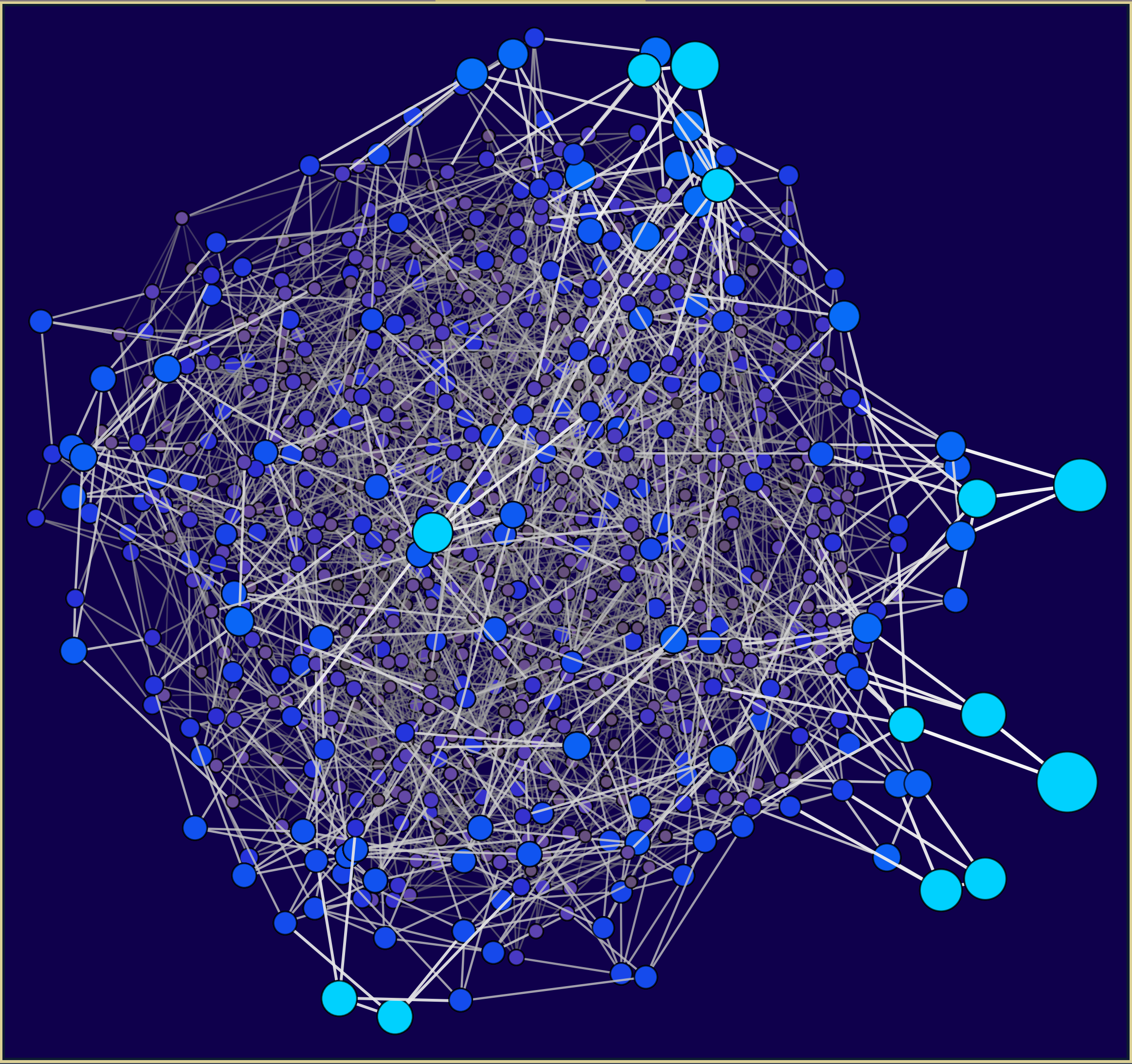
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Computation of paramodular forms

Gustavo Rama and Gonzalo Tornaría



msp

THE OPEN BOOK SERIES 4 (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.353

Computation of paramodular forms

Gustavo Rama and Gonzalo Tornaría

We develop an algorithm to compute paramodular forms of weight 3 as orthogonal modular forms attached to positive definite quinary quadratic forms. For square-free levels we expect that every paramodular form of weight 3 arises in this way.

Introduction

There are many efficient algorithms to compute classical (elliptic) modular forms (the Eichler–Selberg trace formula [Wad71], the method of modular symbols [Cre97], quaternion algebras and Brandt matrices [Piz80; Koh01], ternary quadratic forms [Bir91; Tor05; Ram14; HTV20], etc.) These have been used to compute extensive tables of modular forms [BK75; Cre97; Ste12; Cre19; LMF20].

Paramodular forms are Siegel modular forms for the paramodular group $K(N)$ (see [PY15]). They have gained attention in recent years due to the paramodular conjecture of Brumer and Kramer [BK14; BK19] which relates them to abelian surfaces (see [BPP$^+$19; BK17; BCGP18; CCG19] for recent progress on this conjecture). Poor and Yuen computed in [PY15] paramodular forms of weight 2 for $K(p)$ for primes $p < 600$, and for square-free levels in [PSY17]. These methods compute Fourier coefficients of paramodular forms; from those one can recover the Hecke eigenvalues, although a large number of Fourier coefficients are needed. It is possible to compute Hecke eigenvalues without computing Fourier coefficients by the method of specialization as done in [BPP$^+$19] but this is still expensive.

In this paper we develop an alternative algorithm to compute (Hecke eigenvalues of) paramodular forms of weight 3 using positive definite quinary quadratic forms. This is a generalization of a method of Birch to compute classical modular forms using ternary quadratic forms [Bir91; Hei16; HTV20]. Our method is based on a conjecture of Ibukiyama [Ibu07] which generalizes Eichler correspondence to paramodular forms. In principle it should be possible to extend this method for arbitrary weights ≥ 3.

For prime levels, Ladd shows in his thesis [Lad18] that Ibukiyama conjecture implies that every orthogonal modular form corresponds to a paramodular form, in the sense that computing orthogonal modular forms of level $\mathrm{O}(\Lambda)$ for a well chosen lattice Λ recovers the Hecke eigenvalues of paramodular forms.

MSC2020: 11F55.
Keywords: paramodular forms, orthogonal modular forms.

However, not every paramodular form of prime level comes from an orthogonal modular form with trivial representation, as we show in Example 13. In fact only the forms with sign $+1$ in the functional equation seem to arise in this way. We overcome this limitation in Section 3 by using orthogonal modular forms with a nontrivial character for the spinor norm (this idea has been proposed for ternary quadratic forms in [Tor05; Ram14], and completed in [HTV20]). Based on the dimension formulas of Ibukiyama [Ibu07] and on our computations of spaces of orthogonal modular forms we are led to conjecture that every paramodular form of prime level corresponds to some orthogonal modular form (see Theorem 14 and Conjecture 15). We expect the same holds for composite square-free levels although we do not have as much evidence for composite levels as we do for prime levels.

An interesting feature of the space $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ of orthogonal modular forms with trivial character is the existence of a map Θ from $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ to the space of elliptic modular forms of weight $\frac{5}{2}$. Because of properties of this map with respect to Hecke operators, when f is an eigenform in the cuspidal subspace $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ with $\Theta(f) \neq 0$, the Shimura lift of $\Theta(f)$ is a modular form of weight 4 whose Gritsenko lift corresponds to f, as in the following diagram:

$$\begin{array}{ccc} \mathcal{S}(\mathrm{O}(\hat{\Lambda})) & \xrightarrow{\ \Theta\ } & S_{5/2}(4N) \\ {\scriptstyle \text{Ibukiyama}}\ \updownarrow & & \downarrow\ {\scriptstyle \text{Shimura}} \\ S_3(K(N)) & \xleftarrow[\text{Gritsenko}]{} & S_4(N) \end{array}$$

For prime level Hein, Ladd and Tornaría conjectured that, conversely, if $\Theta(f) = 0$ then f corresponds to a paramodular form which is not a Gritsenko lift (see [Hei16, Conjecture 3.5.6]). The analogue of this conjecture for composite levels fails as shown in Example 10, due to the occurrence of eigenforms of Yoshida type. We propose Conjecture 12 as an alternative.

