of $\Omega^1(X(p)) \otimes_{\mathbf{Q}} \mathbf{C}$. By V_f we denote the $\mathbf{Q}[G]$-subrepresentation of $\Omega^1(X(p))$ generated by a normalized eigenform f in $S_2(\Gamma_T)^{\mathrm{new}}$. It is a vector space over the number field K_f generated by the Fourier coefficients of f.

Proposition 3.2. *Let f be a normalized eigenform in $S_2(\Gamma_T)^{\mathrm{new}}$. Then the subgroup Z of scalar matrices acts trivially on the $\mathbf{C}[G]$-module $V_f \otimes_{K_f} \mathbf{C}$. Moreover, $V_f \otimes_{K_f} \mathbf{C}$ is an irreducible representation of dimension $\neq 1$, which is not isomorphic to the Steinberg representation.*

Proof. See [5, Prop.3.6]. Let V be an irreducible constituent of $V_f \otimes_{K_f} \mathbf{C}$. By semi-simplicity we have that $V^T \neq 0$. The G-action and the Hecke action on $\Omega^1(X(p))$ commute. Therefore, for a prime number $l \neq p$ the Hecke operator T_l acts on V as multiplication by the Fourier coefficient a_l. Then it also acts this way on the subspace V^T of $S_2(\Gamma_T)$. Since f corresponds to a newform in $S_2(\Gamma_0(p^2))$, strong multiplicity one implies that V^T is the 1-dimensional complex vector space generated by f. It follows that $f \in V$, so that V is equal to the irreducible representation $V_f \otimes_{K_f} \mathbf{C}$. The group Z acts trivially on V_f, since it is contained in T.

If V_f had dimension 1, it would be invariant under $\mathrm{PSL}_2(\mathbf{F}_p)$. Since the quotient of $X(p)'$ by $\mathrm{PSL}_2(\mathbf{F}_p)$ is a genus 0 curve over $\mathbf{Q}(\sqrt{\pm p})$, the $\mathrm{SL}_2(\mathbf{F}_p)$-invariants of $\Omega^1(X(p)')$ are zero and V_f must be zero as well. Contradiction. Since the subspace of T-invariant elements of V_f has dimension 1, Proposition 2.1 implies that V_f cannot be the Steinberg representation either.

This proves the proposition.

4. Principal series and twisted Steinberg representations.

In this section we explain how to find elements that are invariant under a non-split Cartan subgroup in the representations V_f generated by a normalized eigenform f, in case V_f is a principal series or twisted Steinberg representation of $G = \mathrm{GL}_2(\mathbf{F}_p)$ on which the center Z acts trivially.

Let $p > 2$ be a prime and let B be the standard Borel subgroup of G. The 1-dimensional characters of the group B that are trivial on the center Z form a cyclic group of order $p-1$. Given such a character μ, we write $\mathbf{Q}(\mu)$ for the number field generated by the values of μ. An explicit model for the induced representation $\mathrm{Ind}_B^G(\mu)$ of G is

$$\{\phi : G \longrightarrow \mathbf{Q}(\mu) : \phi(gb) = \mu^{-1}(b)\phi(g) \text{ for all } g \in G \text{ and } b \in B\}.$$

The group G acts on this $\mathbf{Q}(\mu)$-vector space as follows

$$(\sigma\phi)(x) = \phi(\sigma^{-1}x), \qquad \text{for } \sigma, x \in G \text{ and } \phi \in \mathrm{Ind}_B^G(\mu).$$

A basis of $\mathrm{Ind}_B^G(\mu)$ is given by e_r with $r \in \mathbf{P}_1(\mathbf{F}_p) = \mathbf{F}_p \cup \{\infty\}$, where e_r is the function on G that is equal to μ^{-1} on the B-coset $\{\sigma \in G : \sigma(\infty) = r\}$ and zero elsewhere. For every $r \in \mathbf{F}_p$ the G-action on e_r can easily be computed: for every $k \in \mathbf{F}_p$ we have

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} e_r = e_{r+k}, \quad \text{for } r \in \mathbf{F}_p, \text{ while } \quad \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} e_\infty = e_\infty. \tag{1}$$

For every $a \in \mathbf{F}_p^*$ we have

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} e_r = \mu \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} e_{ar} \quad \text{for } r \in \mathbf{F}_p, \text{ while } \quad \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} e_\infty = \mu \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} e_\infty. \tag{2}$$

The action of the matrix $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is given by

$$we_r = \mu \begin{pmatrix} 1/r & 0 \\ 0 & r \end{pmatrix} e_{-1/r} \quad \text{for } r \in \mathbf{F}_p^*, \tag{3}$$

while w switches e_0 and e_∞. Since $G = B \cup BwB$, these formulas determine the action of G.

If $\mu^2 \neq 1$, we recover the irreducible complex representation V_μ of section 2 as $\mathrm{Ind}_B^G(\mu) \otimes_{\mathbf{Q}(\mu)} \mathbf{C}$. The values of the character of V_μ generate the maximal real subfield $\mathbf{Q}(\mu)^+$ of the cyclotomic field $\mathbf{Q}(\mu)$. Since the subspace of T-invariants is 1-dimensional, it follows from [26, Lemma 1.1] that the representation V_μ itself can actually be defined over $\mathbf{Q}(\mu)^+$. We do not make use of this.

If $\mu^2 = 1$, we have that μ is either 1 or ω, so that $\mathbf{Q}(\mu) = \mathbf{Q}$. In this case, the subspace L of constant functions of $\mathrm{Ind}_B^G(\mu)$, generated by $e_\infty + \sum_{r \in \mathbf{F}_p} e_r$, is preserved by G and the representation $(\mathrm{Ind}_B^G(\mu)/L) \otimes_{\mathbf{Q}} \mathbf{C}$ is irreducible. In fact, we recover the complex Steinberg representation V_{st} and its quadratic twist V_ω. See [8].

We let Z, B, T, T', N, N' and U be the subgroups of G defined in section 2. It is convenient to view μ as a character of $\mathbf{F}_p^*$. For this reason we put

$$\mu(r) \;=\; \mu \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}, \qquad \text{for } r \in \mathbf{F}_p^*.$$

Proposition 4.1. *Let $\mu : B/Z \longrightarrow \mathbf{C}^*$ be a character satisfying $\mu^2 \neq 1$ and let V_μ be the principal series representation associated to μ.*

(a) The subspace of V_μ of U-invariants has dimension 2 and is generated by e_∞ and by $\sum_{r \in \mathbf{F}_p} e_r$. The subgroup B acts via μ on the line generated by e_∞ and via μ^{-1} on the line generated by $\sum_{r \in \mathbf{F}_p} e_r$.

(b) The subspace of T-invariants is generated by

$$\sum_{r \in \mathbf{F}_p^*} \mu(r) e_r.$$

It is invariant under the action of the normalizer N if and only if μ is an even character of $B/ZU = T/Z$.

(c) The subspace of T'-invariants is generated by

$$e_\infty + \sum_{r \in \mathbf{F}_p} \mu^{-1}(r^2 - u) e_r.$$

It is invariant under the action of the normalizer N' if and only if μ is even.

Proof. Parts (a) and (b) easily follow from the formulas given above. The computations are easy and left to the reader. By Proposition 2.1, the subspaces of T-invariants and of T'-invariants have dimension 1. The element listed in (c) is the T'-trace of Proposition 2.2 applied to e_∞.

This proves the proposition.

For the character $\mu = \omega$, the result is similar:

Proposition 4.2. *Let ω be the quadratic character of G and let V_ω be the twisted Steinberg representation.*

(a) The subspace of V_ω of U-invariants has dimension 1 and is generated by e_∞. The subgroup B acts on it via ω.

(b) The subspace of T-invariants is generated by

$$\sum_{r \in \mathbf{F}_p^*} \omega(r) e_r.$$

It is invariant under the action of the normalizer N if and only if $p \equiv 1 \pmod 4$.

(c) The subspace of T'-invariants is generated by

$$e_\infty + \sum_{r \in \mathbf{F}_p} \omega(r^2 - u) e_r.$$

It is invariant under the action of the normalizer N' if and only $p \equiv 1 \pmod 4$.

Proof. Note that in V_ω we have the relation $e_\infty = -\sum_{r \in \mathbf{F}_p} e_r$. The proof is similar to the proof of Proposition 4.1.

The relation with q-expansions of eigenforms is as follows. Suppose that f is a normalized eigenform in the space $S_2(\Gamma_T)^{\text{new}}$. Since f is Γ_T-invariant, Proposition 3.1 (b) implies that we can identify $S_2(\Gamma_T)^{\text{new}}$ with a subspace of $\Omega^1(X(p)) \otimes_{\mathbf{Q}} \mathbf{C}$. By Proposition 3.2, the newform f generates an absolutely irreducible G-representation V_f, defined over the number field K_f generated by the Fourier coefficients of f. Note that this implies that K_f contains the field $\mathbf{Q}(\mu)^+$ of character values.

