VARIANTS OF RECOGNITION PROBLEMS FOR MODULAR FORMS

E. KOWALSKI

ABSTRACT. We consider the problem of distinguishing two modular forms, or two elliptic curves, by looking at the coefficients of their L-functions for small primes (compared to their conductor). Using analytic methods based on large-sieve type inequalities we give various upper bounds on the number of forms having the first few coefficients equal to those of a fixed one. In addition, we consider similar questions of "recognizing" symmetric squares and CM forms from the behavior of small primes.

1. INTRODUCTION

This paper is an addition to [DK], together with some variations on the problem considered there. It was motivated by discussions with F. Brumley who recently approached this question using a very nice method based on density theorems for zeros of L-functions.

Recall the setting, which generalizes the classical question of the least quadratic non-residue modulo a prime p: given two primitive holomorphic cusp forms f, g of the same weight $k \geqslant 1$ and nebentypus ε, with conductors $q(f)$, $q(g)$ respectively, how large should M be (in terms of the parameters described) so that the equality

$$\lambda_f(p) = \lambda_g(p)$$

for all primes $p \leqslant M$ implies that $f = g$? Here

$$f(z) = \sum_{n \geqslant 1} \lambda_f(n) n^{(k-1)/2} e(nz), \qquad g(z) = \sum_{n \geqslant 1} \lambda_g(n) n^{(k-1)/2} e(nz)$$

are the Fourier expansions of f and g, or in other words $\lambda_f(n)$ is the n-th Hecke eigenvalue for f.

The Generalized Riemann Hypothesis for Rankin-Selberg L-functions shows that one can take $M = C(\log kq(f)q(g))^2$, where $C > 0$ is some absolute (and effective) constant (see e.g. [IK, Prop. 5.22]).

The following is a reformulation of the main result of [DK]:

Theorem 1.1. *Let $\alpha > 0$ be any positive number and let $Q \geqslant 2$. For any primitive form f of weight k and conductor $q \leqslant Q$, the number N of primitive non-CM modular forms g of weight k with conductor $q(g) \leqslant Q$ such that*

$$(1) \qquad \lambda_g(p) = \lambda_f(p) \text{ for } p \leqslant (\log Q)^\alpha$$

is bounded by

$$N \ll Q^{10\alpha^{-1}+1/2+\varepsilon}$$

for any $\varepsilon > 0$, the implied constant depending only on α and ε.

Since the number of possible forms g is $\gg Q^2$, it follows that for $\alpha > 10$ the probability of g satisfying (1) tends to 0 as $Q \to +\infty$. However, the exponent $\frac{1}{2}$ is unsatisfactory as it prevents the same conclusion to be reached if we look only for g in a sub-family with less than about $Q^{1/2}$ elements of conductor $\leqslant Q$. In [DK], it is also shown that this exponent can be removed when looking at families with q squarefree.

In [DK], this exponent arises from the need to use the symmetric square L-functions when the Fourier coefficients considered in (1) are "too small", so that one ends up counting not really the modular forms g but their symmetric squares. As shown by Ramakrishnan in the Appendix to [DK], we have $\mathrm{Sym}^2 f = \mathrm{Sym}^2 g$ if and only if $f = g \otimes \chi$ for some primitive real character χ (the twist $g \otimes \chi$ is taken to be the primitive form associated to the modular form with Fourier coefficients $\lambda_g(n)\chi(n)n^{(k-1)/2}$, which may be of smaller level). Thus the exponent $1/2$ arose by simply counting the possible number of characters χ such that the twist has conductor $\leqslant Q$.

In the next section we improve slightly the analysis of this case, removing the exponent $1/2$, but at the cost of introducing a dependency on f in the final estimate. We will see that it does not seem

easy to remove this dependency in general.[1] However in Section 3, we get some uniform results for elliptic curves, using some cute arguments on group representations. In Section 4, we discuss two new variants: distinguishing symmetric squares from small primes, and CM forms from small primes inert in a quadratic field.

Notation. In general we denote by $\lambda_f(p)$ the Hecke eigenvalues for a primitive automorphic form, normalized so that the critical line for $L(f,s)$ is $\mathrm{Re}(s) = \frac{1}{2}$, independently of the weight. If f is associated to an elliptic curve $E/\mathbf{Q}$, we write $a_E(p)$ for the Fourier coefficients so $a_E(p) = \sqrt{p}\lambda_f(p)$. We denote by $q(f)$ the conductor of a primitive form, and by $q(\chi)$ that of a Dirichlet character.

Finally, the notation $f \ll g$ and $f = O(g)$ are synonymous for us and refer to bounds for all x in an explicitly specified set X (sometimes clear from the context), with a well-defined implied constant.

2. Recognizing a fixed form

Instead of fixing a form, it is maybe clearer to formulate the result as a multiplicity bound for a generic sequence of would-be eigenvalues. This viewpoint is inspired by that taken by Sarnak [Sa].