With respect to computations, Hein [Hei16] computed, in the case of trivial representation, the orthogonal modular forms with rational eigenvalues for quinary lattices of prime discriminant with $p < 200$, which (conjecturally) correspond to paramodular forms with $+1$ in the functional equation. This was extended by Ladd [Lad18] for $p < 400$. Using our proposed algorithm we computed the orthogonal modular forms, with the different characters of the spinor norm, for quinary lattices of square-free discriminant $D < 1000$. We expect to have a complete list of all paramodular forms for those levels. This computations can be found in [RT20].

This article is organized as follows. In Section 1 we recall the basic notions of neighbor lattices and orthogonal modular forms over $\mathbb{Q}$. In Section 2 we consider quinary orthogonal modular forms over $\mathbb{Q}$ and define the L-functions associated to a Hecke-eigenform in $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$. We also generalize the conjecture of Hein, Ladd and Tornaría to square-free levels.

In Section 3 we introduce a family of nontrivial representations for O(5) using characters of the spinor norm. We conjecture that with this representation we can obtain all paramodular form of prime level. In Section 4 we study the orthogonal modular forms of discriminant $5 \cdot 61$, classify all the irreducible Hecke-submodules and conjecture that $S_3(K(5 \cdot 61))$ is spanned by orthogonal modular forms. In Section 5 we consider the standard representation and compare the dimensions of spaces of orthogonal modular forms with this representation and the dimension of spaces of paramodular forms of weight 4.

In Section 6 we match some hypergeometric motives with spaces of orthogonal modular forms with not square-free discriminant. In Section 7 we mention the algorithms used to carry out our computations. Finally, in Section 8 we include tables of orthogonal modular forms for prime levels p, with $p < 500$.

1. Neighbor lattices and orthogonal modular forms

In this section we follow the article of Greenberg and Voight [GV14] and the Ph.D. thesis of Hein [Hei16].

1.1. ***Neighbor lattices.*** We fix (V, Q), a positive definite $\mathbb{Q}$-quadratic space.

Definition. Let $\Lambda \subset V$ be a $\mathbb{Z}$-lattice, and $k \geq 1$ an integer. We say that the $\mathbb{Z}$-lattice Π is a p^k-neighbor of Λ if $\Lambda_q = \Pi_q$ for all primes $q \neq p$ and there exist $\mathbb{Z}$-module isomorphisms

$$\Lambda/(\Lambda \cap \Pi) \cong \Pi/(\Lambda \cap \Pi) \cong (\mathbb{Z}/p\mathbb{Z})^k.$$

Remark 1. For $k = 1$ the previous definition agrees with the classical definition of p-neighbors; see for example [Bir91].

Lemma 2. *Let $\Lambda, \Pi \subset V$ be two $\mathbb{Z}$-lattices both locally unimodular at a prime p. Then, Λ and Π are p^k-neighbors if and only if $\Lambda_q = \Pi_q$ for all primes $q \neq p$ and there exists a basis of V_p*

$$e_1, \ldots, e_k, g_1, \ldots, g_{n-2k}, f_1, \ldots, f_k,$$

such that

(1) $\langle e_i, e_j \rangle = \langle f_i, f_j \rangle = 0$,

(2) $\langle e_i, f_j \rangle = \delta_{ij}$,

(3) $\langle e_i, g_j \rangle = \langle f_i, g_j \rangle = 0$,

(4) *$e_1, \ldots, e_k, g_1, \ldots, g_{n-2k}, f_1, \ldots, f_k$ is a $\mathbb{Z}_p$-basis of Λ_p, and*

(5) *$pe_1, \ldots, pe_k, g_1, \ldots, g_{n-2k}, p^{-1} f_1, \ldots, p^{-1} f_k$ is a $\mathbb{Z}_p$-basis of Π_p.*

If Λ is unimodular at p, we say that a basis that satisfies conditions (1)–(4) of the previous lemma is a p^k-standard basis for Λ_p. Consider a hyperbolic lattice $H_p = \mathbb{Z}_p e \oplus \mathbb{Z}_p f$ with $\langle e, e \rangle = \langle f, f \rangle = 0$, and $\langle e, f \rangle = 1$. With respect to this basis, we consider $\omega = \left(\begin{smallmatrix} p & 0 \\ 0 & p^{-1} \end{smallmatrix}\right) \in \mathrm{O}(H_p \otimes \mathbb{Q}_p)$. We extend ω to

$$\omega^{\oplus k} = \underbrace{\omega \oplus \cdots \oplus \omega}_{k} \in \mathrm{O}(V_p),$$

where the i-th entry in the direct sum acts upon the hyperbolic component $\{e_i, f_i\}$ given by a p^k-standard basis of Λ_p. We have that Π is a p^k-neighbor of Λ if and only if there exists $\hat{\sigma}$ in $\mathrm{O}(\hat{\Lambda})$ such that $\hat{\Pi} = \hat{\sigma}\hat{\omega}^{\oplus k}\hat{\Lambda}$. Also we have the following double coset decomposition

$$\mathrm{O}(\hat{\Lambda})\hat{\omega}^{\oplus k}\,\mathrm{O}(\hat{\Lambda}) = \bigsqcup_m \hat{p}_m\,\mathrm{O}(\hat{\Lambda}), \tag{3}$$

where each $\hat{p}_m$ corresponds to a p^k-neighbor of Λ.

Lemma 4. *Lattices (locally unimodular at p) in the same genus have the same number of p^k-neighbors.*

The lemma allows us to define the integers $N(\Lambda;\, p, k) = \#\mathrm{Neighbors}(\Lambda;\, p, k)$, which are genus invariants. By [Hei16, Equation 5.3.8] we have $N(\Lambda;\, p, k) = O(p^{k(n-k-1)})$. When $n = 5$ we have a more precise formula, $N(\Lambda;\, p, k) = p^{k-1}(p^3 + p^2 + p + 1)$ for $k = 1, 2$ and Λ unimodular at p. When Λ is not unimodular at p, and $p \parallel \mathrm{disc}(\Lambda)$, then $N(\Lambda;\, p, 1) = (p^3 + p^2 + p) \pm p^2$.

1.2. *Orthogonal modular forms.* Let $\Lambda \subset V$ be a $\mathbb{Z}$-lattice with $\mathrm{disc}(\Lambda) = D$, let W a finite-dimensional $\mathbb{Q}$-vector space, and let $\rho : \mathrm{O}(V) \to \mathrm{GL}(W)$ a finite-dimensional representation. We define the space of orthogonal modular forms with level $\mathrm{O}(\hat{\Lambda})$ and weight W to be the finite dimensional $\mathbb{Q}$-vector space

$$\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W) = \{ f : \mathrm{O}(\hat{V}) \to W \mid f(\sigma \hat{g} \hat{k}) = \rho(\sigma) f(\hat{g}) \text{ for all } \sigma \in \mathrm{O}(V),\, \hat{g} \in \mathrm{O}(\hat{V}),\, \hat{k} \in \mathrm{O}(\hat{\Lambda}) \}.$$

The class set of Λ is in bijection with $\mathrm{O}(V)\backslash \mathrm{O}(\hat{V}) / \mathrm{O}(\hat{\Lambda})$ and we have the double coset decomposition

$$\mathrm{O}(\hat{V}) = \bigsqcup_{i=1}^{h} \mathrm{O}(V) \hat{x}_i \, \mathrm{O}(\hat{\Lambda}),$$

where h is the class number of Λ, so the values of a modular form $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$ are determined by the values $f(\hat{x}_i)$, for $i = 1, \ldots, h$, and the representation ρ. We also have the following isomorphism

$$\begin{aligned} \mathcal{M}(\mathrm{O}(\hat{\Lambda}), W) &\xrightarrow{\sim} \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)} \\ f &\longmapsto (f(\hat{x}_1), f(\hat{x}_2), \ldots, f(\hat{x}_h)) \end{aligned}$$

where $\Lambda_i = \hat{x}_i \hat{\Lambda} \cap V$, for $i = 1, 2, \ldots, h$, are representatives of the class set of Λ.

If p is a prime such that Λ is unimodular at p, and $k \geq 1$, we define the p^k-Hecke operator on $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$ given by

$$(T_{p,k}\, f)(\hat{g}) = \sum_m f(\hat{g} \hat{p}_m),$$

where the $\hat{p}_m$ are given by the coset decomposition in (3). The Hecke operators $T_{p,k}$ and $T_{q,k'}$ commute for all $p \neq q$ primes.