Suppose that V_f is a principal series or twisted Steinberg representation. In other words, we have an isomorphism

$$V_\mu \cong V_f \otimes_{K_f} \mathbf{C}, \qquad \text{for some non-trivial character } \mu : B/Z \longrightarrow \mathbf{C}^*.$$

By Propositions 4.1 (a) and 4.2 (a), the representation V_μ admits a unique 1-dimensional U-invariant subspace W on which the Borel subgroup B acts via μ. It is generated by the element e_∞. Proposition 3.1 (c) implies then that in V_f, there is a unique element whose classical coordinate is a $\Gamma_1(p)$-invariant normalized eigenform h on which $\Gamma_0(p)$ acts via the character μ^2. In the twisted Steinberg case, we have $\mu = \omega$ and hence $\mu^2 = 1$. In this case h is a $\Gamma_0(p)$-invariant normalized eigenform.

Any G-equivariant linear map $V_\mu \longrightarrow V_f \otimes_{K_f} \mathbf{C}$, must map e_∞ into the 1-dimensional space generated by h. Schur's Lemma implies that for each $c \in \mathbf{C}^*$ there is a unique G-equivariant isomorphism

$$j_c : V_\mu \xrightarrow{\cong} V_f \otimes_{K_f} \mathbf{C},$$

for which $j_c(e_\infty) = ch$.

Let $q = e^{\frac{2\pi i \tau}{p}}$. Since h is $\Gamma_1(p)$-invariant, its Fourier expansion is of the form

$$h = \sum_{n \geq 1} a_n q^{pn}.$$

Note that there is also a unique element in $V_f \otimes_{K_f} \mathbf{C}$ whose classical coordinate is the 'complex conjugate' normalized eigenform $\overline{h} = \sum_{n\geq 1} \overline{a_n} q^{pn} \in S_2(\Gamma_1(p), \mu^{-2})$. The isomorphism j_c maps the element $-\sum_{r \in \mathbf{F}_p} e_r$ to a multiple of $\overline{h}$.

The following proposition relates the Fourier expansion of f to the one of h.

Proposition 4.3. *Let $\mu \neq 1$ and let f and h be the normalized eigenforms described above. Put $\zeta_p = e^{\frac{2\pi i}{p}}$.*

(a) Then the q-expansion of f is given by

$$f = \sum_{n \geq 1} \mu(n) a_n q^n,$$

with the convention that $\mu(n) = 0$, whenever n is divisible by p.

(b) The eigenform h is in the $\mathbf{Q}(\mu)[G]$-span of $\frac{\tau(\mu)\tau(\mu^2)}{a_p} f$. Here $\tau(\mu)$ and $\tau(\mu^2)$ denote the Gaussian sums $\sum_{x \in \mathbf{F}_p} \mu(x)\zeta_p^x$ and $\sum_{x\in\mathbf{F}_p} \mu^2(x)\zeta_p^x$ respectively. When $\mu = \omega$ we have $\mu^2 = 1$ and we put $\tau(\mu^2) = -1$.

Proof. By Prop. 4.1 (b), the subspace of T-invariant elements of V_μ is the 1-dimensional subspace generated by $\sum_{r \in \mathbf{F}_p^*} \mu(r) e_r$. The isomorphism j_c introduced above, maps it to a Γ_T-invariant eigenform in $V_f \otimes_{K_f} \mathbf{C}$. For a suitable choice of c we obtain f itself.

We compute $j_c(\sum_{r\in\mathbf{F}_p^*} \mu(r) e_r)$. The formulas (1), (2) and (3) given above, imply that

$$e_r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} w e_\infty, \qquad \text{for } r \in \mathbf{F}_p.$$

It follows that

$$j_c(e_r) = c \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} wh.$$

By Atkin-Li [1], the modular involution w_p transforms h into the 'complex conjugate' form $\overline{h}$ multiplied by the so-called pseudo-eigenvalue ϵ, which is a complex number of absolute value 1. To be precise, ϵ is equal to $\tau(\mu^2)/a_p$ and we have

$$\frac{1}{p\tau^2}h(-\frac{1}{p\tau}) \;=\; \epsilon\overline{h}(\tau), \qquad \text{for } \tau \in \mathbf{H}.$$

This implies that wh is the element of V_μ whose classical coordinate is equal to the Fourier series

$$wh(\tau) \;=\; \frac{\epsilon}{p}\overline{h}(\tau/p) \;=\; \frac{\epsilon}{p}\sum_{n\geq 1}\overline{a_n}q^n.$$

It follows that for $r \in \mathbf{F}_p$ we have

$$j_c(e_r) \;=\; c\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} wh(\tau) \;=\; c\frac{\epsilon}{p}\sum_{n\geq 1}\overline{a_n}\zeta_p^{rn}q^n.$$

Therefore the classical coordinate of $j_c(\sum_{r\in\mathbf{F}_p^*}\mu(r)e_r)$ is

$$c\frac{\epsilon}{p}\sum_{n\geq 1}\sum_{r\neq 0}\overline{a_n}\mu(r)\zeta_p^{nr}q^n \;=\; c\frac{\epsilon\tau(\mu)}{p}\sum_{n\geq 1}\mu^{-1}(n)\overline{a_n}q^n \;=\; c\frac{\epsilon\tau(\mu)}{p}\sum_{n\geq 1}\mu(n)a_nq^n.$$

The last equality follows from the fact that $\mu^{-1}(n)\overline{a_n}$ is real and hence equal to $\mu(n)a_n$ for all $n \in \mathbf{Z}$.

Since f is a *normalized* eigenform, part (a) follows. When we choose $c = (\epsilon\tau(\mu)/p)^{-1}$, we have that $j_c(\sum_{r\in\mathbf{F}_p^*}\mu(r)e_r) = f$. In particular, f is in the $\mathbf{Q}(\mu)[G]$-span of $j_c(e_\infty) = ch$. Since V_f is irreducible, this is the same as saying that h is in the $\mathbf{Q}(\mu)[G]$-span of $\epsilon\tau(\mu)f$.

This proves the proposition.

We now turn to the computation of the Fourier series of the T'-invariant eigenform in V_μ. See also [15]. Recall that $u \in \mathbf{F}_p^*$ is a fixed non-square. We put

$$\lambda_n = \sum_{r\in\mathbf{F}_p}\mu^{-1}(r^2-u)\zeta_p^{rn}, \qquad \text{for } n \in \mathbf{Z}.$$

Proposition 4.4. *Let $f \in S_2(\Gamma_T)^{\mathrm{new}}$ be the T-invariant eigenform discussed above and let $h = \sum_{n\geq 1}a_nq^{pn}$ be the corresponding $\Gamma_1(p)$-invariant eigenform. Then the element of V_f with classical coordinate equal to*

$$\frac{1}{\tau(\mu)}\left(\frac{p}{\tau(\mu^2)}\sum_{n,\,p|n}a_nq^n \;+\; \sum_{n\geq 1}\lambda_n\overline{a_n}q^n\right)$$

is a generator for the subspace of T'-invariant forms. Moreover, it is in the $\mathbf{Q}(\mu)[G]$-span of the Γ_T-invariant eigenform f.

Proof. Propositions 4.1 (c) and 4.2 (c) give an explicit generators of the 1-dimensional subspace of T'-invariants of V_μ. We apply the ismorphism j_c with $c = p/\epsilon\tau(\mu)$ as we did above. Since

$$e_r \;=\; \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} we_\infty, \qquad \text{for } r \in \mathbf{F}_p,$$

we get

$$\frac{p}{\epsilon\tau(\mu)}\left(\sum_{n\geq 1} a_n q^{pn} + \frac{\epsilon}{p}\sum_{r\in\mathbf{F}_p}\mu^{-1}(r^2-u)\sum_{n\geq 1}\overline{a_n}\zeta_p^{rn}q^n\right).$$

Since $a_{pn} = a_p a_n$ for every $n \geq 1$, this is equal to

$$\frac{p}{\tau(\mu)\tau(\mu^2)}\sum_{n,\, p|n} a_n q^n + \frac{1}{\tau(\mu)}\sum_{n\geq 1}\left(\sum_{r\in\mathbf{F}_p}\mu^{-1}(r^2-u)\zeta_p^{rn}\right)\overline{a_n}q^n,$$

which is easily seen to give the result. By Proposition 4.3 (b) the result is contained in the $\mathbf{Q}(\mu)[G]$-span of f. This proves the proposition.

The numbers $\lambda_n = \sum_{r\in\mathbf{F}_p}\mu^{-1}(r^2-u)\zeta_p^{rn}$ are so-called *Salié sums*. They are related to Kloosterman sums. See [9] and the references therein.

5. Cuspidal Representations.

Let $p > 2$ be prime, let $G = \mathrm{GL}_2(\mathbf{F}_p)$ and let $T \subset G$ be the standard split Cartan subgroup of diagonal matrices. In this section we consider normalized Γ_T-invariant weight 2 eigenforms f, that generate representations $V_f \subset \Omega^1(X(p))$ that are cuspidal. We explain how to find elements in V_f that are invariant under a non-split Cartan subgroup of G.

