Functiones et Approximatio
51.2 (2014), 363–377
doi: 10.7169/facm/2014.51.2.8

DISTINGUISHING EIGENFORMS MODULO A PRIME IDEAL

Sam Chow, Alexandru Ghitza

Abstract: Consider the Fourier expansions of two elements of a given space of modular forms. How many leading coefficients must agree in order to guarantee that the two expansions are the same? Sturm [20] gave an upper bound for modular forms of a given weight and level. This was adapted by Ram Murty [16] and Ghitza [5] to the case of two eigenforms of the same level but having potentially different weights. We consider their expansions modulo a prime ideal, presenting a new bound. In the process of analysing this bound, we generalise a result of Bach and Sorenson [2], who provide a practical upper bound for the least prime in an arithmetic progression.

Keywords: modular forms, Hecke operators, Fourier coefficients, congruences, primes in arithmetic progressions.

1. Introduction

We present a new bound for the number of leading Fourier coefficients that one needs to compare in order to distinguish two eigenforms, of potentially different weights, modulo a prime ideal. Bounds of this flavour are of great practical use in modular forms research, and have received much attention (e.g. [16], [11], [5], [6], [12]) since the groundbreaking work of Sturm [20]:

Theorem 1.1 (Sturm bound, see [18, Theorem 9.18]). *Let f be a modular form of weight k for a congruence subgroup Γ of index $i(\Gamma)$ inside $\mathrm{SL}_2(\mathbb{Z})$. Let R be the ring of integers of a number field, and assume that R contains the Fourier coefficients of f. Let $\mathfrak{p}$ be a prime ideal in R, and assume that $f \not\equiv 0 \mod \mathfrak{p}$. Then there exists*

$$n \leqslant \frac{k \cdot i(\Gamma)}{12} \tag{1.1}$$

such that $a_n(f) \not\equiv 0 \mod \mathfrak{p}$.

2010 Mathematics Subject Classification: primary: 11F11; secondary: 11F25, 11F33, 11N13

We will use Buzzard's adaptation of the Sturm bound to modular forms with character:

Corollary 1.2 (see [18, Corollary 9.20]). *Let f and g be modular forms of weight k and character χ for $\Gamma_0(N)$. Let R be the ring of integers of a number field, and assume that R contains the Fourier coefficients of f and g. Let $\mathfrak{p}$ be a prime ideal in R, and assume that $f \not\equiv g \mod \mathfrak{p}$. Then there exists*

$$n \leqslant \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] \tag{1.2}$$

such that $a_n(f) \not\equiv a_n(g) \mod \mathfrak{p}$.

Our research is strongly motivated by work of Ram Murty [16]:

Lemma 1.3 (see [5, Lemma 2]). *Let f and g be eigenforms of respective weights $k_1 \neq k_2$ for $\Gamma_0(N)$, and let ℓ be the least prime not dividing N. Then there exists $n \leqslant \ell^2$ such that $a_n(f) \neq a_n(g)$.*

Our main result concerns eigenforms modulo a prime ideal:

Theorem 1.4. *Let f and g be normalised eigenforms for $\Gamma_0(N)$, with character χ and respective weights $k_1 \leqslant k_2$. Let R be the ring of integers of a number field containing the Fourier coefficients of f and g, and let $\mathfrak{p}$ be a nonzero prime ideal in R. Define p by $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, assume that $p \geqslant 5$, and assume that $f \not\equiv g \mod \mathfrak{p}$. Then there exists*

$$n \leqslant \max\left\{ g^*(p,N)^2, \frac{k_2}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] \right\} \tag{1.3}$$

such that $a_n(f) \neq a_n(g) \mod \mathfrak{p}$, where $g^*(p,N)$ is the least prime primitive root modulo p that does not divide N.

We note that Kohnen has obtained a similar result [11, Theorem 4], replacing $g^*(p,N)^2$ by the constant 900 in (1.3), at the expense of requiring $(N, 30) = 1$ and only getting a bound for infinitely many (rather than all) prime ideals $\mathfrak{p}$ of R.

Our argument can be modified to deal with the excluded cases $p = 2$ and $p = 3$, yielding (slightly weaker) versions of Theorem 1.4. We relegate these special cases to Section 5. In Section 2 we prove Theorem 1.4. In Section 3, we provide asymptotics (as $N \to \infty$) for the two quantities in the bound (1.3), establishing that the second is asymptotically greater. In Section 4 we determine how large N has to be to ensure that the second expression in (1.3) is indeed the larger of the two. The crucial ingredient in Section 4 is our generalisation (see Corollary 4.5) of an explicit Linnik-type bound (see Theorem 4.3) of Bach and Sorenson.