We can define an inner product in $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$ by

$$\langle\!\langle f, g \rangle\!\rangle = \sum_{i=1}^{h} \frac{f(\hat{x}_i) g(\hat{x}_i)}{\# \mathrm{O}(\Lambda_i)},$$

note that $\# \mathrm{O}(\Lambda_i)$ is finite because V is positive definite. The Hecke operators $T_{p,k}$ on $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$ are self-adjoint with respect to $\langle\!\langle -, - \rangle\!\rangle$.

We define the Eisenstein subspace, denoted by $\mathcal{E}(\mathrm{O}(\hat{\Lambda}), W) \subset \mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$, to be the subspace of constant functions of $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$. The cuspidal subspace, denoted by $\mathcal{S}(\mathrm{O}(\hat{\Lambda}), W) \subset \mathcal{M}(\mathrm{O}(\hat{\Lambda}), W)$, is the subspace orthogonal to $\mathcal{E}(\mathrm{O}(\hat{\Lambda}), W)$. The following lemma is clear.

Lemma 5. *If $\rho : \mathrm{O}(V) \to \mathrm{GL}(W)$ is a nontrivial irreducible representation, then $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W) = \mathcal{S}(\mathrm{O}(\hat{\Lambda}), W)$.*

We denote by $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ the space of orthogonal modular forms when $W = \mathbb{Q}$ and ρ the trivial representation, and the cuspidal subspace by $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$. Let $f_1, \dots, f_h$ be the indicator basis of $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$, so that $f_j(\hat{x}_i) = \delta_{ij}$. We have

$$(T_{p,k} f_j)(\hat{x}_i) = \sum_m f_j(\hat{x}_i \hat{p}_m) = \sum_m f_j(\hat{x}_{m_*}) = \sum_m \delta_{jm_*},$$

where $\hat{x}_i \hat{p}_m \hat{\Lambda} = \sigma \hat{x}_{m_*} \hat{\Lambda}$ for some $\sigma \in \mathrm{O}(V)$ and some m_*. Let $N_{ij}(\Lambda; p, k) = (T_{p,k} f_j)(\hat{x}_i)$, the number of p^k-neighbors of Λ_i which are isomorphic to Λ_j. Then, we can compute $T_{p,k}$ in the basis $f_1, \dots, f_h$ by the formula

$$T_{p,k} f_j = \sum_{i=1}^{h} N_{ij}(\Lambda; p, k) f_i.$$

By Lemma 4 we have

$$N(\Lambda; p, k) = \sum_{j=1}^{h} N_{ij}(\Lambda; p, k),$$

for all $i = 1, \dots, h$, and $f_1 + \dots + f_h$ is an eigenvector of $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ with eigenvalue $N(\Lambda; p, k)$. Also, $f_1 + \dots + f_h$ is a generator of $\mathcal{E}(\mathrm{O}(\hat{\Lambda}))$, and we conclude that $\dim \mathcal{M}(\mathrm{O}(\hat{\Lambda})) = \dim \mathcal{S}(\mathrm{O}(\hat{\Lambda})) + 1$.

We want to define $T_{p,1}$ for $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ when $p \parallel D$. Since Λ is not unimodular at p, we cannot use Lemma 2, so we define it in the indicator basis

$$T_{p,1} f_j = f_j + \sum_{i=1}^{h} N_{ij}(\Lambda; p, 1) f_i.$$

This operator is well defined because $N_{ij}(\Lambda; p, 1)$ is well defined in all cases; see [Tor05, Theorem 3.5].

Sometimes it will be convenient to use the dual basis of $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$, such that $e_j = (1/\#\,\mathrm{O}(\Lambda_i)) f_j$. We define the theta series map as the linear map

$$\Theta : \mathcal{M}(\mathrm{O}(\hat{\Lambda})) \to M_{5/2}(4D),$$

given in the dual basis by

$$\Theta(e_i) = \Theta(\Lambda_i) = \sum_{v \in \Lambda_i} q^{Q(v)}.$$

2. Orthogonal modular forms for O(5)

We consider now positive definite $\mathbb{Q}$-quadratic spaces (V, Q) with $\dim V = 5$. In 2014 Hein, Ladd, and Tornaría conjectured that, if $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ is a Hecke-eigenform, with $\mathrm{disc}(\Lambda) = p$ a prime, and $\Theta(f) = 0$, then the L-function associated to f is attached to a paramodular form of weight 3 which is not a Gritsenko lift. This can be found in [Hei16, Conjecture 3.5.6]. Also, Hein [Hei16] computed the good Euler factors for primes less than 100 for all the forms with rational eigenvalues for prime levels up to 200, and Ladd [Lad18] computed the good Euler factors for odd primes up to 31 for all the forms with rational eigenvalues for prime levels up to 400.

As $\dim V = 5$ we only have p^k-neighbors for $k = 1, 2$. Given $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ a Hecke-eigenform and p prime, let $\lambda_{p,1}$ and $\lambda_{p,2}$ be the eigenvalues of $T_{p,1}$ and $T_{p,2}$ for f. We define its (spin) L-function by the Euler product

$$L(f, s) := \prod_{p \text{ prime}} L_p(f, p^{-s})^{-1},$$

where the local Euler factors are given by

$$L_p(f, X) := 1 - \lambda_{p,1} X + (\lambda_{p,2} + 1 + p^2) p X^2 - \lambda_{p,1} p^3 X^3 + p^6 X^4, \quad \text{if } p \nmid D. \tag{6}$$

This is obtained by considering the Satake polynomial on SO(5), found in Murphy [Mur13, page 76], with a suitable change of variable. And

$$L_p(f, X) := (1 + \epsilon_p p X)(1 - (\lambda_{p,1} + \epsilon_p p) X + p^3 X^2), \quad \text{if } p \parallel D, \tag{7}$$

where the local root number $\epsilon_p = c(V_p)$. Here $c(V_p)$ is the Witt invariant of V at p as defined by Lam in [Lam05, page 117]. Note that for $\dim V = 5$ it coincides for all odd p with the Hasse invariant as defined in Cassels [Cas78, Chapter 4], but is the opposite for $p = 2$ (see [Lam05, Proposition 3.20]). The last polynomial is similar to the one found in [Ibu07, Theorem 4.1]. We define it this way, along $T_{p,1}$ for $p \parallel D$ so that the analogue formula for L_p in the next section, in which we use a nontrivial one dimensional representation, is symmetrical to this one.

When D is square-free it is conjectured that the L-functions satisfy the functional equation

$$\tilde{L}(f, s) = \tilde{L}(f, 4 - s),$$

where

$$\tilde{L}(f, s) = \left(\frac{D}{\pi^2}\right)^{s/2} \Gamma\left(\frac{s-1}{2}\right) \Gamma\left(\frac{s}{2}\right)^2 \Gamma\left(\frac{s+1}{2}\right) L(f, s). \tag{8}$$

Example 9 ($D = 61$). Let the quadratic space $V = \mathbb{Q}^5$, and $Q = x^2 + xy - xt + y^2 - yt + z^2 + 2w^2 - wt + 3t^2$ a quadratic form of discriminant 61, and let $\Lambda = \mathbb{Z}^5$. This is the first example of prime discriminant in O(5) for which the theta series map on the genus has a nontrivial kernel, of dimension 1. As noted in [Hei16], there exists a Hecke-eigenform $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ such that $\Theta(f) = 0$. Also the L factors of f for 2, 3, 5 match those of the nonlift paramodular form of level 61 as computed by Ash, Gunnels and McConnell in [AGM08, Section 4] (see also Poor and Yuen [PY15, Section 8]).

By the formulas of Ibukiyama [Ibu07] we have

$$\dim S_3(K(61)) = \dim \mathcal{S}(\mathrm{O}(\hat{\Lambda})) = \dim S_4^-(61) + \dim \ker \Theta.$$

Therefore we expect the correspondence from $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ to $S_3(K(61))$ is a bijection.