Proposition 2.1. *Let* $\Lambda = (\lambda(p))$ *be a fixed sequence of complex numbers indexed by prime numbers. For any* $\alpha > 0$, *any* $Q \geqslant 2$, *the number* N *of primitive modular forms* g *of weight* 2 *with conductor* $q(g) \leqslant Q$ *such that*

$$\lambda_g(p) = \lambda(p) \text{ for } p \leqslant (\log Q)^\alpha$$

is bounded by

$$N \ll Q^{12\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, *the implied constant depending on* ε *and* Λ.

We first state a slightly more precise version of the counting lemma that was used in [DK] and will be used repeatedly here.

Lemma 2.2. *Let* $Q \geqslant 2$, $\alpha > 2$, $\beta > 0$, $q \geqslant 1$. *Let* $m \geqslant 1$ *be maximal such that* $(\log Q)^{m\alpha} \leqslant Q^\beta$. *Let* $\mathcal{P}$ *be a set of primes* $p \leqslant (\log Q)^\alpha$ *such that*

$$(2) \qquad\qquad |\mathcal{P}| \geqslant \delta \frac{(\log Q)^\alpha}{\log\{\log Q\}^\alpha}.$$

Then the number N *of integers* $n \leqslant Q^\beta$ *such that* n *is squarefree, has* m *prime factors, all of which belong to* $\mathcal{P}$, *satisfies*

$$Q^{\beta-\beta\alpha^{-1}-\varepsilon} \ll N \ll Q^{\beta-\beta\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, *the implied constants depending only on* δ, α *and* ε.

Proof. We have by Stirling's formula

$$N = \binom{|\mathcal{P}_q|}{m} \gg m^{-1/2}\Big(\frac{|\mathcal{P}_q|}{m}\Big)^m$$

with an absolute implied constant, where $\mathcal{P}_q$ is the set of primes $p \in \mathcal{P}$ not dividing q (use $m^2 \leqslant N$). We have

$$|\mathcal{P}_q| \gg \frac{(\log Q)^\alpha}{\log\{\log Q\}^\alpha}$$

by (2), the implied constant depending only on δ since q has $\ll \log\log Q$ prime factors.

Hence we see that

$$N \gg m^{-1/2}\Big(\frac{(\log Q)^\alpha}{\log\{(\log Q)^\alpha\}}\frac{\alpha\log\log Q}{\beta\log Q}\Big)^m \gg Q^{-\varepsilon}\Big((\log Q)^{\alpha-1}\Big)^{\frac{\beta(\log Q)}{(\alpha\log\log Q)}-1} \gg Q^{\beta\frac{\alpha-1}{\alpha}-\varepsilon}.$$

On the other hand, Stirling's formula again yields similarly

$$N \leqslant \binom{|\mathcal{P}|}{m} \ll \Big(\frac{|\mathcal{P}|}{m}\Big)^m \ll Q^{\beta\frac{\alpha-1}{\alpha}+\varepsilon}.$$

$\square$

---

[1] Note that also in the best individual and unconditional bounds currently known, e.g. in [KMV], [Ric] one also has to fix the form to which the others are compared.

Proof of Proposition 2.1. Let S be the set of forms g that is being counted. One can assume S not empty. The argument of [DK] gives the estimate

$$N' \ll Q^{10\alpha^{-1}+\varepsilon}$$

for the number N' of symmetric squares of the forms $g \in S$, and by Ramakrishnan's theorem, two elements g_1, g_2 of S have the same symmetric square if and only if $g_1 = g_2 \otimes \chi$ for some real primitive quadratic character χ.

Fix a form $g \in S$ with symmetric square having maximal multiplicity. For any $g_1 \in S$ with the same symmetric square as g, we have $g_1 = g \otimes \chi$ for some χ hence

$$\lambda_{g_1}(p) = \chi(p)\lambda_g(p)$$

for any p coprime with $q(g_1)$ and $q(g)$. Using the assumption it follows that

$$\lambda(p) = \chi(p)\lambda(p)$$

for $p \leqslant (\log Q)^\alpha$ such that $(p, q(g_1)q(g)) = 1$, so that either $\lambda(p) = 0$ or $\chi(p) = 1$ for those primes.

By results of Serre [Se1], the set of primes p for which $\lambda_g(p) \neq 0$ has positive density $\geqslant \frac{1}{2}$ (in fact, density 1 if g is not a CM form, and density $\frac{1}{2}$ if g is a CM form). Since $S \neq \emptyset$ by assumption, this means that we have

(3)
$$|\{p \leqslant X \mid \lambda(p) \neq 0\}| \gg \frac{X}{\log X}$$

for $X = (\log Q)^\alpha$, the implied constant depending on Λ. Let $\mathcal{P} = \{p \leqslant (\log Q)^\alpha \mid \lambda(p) \neq 0\}$ be this set of primes. For any χ as above we have $\chi(p) = 1$ for $p \in \mathcal{P}$ coprime with $q(g)q(\chi)$.