1.1. Notation and terminology

All modular forms discussed are of positive integer weight k and level N. A modular form of weight k and character χ for $\Gamma_0(N)$ satisfies

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z) \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{1.4}$$

By *eigenform* we mean an eigenvector for the full Hecke algebra. If f is a modular form then $a_n(f)$ denotes the nth Fourier coefficient:

$$f(z) = \sum_n a_n(f) e^{2\pi i n z}. \tag{1.5}$$

The symbols p and ℓ are reserved for prime numbers. A *prime primitive root* modulo p is a prime that is also a primitive root modulo p. We write $f \sim g$ to mean that the ratio of the two functions tends to 1 in some limit, and define the equivalence relation $\sim$ analogously for sequences. The Euler totient function is denoted by φ. By GRH we mean the generalisation of the Riemann hypothesis to Dirichlet L-functions. If a and q are relatively prime positive integers and $x \geqslant 1$ is a real number, then $\pi_{a,q}(x)$ denotes the number of $\ell \leqslant x$ such that $\ell \equiv a \mod q$. We use Landau 'big O' notation in the standard way.

2. Proof of Theorem 1.4

Since $p - 1 \geqslant 4$ is even, we may use the (appropriately normalised) Eisenstein series of weight $p-1$, which is the modular form for $\mathrm{SL}_2(\mathbb{Z})$ given by

$$E_{p-1}(z) = 1 - \frac{2p-2}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-2}(n) e^{2\pi i n z}, \tag{2.1}$$

where B_{p-1} is the $(p-1)$st Bernoulli number (a rational number) and $\sigma_{p-2}(n) = \sum_{d|n} d^{p-2}$; see [18, Subsection 2.1.2].

If $k_1 = k_2$ then the result follows immediately from Corollary 1.2, so henceforth assume that $k_1 < k_2$. Put $\ell = g^*(p, N)$. By standard formulae (see [4, Proposition 5.8.5]),

$$\chi(\ell)\ell^{k_1-1} = a_\ell(f)^2 - a_{\ell^2}(f) \qquad \text{and} \qquad \chi(\ell)\ell^{k_2-1} = a_\ell(g)^2 - a_{\ell^2}(g). \tag{2.2}$$

We may assume that $a_\ell(f) \equiv a_\ell(g) \mod \mathfrak{p}$ and $a_{\ell^2}(f) \equiv a_{\ell^2}(g) \mod \mathfrak{p}$, since otherwise the result is immediate. As $(\ell, N) = 1$, it follows from (2.2) that

$$\ell^{k_1} - \ell^{k_2} \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}. \tag{2.3}$$

As ℓ is a primitive root modulo p, this implies that $p-1$ divides $k_2 - k_1$, so put

$$r = \frac{k_2 - k_1}{p-1} \tag{2.4}$$

and $f' = E_{p-1}^r f$. The von Staudt-Clausen theorem (see [3, Theorem 5.8.4]) implies that p divides the denominator of B_{p-1}, so

$$E_{p-1} \equiv 1 \mod p \tag{2.5}$$

as power series. Now $f' \equiv f \mod pR$, so $f' \equiv f \mod \mathfrak{p}$. As f' is a modular form of weight k_2 and character χ for the congruence subgroup $\Gamma_0(N)$, the result now follows from Corollary 1.2.

3. Asymptotics

We show that, of the two expressions in Theorem 1.4, the second is greater, providing that N is sufficiently large. The key result in this section is:

Theorem 3.1. *Let $p \geqslant 5$. Then*

$$\limsup_{N\to\infty} \frac{g^*(p,N)}{\log N} = \frac{p-1}{\varphi(p-1)}. \tag{3.1}$$

The group index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ is classically known (see [4, Exercise 1.2.3]):

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{\ell \mid N} \left(1 + \frac{1}{\ell}\right). \tag{3.2}$$

In particular $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] \geqslant N$ which, upon proving Theorem 3.1, will verify the assertion made at the beginning of this section.

We include the supremal asymptotics for $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ purely for interest's sake (this is proved in a similar vein to Theorem 3.1):

Proposition 3.2.

$$\limsup_{N\to\infty} \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]}{N \log\log N} = \frac{6e^\gamma}{\pi^2}, \tag{3.3}$$

where γ is the Euler-Mascheroni constant.

Our goal for the remainder of this section is to prove Theorem 3.1. For positive integers t, let x_t be the tth smallest prime primitive root modulo p, and let $N_t = x_1 \cdots x_t$ (also put $N_0 = 1$). The sequence (N_t) is the worst case scenario: if N is a positive integer then there exists $t \geqslant 0$ (defined by $g^*(p,N) = x_{t+1}$) such that $g^*(p,N_t) = g^*(p,N)$ and $N_t \leqslant N$. Put

$$c = \frac{p-1}{\varphi(p-1)} > 1. \tag{3.4}$$

We will establish Theorem 3.1 via the following:

Proposition 3.3.

$$\lim_{t\to\infty} \frac{x_t}{\log N_t} = c. \tag{3.5}$$

This in turn is established by determining the asymptotics of the sequence (x_t):

Lemma 3.4.

$$x_t \sim ct \log t. \tag{3.6}$$

We require some basic results on asymptotic equivalence:

Lemma 3.5.