Example 10 ($D = 55$). We consider the quadratic space $V = \mathbb{Q}^5$, $Q = x^2 + xy + y^2 + z^2 + 2t^2 + yw + zw + tw + 3w^2$, and $\Lambda = \Lambda_1 = \mathbb{Z}^5$. The Hasse invariant of the genus at 5 is $+1$, and at 11 is -1. There are 3 other $\mathbb{Z}$-lattices in the genus of Λ, namely Λ_2, Λ_3, Λ_4. The quadratic forms associated to the bases of Λ_i, for $i = 2, 3, 4$, are

$$Q_2 = x^2 + xy + y^2 + xz + z^2 + 3t^2 + zw + 2tw + 3w^2,$$
$$Q_3 = x^2 + xy + y^2 + xz + z^2 + yt + 3t^2 + zw + 3w^2,$$
$$Q_4 = x^2 + y^2 + 2z^2 + yt + 2zt + 2t^2 + xw + yw + zw + tw + 2w^2.$$

Let $f = 2e_1 - 2e_2 + e_3 - e_4 \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$, which is a Hecke-eigenform, where $\{e_1, e_2, e_3, e_4\}$ is the dual basis of $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$. It is easy to see that $\Theta(f) = 2\Theta(\Lambda_1) - 2\Theta(\Lambda_2) + \Theta(\Lambda_3) - \Theta(\Lambda_4) = 0$. This is because the Sturm bound for the space $M_{5/2}(4 \cdot 55)$ is 90 (note that the Sturm bound of half-integral weight is the same as the integral case; see for example [GK13, Lemma 3.1]), and the first 90 coefficients of $\Theta(f)$ are 0.

By [IK17] we know that $\dim S_3(K(55)) = 3$. On the other hand the space of classical cusp forms of weight 4, level 55 and sign -1 has dimension 3, this can be found in [LMF20]. There are two such forms, one of dimension 1, and one of dimension 2. We conclude that the space $S_3(K(55))$ is spanned by Gritsenko lifts. We verified that f is not a Gritsenko lift by looking at its eigenvalues, and we conclude that the conjecture mentioned is no longer valid when D is not prime.

We computed the eigenvalues of $T_{p,1}$ of f for $p < 300$, also the eigenvalues of $T_{p,2}$ for $p < 50$, and we conclude.

Theorem 11. *For $p < 50$, $p \neq 5, 11$*

$$L_p(f, X) = (1 - pa_pX + p^3X^2)(1 - b_pX + p^3X^2),$$

where a_p is the p-th Fourier coefficient of the Hecke-eigenform of weight 2 and level 11, g_{11}, and b_p is the p-th Fourier coefficient of the Hecke-eigenform of weight 4 and level 5, g_5.

Also, for $p < 300$

$$L_p(f, X) = 1 - (pa_p + b_p)X + O(X^2).$$

The above theorem leads us to conjecture that $L(f, s) = L(g_{11}, s - 1)L(g_5, s)$, so that f should correspond to some Siegel modular form of Yoshida type. By the previous reasoning f cannot correspond to a form in $S_3(K(55))$.

Conjecture 12. *Let $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ be a Hecke-eigenform, with D square-free and $\Theta(f) = 0$. Then f corresponds either to a paramodular form of weight 3 which is not a Gritsenko lift or to a modular form of Yoshida type as in the example above.*

Example 13. ($D = 167$) Let $V = \mathbb{Q}^5$ and

$$Q_{167} = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + tw + 34w^2,$$

a quinary quadratic form with discriminant 167. The genus of $\Lambda = \mathbb{Z}^5$ has 19 isometry classes, so we have that $\dim \mathcal{S}(\mathrm{O}(\hat{\Lambda})) = 18$. On the other hand we have $\dim S_3(K(167)) = 19$, and we see that the correspondence from $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ into $S_3(K(167))$ is not surjective. According to [GPY19, Table 1] this is the first known case of a paramodular newform of weight 3 with sign -1 in the functional equation. See also [AGM10, Table 4].

3. The missing forms

As seen in the previous example, for a prime p, not all forms in $S_3(K(p))$ correspond to forms in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$, with $\mathrm{disc}(\Lambda) = p$. Moreover, the forms in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ have sign $+1$ in their associated L-function. To find the remaining paramodular forms we introduce a representation using the spinor norm. With this representation, we can obtain orthogonal modular forms with sign -1 in their associated L-function. See [HTV20] for a more detailed presentation of this idea in the case of ternary quadratic forms.

If $d \mid D$, we define the character $\nu_d : \mathbb{Q}^{\times}_{>0}/\mathbb{Q}^{\times 2}_{>0} \to \{\pm 1\}$, defined in primes by

$$\nu_d(p) = \begin{cases} -1 & \text{if } p \mid d, \\ 1 & \text{otherwise.} \end{cases}$$

We define the representation $\rho_d : \mathrm{O}(V) \to \{\pm 1\} \subset \mathbb{Q}^{\times} \cong \mathrm{GL}(\mathbb{Q})$ by

$$\rho_d(\sigma) = \nu_d(\theta(\pm\sigma)) \text{ if } \sigma \in \mathrm{O}^{\pm}(V),$$

where $\theta : \mathrm{O}^{+}(V) \to \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$ is the spinor norm. We denote the space of orthogonal modular forms for this representation $\mathcal{M}_d(\mathrm{O}(\hat{\Lambda}))$, and the cuspidal subspace by $\mathcal{S}_d(\mathrm{O}(\hat{\Lambda}))$. In this case

$$\mathcal{M}_d(\mathrm{O}(\hat{\Lambda})) \cong \bigoplus_{i=1}^{h} \mathbb{Q}^{\mathrm{O}(\Lambda_i)},$$

where $\mathbb{Q}^{\mathrm{O}(\Lambda_i)} = \mathbb{Q}$ if and only if $\nu_d(\sigma) = 1$ for all $\sigma \in \mathrm{O}^{+}(\Lambda_i)$.

Let $\{t_1 < \cdots < t_{h_d}\} = \{t : \mathbb{Q}^{\mathrm{O}(\Lambda_t)} = \mathbb{Q}\}$, and $f_{t_j} \in \mathcal{M}_d(\mathrm{O}(\hat{\Lambda}))$ such that $f_{t_j}(\hat{x}_i) = \delta_{t_j i}$, so $\{f_{t_1}, \ldots, f_{t_{h_d}}\}$ is a basis of $\mathcal{M}_d(\mathrm{O}(\hat{\Lambda}))$.

If p is a prime such that Λ is unimodular at p, and $k \geq 1$, by definition of the Hecke operator we have

$$(T_{p,k}\, f_{t_j})(\hat{x}_i) = \sum_m f_{t_j}(\hat{x}_i\, \hat{p}_m) = \sum_m \rho_d(\sigma) f_{t_j}(\hat{x}_{m_*}) = \sum_m \rho_d(\sigma)\delta_{t_j m_*},$$

where $\hat{x}_i\, \hat{p}_m \hat{\Lambda} = \sigma\, \hat{x}_{m_*} \hat{\Lambda}$. Henceforth, to compute $(T_{p,k}\, f_{t_j})(\hat{x}_i)$, we sum $\rho_d(\sigma)$ over $\sigma \in \mathrm{O}(V)$ such that $\sigma \Pi_m = \Lambda_{t_j}$, where the Π_m are the p^k-neighbors of Λ_i, and we define that sum as $N^{d}_{i\, t_j}(\Lambda;\, p, k)$. We get the formula

$$T_{p,k}\, f_{t_j} = \sum_{i=1}^{h_d} N^{d}_{t_i t_j}(\Lambda;\, p, k) f_{t_i}.$$

We define $T_{p,1}$ for $\mathcal{M}_d(\mathrm{O}(\hat{\Lambda}))$ when $p \parallel D$ by

$$T_{p,1}\, f_{t_j} = \nu_d(p)\Big(f_{t_j} + \sum_{s=1}^{h_d} N^d_{t_i t_j}(\Lambda;\, p, 1) f_{t_i}\Big).$$

Given a Hecke-eigenform $f \in \mathcal{S}_d(\mathrm{O}(\hat{\Lambda}))$ we want to define its (spin) L-function. As before, we define it by the Euler product

$$L(f, s) = \prod_p L_p(f, p^{-s})^{-1}$$

where L_p is defined with the same equation as (6), if $p \nmid D$. When $p \parallel D$ we use (7), where the local root number is $\epsilon_p = \nu_d(p)\, c(V_p)$. When D is square-free we conjecture that the L-function satisfy the functional equation

$$\tilde{L}(f, s) = \nu_d(D)\, \tilde{L}(f, 4-s),$$

where $\tilde{L}$ is defined as (8).