Let $u \in \mathbf{F}_p^*$ be a non-square, let T' denote the non-split torus in G introduced in section 2 and let $\theta : T' \longrightarrow \mathbf{Q}(\theta)^*$ be a character that is trivial on the subgroup Z of scalar matrices. We have $\theta^{p+1} = 1$ and assume that $\theta^2 \neq 1$. By $\mathbf{Q}(\theta)$ we denote the field generated by the image of θ. Our model V_θ for the cuspidal representation associated to θ is the quotient of the $\mathbf{Q}(\theta)$-vector space of functions $\phi : \mathbf{F}_p \longrightarrow \mathbf{Q}(\theta)$ by the 1-dimensional subspace of constant functions. The standard Borel subgroup $B \subset G$ acts by fractional linear transformations on $\mathbf{F}_p = \mathbf{P}_1(\mathbf{F}_p) - \{\infty\}$ and hence on the space of functions $\phi : \mathbf{F}_p \longrightarrow \mathbf{Q}(\theta)$: we have $\sigma\phi(x) = \phi(\sigma^{-1}x)$ for $\sigma \in B$ and any function ϕ. Since B preserves the constant functions, it acts on V_θ.

It is easy to see that V_θ is an irreducible $(p-1)$-dimensional representation of B, on which the scalar matrices act trivially. We turn V_θ into an irreducible representation of $\mathrm{PGL}_2(\mathbf{F}_p)$. Let

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

be the usual involution. Since $G = B \cup BwB$, it suffices to describe the action of w. It is given by

$$w\,\phi = -\frac{1}{p}\sum_{y\in\mathbf{F}_{p^2}^*}\theta(y)\begin{pmatrix} \mathrm{N}(y) & \mathrm{Tr}(y) \\ 0 & 1 \end{pmatrix}\phi, \qquad \text{for all } \phi \in V_\theta.$$

Here $\mathbf{F}_{p^2}$ denotes $T' \cup \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$. It is a subfield of the ring of 2×2 matrices over $\mathbf{F}_p$. Let N and Tr denote the norm and trace maps from $\mathbf{F}_{p^2}$ to $\mathbf{F}_p$ respectively.

Proving that the formula for the action of w gives rise to a well defined action of G on V_θ is straightforward but somewhat cumbersome. Alternatively, one can relate V_θ to the representation space described by Bump [8, 4.1]. Let ζ_p denote a fixed p-th root of unity. To every $\phi \in V_\theta$ we associate the function $\tilde{\phi} : \mathbf{F}_{p^2}^* \longrightarrow \mathbf{Q}(\theta)$ given by $\tilde{\phi}(y) = \theta^{-1}(y) \sum_{r\in\mathbf{F}_p} \phi(r)\zeta_p^{r\mathrm{N}(y)}$. This gives an isomorphism of $V_\theta \otimes_{\mathbf{Q}(\theta)} \mathbf{C}$ with Bump's model. Our model has the advantage that it can be defined over $\mathbf{Q}(\theta)$, rather than over a field that contains the p-th roots of unity. The character values of V_θ generate the maximal real subfield $\mathbf{Q}(\theta)^+$ of $\mathbf{Q}(\theta)$. As in the principal series case, it follows from [26, Lemma 1.1] that V_θ can actually be defined over $\mathbf{Q}(\theta)^+$. We do not make use of this.

Let $e_0 : \mathbf{F}_p \longrightarrow \mathbf{Q}(\theta)$ be the characteristic function of 0. For $r \in \mathbf{F}_p$, let $e_r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} e_0$. It is the characteristic function of the element $r \in \mathbf{F}_p$. The functions e_r, $r \in \mathbf{F}_p^*$ form a basis for the V_θ. Since $\sum_{r\in\mathbf{F}_p} e_r$ is the constant function 1, we have the relation $\sum_{r\in\mathbf{F}_p} e_r = 0$ in V_θ.

Proposition 5.1. *Let $\theta : T'/Z \longrightarrow \mathbf{Q}(\theta)^*$ be a character satisfying $\theta^2 \neq 1$ and let V_θ be the cuspidal representation of G associated to the character θ. Then*

(a) the subspace of U-invariants is zero;

(b) the subspace of T-invariants is generated by e_0; it is invariant under the action of the normalizer N of T if and only if θ is an odd character of the cyclic group T'/Z;

(c) there is an $r \in \mathbf{F}_p^*$ for which the element

$$pe_r - \sum_{m\in\mathbf{F}_p} \sum_{y\in\mathbf{F}_{p^2}^*} \theta(y) e_{\frac{(m+r)\mathrm{N}(y)}{m^2-u} + \mathrm{Tr}(y) + m}$$

generates the 1-dimensional subspace of T'-invariants. The space of T'-invariants is also N'-invariant if and only if θ is odd.

Proof. Part (a) and the first statement of (b) easily follow from the formulas given above. The statement about the normalizer N can be proved with a short computation [5, Prop.2.1]. To prove (c), we combine the formula for the action of w with Proposition 2.2. It follows that the T'-trace is equal to

$$\mathrm{id} - \frac{1}{p} \sum_{y\in\mathbf{F}_{p^2}^*} \theta(y) \sum_{m\in\mathbf{F}_p} \begin{pmatrix} \mathrm{N}(y) & m\mathrm{N}(y) + (m^2-u)(\mathrm{Tr}(y)+m) \\ 0 & m^2-u \end{pmatrix}.$$

Applying it to pe_r gives the element of part (c). Since the elements e_r, with $r \in \mathbf{F}_p$, generate V_θ, their T'-traces generate the 1-dimensional space of T'-invariants. In other words, the T'-trace of at least one of the elements e_r is not zero and hence generates the subspace of T'-invariants.

This proves the proposition.

The relation with q-expansions of eigenforms is as follows. Let $q = e^{\frac{2\pi i\tau}{p}}$, let $\zeta_p = e^{\frac{2\pi i}{p}}$ and let

$$f = \sum_{n\geq 1} a_n q^n$$

be a normalized weight 2 eigenform that is invariant under Γ_T. By Prop. 3.1 (b) we may identify $S_2(\Gamma_T)$ with the T-invariant elements in $\Omega^1(X(p)) \otimes_{\mathbf{Q}} \mathbf{C}$. Then f generates an absolutely irreducible G-representation V_f that is defined over the number field K_f generated by the Fourier coefficients of f. Suppose that V_f is a cuspidal representation. In other words, we have

$$V_\theta \cong V_f \otimes_{K_f} \mathbf{C}, \qquad \text{for some character } \theta : T'/Z \longrightarrow \mathbf{Q}(\theta)^* \text{ with } \theta^2 \neq 1.$$

Note that K_f contains the values of the character of V_θ. This means that $\mathbf{Q}(\theta)^+$ is a subfield of K_f.

By Proposition 5.1 (b), the element $f \in V_f$ corresponds to the vector $e_0 \in V_\theta$ or a multiple thereof. More generally, for any $r \in \mathbf{F}_p$ the elements in V_f with classical coordinate equal to

$$f_r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} f = \sum_{n \geq 1} a_n \zeta_p^{nr} q^n,$$

correspond to multiples of e_r.

Proposition 5.2. *The elements in V_f with classical coordinate equal to*

$$pf_r - \sum_{m \in \mathbf{F}_p} \sum_{y \in \mathbf{F}_{p^2}^*} \theta(y) f_{\frac{(m+r)\mathrm{N}(y)}{m^2-u} + \mathrm{Tr}(y) + m}, \qquad \textit{for } r \in \mathbf{F}_p,$$

are all T'-invariant. They are all in the $\mathbf{Q}(\theta)[G]$-span of f and at least one of them generates the subspace of T'-invariants of V_f.

Proof. This follows from the fact that the vectors e_r are in the $\mathbf{Z}[G]$-span of e_0 and the fact that the T'-trace is an element of $\mathbf{Q}(\theta)[G]$.

6. Level 17.

In this section we explain how to compute equations over $\mathbf{Q}$ for the canonical embedding of the genus 6 curve $X_{\mathrm{ns}}^+(17)$. We follow the method in [21]. We exhibit six linearly independent weight 2 cusp forms that are invariant under the normalizer N' of the standard non-split Cartan subgroup T'. We find these forms inside the six representation spaces V_f, generated by six normalized eigenforms $f \in S_2(\Gamma_T(17))^{\mathrm{new}}$, that are invariant under the normalizer N of the standard split Cartan subgroup T. Since the space $S_2(\Gamma_T(17))^{\mathrm{new}}$ is closely related to the space $S_2(\Gamma_0(17^2))^{\mathrm{new}}$, we start from there. We can find the Fourier expansions of the normalized eigenforms in [25], for instance.

Up to Galois conjugation and twists by the quadratic character ω, there are four normalized weight 2 eigenforms invariant under $\Gamma_0(17^2)$. Two of these are twists of normalized eigenforms in $S_2(\Gamma_1(17))$. They give rise to principal series and twisted Steinberg representations. The other two eigenforms generate cuspidal representations.