To estimate the number of χ, we are therefore led back to Linnik's original problem, precisely to a simple variant since the set of primes involved is not the initial segment. For any primitive Dirichlet character ψ, write

$$L(\psi) = \sum_{n \leqslant Q^2} a_n \psi(n)$$

where a_n is the characteristic function of the set T of integers $n \leqslant Q^2$ such that n is squarefree, has a fixed number m of prime factors, and $p \mid n$ implies $p \in \mathcal{P}$ and $(p, q(g)) = 1$. We have moreover

$$L(\chi) = |\{n \in T \mid (n, q(\chi)) = 1\}|$$

if $g \otimes \chi \in S$. By Lemma 2.2 twice (with the same m, but with different q), if m is suitably chosen, we have

$$|T| \geqslant L(\chi) \gg Q^{2(1-\alpha^{-1})-\varepsilon}, \quad |T| \ll Q^{2(1-\alpha^{-1})+\varepsilon}, \quad \text{so } L(\chi) \gg |T|^{1-\varepsilon}$$

for any $\varepsilon > 0$, the implied constants depending on α, ε and Λ (not on χ).

On the other hand, by positivity and the multiplicative large sieve inequality we have

$$|T|^{2-\varepsilon}|\{\chi \mid g \otimes \chi \in S\}| \leqslant \sum_{q \leqslant Q} \sideset{}{^*}\sum_{\chi \,(\mathrm{mod}\, q)} |L(\chi)|^2 \leqslant Q^2 \sum_{n \leqslant Q^2} |a_n|^2 \leqslant Q^2 |T|$$

so the number of characters is $\ll Q^{2\alpha^{-1}+\varepsilon}$ for any $\varepsilon > 0$, the implied constant depending on α, ε and Λ.

This bounds the maximal possible multiplicity of the symmetric square, hence

$$N \ll N' Q^{2\alpha^{-1}+\varepsilon} \ll Q^{12\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, the implied constant depending on Λ, α and ε. $\qquad\square$

To remove the dependency of the result on the sequence Λ amounts to giving a uniform version of (3) for $\lambda(p) = \lambda_f(p)$. This is certainly difficult because the primes involved are very small, so even the existence of one $p \leqslant (\log Q)^\alpha$ with $\lambda_f(p) \neq 0$ is an extremely strong result for f of conductor about Q. And since, if a form exists with many zero coefficients, then many twists may have the same symmetric square and the same first Fourier coefficients, one cannot expect to deal with g on average only.

The case of Maass forms, also considered by Brumley, can not be treated as above because an analogue of (3) is not known in this case; one only knows that there are $\gg_g x/\log x$ values of $n \leqslant x$ such that $\lambda_f(n) \neq 0$ (see Proposition 3 of [KRW]).

3. Recognizing elliptic curves

In the case of elliptic curves, one can derive a strong uniform version on the assumption of the Riemann Hypothesis, not for all L-functions (since GRH for Rankin-Selberg L-functions gives more than what we want!), but for real characters and for holomorphic modular forms of weight 1 (with solvable image, if one wishes). Without GRH, a much weaker uniform result follows by the standard zero-free regions:

Proposition 3.1. *Let $\alpha > 0$, $Q \geqslant 2$ and let X be a set with maximal cardinality of isogeny classes of elliptic curves $E/\mathbf{Q}$ with conductors $\leqslant Q$ such that*

$$a_E(p) = a_F(p) \text{ for } E, \ F \in X, \ p \leqslant (\log Q)^{\alpha}.$$

(1) Assuming GRH for Dirichlet L-functions of real characters and holomorphic modular forms of weight 1, we have

$$|X| \ll Q^{12\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, the implied constant depending on α and ε only.
    (2) Unconditionally, we have

$$|X| \ll Q^{12\alpha^{-1}+\varepsilon}$$

provided X contains at least one curve with conductor $\leqslant \log\{\log Q\}^{\alpha}$. The implied constant depends on α and ε only.

We need a lemma (probably well-known) to bound the conductors of some Artin L-functions. In what follows, we denote by $G_{\mathbf{Q}}$ the Galois group of a separable closure of $\mathbf{Q}$.

Lemma 3.2. *Let $E/\mathbf{Q}$ be an elliptic curve, ℓ be a prime number, $\rho_\ell : G_{\mathbf{Q}} \to GL(2, \mathbf{Z}/\ell\mathbf{Z})$ the Galois representation given by the action on the ℓ-torsion points of E. For any irreducible linear representation $\pi : GL(2, \mathbf{Z}/\ell\mathbf{Z}) \to GL(m, \mathbf{C})$, the Artin conductor of the representation $\pi \circ \rho_\ell$ is $\leqslant c(\ell)q^m$, where q is the conductor of E and $c(\ell) \geqslant 1$ is an integer depending only on ℓ.*

Proof. For any fixed prime p, notice that for any real number $v \geqslant -1$, the upper-numbering ramification group I_p^v (normalized as in [DDT, §2.1], so I_p^v is the inertia group at p for $v \leqslant 0$) acts trivially on ρ_ℓ and on $\pi \circ \rho_\ell$ if it acts trivially on the ℓ-torsion points of E. For $p \neq \ell$, the exponent of the Artin conductor of $\pi \circ \rho_\ell$ at p is given by

$$v_p(\pi \circ \rho_\ell) = \int_{-1}^{+\infty} \operatorname{codim}(\pi \circ \rho_\ell)^{I_p^v} dv$$

