Canad. J. Math. Vol. **57** (3), 2005 pp. 449–470

On the Sizes of Gaps in the Fourier Expansion of Modular Forms

Emre Alkan

Abstract. Let $f = \sum_{n=1}^{\infty} a_f(n)q^n$ be a cusp form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. For $n \geq 1$, let

$$i_f(n) = \begin{cases} \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\} & \text{if } a_f(n) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Concerning bounded values of $i_f(n)$ we prove that for $\epsilon > 0$ there exists $M = M(\epsilon, f)$ such that $\#\{n \leq x : i_f(n) \leq M\} \geq (1-\epsilon)x$. Using results of Wu, we show that if f is a weight 2 cusp form for an elliptic curve without complex multiplication, then $i_f(n) \ll_{f,\epsilon} n^{\frac{51}{134}+\epsilon}$. Using a result of David and Pappalardi, we improve the exponent to $\frac{1}{3}$ for almost all newforms associated to elliptic curves without complex multiplication. Inspired by a classical paper of Selberg, we also investigate $i_f(n)$ on the average using well known bounds on the Riemann Zeta function.

1 Introduction

Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ ($q = e^{2\pi i z}$, $\mathrm{Im}(z) > 0$) be a cusp form with integer weight $k \geq 2$ which is not a linear combination of forms with complex multiplication. To estimate the size of possible gaps in the Fourier expansion of $f(z)$, Serre introduced the gap function

$$(1) \qquad i_f(n) = \begin{cases} \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\} & \text{if } a_f(n) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

(Here one could alternatively define $i_f(n) = 1 + \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\}$ if $a_f(n) = 0$. This definition has the advantage that one can see $a_f(n) \neq 0$ for all n if and only if $i_f(n) = 0$ for all n. Nevertheless, this would have no effect on any of our results, so for simplicity we will use (1) as our definition of the gap function). He proved [12] that

$$i_f(n) \ll_f n.$$

The Rankin–Selberg asymptotic formula (see [10])

$$\sum_{n \leq x} \frac{|a_f(n)|^2}{n^{k-1}} = c_f x + O\left(x^{\frac{3}{5}}\right)$$

Received by the editors May 14, 2003; revised March 25, 2004.
AMS subject classification: 11F30.

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

clearly implies the sharper estimate

$$i_f(n) \ll_f n^{\frac{3}{5}}.$$

However using local methods such as sieve arguments with weights, it is possible to make substantial improvements on the exponent $\frac{3}{5}$. Using this type of an approach, the author [1] recently proved that

$$i_f(n) \ll_{f,\phi} \phi(n)$$

for almost all n, where ϕ is essentially any function tending monotonically to infinity (such as $\phi(x) = \log\log x$). This shows that most of the time the possible gaps are extremely short. Another interesting question about these gaps is to find a lower bound for the number of $n \leq x$ with $i_f(n) \leq M$ where M is a large integer. Here we prove the following on this question:

Theorem 1 *Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be a nonzero cusp form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. If $\epsilon > 0$, then there exists $M = M(\epsilon, f)$ such that*

$$\#\{n \leq x : i_f(n) \leq M\} \geq (1-\epsilon)x.$$

Elkies [5] proved the existence of infinitely many supersingular primes for an elliptic curve $E/\mathbb{Q}$ without complex multiplication. This is equivalent to the fact that the set

$$B_E = \{p \ \text{ prime } : a_E(p) = 0\} \tag{2}$$

is infinite, where

$$f_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n$$

is the weight 2 newform associated to the Hasse–Weil L-function of this elliptic curve. It is well known that the Fourier coefficients $a_E(n)$ form a multiplicative function. Using this fact, let us briefly see that $\limsup i_{f_E}(n) = \infty$. Let $p_0 < p_1 < \cdots < p_m < \cdots$ be the sequence of supersingular primes of E. By the Chinese Remainder theorem, we can find n such that $n \equiv p_j - j \pmod{p_j^2}$ for $0 \leq j \leq m$. Hence $n + j$ is divisible by p_j but not by p_j^2 so that $a_E(n + j) = a_E(p_j)a_E((n + j)/p_j) = 0$ for $0 \leq j \leq m$. This shows that we can find arbitrarily large gaps in the Fourier expansion of $f_E(z)$. Hence there is a sequence n_i such that $i_{f_E}(n_i)$ is monotonically tending to infinity. We might expect this sequence to be quite sparse. Our next results will give quantitative estimates on the number of terms of this sequence that are $\leq x$.