There is a unique $\Gamma_0(17)$-invariant normalized eigenform $f_0 = \sum_n a_n q^{17n}$. Its 17-th Fourier coefficient a_{17} is equal to $+1$. Its quadratic twist $\sum_n \omega(n) a_n q^{17n}$ is a normalized $\Gamma_0(17^2)$-invariant eigenform. Here we put $q = e^{\frac{2\pi i\tau}{17}}$ for $\tau \in \mathbf{H}$. By convention $\omega(n) = 0$

whenever n is divisible by 17. The corresponding Γ_T-invariant form is $\sum_n \omega(n) a_n q^n$. The first few terms of its Fourier expansion are

$$f_1 \;=\; q - q^2 - q^4 + 2q^5 - 4q^7 + 3q^8 - 3q^9 - 2q^{10} - 2q^{13} + 4q^{14} - q^{16} + 3q^{18} + \ldots$$

The irreducible subrepresentation V_{f_1} of $\Omega^1(X(p)')$ is isomorphic to the twisted Steinberg representation. The form f_1 is also invariant under the normalizer N of T because $17 \equiv 1 \pmod 4$. See Prop. 4.2.

One finds in Stein's tables that the space $S_2(\Gamma_1(17))$ is the direct product of the 1-dimensional space of $\Gamma_0(17)$-invariant forms and a 4-dimensional subspace W spanned by the Galois conjugates of an eigenform h on which the diamond operators act through a character of order 8 of $(\mathbf{Z}/17\mathbf{Z})^*$. Any such character is of the form μ^2, where μ has order 16. Since μ is then an odd character of T/Z, Prop. 4.1 implies that the normalizer N acts as -1 on the T-invariants.

Therefore the twist by μ of h as described in section 4, is a $\Gamma_0(17^2)$-invariant normalized weight 2 eigenform, corresponding to a Γ_T-invariant form that is not N-invariant. It plays no role in our computation of the canonical embedding of $X^+_{\rm ns}(17)$.

The remaining normalized eigenforms in Stein's tables both generate cuspidal representations. Put $a = \frac{-1+\sqrt{13}}{2}$. Then the modular form

$$\begin{aligned} f_2 \;=&\; q - (a+1)q^2 + aq^3 + (a+2)q^4 - (a+1)q^5 - 3q^6 + (a-1)q^7 - 3q^8 - aq^9 + \\ &+ (a+4)q^{10} - 3q^{11} + (a+3)q^{12} - (a+2)q^{13} + (a-2)q^{14} - 3q^{15} + (a-1)q^{16} + \ldots \end{aligned}$$

is the Γ_T-invariant form associated to a newform in $\Gamma_0(17^2)$. The representation V_{f_2} is cuspidal with respect to some character θ of order dividing 18. Since the field K_{f_2} generated by the Fourier coefficients, contains $\mathbf{Q}(\theta)^+$, we actually must have that $\theta^6 = 1$. Figuring out what character θ of T'/Z is involved, can be done by numerically computing the action of w on f_2 for every possible θ in a suitable $\tau \in \mathbf{H}$ as in Baran's paper [5, section 6]. It turns out that in this case θ has order 6. The twist of f_2 by ω is cuspidal with character $\theta\omega$, which has order 3. By Prop. 5.1 the form f_2 is N-invariant, while its twist is anti-invariant.

The fourth normalized eigenform is the Γ_T-invariant form associated to one of the $\Gamma_0(17^2)$-invariant eigenforms in Stein's table with Fourier coefficients in $\mathbf{Q}(\zeta_9)^+$. The first few terms of its Fourier expansion are

$$\begin{aligned} f_3 \;=&\; q - (b^2+b-2)q^2 - (b+1)q^3 + bq^4 + (b^2+b-4)q^5 + (2b^2+2b-3)q^6 + bq^7 + \\ &+ (b^2+b-3)q^8 + (b^2+2b-2)q^9 + (2b^2+b-6)q^{10} - (2b^2-2)q^{11} - (b^2+b)q^{12} + \ldots \end{aligned}$$

Here $b = \zeta_9 + \zeta_9^{-1}$. It is a zero of $x^3 - 3x + 1$. The representation V_{f_3} is cuspidal with character θ of order 18. The twist by ω is cuspidal with character $\theta\omega$ of order 9. By Prop. 5.1 the form f_3 is N-invariant, while its twist is anti-invariant.

At this point we have six T-invariant eigenforms: f_1, f_2 and its Galois conjugate and f_3 with its two Galois conjugates. To f_1 we apply the T'-trace fomula in Proposition 4.4. This gives us a T'-invariant form g_1 with Fourier coefficients in $\mathbf{Q}(\zeta_{17})^+$. Applying the formula of Proposition 5.2 to f_2 and its conjugate over $K_{f_2} = \mathbf{Q}(\sqrt{13})$, we obtain the

T'-invariant form f_2' and its conjugate. Their Fourier coefficients are in $K_{f_2}(\zeta_{17})^+$. We put $g_2 = \mathrm{Tr}(f_2')$ and $g_3 = \mathrm{Tr}(\sqrt{13}f_2')$. Here Tr denotes the trace map from $\mathbf{Q}(\zeta_{17})^+(\sqrt{13})$ to $\mathbf{Q}(\zeta_{17})^+$. Then g_2 and g_3 are T'-invariant forms with Fourier coefficients in $\mathbf{Q}(\zeta_{17})^+$. Similarly, we apply the T'-trace map given in Proposition 5.2 to f_3 and its conjugates over $K_{f_3} = \mathbf{Q}(\zeta_9)^+$ and obtain the T'-invariant form f_3'. Its Fourier coefficients are in $K_{f_3}(\zeta_{17})^+$. For $i = 1, 2, 3$, we put $g_{3+i} = \mathrm{Tr}(e_i f_3')$, where e_1, e_2, e_3 denotes the basis of $K_{f_3}(\zeta_{17})^+$ over $\mathbf{Q}(\zeta_{17})^+$ given by $1, \alpha, \alpha^2$, where α is a zero of the defining polynomial $x^3 + 3x^2 - 3$ used in Stein's table. Then g_4, g_5 and g_6 are T'-invariant forms with Fourier coefficients in $\mathbf{Q}(\zeta_{17})^+$.

We list the first few Fourier coefficients of the T'-invariant forms $g_1, \ldots, g_6$. By an 8-tuple $[x_1, \ldots, x_8] \in \mathbf{Z}^8$ we denote the element $\sum_{j=1}^{8} x_j(\zeta_{17}^j + \zeta_{17}^{-j})$. For every i we have divided the coefficients of g_i by a common divisor in $\mathbf{Z}$.

$$
\begin{aligned}
g_1 &= [7,1,2,5,4,5,4,6]q - [6,7,4,1,5,2,4,5]q^2 + [-5,6,4,7,2,4,5,1]q^4 \ldots\\
g_2 &= [4,16,2,-4,-2,8,-8,18]q + [9,2,-4,8,4,1,-1,-2]q^2 - [4,-1,2,-4,-2,8,9,1]q^3 \ldots\\
g_3 &= [9,2,-4,8,4,1,-1,-2]q^2 - [4,-1,2,-4,-2,8,9,1]q^3 - [-2,9,-1,2,1,-4,4,8]q^4 \ldots\\
g_4 &= [8,8,-2,4,5,-2,-1,-3]q - [3,2,-1,2,-2,7,-4,10]q^2 - [12,9,12,6,18,12,9,24]q^3 ..\\
g_5 &= -[4,4,8,6,3,4,2,3]q + [1,4,-1,4,-2,4,-1,8]q^2 + [2,5,10,1,12,10,2,9]q^3 \ldots\\
g_6 &= [10,10,9,12,5,2,1,2]q - [5,12,0,12,0,16,1,22]q^2 - [8,10,22,4,32,22,9,29]q^3 \ldots
\end{aligned}
$$

By [23] the canonical embedding of a genus 6 curve is typically cut out by six quadrics. See also [12, Thm. 1.1] and [21]. We compute six quadrics that vanish on the canonically embedded curve $X_{\mathrm{ns}}^+(17)$ and then use MAGMA to check that the intersection of the quadrics is a curve of genus 6. Then we know that the quadrics are indeed equations for $X_{\mathrm{ns}}^+(17)$.

To do this, we compute Fourier series of the 21 products $g_i g_j$ with $1 \le i \le j \le 6$. Even though the Fourier coefficients of the forms g_i are in $\mathbf{Q}(\zeta_{17})^+$ and are usually not rational, the corresponding Kähler differentials are rational. This is explained by the fact that the cusps of $X_{\mathrm{ns}}^+(17)$ are not rational, but conjugate over $\mathbf{Q}(\zeta_{17})^+$. Since the curve $X_{\mathrm{ns}}^+(17)$ is defined over $\mathbf{Q}$, we search for quadrics

$$\sum_{1 \le i \le j \le 6} a_{ij} x_i x_j,$$

with coefficients a_{ij} in $\mathbf{Q}$. From the equation $\sum_{1\le i \le j \le 6} a_{ij} g_i g_j = 0$ we obtain infinitely many equations with coefficients in $\mathbf{Q}(\zeta_{17})^+$, one for every term q^n in the Fourier expansion. Since the coefficients are in the degree 8 number field $\mathbf{Q}(\zeta_{17})^+$, each equation gives rise to *eight* equations with coefficients in $\mathbf{Z}$. For instance, a consideration of the Fourier coefficients of q^2 and q^3 gives rise to the following 16 equations. Here the columns correspond to the coefficients a_{ij} in lexicographic order.