(see e.g. [DDT, p. 49]). Let V be such that I_p^v acts trivially on $E[\ell]$ for $v > V$ and non-trivially for $v < V$. Then we have

$$(4) \qquad v_p(\pi \circ \rho_\ell) = \int_{-1}^{V} \operatorname{codim}(\pi \circ \rho_\ell)^{I_p^v} dv \leqslant m(V+1)$$

and similarly the exponent of the conductor for the representation modulo ℓ is

$$v_p(\rho_\ell) = \int_{-1}^{V} \operatorname{codim}(\rho_\ell)^{I_p^v} dv \geqslant V+1,$$

since $\operatorname{codim}(\rho_\ell)^{I_p^v}$ must be $\geqslant 1$ if the action is non-trivial. Since $p^{v_p(\rho_\ell)} \mid q$ (see e.g. [DDT, Lemma 2.7, Remark 2.14]), we obtain the result at p.
    For $p = \ell$, let $K_\ell = \mathbf{Q}(E[\ell])$ be the field generated by coordinates of ℓ-torsion points of E and $n = [K_\ell : \mathbf{Q}]$. The exponent of ℓ in the discriminant of $K_\ell/\mathbf{Q}$ is the same as the exponent of the conductor of the regular representation $\omega : G_{\mathbf{Q}} \to \mathbf{C}[\operatorname{Gal}(K_\ell/\mathbf{Q})] \simeq GL(n, \mathbf{C})$ (see e.g. [Se3, VI.3, Cor. 1]). Hence as above it is given by

$$v_\ell(K_\ell/\mathbf{Q}) = \int_{-1}^{+\infty} \operatorname{codim}(\omega)^{I_p^v} dv.$$

Let V be as above for ℓ, so also I_p^v acts trivially on ω for $v > V$. We have

$$v_\ell(\pi \circ \rho_\ell) = \int_{-1}^{V} \operatorname{codim}(\pi \circ \rho_\ell)^{I_\ell^v} dv \leqslant m(V+1)$$

$$v_\ell(K_\ell/\mathbf{Q}) = \int_{-1}^{V} \operatorname{codim}(\omega)^{I_p^v} dv \geqslant V+1.$$

Hence to prove the desired result it is enough to find an upper bound for $v_\ell(K_\ell/\mathbf{Q})$ which is independent of E. Such a bound follows, for instance, from the fact that the degree of K_ℓ is bounded independently of E, and from universal bounds for the discriminant of extensions of local fields of bounded degree (see, e.g., [Se1, Cor. to Prop. 2]). $\square$

Remark 3.3. For our application, one could also simply bound the conductor of $\pi \circ \rho_\ell$ by the discriminant of K_ℓ and apply a general bound like [Se1, Prop. 6].

Although we will use only the case $q = 3$ of the next lemma, it is nice enough to state generally.

Lemma 3.4. *Let $\mathbf{F}_q$ be a field with q elements of characteristic $\neq 2$. Let N be the set of elements in $GL(2, \mathbf{F}_q)$ which are not diagonalizable over $\bar{\mathbf{F}}_q$, f_N the characteristic function of N. Then we have*

$$(5) \qquad q f_N = 1 + \chi \circ \det + \sum_{\psi^2 \neq 1} \chi_{\psi, \psi^{-1}} - \sum_{\varphi \mid \mathbf{F}_q = 1} \chi_\varphi$$

where χ is the quadratic character of $\mathbf{F}_q$, ψ runs over characters of $\mathbf{F}_q^\times$ and $\chi_{\psi, \psi^{-1}}$ is the character of the associated irreducible representations of degree $q + 1$, φ runs over characters of $\mathbf{F}_{q^2}^\times$ with $\varphi^q \neq \varphi$ and χ_φ is the character of the associated irreducible representation of degree $q - 1$; see the discussion below for details.

Proof. The set N is the union of the $q - 1$ conjugacy classes of the elements

$$n_x = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$$

with $x \neq 0$, each of which has $q^2 - 1$ elements. To decompose f_N in terms of characters, we need only look at the corresponding column of the character table, which we quote with the notation of [FH, p. 70] (transposed for easier reading, and with the degree of the representations for reference):

	U_α	V_α	$W_{\alpha,\beta}$	X_φ
degree	1	q	$q + 1$	$q - 1$
n_x	$\alpha(x^2)$	0	$\alpha(x)\beta(x)$	$-\varphi(x)$

(U_α is the character $\alpha(\det(x))$, V_α is the irreducible component of degree q of the permutation representation on $\mathbf{P}^1(\mathbf{F}_q)$, twisted by α, $W_{\alpha,\beta}$ is induced from the character (α, β) of the Borel subgroup (up to permutation) with $\alpha \neq \beta$, and X_φ, for φ a character of $\mathbf{F}_{q^2}^\times$ such that $\varphi^q \neq \varphi$, is the (a priori virtual) representation $V_1 \otimes W_{1,\varphi} - W_{1,\varphi} - \mathrm{Ind}(\varphi)$).