(i) *Let (a_t) and (b_t) be sequences of positive real numbers. Assume that $a_t \sim b_t$ and that $b_t \to \infty$ as $t \to \infty$. Then $\log a_t \sim \log b_t$.*
(ii) *Let $(a_t), (b_t), (c_t)$, and (d_t) be sequences of positive real numbers such that $a_t \sim c_t$ and $b_t \sim d_t$. Then $a_t + b_t \sim c_t + d_t$.*

Armed with these tools, we prove Lemma 3.4, Proposition 3.3, and Theorem 3.1.

Proof of Lemma 3.4. We interpret t as the number of prime primitive roots modulo p that are less than or equal to x_t. Each of these lies in one of the $\varphi(p-1)$ primitive root residue classes, so summing the prime number theorem for arithmetic progressions over these residue classes yields

$$t \sim \frac{\varphi(p-1)}{p-1} \cdot \frac{x_t}{\log x_t}, \tag{3.7}$$

so

$$\log t \sim \log \frac{\varphi(p-1)}{p-1} + \log x_t - \log\log x_t \sim \log x_t. \tag{3.8}$$

Combining the equivalences (3.7) and (3.8) completes the proof. ∎

Proof of Proposition 3.3. Fix $\varepsilon \in (0, c-1)$, and choose (by Lemma 3.4) a positive integer T such that if $t > T$ then

$$(c-\varepsilon)t\log t < x_t < (c+\varepsilon)t\log t. \tag{3.9}$$

Consider $r > T$, and define

$$u_r = \log(x_t \cdots x_T) + (r-T)\log(c-\varepsilon) + \log\left(\prod_{t=T+1}^{r} t\right) + \log \prod_{t=T+1}^{r} \log t \tag{3.10}$$

and

$$v_r = \log(x_t \cdots x_T) + (r-T)\log(c+\varepsilon) + \log\left(\prod_{t=T+1}^{r} t\right) + \log \prod_{t=T+1}^{r} \log t. \tag{3.11}$$

Using Stirling's approximation and Lemma 3.4,

$$u_r \sim r\log(c-\varepsilon) + \log(r!) \sim r\log(c-\varepsilon) + r\log r \sim r\log r \sim \frac{1}{c}x_r, \tag{3.12}$$

and similarly $v_r \sim \frac{1}{c}x_r$. Since $u_r < \log N_r < v_r$, the result now follows from the sandwich rule. ∎

Proof of Theorem 3.1. By Lemma 3.4 and Proposition 3.3,

$$\frac{g^*(p,N_t)}{\log N_t} = \frac{x_{t+1}}{\log N_t} = \frac{x_{t+1}}{x_t} \cdot \frac{x_t}{\log N_t} \sim \frac{c(t+1)\log(t+1)}{ct\log t} \cdot \frac{x_t}{\log N_t} \to c, \quad (3.13)$$

so it remains to show that $\limsup_{N\to\infty} \frac{g^*(p,N)}{\log N} \leqslant c$. Fix $\varepsilon > 0$. For each positive integer N, choose (by our 'worst case scenario' property) $t_N \geqslant 0$ such that $g^*(p,N_{t_N}) = g^*(p,N)$ and $N_{t_N} \leqslant N$. Choose a positive integer C such that if $t \geqslant C$ then $\frac{g^*(p,N_t)}{\log N_t} \leqslant c+\varepsilon$, define the real number

$$M = \sup_{t>0} \frac{g^*(p,N_t)}{\log N_t}, \quad (3.14)$$

and put

$$K = \exp \frac{M \log N_C}{c+\varepsilon}. \quad (3.15)$$

Let $N \geqslant K$. If $t_N \geqslant C$ then

$$\frac{g^*(p,N)}{\log N} \leqslant \frac{g^*(p,N_{t_N})}{\log N_{t_N}} \leqslant c+\varepsilon, \quad (3.16)$$

while if $t_N < C$ then

$$\frac{g^*(p,N)}{\log N} = \frac{\log N_{t_N}}{\log N} \cdot \frac{g^*(p,N_{t_N})}{\log N_{t_N}} < \frac{\log N_C}{\log K} \cdot \frac{g^*(p,N_{t_N})}{\log N_{t_N}} \quad (3.17)$$

$$= \frac{c+\varepsilon}{M} \cdot \frac{g^*(p,N_{t_N})}{\log N_{t_N}} \leqslant c+\varepsilon, \quad (3.18)$$

which completes the proof since $\varepsilon > 0$ was chosen arbitrarily. ∎

4. A practical comparison

We know from Section 3 that, for sufficiently large N,

$$g^*(p,N)^2 \leqslant \frac{1}{12} N \prod_{\ell \mid N} \left(1+\frac{1}{\ell}\right) \leqslant \frac{k_2}{12} N \prod_{\ell \mid N} \left(1+\frac{1}{\ell}\right), \quad (4.1)$$

in the context of Theorem 1.4. In this section we describe how large N has to be, given p, to ensure that

$$12 g^*(p,N)^2 \leqslant N \prod_{\ell \mid N} \left(1+\frac{1}{\ell}\right). \quad (4.2)$$