Example 13 ($D = 167$, continued). For $d = p$ we have $\dim \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda})) = 1$, and

$$\dim S_3(K(167)) = \dim \mathcal{S}(\mathrm{O}(\hat{\Lambda})) + \dim \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda})).$$

Let $f \in \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda}))$, $f \neq 0$. It is a Hecke-eigenform because the dimension of the space is 1. In Table 1 we show the Hecke-eigenvalues of $T_{p,1}$ for f with $p < 500$. And in Table 2 the Hecke-eigenvalues of $T_{p,2}$ for f with $p < 50$. With the previous data we constructed an L-function in PARI/GP [PAR18] using the routine `lfuncreate` providing the first 502 Dirichlet coefficients, and verified by the `lfuncheckfeq` routine, returning a verification accuracy of 90 bits of precision.

3.1. ***A conjecture for prime level.*** Let p prime, and Λ_p be a lattice in the unique genus of quinary quadratic forms of discriminant p. We verified computationally the following theorem.

Theorem 14. *For* $p < 7000$

$$\dim S_3(K(p)) = \dim \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p)) + \dim \mathcal{S}_p(\mathrm{O}(\hat{\Lambda}_p)).$$

Which leads us to the following conjecture.

Conjecture 15. *For prime p there is a Hecke-equivariant isomorphism*

$$S_3(K(p)) \cong \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p)) \oplus \mathcal{S}_p(\mathrm{O}(\hat{\Lambda}_p)).$$

Also, $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p))$ correspond to the forms of $S_3(K(p))$ such that their associated L-function has sign $+1$ in its functional equation, and $\mathcal{S}_p(\mathrm{O}(\hat{\Lambda}_p))$ correspond to the forms such that their associated L-function has sign -1 in its functional equation.

p	$\lambda_{p,1}$	p	$\lambda_{p,1}$	p	$\lambda_{p,1}$	p	$\lambda_{p,1}$	p	$\lambda_{p,1}$
2	−8	71	−481	167	−2707	271	2954	389	5316
3	−10	73	−744	173	−182	277	−8334	397	4324
5	−4	79	927	179	2568	281	−2942	401	−4679
7	−14	83	−632	181	−2804	283	6360	409	−3476
11	−22	89	−297	191	−3035	293	−856	419	−910
13	−4	97	2	193	583	307	3548	421	3552
17	−47	101	−992	197	2276	311	−6322	431	−4878
19	−12	103	−1222	199	6754	313	−9443	433	15213
23	41	107	1436	211	360	317	108	439	−6909
29	50	109	−954	223	3569	331	1596	443	−7130
31	−504	113	19	227	−3346	337	−2129	449	12908
37	−102	127	516	229	2220	347	1856	457	−4005
41	174	131	−258	233	−2780	349	480	461	−7334
43	30	137	1080	239	−3878	353	1704	463	−77
47	42	139	1030	241	−819	359	4601	467	12248
53	156	149	−974	251	6112	367	6298	479	6447
59	−252	151	−1119	257	−5343	373	−4998	487	−14197
61	472	157	1152	263	−808	379	7706	491	1960
67	106	163	108	269	3592	383	−18293	499	3288

Table 1. Hecke-eigenvalues of $T_{p,1}$ for $f \in \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda}))$, $p < 500$.

4. Composite levels

When D is composite, as already seen in Example 10, the space of orthogonal modular forms includes Yoshida lifts, which do not correspond to paramodular forms.

In this section we investigate orthogonal modular forms for $D = 305 = 5 \cdot 61$. We have two genera of quintic positive definite quadratic forms, namely, let Λ_1 and Λ_2 be lattices of dimension 5 such that $\operatorname{disc}(\Lambda_i) = 5 \cdot 61$ and

$$\begin{matrix} \epsilon_5(\Lambda_1) = -1 \\ \epsilon_{61}(\Lambda_1) = +1 \end{matrix}, \qquad \begin{matrix} \epsilon_5(\Lambda_2) = +1 \\ \epsilon_{61}(\Lambda_2) = -1 \end{matrix}.$$

We computed $\mathcal{S}_d(\mathrm{O}(\hat{\Lambda}_i))$, for $d \in \{1, 5, 61, 5 \cdot 61\}$, $i = 1, 2$, as well as $T_{p,1}$ and $T_{p,2}$ for p prime $p < 20$, with the convention that

$$\mathcal{S}_1(\mathrm{O}(\hat{\Lambda}_i)) := \mathcal{S}(\mathrm{O}(\hat{\Lambda}_i)).$$

p	$\lambda_{p,2}$	p	$\lambda_{p,2}$	p	$\lambda_{p,2}$	p	$\lambda_{p,2}$	p	$\lambda_{p,2}$
2	10	7	−9	17	260	29	−187	41	800
3	11	11	−67	19	41	31	2744	43	442
5	−44	13	−158	23	−198	37	−730	47	−5052

Table 2. Hecke-eigenvalues of $T_{p,2}$ for $f \in \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda}))$, $p < 50$.

		A-L				Traces				
		ϵ_5	ϵ_{61}	Dim	$\subset \ker\Theta$	$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$
$\mathcal{S}_1(\mathrm{O}(\hat\Lambda_1))$	A_1	$-$	$+$	8	Yes	1	-21	12	-28	-10
	A_2	$-$	$+$	9	No	57	119	69	505	1338
	A_3	$-$	$+$	13	No	73	129	455	647	1660
$\mathcal{S}_{61}(\mathrm{O}(\hat\Lambda_1))$	B_1	$-$	$-$	1		-4	-12	-4	9	-13
$\mathcal{S}_{5\cdot 61}(\mathrm{O}(\hat\Lambda_1))$	C_1	$+$	$-$	1		-2	2	-2	-19	21
	C_2	$+$	$-$	1		2	-6	10	-3	29
	C_3	$+$	$-$	8		3	-27	-6	-58	-54
	C_4	$+$	$-$	13		81	157	325	669	1652
$\mathcal{S}_1(\mathrm{O}(\hat\Lambda_2))$	D_1	$+$	$-$	1	No	2	14	25	62	164
	D_2	$+$	$-$	1	Yes	-7	-3	28	-9	-4
	D_3	$+$	$-$	1	Yes	-2	2	-2	-19	21
	D_4	$+$	$-$	1	Yes	2	-6	10	-3	29
	D_5	$+$	$-$	3	Yes	-10	12	-20	-3	239
	D_6	$+$	$-$	6	No	29	59	314	309	612
	D_7	$+$	$-$	8	Yes	3	-27	-6	-58	-54
	D_8	$+$	$-$	13	No	81	157	325	669	1652
$\mathcal{S}_5(\mathrm{O}(\hat\Lambda_2))$	E_1	$-$	$-$	1		-7	-3	-22	-9	-4
	E_2	$-$	$-$	1		-4	-12	-4	9	-13
$\mathcal{S}_{61}(\mathrm{O}(\hat\Lambda_2))$	F_1	$+$	$+$	1		-6	-4	-20	13	-23
$\mathcal{S}_{5\cdot 61}(\mathrm{O}(\hat\Lambda_2))$	G_1	$-$	$+$	8		1	-21	12	-28	-10
	G_2	$-$	$+$	13		73	129	455	647	1660

Table 3. Decomposition of $\mathcal{S}_d(\mathrm{O}(\hat\Lambda_i))$, with $\mathrm{disc}(\Lambda_i) = 5\cdot 61$.

The decomposition of these spaces is shown in Table 3. We show the dimensions of the subspaces, the local root numbers, for $d = 1$ whether they are in the kernel of the theta map, and the traces of the eigenvalues $\lambda_{p,1}$ for $p \le 11$.

The subspaces A_2 and D_1 correspond to the classical modular forms of weight 4 and sign $+$ of levels 61 and 5 respectively (`61.4.a.b` and `5.4.a.a` in [LMF20]). By this we mean that $\lambda_{p,1} = a_p + p + p^2$ where a_p is the eigenvalue of the classical modular form, just as for Gritsenko lifts, but since the sign is $+$ they do not lift to $S_3(K(D))$.

The subspaces D_5 and F_1 are of Yoshida type as in Example 10 (D_5 corresponds to the pair `61.2.a.b` and `5.4.a.a` , and F_1 corresponds to the pair `61.2.a.a` and `5.4.a.a`). By [Sch18] they also do not lift to $S_3(K(D))$.

The subspaces A_3, C_4, D_6, D_8 and G_2 correspond to classical modular forms of weight 4 and sign $-$ of level 61 (for D_6) and 305 (for the other four), so they appear as Gritsenko lifts in $S_3(K(D))$. Also A_3 and G_2, C_4 and D_8 lift from the same space.