The obvious point now is that for each irreducible character χ, χ restricted to $n_x \in N$ is, as function of x, a constant multiple of some multiplicative character of $\mathbf{F}_q^\times$. Hence the scalar product $\langle f_N, \chi \rangle$ vanishes by orthogonality unless the corresponding character is trivial on $\mathbf{F}_q^\times$. This immediately implies (5) by inspection. $\square$

Remark 3.5. In particular, among the $q^2 - 1$ irreducible representations of $GL(2, \mathbf{F}_q)$, only q occur in the decomposition of f_N. One can prove more conceptually that characters restricted to N are multiples of multiplicative characters, as pointed out by D. Bump: the matrix n_x is conjugate to

$$\begin{pmatrix} x & x \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

hence, if ψ is the central character, we have

$$\chi(n_x) = c\psi(x) \text{ with } c = \chi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right).$$

Proof of Proposition 3.1. By modularity of elliptic curves and the reasoning at the beginning of the proof of Proposition 2.1, it suffices to prove a uniform lower bound for the number of primes $\leqslant (\log Q)^\alpha$ where $a_E(p) = 0$.

For any prime ℓ, the Galois representation $\rho_\ell : G_{\mathbf{Q}} \to GL(2, \mathbf{Z}/\ell\mathbf{Z})$ on ℓ-torsion points satisfies $a_E(p) \equiv \mathrm{Tr}\, \rho_\ell(\mathrm{Fr}_p) \pmod{\ell}$ for any unramified prime $p \neq \ell$. In particular, if $\rho_\ell(\mathrm{Fr}_p)$ is in the set of conjugacy classes with non-zero trace in $\mathbf{Z}/\ell\mathbf{Z}$, we have $a_E(p) \neq 0$.

If E does not have non-trivial rational 2-torsion points, one can use $\ell = 2$, but if $E[2](\mathbf{Q}) \neq 0$ we have $a_E(p) \equiv 0 \pmod{2}$ for any odd prime. To avoid considering an unnecessary case, we take $\ell = 3$.

We distinguish two cases, depending on whether $G_3 = \rho_3(G_{\mathbf{Q}}) \subset GL(2, \mathbf{Z}/3\mathbf{Z})$ has order divisible by 3 or not. If G_3 has order divisible by 3, it must contain elements of the set N described in Lemma 3.4

for $q = 3$. For any $x \in N$, we have $\operatorname{Tr} x = \pm 1 \neq 0$, so any prime p for which $\rho_3(\operatorname{Fr}_p) \in G_3 \cap N$ satisfies $a_E(p) \neq 0$, and we know a priori from the Chebotarev density theorem that this set of primes has positive density.

By Lemma 3.4, all characters of $\mathbf{F}_3^\times$ being quadratic, the characteristic function f_N of N is given by

$$(6) \qquad\qquad 3 f_N = 1 + \det - \chi_2,$$

where 1 denotes the character of the trivial representation, det is the determinant quadratic character, and χ_2 is the character of an irreducible representation of degree 2 (precisely of X_φ where φ is the character of $\mathbf{F}_9^\times = \mathbf{F}_3[X]^\times$, with $X^2 = -1$, that maps the primitive root $1 + X \in \mathbf{F}_9^\times$ to $i \in \mathbf{C}$).

It might be that χ_2 restricted to G_3 is not irreducible, in which case it splits into a direct sum of two characters of degree 1, say ε_1, ε_2. Since the set of primes we're counting has density > 0 by assumption, the trivial representation occurs with coefficient > 0 in the decomposition of f_N so one has $\varepsilon_i \neq 1$ (see (6)).

The Artin L-functions of 1, det (and ε_1, ε_2 possibly) are Dirichlet L-functions, and since G_3 is solvable, the Artin L-function of χ_2 is the L-function of a primitive holomorphic cusp form of weight 1 by the Langlands-Tunnell Theorem. The conductors of all those L-functions are $\ll Q^2$ by Lemma 3.2 and we obtain

$$3 \sum_{\substack{p \leqslant X \\ a_E(p) \neq 0}} \log p \geqslant 3 \sum_{p \leqslant X} f_N(\rho_3(\operatorname{Fr}_p)) \log p$$

$$= \sum_{p \leqslant X} \log p + \sum_{p \leqslant X} \det(\rho_3(\operatorname{Fr}_p)) \log p - \sum_{p \leqslant X} \chi_2(\rho_3(\operatorname{Fr}_p)) \log p + O(1).$$

By GRH for 1, det, χ_2 (or ε_1, ε_2) we get for $X \geqslant 2$ that

$$3 \sum_{\substack{p \leqslant X \\ a_E(p) \neq 0}} \log p \geqslant X + O(\sqrt{X}(\log QX)^2),$$

with an absolute implied constant (see e.g. [IK, Th. 5.15]). Taking $X = (\log Q)^\alpha$, it follows by partial summation that for $\alpha > 5$ we have

$$(7) \qquad\qquad |\{p \leqslant (\log Q)^\alpha \mid a_E(p) \neq 0\}| \gg \frac{(\log Q)^\alpha}{\log\{(\log Q)^\alpha\}}$$

with an absolute implied constant, which is the required uniform version of (3). If $\alpha \leqslant 5$, the statement of Proposition 3.1 is trivial in any case.