6	0	0	3	−2	5	−3840	0	0	−2	2	0	0	0	0	15	2	7	3	−3	10
3	0	0	3	1	1	10620	0	6	−2	4	0	0	0	0	18	2	8	4	−5	14
4	−2	0	−1	0	−1	−5256	0	−4	0	2	0	0	0	0	7	0	4	6	−9	17
5	2	0	1	0	1	2820	0	−14	0	−8	0	0	0	0	20	0	14	6	−9	24
3	0	0	0	1	−2	−3948	0	12	10	−8	0	0	0	0	24	−1	17	4	−6	20
6	6	0	−3	−1	0	9972	0	6	2	0	0	0	0	0	18	−2	15	4	−7	21
4	−8	0	−1	1	−2	−3018	0	−16	−2	−8	0	0	0	0	25	−1	20	3	−5	23
5	2	0	−2	0	−2	852	0	10	−6	16	0	0	0	0	26	0	17	4	−7	24
−2	−12	8	−10	2	−8	8	−4	−51	26	−76	0	13	0	10	4	4	−7	−2	7	−20
0	−24	6	−9	2	−8	24	−12	−45	17	−56	0	15	3	6	0	1	−4	−2	5	−12
0	−9	3	−3	1	−2	24	−12	−30	23	−54	0	6	1	2	6	−4	8	0	1	−2
0	−12	6	−9	3	−12	36	−18	−54	23	−64	0	18	−1	14	18	−3	15	−2	3	2
−4	−15	1	−8	−1	−3	4	−2	−51	25	−71	0	17	−1	13	2	−5	9	8	−14	26
2	−12	4	−14	5	−16	−8	4	−39	22	−61	0	11	−4	15	8	−2	10	0	0	8
0	−3	3	−3	1	−4	48	−24	−39	11	−43	0	21	1	15	24	−7	28	2	−7	30
0	−15	3	−12	4	−15	0	0	−48	23	−68	0	18	1	10	6	−1	9	−4	5	2

Rather than two, we use the first 10 Fourier coefficients and hence obtain a grossly overdetermined linear system of 80 equations in 21 unknowns. As expected, the solution space has dimension 6. In this way we obtain six independent quadrics $\sum_{1\le i\le j\le 6} a_{ij}x_ix_j$ with coefficients in $\mathbf{Q}$. By means of a linear change of variables and by replacing the quadrics by suitable linear combinations, we obtain equations that have very small coefficients and have good reduction modulo primes different from 17. Here we use the LLL-algorithm as in [21]. The independent quadrics $q_1, \ldots, q_6$ we obtained, are listed below. They cut out a genus 6 curve, which must be $X^+_{\mathrm{ns}}(17)$.

$$\begin{aligned}
q_1 =& -3x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + 2x_2x_4 + x_2x_5 - x_2x_6 - 2x_3^2 +\\
&+ 2x_3x_4 + 2x_3x_5 + x_3x_6 + x_4x_5 - x_4x_6 + x_5^2 - x_5x_6,\\
q_2 =&\ x_1x_2 - 2x_1x_3 - 2x_1x_4 + x_1x_6 + x_2x_5 + 2x_2x_6 - x_3x_4 - 2x_3x_5 + x_4^2 -\\
&- x_4x_5 + x_4x_6 - 2x_5^2 + x_6^2,\\
q_3 =&\ 3x_1^2 + 3x_1x_2 + x_1x_3 - x_1x_4 + x_1x_6 + x_2x_3 - x_2x_4 + x_2x_5 + 2x_2x_6 + x_3^2 -\\
&- x_3x_4 - x_4^2 - x_4x_5 - x_4x_6 + x_5^2 + 2x_5x_6,\\
q_4 =&\ 2x_1^2 + 2x_1x_2 - 2x_1x_3 + x_1x_4 - 2x_1x_5 + x_1x_6 - x_2x_3 - x_2x_5 + 3x_2x_6 - x_3^2 +\\
&+ 3x_3x_4 - 3x_3x_5 - x_4^2 - x_4x_5 + 2x_5^2 - x_5x_6 + x_6^2,\\
q_5 =&\ x_1x_2 + 5x_1x_3 + 2x_1x_4 - x_1x_5 + x_2^2 + 3x_2x_3 + 2x_2x_4 - x_2x_5 - x_3^2 + 2x_3x_4 -\\
&- 3x_3x_5 + x_4^2 + 3x_4x_6 - x_5^2 - 2x_5x_6 - x_6^2,\\
q_6 =& -3x_1x_2 + x_1x_3 - 2x_1x_4 + 4x_1x_5 - 3x_1x_6 - 3x_2^2 - 2x_2x_3 - 5x_2x_4 + x_2x_5 -\\
&- x_2x_6 + x_3^2 + x_3x_4 - 3x_3x_5 + x_4^2 - 2x_4x_5 - 2x_4x_6 + x_5^2 + 3x_5x_6 - x_6^2.
\end{aligned}$$

CM-points or Heegner points are points on modular curves parametrizing elliptic curves with complex multiplication by imaginary quadratic orders $\mathcal{O} \subset \mathbf{C}$. Only if $\mathcal{O}$ is one of the thirteen quadratic orders of class number 1, the CM-points may give rise to rational points. Since the prime 17 is inert in the orders $\mathcal{O}$ of discriminant $-3, -7, -11, -12$, -27, -28 and -163, there is for each of these orders $\mathcal{O}$, a unique rational CM-point on the curve $X_{\rm ns}^{+}(17)$. We have determined the projective coordinates of these CM-points by evaluating the Fourier series of the modular forms g_i numerically in suitable $\tau \in \mathbf{H}$ for which $17\tau \in R$.

Table. CM-points on $X_{\rm ns}^{+}(17)$.

discriminant	CM-point
-3	$(2 : -2 : -1 : 3 : -2 : 1)$
-7	$(-6 : -2 : -4 : 1 : -3 : 13)$
-11	$(3 : 1 : 2 : -9 : -7 : 2)$
-12	$(-4 : 10 : 3 : -5 : -2 : 3)$
-27	$(2 : -5 : -10 : -6 : 1 : 7)$
-28	$(0 : 0 : 0 : 1 : 1 : 1)$
-163	$(-7 : 9 : 35 : 21 : 5 : 1)$

A short computer calculation revealed that there are no rational points $(x_1 : x_2 : x_3 : x_4 : x_5 : x_6)$ on $X_{\rm ns}^{+}(17)$ with $x_i \in \mathbf{Z}$ and $|x_i| < 10\,000$, other than the seven CM-points listed in the table.

7. Level 19 and 23.

In this section we present quadrics that cut out the modular curves $X_{\mathrm{ns}}^{+}(19)$ and $X_{\mathrm{ns}}^{+}(23)$. They were obtained by the method explained in the previous section.

The modular curve $X_{\mathrm{ns}}^{+}(19)$ has genus 8. Its canonical embedding in $\mathbf{P}_7$ is cut out by fifteen quadrics. These are listed in Table 1. Here the rows contain the coefficients of the 36 monomials $x_i x_j$ with $1 \leq i \leq j \leq 8$ in lexicographic order. Each column corresponds to the equation of a quadric in $\mathbf{P}_7$.

Table 1.

−1	1	0	0	−1	0	0	−1	1	1	0	2	0	1	0
1	0	0	0	1	0	0	−1	−2	−1	1	0	3	−2	4
0	−1	−1	0	1	0	1	2	−1	0	1	−3	1	0	1
0	1	−1	0	−1	1	0	1	−2	0	1	2	1	0	0
−1	−1	1	−2	1	0	0	−1	1	−1	0	1	1	2	2
0	0	0	−1	2	0	−1	0	−1	−1	0	−2	0	0	1
0	1	0	−1	0	0	0	0	−1	−1	−1	−1	0	0	−1
0	0	0	0	1	−1	1	−1	0	0	0	1	2	−1	−1
0	0	1	1	0	0	0	0	0	0	−1	0	0	0	1
1	−1	1	0	−1	0	−1	2	1	−1	0	0	−1	0	0
0	−1	1	0	1	0	0	0	−1	1	0	−1	2	−1	0
0	1	−1	0	0	1	0	−1	0	1	0	0	1	−1	−1
0	0	0	0	0	2	−1	0	1	2	−1	0	2	−1	−1
1	0	−1	−1	−1	1	1	1	−1	0	0	0	0	1	−2
0	0	1	1	0	0	0	0	0	−1	1	1	0	1	−1
0	−2	0	0	0	0	0	2	0	0	−1	−1	−1	0	0
0	1	1	0	−1	−1	0	−2	2	−1	0	0	0	1	−1
1	−1	0	−2	1	−1	0	1	1	1	2	−1	0	0	−1
1	−1	1	−1	0	−1	−1	−2	2	0	−1	0	0	0	−1
1	−1	0	−1	−1	1	0	1	−1	0	−1	0	0	0	0
1	0	1	0	−2	2	−2	1	−1	0	0	−1	0	−1	0
1	0	1	0	0	1	0	1	−2	−1	1	1	1	−1	1
0	0	−1	0	−1	0	0	−1	0	−1	0	2	−1	−1	−3
1	−1	1	0	0	1	0	0	0	0	−1	0	0	−3	0
−1	2	0	0	−1	1	0	0	0	1	−1	−1	−2	0	−1
1	0	1	0	1	0	0	−1	0	−1	0	1	1	−1	1
−1	0	−1	−1	0	0	0	−1	1	0	0	0	−1	0	−2
−1	1	−1	0	0	−1	2	−2	0	−1	0	0	−2	−1	−1
0	−2	1	−1	1	−2	−1	1	0	1	−1	−1	−2	−1	−1
−1	0	0	1	1	−1	−1	0	−1	1	1	−1	0	−3	−1
0	0	0	0	0	0	1	0	0	0	0	0	0	−1	0
0	0	0	−1	0	0	0	2	0	1	1	0	−2	0	0
0	0	0	0	1	0	−1	0	0	0	0	−1	−3	−1	1
1	0	0	−1	−1	0	0	0	1	0	1	1	0	0	0
0	0	−1	−1	−2	1	1	1	1	0	−1	0	−1	1	1
0	0	0	0	1	0	−1	0	0	0	0	−1	0	0	2