Fix $p \geqslant 5$, and let $\hat{N}$ be minimal such that if $N \geqslant \hat{N}$ then the inequality (4.2) holds. Our strategy will be to first establish a theoretical upper bound for $\hat{N}$, and then to determine $\hat{N}$ precisely using the software *Sage* [19]. Our theoretical upper bound is N_{r-1} in the following:

Theorem 4.1. *Assume GRH and let $p \geqslant 5$. Let $r = r(p)$ be minimal such that $N_{r-1} \geqslant 29.2032p^4(\log p)^4$, and suppose $N \geqslant N_{r-1}$. Then*

$$N \geqslant 12g^*(p,N)^2, \tag{4.3}$$

so in particular the inequality (4.2) *holds.*

To obtain this bound, we study the 'worst case scenario' $N = N_{r-1}$. Our bound in this situation is:

Proposition 4.2. *Assume GRH, let $p \geqslant 5$, and let r be a positive integer such that*

$$N_{r-1} \geqslant 29.2032p^4(\log p)^4. \tag{4.4}$$

Then

$$N_{r-1} \geqslant 12x_r^2. \tag{4.5}$$

4.1. The distribution of prime primitive roots modulo p, and more generally that of primes in arithmetic progression

In pursuit of Proposition 4.2, we study the distribution of prime primitive roots modulo p. Specifically, we seek an explicit lower bound for the counting function. As this task is of intrinsic interest, we now indulge in a discussion that goes slightly beyond what is strictly necessary for our purposes. For a more comprehensive review, see the introduction of [2]. Many of the results in this section can be generalised to composite moduli.

There are two main approaches to our task: (i) break the problem into $\varphi(p-1)$ primitive root residue classes modulo p and study the distribution of primes in arithmetic progression, or (ii) specifically use the primitive root property. The approach (ii) is currently superior for deriving upper bounds for the least prime primitive root modulo p, for instance (assuming the Riemann hypothesis for all Hecke characters) Shoup [17] uses sieve methods to provide the upper bound

$$O(r^4(\log r + 1)^4(\log p)^2), \tag{4.6}$$

where r is the number of distinct prime divisors of $p-1$; note the discussion following [15, Corollary 3.1].

It is difficult to understand the distribution of such primes via the approach (ii), so we focus on (i). There are many classical asymptotic results, such as the prime number theorem for arithmetic progressions. For the least prime in an arithmetic progression $a \mod p$, where p does not divide a, Linnik (see [13] and [14]) famously provided the upper bound

$$p^{O(1)}, \tag{4.7}$$

and the exponent can be 5.2 unconditionally, if the bound is multiplied by a constant (see [21]). Conditional results are much stronger, and the conjectured upper bound is p^2 (see [8]).

Bach and Sorenson [2] derived an explicit version of Linnik's theorem:

Theorem 4.3 (see [2, Theorem 5.3]). *Assume GRH. Let a and q be relatively prime positive integers. Then there exists $\ell \equiv a \mod q$ such that*

$$\ell < 2(q \log q)^2. \tag{4.8}$$

Summary of their approach. For (Dirichlet) characters χ modulo q, real numbers $x > 1$, and real numbers α, put

$$S(x, \chi) = \sum_{n<x} \Lambda(n)\chi(n)(n/x)^\alpha \log(x/n), \tag{4.9}$$

where Λ is the von Mangoldt function. Let a^{-1} denote the multiplicative inverse of a modulo q. By orthogonality,

$$\sum_{\chi \bmod q} \chi(a^{-1})S(x, \chi) = \varphi(q) \sum_{\substack{n<x \\ n \equiv a \bmod q}} \Lambda(n)(n/x)^\alpha \log(x/n). \tag{4.10}$$

Suppose there exist no primes $\ell < x$ that are congruent to a modulo q. Then

$$\sum_{\chi \bmod q} \chi(a^{-1})S(x, \chi) = p(x), \tag{4.11}$$

where $p(x)$ is the contribution of proper prime powers n to the right hand side of equation (4.10). For characters $\chi \mod q$, let $\hat{\chi}$ denote the primitive character induced by χ. Then

$$\Big| \sum_{\chi \bmod q} \chi(a^{-1})S(x, \hat{\chi}) \Big| \leqslant |i(x)| + p(x), \tag{4.12}$$

where

$$i(x) = \sum_{\chi \bmod q} \chi(a^{-1})(S(x, \hat{\chi}) - S(x, \chi)). \tag{4.13}$$