If G_3 has order divisible by 3 (which means that the discriminant of E is a cube, see e.g. [Se2, p. 305]), it only contains semisimple elements and its order is at most 16. It is either abelian or dihedral and its irreducible representations are thus of degree 1 or 2. Decomposing the characteristic function of the identity (with trace $-1 \neq 0$) in characters, one gets a lower bound like (7) using L-functions of degree 1 or 2 again.

We now come to what can be proved without GRH. For any primitive Dirichlet character χ modulo q we have

$$\sum_{p \leqslant X} \chi(p) \log p = \delta(\chi) X + O\left(\frac{\sqrt{q}X}{(\log X)^A}\right)$$

for $X \geqslant 2$ and $A > 0$, the implied constant depending on A only. For a holomorphic cusp form f of weight 1 with conductor q we have

$$\sum_{p \leqslant X} \lambda_f(p) \log p \ll \frac{\sqrt{q}X}{(\log X)^A}$$

for $X \geqslant 2$ and $A > 0$, the implied constant depending on A only (see e.g. [IK, Cor. 5.29, Th. 5.40]; by a result of Stark [St] for Artin L-functions of degree > 1, or of Hoffstein and Ramakrishnan [HR] for cusp forms, the L-function of the forms that occur here do not have exceptional zeros). Denoting by q the conductor of E and taking again the case of $\ell = 3$ with G_3 of order divisible by 3, we have now

$$3 \sum_{\substack{p \leqslant X \\ a_E(p) \neq 0}} \log p \geqslant X + O\left(\frac{qX}{(\log X)^A}\right).$$

by (6) and the upper bound for the conductors of the L-functions for det and χ_2. Take $A = 2$. If $X = (\log Q)^\alpha$ and $q \leqslant \log X$, we obtain

$$|\{p \leqslant (\log Q)^\alpha \mid a_E(p) \neq 0\}| \gg \frac{(\log Q)^\alpha}{\log\{(\log Q)^\alpha\}}$$

where the implied constant is absolute. The other case is obviously similar. □

4. Variations: recognizing symmetric squares and CM forms

The theorem of Ramakrishnan characterizing the non-injectivity of the symmetric square on modular forms suggests the following problem: assume that f and g are primitive forms (with same weight k) and that $\lambda_f(p^2) = \lambda_g(p^2)$ for $p \leqslant M$. How large should M be so that $\operatorname{Sym}^2 f = \operatorname{Sym}^2 g$, or in other words, so that $f = g \otimes \chi$ for some real primitive character χ?

By GRH for the Rankin-Selberg L-functions $L(\operatorname{Sym}^2 f \otimes \operatorname{Sym}^2 g, s)$ and $L(\operatorname{Sym}^2 f \otimes \operatorname{Sym}^2 f, s)$, it follows that if f and g are not CM forms, the conclusion $\operatorname{Sym}^2 f = \operatorname{Sym}^2 g$ follows for $M = C(\log kq(f)q(g))^2$ for some absolute constant $C > 0$. (In the CM case, one gets a bound of same size by working over the CM field, using the corresponding Hecke characters).

Using the Linnik method we get:

Theorem 4.1. *Let $\alpha > 0$ be any positive number and let $Q \geqslant 2$. For any weight 2 primitive form f of conductor $q \leqslant Q$, the number N of symmetric squares of primitive non-CM modular forms g of weight 2 and conductor $q(g) \leqslant Q$ such that*

$$(8) \qquad \lambda_g(p^2) = \lambda_f(p^2) \text{ for } p \leqslant (\log Q)^\alpha$$

is bounded by

$$N \ll Q^{24\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, the implied constant depending only on α and ε.

There is no extraneous exponent here, but as the proof will clearly show this is because we fix the nebentypus to be trivial. The proof follows [DK] again, but this time we must use a mean-value estimate for the symmetric fourth power L-functions (available from [DK] thanks to Kim's result [K] that for a non-CM modular form g, its fourth symmetric power $\operatorname{Sym}^4 g$ is a cuspidal automorphic representation on $GL(5)$ with conductor $\leqslant q^4 \leqslant Q^4$) if the $\lambda_f(p^2)$ are too small for small p. An issue of multiplicity arises for the symmetric fourth power. The simplest case, which suffices our purpose, is as follows:

Lemma 4.2. *For any two holomorphic primitive forms f and g of weight $\geqslant 2$ and trivial nebentypus, we have $\operatorname{Sym}^4 f = \operatorname{Sym}^4 g$ if and only if $\operatorname{Sym}^2 f = \operatorname{Sym}^2 g$.*

This follows either from Proposition 5.1 of [CM], or from more general results of Rajan [R] on recovering ℓ-adic representations. This case is an easy application of Serre's ℓ-adic methods, and the non-expert reader is invited to see it as an interesting exercise (it boils down to showing that $\lambda_f(p^2) = 1 - \lambda_g(p^2)$ can not occur very often). Note that other cases of this lemma are a little bit different. With non-trivial nebentypus, further multiplicity comes trivially from quartic twists $f \otimes \chi_4$, where χ_4 is of order 4 exactly. More interestingly, for forms of weight 1 there is a different source of multiplicity: if f corresponds to an icosahedral Galois representation, then f has a Galois conjugate f^τ (where τ basically is the non-trivial automorphism of $\mathbf{Q}(\sqrt{5})/\mathbf{Q}$), with f^τ not a quartic twist of f, and $\operatorname{Sym}^4 f^\tau = \operatorname{Sym}^4 f$. (The proof above fails because $(1 - \sqrt{5})/2 = 1 - (1 + \sqrt{5})/2...$)

This in particular means that the corresponding statement for Maass forms is certainly quite deep as the Langlands-type correspondance is not known to exist for even icosahedral representations.