Theorem 2 *Let $f(z) \in S_k(\Gamma_0(N), \chi)$ be a newform of weight $k \geq 2$ without complex multiplication and let $\phi(n)$ be a strictly increasing sequence of positive integers. If $\epsilon > 0$, then*

$$\#\{n \leq x : i_f(n) = \phi(n)\} \ll_{f,\phi,\epsilon} \frac{x}{\phi(\sqrt{x})(\log\log\phi(\sqrt{x}))^{1-\epsilon}} + \sqrt{x}.$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

For $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$, let us define

$$B = \{p \text{ prime } : a_f(p) = 0\} \tag{3}$$

and

$$B(x) = \#\{p \le x \text{ prime } : p \in B\}. \tag{4}$$

Assuming a mild condition on the set B, it is possible to improve considerably the estimate in Theorem 2.

Theorem 3 *Let $f(z)$ and $\phi(n)$ be as in Theorem 2. If*

$$\sum_{r \in B} \frac{1}{r} \le \frac{1}{4},$$

then for every $\epsilon > 0$ we have

$$\#\{n \le x : i_f(n) = \phi(n)\} \ll_{f,\phi,\epsilon} \frac{x}{\phi(\sqrt{x})(\log \phi(\sqrt{x}))^{1-\epsilon}} + \sqrt{x}.$$

We also note that at the other extreme, Lehmer's Conjecture says that $\tau(n) \neq 0$ for all n where

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n = q\prod_{n=1}^{\infty}(1 - q^n)^{24}$$

is the unique normalized cusp form of weight 12 on $SL_2(\mathbb{Z})$. Hence in terms of the gap function, Lehmer's Conjecture says that $i_\Delta(n) = 0$ for all n, so that in this case the gap function is conjectured to be as small as it can be unlike the elliptic curve case.

Using a result of Fouvry and Iwaniec [7] and improving on work of Balog and Ono [2], the author proved [1] that for every $\epsilon > 0$,

$$i_{f_E}(n) \ll_{E,\epsilon} n^{\frac{69}{169}+\epsilon}$$

for a weight 2 newform $f_E(z)$ associated to $E/\mathbb{Q}$ without complex multiplication. More generally, it was shown that the Generalized Riemann Hypothesis for Dedekind Zeta functions imply the same bound for a general nonzero cusp form of weight $k \ge 2$ which is not a linear combination of forms with complex multiplication. Here we improve these results using work by Wu [18] and Sargos and Wu [14].

Theorem 4

(i) *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. For every $\epsilon > 0$ and $x^{\frac{51}{134}+\epsilon} \le y$ we have*

$$\#\{x - y < n \le x : a_E(n) \neq 0\} \gg_{E,\epsilon} y.$$

In particular, $i_{f_E}(n) \ll_{E,\epsilon} n^{\frac{51}{134}+\epsilon}$.

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

(ii) *Let $f(z)$ be as in Theorem 1. Assuming the Generalized Riemann Hypothesis for Dedekind Zeta functions, for every $\epsilon > 0$ and $x^{\frac{51}{134}+\epsilon} \le y$ we have*

$$\#\{x - y < n \le x \,:\, a_f(n) \ne 0\} \gg_{f,\epsilon} y.$$

In particular, $i_f(n) \ll_{f,\epsilon} n^{\frac{51}{134}+\epsilon}$.

Theorem 5 *Let $f(z)$ be as in Theorem 1. For every $\epsilon > 0$ and $x^{\frac{40}{97}+\epsilon} \le y$ we have*

$$\#\{x - y < n \le x : a_f(n) \ne 0\} \gg_{f,\epsilon} y.$$

In particular, $i_f(n) \ll_{f,\epsilon} n^{\frac{40}{97}+\epsilon}$.

Using a result of David and Pappalardi [3], we can further improve the exponent in the above theorems to $\frac{1}{3}$ for almost all newforms associated to elliptic curves without complex multiplication whose coefficients are in a large rectangle.

Theorem 6 *Consider the family of elliptic curves*

$$E(a, b) : v^2 = u^3 + au + b$$

without complex multiplication where a and b are integers with $|a| \le A$, $|b| \le D$. Let

$$f_{E(a,b)}(z) = \sum_{n=1}^{\infty} a_{E(a,b)}(n) q^n$$

be the weight 2 newform associated to $E(a, b)$. Let X be a parameter tending to infinity such that both A and D are $> X^{2+\lambda}$ for some $\lambda > 0$. Then for every $\epsilon > 0$ and $x^{\frac{1}{3}+\epsilon} \le y$ we have

$$\#\{x - y < n \le x : a_{E(a,b)}(n) \ne 0\} \gg_{E(a,b),\epsilon} y$$

with at most

$$O\Big(\frac{AD}{(\log X)^c}\Big)$$

exceptions of $E(a, b)$. In particular, for these $E(a, b)$ we have $i_{f_{E(a,b)}}(n) \ll_{E(a,b),\epsilon} n^{\frac{1}{3}+\epsilon}$. Here $c > 0$ is arbitrary and the O constant depends only on c.

Our final results give good upper bounds on the average value of $i_f(n)$ when ρ is very close to $\frac{1}{2}$. Here ρ measures the sparseness of the primes in B (see Theorem 7 below). In particular, we obtain quantitative estimates on the problem of the frequency of large values of $i_f(n)$.