The subspaces D_2 and E_1 come from the nonlift orthogonal modular form in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{61}))$ (see Example 9). The subspace D_2 has sign $-$, and E_1 has sign $+$, and the eigenvalues $\lambda_{5,1}$ are different, and they have the same eigenvalues otherwise. The subspaces A_1, B_1, C_1, C_2, C_3, D_3, D_4, D_7, E_2 and G_1 are nonlifts. Also, we conjecture that A_1 and G_1, B_1 and E_2, C_1 and D_3, C_2 and D_4, and C_3 and D_7 are isomorphic as Hecke-modules.

By the formulas found in [IK17] $\dim S_3(5 \cdot 61) = 53$. By counting dimensions and the previous descriptions, we conjecture

$$S_3(K(5 \cdot 61)) \cong A_1 \oplus B_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus D_2 \oplus E_1 \oplus A_3 \oplus C_4 \oplus D_6$$

We expect that, for square-free D, the space $S_3(K(D))$ is always spanned, as Hecke module, by orthogonal modular forms corresponding to quinary lattices of discriminant D as in this example, which would give a nice algorithm to compute (the eigenvalues of) all paramodular forms of square-free level.

5. Paramodular forms of higher dimension

Prompted by a question of Eran Assaf we consider the proper standard representation of O(5)

$$\begin{aligned} \mathrm{std}^+ : \mathrm{O}(V) &\to \mathrm{GL}(V) \\ \sigma &\mapsto \det(\sigma)\sigma \end{aligned}$$

If $\mathrm{disc}(V) = p$, for a prime p, we also consider the representation $\mathrm{std}_p^+ := \mathrm{std}^+ \otimes \rho_p$. We computed the dimensions of $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}_p^+)$ and $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+)$, for primes $p < 100$, as seen in Table 4. We can see that

$$\dim S_4(K(p)) = \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}_p^+) + \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+).$$

As before we have the Gritenko lift from $S_6^-(p)$ to $S_4(K(p))$. We note that the first prime such that the difference of the dimensions of the mentioned spaces is 1 is $p = 31$. We conjecture that there is an eigenform in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{31}), \mathrm{std}_{31}^+)$ corresponding to a nonlift paramodular form in $S_4(K(31))$, with sign $+$ in the functional equation of its spin L-function.

We also note that the first p where $\dim \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+) > 0$ is 83. We conjecture that the eigenform in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{83}), \mathrm{std}^+)$ correspond to a nonlift paramodular form in $S_4(K(83))$, with sign $-$ in the functional equation of its spin L-function.

In future work we plan to compute the decomposition of these spaces for weights higher than 4.

6. Hypergeometric motives

Hypergeometric motives with Hodge vector (1, 1, 1, 1) are geometric objects which are (conjecturally) expected to correspond to Siegel modular forms of weight 3. For an introduction to hypergeometric motives see [Rob15]. David Roberts (personal communication, 2018) has computed a list of some such hypergeometric motives with conductors at most 400. David Yuen and Chris Poor have found matching

p	2	3	5	7	11	13	17	19	23	29	31	37
$\dim(\mathcal{S}(\hat{\Lambda}_p), \mathrm{std}_p^+)$	0	0	0	1	1	2	2	3	3	3	6	8
$\dim(\mathcal{S}(\hat{\Lambda}_p), \mathrm{std}^+)$	0	0	0	0	0	0	0	0	0	0	0	0
$\dim S_4(K(p))$	0	0	0	1	1	2	2	3	3	3	6	8
$\dim S_6^-(p)$	0	0	0	1	1	2	2	3	3	3	5	7
p	43	47	53	59	61	67	71	73	79	83	89	97
$\dim(\mathcal{S}(\hat{\Lambda}_p), \mathrm{std}_p^+)$	9	8	10	11	16	17	15	21	22	18	23	32
$\dim(\mathcal{S}(\hat{\Lambda}_p), \mathrm{std}^+)$	0	0	0	0	0	0	0	0	0	1	0	0
$\dim S_4(K(p))$	9	8	10	11	16	17	15	21	22	19	23	32
$\dim S_6^-(p)$	8	7	9	9	11	13	11	14	14	14	15	19

Table 4. Dimensions of spaces of orthogonal modular forms for std_p^+ and std^+, paramodular forms $S_4(K(p))$ and modular forms $S_6^-(p)$ for $p < 100$

Siegel modular forms for four cases with square-free conductor: 182, 205, 255, and 257. Also, Ladd [Lad18, page 24] found an orthogonal modular form such that the odd Euler factors of its L-function coincides with the Euler factors of the L-series of the hypergeometric motive of conductor 257.

The remaining four cases provided by Roberts have not square-free conductors 128, 378, 384 and 256. For the first three we have found Hecke-eigenvectors f in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$, such that the first 50 coefficients of the L-function of f coincide with the coefficients of the L-function of H. The coefficients of the L-function of H were computed using MAGMA [BCP97] as in [Rob15]. For the local Euler factors with $p^2 \mid \mathrm{disc}(Q)$ we used the one given by the L-function of the hypergeometric motive.

(1) For the hypergeometric motive H of conductor 128, with data $A = [2, 2, 8]$, $B = [1, 1, 4, 4]$, $t = 1$, and $L_2(x) = 1 + 2x + 8x^2$. The quadratic space is $\mathbb{Q}^5$ with

$$Q = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + zw + 26w^2, \quad \mathrm{disc}(Q) = 128 = 2^7, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

(2) For the hypergeometric motive H of conductor 378, with data $A = [3, 2, 2]$, $B = [1, 1, 6]$, $t = 64$, and $L_3 = 1 + 3x$. The quadratic space is $\mathbb{Q}^5$ with

$$Q = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + zw + 76w^2, \quad \mathrm{disc}(Q) = 378 = 2 \cdot 3^3 \cdot 7, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

(3) For the hypergeometric motive H of conductor 384, with data $A = [2, 2, 2, 2]$ $B = [1, 1, 1, 1]$, $t = 1/4$, and $L_2 = 1$. The quadratic space is $\mathbb{Q}^5$ with

$$Q = x^2 + xy + y^2 + xz + 2z^2 + xt + 2t^2 + 12w^2, \quad \mathrm{disc}(Q) = 384 = 2^7 \cdot 3, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

We have not been able to find matching Hecke-eigenvectors in $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ for the hypergeometric motive of conductor 256, with data

$$A = [2, 2, 2, 2, 4], \quad B = [1, 1, 8], \quad t = 1, \quad \text{and} \quad L_2 = 1 - 2x.$$

The Euler factors for this motive can be computed from the given data using MAGMA:

```
> R<x> := PolynomialRing(Integers());
> L:=LSeries(HypergeometricData([2, 2, 2, 2, 4], [1, 1, 8]), 1:
> BadPrimes:=[<2, 8,1-2*x>]);
> EulerFactor(L, 3);
729*x^4 - 54*x^3 - 2*x^2 - 2*x + 1
```

As a reference, the first Euler factors are

$$L_2 = 1 - 2x,$$
$$L_3 = 1 - 2x - 2x^2 - 54x^3 + 729x^4,$$
$$L_5 = 1 + 12x + 142x^2 + 1500x^3 + 15625x^4.$$

7. Algorithms

To carry out the computations mentioned throughout the article we relied on [Hei16], and Greenberg and Voight [GV14]. Hein gives a very detailed description to compute spaces of orthogonal modular forms over totally real number fields, as well as their Hecke-operators for good primes.

We implemented the algorithms to compute $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ and $\mathcal{M}_d(\mathrm{O}(\hat{\Lambda}))$, as well as $T_{p,k}$ for $k = 1, 2$, in Sage [Sag19]. One of the most important parts of the algorithm to compute $T_{p,k}$ relies on isomorphism testing of quadratic forms, for which Sage uses PARI [PAR18], which implements an algorithm of Plesken and Souvignier [PS97]. To compute the representation given in Section 3, we implemented a function to compute the spinor norm based in Example 8 in [Cas78, page 30]. Cassels give an algorithm to decompose an autometry A of a positive definite quadratic space V of dimension n as a product of at most n transpositions τ_{v_i}, $v_i \in V$. The spinor norm is computed as the product of the norm of v_i modulo squares. In our case, any proper autometry is a product of at most 4 transpositions. The implemented code can be found in [Ram20].