The prime 19 is inert in the imaginary quadratic orders $\mathcal{O}$ of discriminant $-4, -7, -11, -16, -28, -43$ and -163. For each order $\mathcal{O}$ there is a rational CM-point on $X_{\mathrm{ns}}^{+}(19)$, corresponding to an elliptic curve with complex multiplication by $\mathcal{O}$. As in the previous section, the CM-points have been computed numerically. They are the only rational points $(x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8)$ with $x_i \in \mathbf{Z}$ satisfying $|x_i| \leq 10\,000$.

Table 2. CM-points on $X_{\rm ns}^{+}(19)$.

discriminant	CM-point
-4	$(0:0:-1:1:0:-1:1:0)$
-7	$(2:7:-12:-4:3:3:10:-4)$
-11	$(3:1:1:-6:-5:-5:-4:13)$
-16	$(-2:12:7:-15:16:-3:9:4)$
-28	$(0:1:0:0:1:-1:0:0)$
-43	$(-10:3:3:1:4:-15:7:1)$
-163	$(2:0:0:-3:-1:0:0:3)$

The modular curve $X_{\rm ns}^{+}(23)$ has genus 13. Its canonical embedding in $\mathbf{P}_{12}$ is cut out by 55 quadrics. These are listed in Table 3. Here the rows contain the coefficients of the 78 monomials $x_i x_j$ with $1 \le i \le j \le 13$ in lexicographic order. Each column corresponds to the equation of a quadric in $\mathbf{P}_{12}$.

Table 3.

```
0 1 -1 1 3 0 0 2 1 0 -1 0 0 0 1 -2 1 2 2 1 1 0 1 0 0 0 1 -1 1 3 -2 1 -1 -1 0 0 -1 0 0 1 -1 1 -1 -1 0 2 2 -1 -1 2 1 1 1 -1 0
-2 1 -1 2 2 1 -1 0 -2 -1 -3 0 0 -2 1 2 3 -1 -1 -1 0 1 3 -1 -1 0 -2 0 -1 -1 1 0 1 -1 2 1 -3 1 0 0 1 0 -1 -1 -1 -1 -1 1 0 2 -1 -2 -1 -1 2
0 0 2 -3 -2 2 -2 0 -2 1 0 0 0 -2 -3 -1 2 -2 -2 0 -1 0 1 -1 -1 0 -1 -1 -3 -2 3 1 1 1 -1 1 0 0 2 -2 0 0 0 1 1 -1 -1 0 0 0 0 0 0 0 0
2 0 0 1 -1 -1 1 1 1 0 0 1 0 0 2 0 -1 1 1 1 1 -2 -1 -1 2 -1 1 -2 1 2 -2 -2 -1 0 -1 -3 3 -1 -1 2 0 0 0 2 -2 0 1 0 0 0 0 0 0 2 0
-1 0 0 -1 0 0 -1 0 -1 0 1 -1 0 0 -1 -1 1 0 0 0 -3 1 -1 -1 -2 1 0 1 -1 -1 1 1 0 1 -1 1 -1 -1 1 -1 0 -1 0 -1 1 0 0 1 -1 1 1 2 0 -1 0
0 0 1 0 0 -2 2 -1 -3 0 -1 -1 1 2 3 2 1 1 -5 3 -3 2 1 0 0 2 1 -2 1 -1 -2 0 -2 1 0 1 -2 4 0 0 -3 -2 0 1 0 -1 -1 2 1 -1 1 0 -1 -1 0
-1 -2 1 0 3 2 0 -3 1 0 -2 0 0 0 1 1 2 0 -2 0 0 0 2 -1 -3 3 1 -2 2 -1 -1 1 1 1 -1 1 -2 1 1 3 -1 1 2 1 2 -1 0 1 2 -1 2 -1 1 -1 1
0 -2 1 0 -1 2 -3 0 3 1 -2 2 -1 -5 1 3 1 -1 2 -2 3 -3 2 0 0 -2 -1 1 0 1 2 1 1 -1 0 0 -1 -2 1 2 -1 1 1 1 2 0 1 0 2 0 0 -2 0 2 1
-1 1 0 0 3 -3 0 3 -1 2 -1 0 1 1 -1 0 1 1 0 0 1 0 2 -3 -1 -1 0 -2 1 1 -1 5 0 -2 0 1 1 2 0 0 -2 2 -2 -2 2 2 0 2 -3 -1 0 1 -2 0 -1
-1 -1 1 0 -1 0 -4 0 -2 -1 -1 -2 1 -3 4 2 1 -4 0 1 -1 -1 0 1 0 4 -2 -2 -2 -4 0 -1 0 2 0 -1 -1 -2 0 0 0 -2 -2 4 -1 -3 0 3 1 0 -1 -1 -2 1 1
0 -4 -1 2 0 -1 1 0 4 -3 1 2 -3 -1 2 0 -1 4 0 -1 -1 1 1 -1 -1 -2 1 2 1 2 -2 -2 -2 0 -1 -2 -1 -2 -1 3 0 -1 -1 0 2 3 1 1 -1 0 3 -2 1 1 1
1 -1 -1 2 -2 1 -1 1 0 1 0 -1 1 -2 0 -1 -2 -1 0 -3 2 -2 1 -3 1 -1 -1 3 -2 -2 -2 -1 0 1 0 -2 3 -3 -1 -1 1 -1 1 2 2 -2 0 -1 0 1 0 -1 0 1 -2
-3 -2 0 -1 0 1 -1 -3 2 -1 1 2 0 1 1 4 2 0 -1 -2 -2 1 0 1 0 -1 -1 4 1 -2 2 1 1 -1 1 3 -3 0 3 1 0 -1 1 -4 1 -1 -1 1 2 -1 1 0 0 1 3
0 2 -1 3 -1 0 0 2 -2 -1 -2 -1 -1 -3 1 1 0 -2 1 0 0 -1 1 -1 3 -1 -1 -1 -1 1 1 -2 0 -1 2 -2 1 0 -1 -1 2 0 -1 1 -3 -1 -1 1 -1 2 -4 -1 -1 0 1
0 0 1 1 -1 1 -1 0 -1 -2 0 0 0 -1 1 2 1 -1 -1 0 0 0 1 2 2 2 -1 -2 0 -2 2 -1 1 1 -1 -2 -1 0 1 -1 0 0 0 0 -2 -1 0 1 -1 0 -1 -2 -1 -1 0
-2 0 -1 -1 2 0 0 -1 0 1 0 -1 0 1 -2 -1 0 0 0 -1 0 2 1 -2 -2 0 0 1 0 0 1 3 2 0 1 3 0 0 0 1 0 0 0 -1 3 0 0 0 2 0 1 2 1 -1 0
2 0 1 1 -1 1 1 0 1 0 -2 2 0 -1 1 2 -1 -1 -1 0 2 -2 -1 1 1 1 -1 -1 1 0 -1 -2 -1 1 -1 -2 -1 0 -1 1 0 0 1 1 -1 -1 0 1 -1 -1 0 -2 -1 1 0
0 0 -2 2 0 0 1 -1 -2 1 -3 1 2 2 -2 2 1 1 -3 0 1 1 1 -3 -1 -1 0 0 0 0 -2 2 0 0 2 -1 0 0 -1 2 3 1 -3 1 2 -2 -3 1 0 2 0 -1 -4 -2 0
-3 1 -2 2 2 1 -1 -1 -3 0 -3 -3 -1 -2 -1 -1 2 -1 0 -1 -2 1 2 -3 0 1 0 -1 -1 -1 1 1 1 -1 3 1 -1 0 1 0 2 0 0 0 0 -2 -2 1 2 3 -2 1 0 -1 2
-1 1 -1 1 3 2 -3 0 -1 1 -1 -2 1 0 0 -1 3 2 2 0 0 -1 0 -1 -1 1 1 -1 -1 0 0 2 0 0 -1 1 -2 -1 2 0 -1 2 1 -2 -1 0 2 -1 0 4 0 1 2 -1 0
1 0 1 -1 -2 -2 2 -1 0 1 0 3 1 0 0 0 0 1 -1 -1 -1 0 -1 1 0 -1 -2 0 2 -1 -1 -1 0 -2 1 -2 0 0 0 -1 -2 -2 0 1 -2 0 -1 -1 1 -2 2 0 -2 2 2
0 0 0 0 2 2 -2 1 1 0 0 -1 -1 -2 2 2 0 -2 0 0 2 -2 0 -2 -1 1 1 0 -2 0 1 -1 1 3 -1 3 1 0 -2 0 0 1 1 -1 0 -1 1 1 -1 -1 -1 -1 3 0 -1
1 0 0 -1 0 -1 2 0 3 -1 -1 0 -4 0 0 0 0 -2 -1 -1 -1 1 -2 -2 1 -2 0 -1 2 4 0 0 -4 0 1 0 -2 2 0 4 -2 2 1 -1 0 0 -2 3 -1 -1 0 -3 1 3 2
0 -2 2 -2 -1 1 -2 0 1 -2 1 -1 -4 -1 2 2 -1 -3 1 -2 0 1 1 -1 3 1 -2 0 -1 -1 1 0 -1 5 -3 0 0 2 0 0 0 -1 0 0 3 1 0 2 -1 -1 -1 -2 1 1 -1
0 -1 1 -1 -1 0 0 1 1 0 1 0 -1 -1 1 0 -1 -1 1 2 -2 -2 0 0 0 0 1 1 -3 1 0 0 -1 0 -1 1 1 1 0 -1 0 0 0 1 2 1 1 1 -1 -1 -2 2 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 -1 -1 0 0 0 0 0 0 0 -1 1 0 0 1 0 0 0 0 1 0 1 0 1 0 -1 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 -1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 -1 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 -1 1 0 -1 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 -1 0 0 0 -1 -1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 -1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 -1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 -1 -1 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 0 0 0 0 0
```