In [2, Subsection 4.1], tools from algebraic number theory and analytic number theory are used to bound $|i(x)|$ from above. In [2, Subsection 4.2], complex integration is used to estimate $|\sum_{\chi \bmod q} \chi(a^{-1})S(x, \hat{\chi})|$. In [2, Subsection 4.3], known estimates for a certain arithmetic function provide an upper bound for $p(x)$. In [2, Subsection 5.2], the cases $q \geqslant 1000$ and $q < 1000$ are considered separately. In the first case computer programs are used to choose x and α so that the inequality (4.12) is invalidated, thereby proving that some prime $\ell < x$ is congruent to a modulo q; the second case is handled by brute force. ■

If further details are sought then [1, special case (1) on p362] and the proof of [2, Corollary 3.4] describe our specific context within [2]. Note that [2, Theorem 5.3] assumes the generalisation of the Riemann hypothesis to all Hecke L-functions, whereas the statement of Theorem 4.3 merely assumes it for Dirichlet

L-functions. The stronger assumption is necessary for the more general results in [2], but only GRH is needed for [2, Theorem 5.3]. To justify this claim we use the notation of [2, Subsection 4.2], where Bach and Sorenson use the assumption for ζ_E and $L(\cdot, \hat{\chi})$. The latter is a Dirichlet L-function, since $K = \mathbb{Q}$ in our context, and the former is a product of Dirichlet L-functions (see [2, equation (2.2)]), since for our purposes $E = \mathbb{Q}(\zeta_q)$ is an abelian extension of $K = \mathbb{Q}$, where ζ_q is a primitive qth root of unity.

The constant 2 appears to have been chosen for simplicity. Following the proof of [2, Theorem 5.3], but not rounding up until the end, and insisting that $q > 2$, the constant 2 can be improved to 1.56:

Theorem 4.4. *Assume GRH. Let a and $q > 2$ be relatively prime integers. Then there exists $\ell \equiv a \mod q$ such that*

$$\ell < 1.56(q \log q)^2. \tag{4.14}$$

In fact the constant can be improved a little more (for $q > 2$), but our theoretical bound for $\hat{N}$ will serve only as a ceiling for brute force computation, so we satisfy ourselves with the constant 1.56.

4.2. A generalisation of Theorem 4.4

We seek not the least prime in an arithmetic progression but the distribution of such primes, so we provide the following corollary:

Corollary 4.5. *Assume GRH. Let a and $q > 2$ be relatively prime integers, and let t be a positive integer. Then*

$$\pi_{a,q}(1.56t^2q^{2t}(\log q)^2) \geqslant q^{t-1}. \tag{4.15}$$

Proof. For each $s = 0, 1, \ldots, q^{t-1} - 1$, there exists $\ell \equiv a + sq \mod q^t$ such that

$$\ell \leqslant 1.56t^2q^{2t}(\log q)^2, \tag{4.16}$$

by Theorem 4.4, since $(a + sq, q^t) = 1$. These ℓ are distinct and congruent to a modulo q. ∎

There are many ways in which to convert Corollary 4.5 into an explicit lower bound for $\pi_{a,q}(x)$ for all sufficiently large x; some are better asymptotically, while others do not require x to be as large. Since our theoretical upper bound for $\hat{N}$ will serve merely as a ceiling for machine calculations, we have executed this fairly arbitrarily, and there may be other ways to improve our bound:

Lemma 4.6. *Assume GRH. Let a and $q \geqslant 5$ be relatively prime integers, and let*

$$x \geqslant 6.24q^4(\log q)^2. \tag{4.17}$$

Then

$$\pi_{a,q}(x) > x^{1/9}. \tag{4.18}$$

Proof. Choose $t \geqslant 2$ such that

$$1.56t^2q^{2t}(\log q)^2 \leqslant x < 1.56(t+1)^2q^{2(t+1)}(\log q)^2. \tag{4.19}$$

By Corollary 4.5,

$$\pi_{a,q}(x) \geqslant \pi_{a,q}\left(1.56t^2q^{2t}(\log q)^2\right) \geqslant q^{t-1}. \tag{4.20}$$

Straightforward arithmetic confirms that $q^{t-1} > x^{1/9}$, completing the proof. ∎

By summing the bound (4.15) over the primitive root residue classes, we deduce:

Corollary 4.7. *Assume GRH, let $p > 2$, and let t be a positive integer. Then*

$$x_{\varphi(p-1)p^{t-1}} \leqslant 1.56t^2p^{2t}(\log p)^2. \tag{4.21}$$

4.3. Completion of the proof of Theorem 4.1

Now that we have an upper bound for the sequence (x_r), we formulate a crude upper bound for the sequence (N_r):

Lemma 4.8. *Let $p \geqslant 5$. Then*

$$N_{\varphi(p-1)} \geqslant (p+1)^{\varphi(p-1)/2}. \tag{4.22}$$

Proof. Let $g_1, \ldots, g_{\varphi(p-1)}$ be integer representatives for the primitive root residue classes modulo p, with

$$1 < g_1 < g_2 < \ldots < g_{\varphi(p-1)} < p. \tag{4.23}$$

These come in pairs of inverses modulo p, and no g_i can pair with itself because its order modulo p is $p-1 > 2$. The product of each pair is at least $p+1$, so

$$N_{\varphi(p-1)} = x_1 \cdots x_{\varphi(p-1)} \geqslant g_1 \cdots g_{\varphi(p-1)} \geqslant (p+1)^{\varphi(p-1)/2}. \tag{4.24}$$

∎

We show Proposition 4.2 by first establishing a weaker bound:

Proposition 4.9. *Assume GRH, let $p \geqslant 5$, and let r be a positive integer such that*

$$N_{r-1} \geqslant 467.2512p^8(\log p)^4. \tag{4.25}$$

Then $N_{r-1} \geqslant 12x_r^2$.