To do the computations of Theorem 14, we did a random search of quinary positive definite quadratic forms of prime discriminant. For each prime $p < 7000$ we found a representative of the unique genus of discriminant p. To find the matches of hypergeometric motives of Section 6, we used tables of Nipp of reduced regular primitive positive-definite quinary quadratic forms over $\mathbb{Z}$ [Nip].

8. Tables

In Tables 5 and 6 we show the orthogonal modular forms from $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p))$, $\mathcal{S}_p(\mathrm{O}(\hat{\Lambda}_p))$ for $p < 300$ that are not Gritsenko lifts. These tables can be found in [RT20], as well as for squarefree $D < 1000$. We include the dimension and the traces of $\lambda_{p,1}$ for $p \leq 13$ and $\lambda_{p,2}$ for $p \leq 5$. The rational ones for $d = 1$ and $p < 200$ were first computed by Hein [Hei16], and for $p < 400$ by Ladd [Lad18].

p	d	label	dim	$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$	$\lambda_{13,1}$	$\lambda_{2,2}$	$\lambda_{3,2}$	$\lambda_{5,2}$
61	1	61*a*	1	−7	−3	3	−9	−4	−3	7	−9	−9
73	1	73*a*	1	−6	−2	0	7	−66	16	6	−9	0
79	1	79*a*	1	−5	−5	3	15	26	−15	2	4	−10
89	1	89*a*	1	−4	−6	16	−17	−2	−46	2	−6	27
97	1	97*a*	2	−9	−4	−4	16	−64	24	6	−14	4
101	1	101*a*	2	−7	−11	22	−32	46	−54	2	0	−21
103	1	103*a*	2	−9	−2	−15	26	−9	29	5	−10	−30
109	1	109*a*	3	−10	−15	−7	37	27	20	−3	7	−20
113	1	113*a*	1	−3	−4	8	4	−4	−40	2	−4	−4
127	1	127*a*	3	−9	−9	−12	45	18	69	0	6	−12
131	1	131*a*	2	−6	−4	8	−10	64	−84	4	−8	−4
137	1	137*a*	2	−4	−10	12	0	16	−8	0	8	12
139	1	139*a*	4	−14	−4	−22	14	−6	76	4	−10	−26
149	1	149*a*	4	−6	−23	16	−17	77	−9	−6	12	−15
151	1	151*a*	5	−12	−17	−33	57	81	75	−9	12	−28
157	1	157*a*	2	6	2	−14	8	−36	46	2	−22	−12
	1	157*b*	5	−15	−12	0	−11	9	217	3	16	−78
163	1	163*a*	4	−10	−4	−16	38	4	84	2	−8	−12
167	167	167*a*	1	−8	−10	−4	−14	−22	−4	10	11	−44
	1	167*b*	1	−2	0	−2	2	−14	−34	2	−17	16
	1	167*c*	2	−3	−9	2	3	92	−41	−3	12	−28
173	173	173*a*	1	−8	−9	−10	−4	−4	−72	10	7	−3
	1	173*b*	1	−2	−1	0	−16	−24	2	0	−23	−9
	1	173*c*	4	−7	−15	14	−27	92	43	−2	22	−90
179	1	179*a*	4	−6	−10	−6	2	134	−134	−2	−8	−32
181	1	181*a*	10	−27	−16	−14	−38	59	249	0	−24	−91
191	1	191*a*	2	−3	−6	−7	−23	93	−19	−5	12	−10
	1	191*b*	4	−6	−10	8	10	126	−136	2	−12	−52
193	1	193*a*	10	−15	−26	−38	56	−78	200	−11	−2	26
197	197	197*a*	1	−7	−10	−8	5	2	−66	7	14	−2
	1	197*b*	1	1	−8	9	23	−12	−38	1	6	−24
	1	197*c*	2	−4	−4	0	−20	78	−10	−4	−6	−42
	1	197*d*	3	−2	−13	0	−19	25	101	−5	14	−6
199	1	199*a*	10	−27	−8	−43	41	33	170	1	−22	−120

Table 5. Forms in $\mathcal{S}_d(\mathrm{O}(\hat{\Lambda}_p))$ for $d = 1$, p and $p < 200$.

p	d	label	dim	$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$	$\lambda_{13,1}$	$\lambda_{2,2}$	$\lambda_{3,2}$	$\lambda_{5,2}$
211	1	211*a*	10	−18	−16	−48	38	24	118	−12	−8	16
223	223	223*a*	1	−6	−11	6	−28	8	−42	6	13	−33
	1	223*b*	1	−2	1	−8	−6	−30	36	−2	−17	5
	1	223*c*	10	−22	−4	−47	72	40	175	2	−6	−74
227	227	227*a*	2	−13	−18	−14	−22	−56	−15	13	12	16
	1	227*b*	6	−7	−8	−6	−14	92	−85	−3	−12	−46
229	1	229*a*	1	−2	−1	−9	−2	−13	24	−5	−12	−18
	1	229*b*	1	0	−5	17	−40	57	10	−1	−4	30
	1	229*c*	14	−33	−18	−17	7	−64	316	2	−20	−136
233	233	233*a*	1	−6	−10	−7	4	−22	−40	5	10	22
	1	233*b*	1	0	−2	8	−6	−38	32	2	−14	−6
	1	233*c*	4	−4	−12	−4	−28	24	−96	0	0	−8
	1	233*d*	5	−2	−16	−9	−10	72	76	−6	14	−18
239	239	239*a*	1	−6	−9	−8	10	−49	7	6	13	−13
	1	239*b*	10	−5	−30	−14	−9	266	−164	−14	1	−75
241	1	241*a*	18	−31	−32	−38	−14	−146	302	−14	−54	−88
251	251	251*a*	1	−6	−8	−11	6	−63	2	6	3	−15
	1	251*b*	1	−2	−2	9	−20	39	18	−4	3	17
	1	251*c*	10	−14	−4	−4	−36	222	−202	6	−28	−62
257	1	257*a*	1	−1	0	−4	−8	24	12	−2	−8	−52
	257	257*b*	2	−13	−13	−26	−16	−9	−51	14	0	18
	1	257*c*	12	−13	−23	24	−82	1	−23	−5	−28	−6
263	263	263*a*	2	−11	−20	−15	−3	−10	−23	7	26	−2
	1	263*b*	11	−7	−25	−8	−10	206	−78	−10	6	−14
269	269	269*a*	1	−7	−4	−20	−4	4	49	8	0	23
	269	269*b*	1	−5	−10	−8	20	−60	−75	4	12	−25
	1	269*c*	1	−1	2	−1	8	21	30	1	6	−10
	1	269*d*	15	−20	−28	67	−145	114	14	−3	−52	−77
271	271	271*a*	1	−5	−10	2	−10	−27	−25	5	13	−25
	1	271*b*	19	−35	−19	−70	81	−20	245	−13	−25	−83
277	277	277*a*	1	−5	−10	−1	−10	38	−94	4	13	0
	1	277*b*	22	−25	−35	−44	48	−104	438	−19	−7	−56
281	281	281*a*	1	−6	−6	−16	6	−26	14	6	2	29
	1	281*b*	18	−4	−50	8	−116	142	−96	−23	−20	−42
283	283	283*a*	1	−6	−6	−6	−29	15	−47	7	−4	−24
	283	283*b*	1	−4	−14	8	−17	−15	−33	1	22	8
	1	283*c*	1	−2	−2	6	−7	−11	33	−5	0	−24
	1	283*d*	17	−26	2	−74	85	−95	213	1	−36	−82
293	293	293*a*	4	−24	−27	−57	−14	−7	−94	21	13	36
	1	293*b*	17	−13	−36	49	−117	37	99	−14	−11	−80

Table 6. Forms in $\mathcal{S}_d(\mathrm{O}(\hat{\Lambda}_p))$ for $d = 1$, p and $200 < p < 300$.