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
-4	0	-2	2	4	0	0	-2	0	-2	0	-2	0	2	0	2	0	0	0	-2	-1	4	1	-1	-2	2	0	2	3	0	2	2	4	1	1	3	-3	-1	0	1	2	-1	0	-3	1	0	0	2	2	1	1	0	0	-4	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	1	-2	0	3	1	-1	-1	0	-1	1	0	0	2	0	2	3	0	1	0	0	0	-1	-1	-2	2	1	0	-2	-1	1	2	1	2	-1	1	0	2	-2	1	2	4	0	-4	-1	0	-2	-1	-2	0	-1	-1	0	-2	0
-2	3	-3	3	4	1	-1	1	-1	2	-1	-4	2	3	-3	0	2	1	1	-2	1	0	-2	-3	-1	-1	2	0	3	2	0	5	1	-1	1	3	-2	0	2	1	0	5	1	-4	0	-2	0	1	0	5	-1	1	1	-4	-2
0	1	3	1	-1	2	1	0	-4	2	-1	-2	-2	0	-3	1	0	1	-1	1	-1	1	-3	-1	1	1	5	-4	3	0	2	0	-2	3	-1	3	-2	1	-1	0	0	3	3	0	-2	0	0	2	0	0	-3	-2	2	-3	3
0	1	-4	0	4	-3	1	-1	4	-2	3	-2	1	2	-1	-4	-1	-1	1	0	-1	3	-1	-1	-4	1	-3	2	0	1	1	3	2	-2	1	-1	1	-3	-1	1	0	2	-1	-3	-1	2	0	-1	-1	-1	2	1	0	1	-2
3	0	1	-2	1	0	1	-2	3	-1	1	0	-2	1	2	2	1	1	-2	3	0	1	-1	0	-3	0	1	-2	0	4	2	0	-1	2	-2	1	-2	2	0	2	-3	2	3	-1	-1	2	2	0	0	-1	2	-3	3	1	0
-1	-2	0	-2	0	1	-2	-4	-2	-2	0	1	-3	2	-4	1	1	3	-1	0	-2	3	0	0	-1	1	0	-2	-2	-2	3	1	0	1	-1	-1	-1	0	1	0	4	1	-1	-2	2	3	-2	1	-3	1	1	0	-2	0	0
-1	0	0	2	0	0	0	2	0	-2	-1	0	2	3	2	2	1	-1	0	0	1	-1	2	1	2	-1	-1	-1	1	1	-2	1	0	-1	-2	-3	-1	2	3	1	1	-1	-3	1	2	-2	0	3	-1	3	-1	0	-2	-2	-2
-1	-1	0	0	1	1	-1	-2	-1	0	-1	-1	0	0	0	-1	2	1	-1	0	-2	0	0	0	-1	2	1	-1	0	-2	-1	0	-1	0	0	0	-2	0	1	1	0	0	1	0	0	-1	-1	0	1	1	1	0	0	0	1
-1	-1	2	1	-2	3	-2	-1	-3	2	-3	0	1	-4	-1	1	1	0	-1	0	0	-1	3	0	1	0	0	0	0	-2	1	-1	1	0	1	1	-1	-2	1	-1	1	-1	1	3	0	-1	0	0	2	2	-1	0	-1	-1	1
-1	0	1	3	2	-1	1	0	-1	2	-1	-1	2	1	2	3	0	1	1	1	-1	-1	0	-3	-1	2	3	-1	4	1	-1	2	0	1	-1	1	0	0	-1	2	-1	0	3	0	0	0	3	3	0	-1	-1	1	0	-1	0
-1	-1	-1	-2	1	-1	0	-1	2	-2	0	-1	-1	0	-1	-1	-2	-2	-4	0	0	2	1	0	-3	0	-3	0	-2	0	1	1	3	-1	1	1	-1	-1	1	-1	0	-1	-3	1	3	0	-2	2	1	-1	2	0	0	0	-1
-2	-4	-2	4	1	0	0	-4	0	-3	0	1	-1	0	1	1	0	5	1	-1	-3	2	1	-1	-3	2	1	1	1	-2	-1	-2	1	1	0	-3	-1	-3	-1	3	4	-2	0	1	0	2	1	1	0	2	2	-1	-1	-1	2
-1	-3	1	-1	-1	-1	-2	-2	-1	-2	0	-2	-1	2	0	-1	0	3	-4	1	-3	3	2	-1	1	-1	-1	-2	0	-1	-1	1	-2	0	-2	-2	-3	-1	4	0	0	-3	-1	1	3	2	0	3	-1	3	3	0	-2	2	-1
1	1	-1	0	-1	2	1	0	1	1	0	2	0	0	-2	-1	0	2	-1	-1	1	-1	-1	0	1	-4	0	2	0	2	0	-2	0	-2	2	1	0	0	1	-2	0	1	2	-2	-1	-1	0	-3	-1	2	1	1	2	0	1
1	-2	2	-1	-2	1	0	-2	0	0	0	2	-1	-2	0	2	-1	0	-1	1	0	0	1	0	-1	0	0	0	-1	-1	2	-2	1	2	-1	0	1	-1	-2	0	1	-1	1	2	0	1	0	0	0	-2	0	-1	0	1	1
-1	-1	0	2	0	0	-2	1	0	1	-1	0	3	-1	3	3	1	0	1	0	1	-2	3	0	1	0	0	2	1	0	-1	2	1	-1	0	0	0	-1	1	1	-1	-1	0	1	2	-1	2	1	1	1	0	1	-2	-1	-2
2	-2	0	-2	1	-1	1	-1	3	0	0	3	-1	2	1	1	-2	2	-2	0	2	0	-1	-1	-2	-1	-1	0	-1	1	-3	0	-1	2	-1	0	0	1	-2	1	-1	0	-2	0	2	2	0	0	-1	-2	3	-1	1	2	0
-3	-3	0	2	-2	1	-3	0	-2	-1	0	0	0	-3	-1	0	1	2	1	-1	-2	0	2	0	0	0	1	1	-1	-3	1	-1	1	-1	0	-1	0	-4	1	0	3	-2	-2	2	1	0	0	1	1	2	0	0	-2	1	1
-1	0	2	-1	1	2	0	2	-1	-1	1	-1	1	-1	2	-3	0	-3	-2	2	-2	2	3	0	2	3	-1	1	-2	-2	-1	-1	0	3	-1	3	0	0	0	-3	0	-2	-1	0	0	1	1	0	-1	-1	0	1	2	-1	1
1	1	-1	1	-1	2	-1	0	-3	1	0	-1	0	-1	-2	-2	1	2	0	0	0	0	0	-1	1	-1	1	0	-2	-1	0	-2	-1	1	1	0	1	0	-1	-2	1	1	1	0	-2	-1	0	-3	-2	3	-1	0	1	-1	0
0	0	1	2	1	-1	0	3	-2	1	0	0	2	1	2	0	0	1	1	1	1	0	1	-1	2	0	1	-1	3	0	-4	0	-2	1	0	0	1	1	-2	0	0	0	-2	1	-1	1	2	1	-3	0	-1	0	-1	-1	0
-1	0	-2	-1	0	-1	-2	-1	0	-1	-2	0	1	-1	2	0	1	-2	0	-1	-1	0	1	2	0	2	-4	1	-3	-1	0	1	1	-2	2	-2	-1	0	2	0	-1	-3	-3	1	2	-2	-2	0	2	2	2	1	-3	1	-1
-3	-1	-1	2	1	-3	1	2	-1	-1	1	-1	0	1	0	0	-1	2	-1	-1	-1	1	2	-1	-1	-1	2	1	1	-1	-2	1	1	-2	1	1	0	1	0	-1	1	-2	-2	-1	2	1	-1	2	-1	-1	0	0	-2	-2	-1
-3	0	-2	1	4	2	-1	0	1	-3	0	-2	0	1	2	0	0	-2	0	0	-1	1	3	-1	0	3	-1	2	-3	0	0	1	3	2	-1	2	-1	1	1	-1	2	-1	-1	-2	3	0	1	1	0	2	0	2	2	-2	-2
0	-2	3	-2	-1	4	-2	-1	1	-2	3	2	1	0	2	1	3	-1	-1	1	-1	1	2	2	1	1	-1	1	-1	-3	2	-1	1	3	-3	1	-1	-1	2	-1	0	0	1	-1	-1	0	2	-1	-1	-1	1	-1	2	-1	2
1	-1	2	-1	-1	2	0	0	1	1	0	2	-1	0	0	3	0	1	-1	0	2	-2	0	-1	0	-2	2	0	0	1	0	-1	0	2	-2	2	0	1	0	0	0	1	2	0	1	0	1	0	0	-1	0	-1	2	0	0
0	0	2	-2	-1	0	-4	0	-2	2	-1	-1	2	-2	2	1	2	-3	1	1	-1	-1	-1	0	1	3	-2	-2	0	-2	0	1	-1	1	0	0	0	-2	1	0	-2	0	-1	3	-1	-2	1	1	1	0	0	1	-2	2	1
0	1	1	-2	-1	1	1	1	2	0	1	1	0	-2	0	-1	0	-1	-1	0	1	-2	1	3	-1	-2	0	1	-1	1	2	-1	4	-3	0	2	-1	1	2	-3	-2	-1	2	0	0	-1	0	-3	3	-1	1	1	3	-1	0
-2	1	-3	2	0	-3	1	0	-3	2	-4	-3	-2	-1	-2	-1	-2	1	0	-2	-1	0	0	-2	1	-1	1	0	0	1	-2	1	-2	-3	5	0	0	2	0	1	0	-2	-1	1	3	-1	-3	2	2	2	-2	2	-2	1	-1
0	-2	-2	1	-1	-2	1	-1	3	-2	1	1	-1	-1	1	1	-1	1	-1	-2	0	0	1	0	-3	-2	-1	3	-1	0	0	-1	1	-2	1	-2	0	-1	0	1	0	-2	0	0	2	0	-1	0	1	-1	2	-2	-1	1	-1
-1	-2	-1	4	0	4	-2	-1	0	-1	-1	0	1	0	0	2	0	0	1	-3	1	0	1	-2	2	0	-1	3	1	-2	-1	0	0	3	-1	-1	-1	-3	0	1	4	1	0	0	2	-1	1	1	-1	4	-1	-1	0	-2	0
-3	-2	1	-3	0	1	-2	-2	2	-3	2	0	-3	1	0	2	2	-1	-1	-1	-3	2	0	1	0	0	0	1	-1	-1	4	1	0	0	-1	2	-3	0	4	1	0	-1	1	-4	2	0	-1	3	0	-1	1	-1	1	1	2
0	0	0	0	1	0	0	0	2	0	1	-1	1	1	0	-1	1	1	-1	1	0	0	0	-1	-1	-2	1	-1	2	2	0	1	1	-1	-1	1	-1	-1	2	1	-1	1	1	0	-1	0	1	0	1	1	1	0	1	0	0
1	1	-1	-1	4	-3	2	-1	1	1	-1	1	-1	2	2	1	-3	0	1	0	1	2	-2	-1	-1	3	-2	0	2	2	-2	1	-1	2	2	1	1	2	-4	1	-2	0	0	-2	0	3	1	1	-2	-3	2	1	0	2	0
2	-1	2	0	-3	1	0	1	-1	-2	2	0	-1	0	-1	-1	0	0	0	2	-1	0	0	1	1	0	1	-2	-2	-1	1	-2	-2	2	-4	-3	1	0	-1	-1	2	1	-1	2	-1	1	0	0	-3	0	-2	-2	0	-1	-1