Proof. Proof by contradiction: assume that $N_{r-1} < 12x_r^2$. Then

$$x_r > 6.24p^4(\log p)^2, \tag{4.26}$$

so Lemma 4.6 gives

$$\pi_{a,p}(x_r) > x_r^{1/9} \tag{4.27}$$

for all integers a that are not divisible by p. Since r is the number of prime primitive roots modulo p that are less than or equal to x_r, summing the inequality (4.27) over all primitive root residue classes a modulo p yields

$$r > \varphi(p-1)x_r^{1/9}. \tag{4.28}$$

Now

$$N_{r-1} < 12x_r^2 < 12\left(\frac{r}{\varphi(p-1)}\right)^{18}. \tag{4.29}$$

Specialising $t = 2$ in Corollary 4.7 yields

$$x_{p\varphi(p-1)} \leqslant 6.24p^4(\log p)^2, \tag{4.30}$$

which together with the inequality (4.26) implies that $r > p\varphi(p-1)$. Induction shows that if $r > 44$ then $N_{r-1} \geqslant 12(0.5r)^{18}$ (use the product of the first $r-1$ primes as a crude lower bound for N_{r-1}), which would contradict the inequality (4.29). Hence $p\varphi(p-1) < r \leqslant 44$, so $p = 5, 7$. In each of these cases $10 < r \leqslant 44$ and $N_{10} > 12x_{44}^2$ (by computer check), completing the proof. ■

Finally we prove Proposition 4.2 and Theorem 4.1.

Proof of Proposition 4.2. First assume that $p \geqslant 71$. In this case it is easy to show, by considering cases, that $\varphi(p-1) \geqslant 24$. Specialising $t = 1$ in Corollary 4.7 yields

$$x_{\varphi(p-1)} \leqslant 1.56p^2(\log p)^2, \tag{4.31}$$

so the result follows immediately if $r \leqslant \varphi(p-1)$. However, if $r > \varphi(p-1)$ then, using Lemma 4.8,

$$N_{r-1} \geqslant N_{\varphi(p-1)} \geqslant (p+1)^{\varphi(p-1)/2} \geqslant (p+1)^{12} \geqslant 467.2512p^8(\log p)^4, \tag{4.32}$$

whereupon the result follows from Proposition 4.9.

For each p with $5 \leqslant p < 71$, there are very few values of r for which

$$29.2032p^4(\log p)^4 \leqslant N_{r-1} < 467.2512p^8(\log p)^4, \tag{4.33}$$

so we computer check these cases and apply Proposition 4.9 otherwise. ■

Proof of Theorem 4.1. Let $g^*(p, N) = x_s$, so that $N \geqslant N_{s-1}$, and put $t = \max(r, s)$. Then

$$N_{t-1} \geqslant N_{r-1} \geqslant 29.2032p^4(\log p)^4 \tag{4.34}$$

so, by Proposition 4.2, $N_{t-1} \geqslant 12x_t^2$. Now

$$N \geqslant N_{t-1} \geqslant 12x_t^2 \geqslant 12x_s^2 = 12g^*(p, N)^2. \tag{4.35}$$

■

4.4. Computation of $\hat{N}$ given p

Henceforth, let r be as in Theorem 4.1, and assume GRH. Now that we have a theoretical upper bound for $\hat{N}$, it is not too difficult to write a program that, given p, will compute $\hat{N}$ exactly. Still, it would be awfully slow to test the inequality (4.2) for every $N < N_{r-1}$, so we shall describe an economising manoeuvre based on the following observation:

Lemma 4.10. *Let t be a positive integer, and suppose that $N \geqslant 12x_t^2$ is such that the inequality* (4.2) *does not hold. Then N_t divides N.*

Proof. The hypotheses imply that $g^*(p, N) > x_t$, so N_t divides N. ∎

So we only need to test the inequality (4.2) for $N \leqslant 12x_1^2$ and for multiples of N_t in the range

$$\big[12x_t^2, 12x_{t+1}^2\big) \tag{4.36}$$

($t = 1, 2, \ldots, r-2$), since Lemma 4.10 and Theorem 4.1 imply that if $N \geqslant 12x_{r-1}^2$ then the inequality (4.2) holds.