Proof. Let p be an unramified prime for f, and let α and β be the usual local roots of f at p, so that $\alpha + \beta = \lambda_f(p)$ and $\alpha\beta = 1$. We have $\lambda_f(p^2) = \alpha^2 + \beta^2 + 1$ and

$$(9) \qquad \lambda_f(p^4) = \alpha^4 + \alpha^2 + 1 + \beta^2 + \beta^4 = (\alpha^2 + \beta^2 + 1)^2 - \alpha^2 - \beta^2 - 2 = \lambda_f(p^2)^2 - \lambda_f(p^2) - 1.$$

In particular if $|\lambda_f(p^2)| < \frac{1}{2}$, we have $|\lambda_f(p^4)| \geqslant 1/4$. If more than half the primes $p \leqslant (\log Q)^\alpha$ satisfy $|\lambda_f(p^2)| < \frac{1}{2}$, then we derive

$$N \ll Q^{10\alpha^{-1}+\varepsilon}$$

from the argument of [DK].

Otherwise we have $|\lambda_f(p^4)| \geqslant 1/4$ for at least half the primes $\leqslant (\log Q)^\alpha$. For the usual parameters $X \geqslant 2$ and $m \geqslant 1$ to be chosen later, denote

$$L(g) = \sum_{n \leqslant X} b_n \lambda_g(n^4)$$

where $b_n = a_n \lambda_f(n^4)$, and a_n is the characteristic function of those integers $n \leqslant X$ such that n is squarefree and has m prime factors, all unramified for f, with $|\lambda_f(p^4)| \geqslant 1/4$. For any g where $\mathrm{Sym}^2 g$ contributes to N we have

$$L(g) \geqslant \frac{1}{16^m} \sum_{n \leqslant X} a_n.$$

By positivity we have

$$\frac{N}{256^m} \Big(\sum_{n \leqslant X} a_n \Big)^2 \leqslant \sum_{q \leqslant Q} \sum_g |L(g)|^2$$

where g runs over non-CM forms of weight 2 and conductor q. Let

$$L(\mathrm{Sym}^4 g, s) = \sum_{n \geqslant 1} \nu_g(n) n^{-s}$$

be the Dirichlet series expansion of the fourth symmetric power L-function of f. By the above properties of $\lambda_f(p^4)$ we can write

$$\sum_{q \leqslant Q} \sum_g |L(g)|^2 = \sum_{q \leqslant Q} \sum_g \Big| \sum_{n \leqslant X} a_n \nu_g(n) \Big|^2.$$

By Kim's functoriality theorem and Theorem 4 of [DK], we have

$$\sum_{q \leqslant Q} \sum_{\mathrm{Sym}^4 g} \Big| \sum_{n \leqslant X} a_n \nu_g(n) \Big|^2 \ll X^{1+\varepsilon} \sum_{n \leqslant X} |a_n|^2 = X^{1+\varepsilon} \sum_{n \leqslant X} a_n$$

if $X > Q^\beta$ with $\beta > 24$, for any $\varepsilon > 0$, the implied constant depending on β and ε. (The exponent 24 arises because the conductor is $\leqslant Q^4$, and the number of forms $\ll Q^2 = Q^{4/2}$ so $d = 1/2$, $n = 5$, in the notation of loc. cit.)

Note the last sum is over the symmetric fourth powers of g. By Lemma 4.2, we can rewrite the sum over $\mathrm{Sym}^4 g$ as one over $\mathrm{Sym}^2 g$, which is precisely what we are counting. By Lemma 2.2, for suitable m (maximal such that $(\log Q)^{m\alpha} \leqslant Q^{24}$), we have for any $\varepsilon > 0$ the lower bound

$$\sum_{n \leqslant X} a_n \gg Q^{24(1-\alpha^{-1})-\varepsilon}$$

when choosing m maximal with $(\log Q)^{\alpha m} \leqslant Q^\beta$, $\beta > 24$, the implied constant depending only on α and ε. Hence the result follows as before, m being small enough that $256^m \ll X^\varepsilon$ for any $\varepsilon > 0$. $\qquad\square$

The final problem we consider is motivated now by the result of Serre used in the proof of Proposition 2.1: let $k/\mathbf{Q}$ be a fixed quadratic field, and let f be primitive form of weight $k \geqslant 2$; assume that $\lambda_f(p) = 0$ for all $p \leqslant M$ which are inert in k. How large should M be so that this implies that f is a CM form?