The prime 23 is inert in the imaginary quadratic orders $\mathcal{O}$ of discriminant $-3, -4, -8$, -12, -16, -27 and -163. For each order $\mathcal{O}$ there is a rational CM-point on $X_{\mathrm{ns}}^{+}(23)$, corresponding to an elliptic curve with complex multiplication by $\mathcal{O}$. The CM-points have been computed numerically. They are the only rational points $(x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8 : x_9 : x_{10} : x_{11} : x_{12} : x_{13})$ with $x_i \in \mathbf{Z}$ satisfying $|x_i| \leq 10\,000$.

Table 4. CM-points on $X_{\mathrm{ns}}^{+}(23)$.

discriminant	CM-point
-3	$(-3:4:0:1:0:6:-1:6:-6:-6:0:-6:-12)$
-4	$(1:-2:0:-2:-1:0:1:-2:-1:0:-1:0:0)$
-8	$(3:13:-19:-4:16:8:-11:10:1:-7:-12:18:-5)$
-12	$(-15:4:-20:-3:12:6:9:-4:18:12:14:2:2)$
-16	$(3:-10:4:-4:-7:8:-11:10:1:16:11:18:18)$
-27	$(0:1:0:1:0:0:-1:0:0:0:0:0:0)$
-163	$(0:-1:0:-1:0:-2:1:-2:-4:0:4:-2:2)$

Bibliography

[1] Atkin, A. and Li, W.: Twists of Newforms and Pseudo-Eigenvalues of W-Operators, *Inventiones math.* **48** (1978), 221–243.

[2] Balakrishnan, J., Dogra, N., Müller, J.S., Tuitman, J. and Vonk, J.: Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13, arXiv:1711.05846, November 2017.

[3] Banwait, B. and Cremona, J.: Tetrahedral elliptic curves and the local-global principle for isogenies, *Algebra and Number Theory*, **8** (2014) 1201–1229.

[4] Baran, B.: Normalizers of non-split Cartan subgroups, modular curves and the class number one problem, *Journal of Number Theory* **130** (2010) 2753–2772.

[5] Baran, B.: An exceptional isomorphism between modular curves of level 13, *Journal of Number Theory* **145** (2014) 273–300.

[6] Bilu, Y., Parent, P. and Rebolledo, M.: Rational points on $X_0^+(p^r)$, *Annales de l'institut Fourier*, **63** (2013), 957–984

[7] Birch, B. and Kuyk, W.: *Modular Functions of One Variable IV*, Springer Lecture Notes **476**, Springer-Verlag 1972.

[8] Bump, D.: *Automorphic Forms and Representations*, Cambridge Studies in Advanced Mathematics **55**, CUP 1998.

[9] Conrad, K.: On Weil's proof of the bound for Kloosterman sums, *J. Number Theory* **97** (2002), 439–446.

[10] De Smit, B. and Edixhoven, B.: Sur un résultat d'Imin Chen, *Math. Res. Lett.* **7** (2000) 147–153.

[11] Dose, V., Fernández, J., González, J. and Schoof, R.: The automorphism group of the non-split Cartan modular curve of level 11, *Journal of Algebra* **417** (2014), 95–102.

[12] Dose, V.: On the automorphisms of the non-split Cartan modular curves of prime level, *Nagoya Math. J.* **224** (2016), 74–92.

[13] Dose, V., Mercuri, P. and Stirpe, C.: Cartan modular curves of level 13, to appear in *Journal of Number Theory*.

[14] Lang, S.: *Algebra*, Graduate Texts in Math **73**, Springer-Verlag 2002.
[15] Le Hung, Bao V.: Modularity of some elliptic curves over totally real fields, preprint 2013, arXiv:1309.4134
[16] Ligozat, G.: Courbes modulaires de niveau 11, pp. 149–237 in: *Modular functions of one variable, V* , Lecture Notes in Math. **601** Springer-Verlag, Berlin, 1977.
[18] The modular forms data base LMFDB, `http://www.lmfdb.org`.
[17] Magma Computational Algebra System. `http://magma.maths.usyd.edu.au/magma/`
[19] Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* **44** (1978) 129–162.
[20] Mercuri, P.: *Rational Points on Modular Curves*, PhD thesis, Università di Roma "La Sapienza" 2013/2014.
[21] Mercuri, P.: Equations and rational points of the modular curves $X_0^+(p)$, *The Ramanujan Journal*, doi: 10.1007/s11139-017-9925-2, to appear.
[22] Sagemath: `http://www.sagemath.org`.
[23] Saint-Donat, B.: On Petri's analysis of the linear system of quadrics through a canonical curve, *Math. Ann.* **206** (1973), 157–175.
[24] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331.
[25] Stein, W.: The modular forms database, `http://wstein.org/Tables/tables.html`.
[26] Waldspurger, J.-L.: Quelques propriétés arithmétiques de certaines formes automorphes sur GL(2), *Compositio Math.* **54** (1985), 121–171.