There is a reasonable upper bound (4.31) for $x_{\varphi(p-1)}$, and hence for x_1, however in practice x_1 is very small. Moreover, for each t there are very few (if any) multiples of N_t in the range (4.36). Consequently, we have an extremely efficient method for determining $\hat{N}$ given p, and we could easily have done so for much larger p than discussed below. By running the program we conclude as follows:

Proposition 4.11. *For $p \geqslant 5$, the inequality* (4.2) *holds if $p < p^*$ and $N \geqslant N^*$ for the following pairs (p^*, N^*):*

$$\begin{array}{llll} (4243, 121424) & (2791, 81550) & (691, 48204) & (271, 44158) \\ (199, 38858) & (151, 24796) & (43, 9049) & (19, 5853). \end{array}$$

In particular, in any of these cases the bound in Theorem 1.4 becomes

$$\frac{k_2}{12} N \prod_{\ell \mid N} \left(1 + \frac{1}{\ell}\right). \tag{4.37}$$

These are best possible bounds for $\hat{N}$, since for each p we computed $\hat{N}$ exactly. One might wonder why $\hat{N}$ is so large. Indeed $g^*(p, N)$ is typically very small, however there are some values (small multiples of the N_t) for which $g^*(p, N)$ is somewhat large, which can mean that the inequality (4.2) suddenly fails.

5. The special cases $p = 2$ and $p = 3$

As the considerations in this section are not crucial to the main point of the paper, we do not recall here the algebro-geometric definition of modular forms due to Deligne and Katz. The interested reader is invited to consult [9] or [7].

For any prime p, the Hasse invariant A_p is a Katz modular form (mod p) of level one and weight $p-1$, with q-expansion

$$A_p(q) = 1.$$

As recalled in Section 2, if $p \geqslant 5$ then A_p can be obtained as the reduction modulo p of the Eisenstein series E_{p-1}. We say that E_{p-1} is a lifting of A_p to characteristic zero. If $p < 5$, we can still lift A_p to a form in characteristic zero, at the expense of increasing the level. We will use the following two results of Katz:

Theorem 5.1 (see [9, Theorem 1.7.1]). *Let k and N be positive integers such that either ($k = 1$ and $3 \leqslant N \leqslant 11$) or ($k \geqslant 2$ and $N \geqslant 3$). Let p be a prime not dividing N. Then every modular form (mod p) of weight k and level $\Gamma(N)$ can be lifted to characteristic zero.*

Theorem 5.2 (see [9, Theorem 1.8.1]). *Let k be a positive integer and let $p \neq 2$ be a prime. Every modular form (mod p) of weight k and level $\Gamma(2)$ can be lifted to characteristic zero.*

5.1. The case $p = 3$

- If N is a power of 3, we can use Theorem 5.2 to lift A_3 to $\tilde{A}_3$:

$$\begin{array}{ccccc} A_3 & \in & M_2(\mathrm{SL}_2(\mathbb{Z}); \overline{\mathbb{F}}_3) & \subset & M_2(\Gamma(2); \overline{\mathbb{F}}_3) \\ & & & & \wr \\ \tilde{A}_3 & & \in & & M_2(\Gamma(2); \overline{\mathbb{Z}}) \quad \subset \quad M_2(\Gamma_0(2), \mathrm{triv}; \overline{\mathbb{Z}}). \end{array}$$

  Going through the proof in Section 2 with E_{p-1} replaced by $\tilde{A}_3$, we have $f' = \tilde{A}_3^r f \in M_{k_2}(\Gamma_0(2N), \chi; \overline{\mathbb{Z}})$, so we must use the Sturm bound for $\Gamma_0(2N)$. Therefore the inequality in Theorem 1.4 must be replaced by

$$n \leqslant \max\left\{ g^*(p,N)^2, \frac{k_2}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2N)] \right\} \tag{5.1}$$

- If N is divisible by 2, the same process as in the previous part gives us the lifting $\tilde{A}_3 \in M_2(\Gamma_0(2), \mathrm{triv}; \overline{\mathbb{Z}})$. However, since 2 divides N, we obtain the exact same inequality as in Theorem 1.4.
- If N is divisible by a prime $p_0 \notin \{2, 3\}$, we can use Theorem 5.1 to lift

$$\begin{array}{ccccc} A_3 & \in & M_2(\mathrm{SL}_2(\mathbb{Z}); \overline{\mathbb{F}}_3) & \subset & M_2(\Gamma(p_0); \overline{\mathbb{F}}_3) \\ & & & & \wr \\ \tilde{A}_3 & & \in & & M_2(\Gamma(p_0); \overline{\mathbb{Z}}) \quad \subset \quad M_2(\Gamma_0(p_0), \mathrm{triv}; \overline{\mathbb{Z}}). \end{array}$$

  Since p_0 divides N, we again obtain the same inequality as in Theorem 1.4.