Denote by χ the quadratic character associated with k and by D the discriminant of k. The assumption implies that $\lambda_f(p) = \chi(p) \lambda_f(p) = \lambda_{f \otimes \chi}(p)$ for all $p \leqslant M$ unramified in k. Hence by GRH again, it follows that $f = f \otimes \chi$ if $M \geqslant C(\log |D| q(f))^2$ with an absolute constant $C \geqslant 0$. Since this condition implies that f is a CM form, this solves the problem.

Here is a Linnik-style result about this problem. Since the condition $\lambda_f(p) = 0$ is stable by any twist by a character, it is natural to count the forms up to twist; fixing the nebentypus, this means up to quadratic twist (to put it differently, a twist of a CM form is itself a CM form, but the nebentypus changes except for quadratic twists). So it is natural to count only the number of possible symmetric squares.

Theorem 4.3. *Let $\alpha > 0$ be any positive number and let $Q \geqslant 2$. For any quadratic field $k/\mathbf{Q}$, the number N of symmetric squares of primitive modular forms of weight 2 and conductor $\leqslant Q$ such*

(10) $$\lambda_f(p) = 0 \text{ for } p \leqslant (\log Q)^\alpha \text{ inert in } k$$

is bounded by

$$N \ll Q^{10\alpha^{-1}+\varepsilon}$$

for any $\varepsilon > 0$, the implied constant depending only on α and ε.

Proof. If f satisfies (10), we have $\lambda_f(n^2) = 1$ for all n squarefree which is divisible only by primes $p \leqslant (\log Q)^\alpha$ which are inert in k, and unramified for f. Thus with

$$L(f) = \sum_{n \leqslant X} a_n \lambda_f(n^2)$$

where a_n is the characteristic function of numbers of this type having exactly m prime factors, we have for such f

$$L(f) = \sum_{n \leqslant X} a_n,$$

and by positivity we have

$$N\Big(\sum_{n \leqslant X} a_n\Big)^2 \leqslant \sum_f^* |L(f)|^2,$$

where $\sum^*$ indicates that we sum over the distinct symmetric squares only. By the large-sieve type inequality for symmetric square L-functions, we have

$$\sum_f^* |L(f)|^2 \ll X^{1+\varepsilon} \sum_{n \leqslant X} |a_n|^2 = X^{1+\varepsilon} \sum_{n \leqslant X} a_n,$$

if $X > Q^\beta$ for any $\beta > 10$ and $\varepsilon > 0$, the implied constant depending only on β and ε.

To estimate the number of n with $a_n = 1$, we have the analogue of (3)

$$|\{p \leqslant X \mid p \text{ is inert in } k\}| \gg \frac{X}{\log X},$$

for $X \geqslant 2$, the implied constant depending on k. Applying Lemma 2.2 to this situation (again for m as described in the statement), this gives the bound $Q^{10\alpha^{-1}+\varepsilon}$ for the number of symmetric squares. $\qquad\square$

References

[CM]   J. Cogdell and P. Michel: *On the complex moments of symmetric power L-functions at $s = 1$*, I.M.R.N 2004, no. 31, 1561–1617.

[DDT]   H. Darmon, F. Diamond and M. Taylor: *Fermat's Last Theorem*, Current Developments in Math., International Press (1995), 1–154.

[DK]   W. Duke and E. Kowalski: *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. math. 139 (2000), 1–39.

[FH]   W. Fulton and J. Harris: *Representation theory. A first course*, GTM 129, Springer 1991.

[HR]   J. Hoffstein and D. Ramakrishnan: *Siegel zeros and cusp forms*, I.M.R.N 1995, No.6, 279-308 (1995).

[IK]   H. Iwaniec and E. Kowalski: *Analytic Number Theory*, A.M.S Colloquium Series 53, 2004.

[K]   H. Kim: *Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2*, with appendix 1 by D. Ramakrishnan and appendix 2 by H. Kim and P. Sarnak, J. Amer. Math. Soc. 16 (2003), no. 1, 139–183.

[KMV]   E. Kowalski, P. Michel and J. VanderKam: *Rankin-Selberg L-functions in the level aspect*, Duke Math. J. 114 (2002), no. 1, 123–191.

[KRW]   E. Kowalski, O. Robert and J. Wu: *Small gaps in coefficients of L-functions and 𝕭-free numbers in small intervals*, preprint (2003).

[R]   C.S. Rajan: *Recovering ℓ-adic representations*, preprint (2002).

[Ric]   G. Ricotta: *Zéros réels et taille des fonctions L de Rankin-Selberg par rapport au niveau*, thèse de doctorat, Université Montpellier II (2004).

[Sa]   P. Sarnak: letter to Zeev Rudnick.

[Se1]   J-P. Serre: *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. I.H.E.S 54 (1981), 123–201.

[Se2]   J-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. math. 15 (1972), 259–331.

[Se3]   J-P. Serre: *Corps locaux*, 3ème ed., Hermann 1968.

[St]   H. Stark: *Some effective cases of the Brauer-Siegel theorem*, Invent. math. 23 (1974), 135–152.

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: emmanuel.kowalski@math.u-bordeaux1.fr