References

[AGM08] Avner Ash, Paul Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of* $\mathrm{SL}(4,\mathbb{Z})$*. II*, J. Number Theory **128** (2008), no. 8, 2263–2274. MR 2394820

[AGM10] Avner Ash, Paul Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of* $\mathrm{SL}_4(\mathbb{Z})$*. III*, Math. Comp. **79** (2010), no. 271, 1811–1831. MR 2630015

[BCGP18] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian surfaces over totally real fields are potentially modular*, preprint, 2018. arXiv 1812.09269

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[Bir91] Bryan John Birch, *Hecke actions on classes of ternary quadratic forms*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 191–212. MR 1151865

[BK75] Bryan John Birch and Willem Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin-New York, 1975. MR 0376533

[BK14] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366** (2014), no. 5, 2463–2516. MR 3165645

[BK17] Tobias Berger and Krzysztof Klosin, *Deformations of Saito-Kurokawa type and the paramodular conjecture*, preprint, 2017, With an appendix by Cris Poor, Jerry Shurman, and David S. Yuen. arXiv 1710.10228

[BK19] Armand Brumer and Kenneth Kramer, *Corrigendum to "Paramodular abelian varieties of odd conductor"*, Trans. Amer. Math. Soc. **372** (2019), no. 3, 2251–2254. MR 3976591

[BPP+19] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen, *On the paramodularity of typical abelian surfaces*, Algebra Number Theory **13** (2019), no. 5, 1145–1195. MR 3981316

[Cas78] John William Scott Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR 522835

[CCG19] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza, *Some modular abelian surfaces*. arXiv 1906.10939

[Cre97] John Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR 1628193

[Cre19] John Cremona, *ecdata: 2019-10-29*, October 2019, http://doi.org/10.5281/zenodo.3522235.

[GK13] Sanoli Gun and Narasimha Kumar, *A note on Fourier-Jacobi coefficients of Siegel modular forms*, Arch. Math. (Basel) **101** (2013), no. 6, 519–524. MR 3133725

[GPY19] Valery Gritsenko, Cris Poor, and David S Yuen, *Antisymmetric paramodular forms of weights 2 and 3*, International Mathematics Research Notices (2019).

[GV14] Matthew Greenberg and John Voight, *Lattice methods for algebraic modular forms on classical groups*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, pp. 147–179. MR 3381452

[Hei16] Jeffery Hein, *Orthogonal modular forms: An application to a conjecture of Birch, algorithms and computations*, Ph.D. thesis, Dartmouth College, 2016. MR 3553638

[HTV20] Jeffery Hein, Gonzalo Tornaría, and John Voight, *Hilbert modular forms as orthogonal modular forms*, preprint (2020).

[Ibu07] Tomoyoshi Ibukiyama, *Paramodular forms and compact twist*, Automorphic Forms on GSp(4), Proceedings of the 9th Autumn Workshop on Number Theory, (ed. M. Furusawa), 2007, pp. 37–48.

[IK17] Tomoyoshi Ibukiyama and Hidetaka Kitayama, *Dimension formulas of paramodular forms of squarefree level and comparison with inner twist*, J. Math. Soc. Japan **69** (2017), no. 2, 597–671. MR 3638279

[Koh01] David R. Kohel, *Hecke module structure of quaternions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 177–195. MR 1846458

[Lad18] Watson Bernard Ladd, *Algebraic modular forms on* $\mathrm{so}_5(\mathbb{Q})$ *and the computation of paramodular forms*, Ph.D. thesis, University of California, Berkeley, 2018.

[Lam05] Thomas Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. MR 2104929

[LMF20] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2020, [Online; accessed 10 February 2020].

[Mur13] Daniel Kim Murphy, *Algebraic modular forms on definite orthogonal groups*, Ph.D. thesis, Stanford University, 2013.

[Nip] Gordon L. Nipp, *Tables of quinary quadratic forms*, http://www.math.rwth-aachen.de/ Gabriele.Nebe/LATTICES /nipp5.html.

[PAR18] The PARI Group, Univ. Bordeaux, *Pari/gp version* `2.11.0`, 2018, http://pari.math.u-bordeaux.fr/.

[Piz80] Arnold Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), no. 2, 340–390. MR 579066

[PS97] Wilhelm Plesken and Bernd Souvignier, *Computing isometries of lattices*, vol. 24, 1997, Computational algebra and number theory (London, 1993), pp. 327–334. MR 1484483

[PSY17] Cris Poor, Jerry Shurman, and David S. Yuen, *Siegel paramodular forms of weight 2 and squarefree level*, Int. J. Number Theory **13** (2017), no. 10, 2627–2652. MR 3713095

[PY15] Cris Poor and David S. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438. MR 3315514

[Ram14] Gustavo Rama, *Módulo de Brandt generalizado*, M.Sc., Universidad de la República, 2014.

[Ram20] Gustavo Rama, *Quinary orthogonal modular forms code repository*, preprint, 2020.

[Rob15] David P. Roberts, *Hypergeometric motives I*, lecture notes, 2015.

[RT20] Gustavo Rama and Gonzalo Tornaría, *Quinary orthogonal modular forms*, preprint, 2020.

[Sag19] *Sagemath, the Sage Mathematics Software System (Version 8.7)*, 2019, https://www.sagemath.org.

[Sch18] Ralf Schmidt, *Packet structure and paramodular forms*, Trans. Amer. Math. Soc. **370** (2018), no. 5, 3085–3112. MR 3766842

[Ste12] William Stein, *The Modular Forms Database*, 2012, http://wstein.org/Tables.

[Tor05] Gonzalo Tornaría, *The Brandt module of ternary quadratic lattices*, Ph.D. thesis, The University of Texas at Austin, 2005. MR 2717378

[Wad71] Hideo Wada, *Tables of Hecke operations. I*, Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 39, 1971, p. 10. MR 0379377

Received 28 Feb 2020.

GUSTAVO RAMA: `grama@fing.edu.uy`
Facultad de Ingeniería, Universidad de La República, Montevideo, Uruguay

GONZALO TORNARÍA: `tornaria@cmat.edu.uy`
Centro de Matemática, Universidad de la República, Montevideo, Uruguay

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS

798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840

contact@msp.org http://msp.org

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS

Commitment schemes and diophantine equations — José Felipe Voloch 1

Supersingular curves with small noninteger endomorphisms — Jonathan Love and Dan Boneh 7

Cubic post-critically finite polynomials defined over $\mathbb{Q}$ — Jacqueline Anderson, Michelle Manes and Bella Tobin 23

Faster computation of isogenies of large prime degree — Daniel J. Bernstein, Luca De Feo, Antonin Leroux and Benjamin Smith 39

On the security of the multivariate ring learning with errors problem — Carl Bootland, Wouter Castryck and Frederik Vercauteren 57

Two-cover descent on plane quartics with rational bitangents — Nils Bruin and Daniel Lewis 73

Abelian surfaces with fixed 3-torsion — Frank Calegari, Shiva Chidambaram and David P. Roberts 91

Lifting low-gonal curves for use in Tuitman's algorithm — Wouter Castryck and Floris Vermeulen 109

Simultaneous diagonalization of incomplete matrices and applications — Jean-Sébastien Coron, Luca Notarnicola and Gabor Wiese 127

Hypergeometric L-functions in average polynomial time — Edgar Costa, Kiran S. Kedlaya and David Roe 143

Genus 3 hyperelliptic curves with CM via Shimura reciprocity — Bogdan Adrian Dina and Sorina Ionica 161

A canonical form for positive definite matrices — Mathieu Dutour Sikirić, Anna Haensch, John Voight and Wessel P.J. van Woerden 179

Computing Igusa's local zeta function of univariates in deterministic polynomial-time — Ashish Dwivedi and Nitin Saxena 197

Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs — Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison and Jennifer Park 215

New rank records for elliptic curves having rational torsion — Noam D. Elkies and Zev Klagsbrun 233

The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP — Thomas Espitau and Paul Kirchner 251

Cryptanalysis of the generalised Legendre pseudorandom function — Novak Kaluđerović, Thorsten Kleinjung and Dušan Kostić 267

Counting Richelot isogenies between superspecial abelian surfaces — Toshiyuki Katsura and Katsuyuki Takashima 283

Algorithms to enumerate superspecial Howe curves of genus 4 — Momonari Kudo, Shushi Harashita and Everett W. Howe 301

Divisor class group arithmetic on $C_{3,4}$ curves — Evan MacNeil, Michael J. Jacobson Jr. and Renate Scheidler 317

Reductions between short vector problems and simultaneous approximation — Daniel E. Martin 335

Computation of paramodular forms — Gustavo Rama and Gonzalo Tornaría 353

An algorithm and estimates for the Erdős–Selfridge function — Brianna Sorenson, Jonathan Sorenson and Jonathan Webster 371

Totally p-adic numbers of degree 3 — Emerald Stacy 387

Counting points on superelliptic curves in average polynomial time — Andrew V. Sutherland 403