5.2. The case $p = 2$

- If N is not divisible by 5, 7 or 11, use Theorem 5.2 to lift A_2 to $\tilde{A}_2$:

$$\begin{array}{ccccc} A_2 & \in & M_1(\mathrm{SL}_2(\mathbb{Z}); \overline{\mathbb{F}}_2) & \subset & M_1(\Gamma(5); \overline{\mathbb{F}}_2) \\ & & & & \downarrow \\ \tilde{A}_2 & & \in & & M_1(\Gamma(5); \overline{\mathbb{Z}}) \quad \subset \quad M_1(\Gamma_0(5), \mathrm{triv}; \overline{\mathbb{Z}}). \end{array}$$

  The inequality in Theorem 1.4 must then be replaced by

$$n \leqslant \max\left\{ g^*(p,N)^2, \frac{k_2}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(5N)] \right\} \tag{5.2}$$

- If N is divisible by $p_0 \in \{5, 7, 11\}$, use Theorem 5.1 to lift

$$\begin{array}{ccccc} A_2 & \in & M_1(\mathrm{SL}_2(\mathbb{Z}); \overline{\mathbb{F}}_2) & \subset & M_1(\Gamma(p_0); \overline{\mathbb{F}}_2) \\ & & & & \downarrow \\ \tilde{A}_2 & & \in & & M_1(\Gamma(p_0); \overline{\mathbb{Z}}) \quad \subset \quad M_1(\Gamma_0(p_0), \mathrm{triv}; \overline{\mathbb{Z}}). \end{array}$$

  Since p_0 divides N, we get the same inequality as in Theorem 1.4.

We summarise our findings in Table 1. (The third column gives the subgroup index that has to be used in the inequality of Theorem 1.4 in each case.)

Table 1. Inequalities obtained for the various combinations of p and N

Prime	Level	Inequality in Theorem 1.4
$p \geqslant 5$	$N \geqslant 1$	
$p = 3$	$N \neq 3^a$, some a	$n \leqslant \max\{\ldots [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]\}$
$p = 2$	N divisible by 5, 7 or 11	
$p = 3$	$N = 3^a$, some a	$n \leqslant \max\{\ldots [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2N)]\}$
$p = 2$	N not divisible by 5, 7 or 11	$n \leqslant \max\{\ldots [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(5N)]\}$

Acknowledgements. We thank James Withers for several fruitful discussions and observations. We thank M. Ram Murty and David Loeffler for some useful comments. The first author was supported by the Elizabeth and Vernon Puzey scholarship, and is grateful towards the University of Melbourne for their hospitality while preparing this memoir. The second author was supported by Discovery Grant DP120101942 from the Australian Research Council.

References

[1] E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380.

[2] E. Bach and J. Sorenson, *Explicit bounds for primes in residue classes*, Mathematics of Computation **65** (1996), 1717–1735.
[3] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, 1966.
[4] F. Diamond and J. Shurman, *A first course in modular forms*, Springer, 2005.
[5] A. Ghitza, *Distinguishing Hecke eigenforms*, International Journal of Number Theory **7** (2011), 1247–1253.
[6] D. Goldfeld and J. Hoffstein, *On the number of terms that determine a modular form*, Contemp. Math., AMS, **143** (1993), 385–393.
[7] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Mathematical Journal **61** (1990), no. 2, 445–517.
[8] D.R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proceedings of the London Mathematical Society **64** (1992), no. 3, 265–338.
[9] N. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Mathematics **350** (1973), Springer-Verlag, 69–190.
[10] L. Kilford, *Modular Forms: A classical and computational introduction*, Imperial College Press, 2008.
[11] W. Kohnen, *On Fourier coefficients of modular forms of different weights*, Acta Arithmetica **113** (2004), no. 1, 57–67.
[12] E. Kowalski, *Variants of recognition problems for modular forms*, Archiv der Mathematik **84** (2005), no. 1, 57–70.
[13] U.V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. (Mat. Sbornik) N.S., **15 (57)** (1944), 139–178.
[14] U.V. Linnik, *On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon*, Rec. Math. (Mat. Sbornik) N.S., **15 (57)** (1944), 347–368.
[15] G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arithmetica **80** (1997), no. 3, 277–288.
[16] M. Ram Murty, *Congruences between modular forms*, London Mathematical Society Lecture Note Series **247** (1997), Cambridge University Press, 309–320.
[17] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), 369–380.
[18] W. Stein, *Modular Forms, a Computational Approach*, Graduate Studies in Mathematics **79**, American Mathematical Society, 2007. With an appendix by Paul E. Gunnells.
[19] W. Stein et al., Sage Mathematics Software (Version 5.1), The Sage Development Team, 2012, http://www.sagemath.org.
[20] J. Sturm, *On the congruence of modular forms*, Lecture Notes in Mathematics **1240** (1987), Springer-Verlag, 275–280.
[21] T. Xylouris, *On Linnik's constant*, Acta Arithmetica **150** (2011), no. 1, 65–91.

Addresses: Sam Chow: Department of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom;
Alexandru Ghitza: Department of Mathematics and Statistics, University of Melbourne, Parkville VIC 3010, Australia.

E-mail: sam.chow42@gmail.com, aghitza@alum.mit.edu

Received: 8 August 2013