Theorem 7 *Let $f(z) \in S_k(\Gamma_0(N), \chi)$ be a newform of weight $k \ge 2$ without complex multiplication. If $B(x) \ll x^\rho$ for some $\frac{1}{2} \le \rho < 1$, then*

$$\frac{1}{x} \sum_{n \le x} i_f(n) \ll_{f,\rho} x^{8\rho-4} e^{\frac{8 \log x}{\log\log x}}.$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

If $f(z)$ is a newform in $S_k(\Gamma_0(N),\chi)$, then $a_f(n)$ is nonzero when n is square-free and B-free. It is known by the work of Serre [12] that $\sum_{p\in B}\frac{1}{p}$ is finite. Assuming this as a general hypothesis, Erdős [4] was the first to define B-free numbers as a natural generalization of square-free numbers. He conjectured that $q_{n+1}-q_n \ll_\epsilon q_n^\epsilon$ for $\epsilon > 0$ arbitrarily small where q_n is the sequence of B-free numbers. About this conjecture the best short interval result is due to Sargos and Wu [14], who proved that

$$q_{n+1} - q_n \ll_\epsilon q_n^{\frac{40}{97}+\epsilon}$$

by using deep analytic estimates on exponential sums improving on earlier work of Fouvry and Iwaniec [7]. In the case of square-free numbers the best result is due to Filaseta and Trifonov [8], who proved that $r_{n+1} - r_n \ll_\epsilon r_n^{1/5+\epsilon}$ where r_n is the sequence of square-free numbers. We should also mention that Granville [9] has shown $r_{n+1} - r_n \ll_\epsilon r_n^\epsilon$ for arbitrarily small $\epsilon > 0$, assuming the abc-Conjecture. Note that Erdős' Conjecture would immediately imply that $i_f(n) \ll_{f,\epsilon} n^\epsilon$ for arbitrarily small $\epsilon > 0$. Our next result shows that this holds on the average for almost all newforms associated to elliptic curves $E(a,b)$ over $\mathbb{Q}$ without complex multiplication. In fact we obtain a slightly stronger result on the average.

Corollary 8 *Let $f_{E(a,b)}(z)$ be as in Theorem 6. If $A, D > X^{2+\lambda}$ with $\lambda > 0$, then we have*

$$\frac{1}{x}\sum_{n\leq x} i_{f_{E(a,b)}}(n) \ll_{E(a,b)} e^{\frac{8\log x}{\log\log x}} \ll_\epsilon x^\epsilon$$

for arbitrarily small $\epsilon > 0$ with at most

$$O\Big(\frac{AD}{(\log X)^c}\Big)$$

exceptions of $E(a,b)$. Here $c > 0$ is arbitrary and the O constant depends only on c.

We observe that for those $E(a,b)$ of Corollary 8, the number of $\frac{x}{2} < n \leq x$ satisfying $i_{f_{E(a,b)}}(n) \gg n^\epsilon$ is

$$O\big(x^{1-\epsilon} e^{\frac{8\log x}{\log\log x}}\big)$$

where $\epsilon > 0$ can be arbitrarily small. Finding upper bounds for the frequency of large values of $i_f(n)$ for a general newform $f(z)$ without complex multiplication is an interesting problem. Let us briefly discuss a heuristic about this problem. Let q_m be the sequence of square-free and B-free numbers where B is defined as in (3). From [1] we know that

$$\sum_{\substack{n\leq x\\ i_f(n)>\log n}} 1 = o(x).$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

If $q_{m-1} < n \le q_m$, then $i_f(n) \le q_m - q_{m-1}$. Since there is always a square-free and B-free number between $x - \sqrt{x}$ and x, it follows that

$$\sum_{\substack{n\le x\\ i_f(n)>\log n}} 1 \ll \sqrt{x} + \sum_{q_m\le x}\ \sum_{\substack{q_{m-1}<n\le q_m\\ i_f(n)>\log n}} 1 \ll \sqrt{x} + \sum_{\sqrt{x}<q_{m-1}<q_m\le x}\ \sum_{\substack{q_{m-1}<n\le q_m\\ i_f(n)>\log n}} \frac{i_f(n)}{\log n}$$

$$\ll \sqrt{x} + \frac{1}{\log x} \sum_{\substack{\sqrt{x}<q_{m-1}<q_m\le x\\ q_m-q_{m-1}>\frac{1}{2}\log x}}\ \sum_{q_{m-1}<n\le q_m} (q_m - q_{m-1})$$

$$\ll \sqrt{x} + \frac{1}{\log x} \sum_{\substack{q_m\le x\\ q_m-q_{m-1}>\frac{1}{2}\log x}} (q_m - q_{m-1})^2.$$

Note that square-free and B-free numbers have positive density so that we might expect

$$\sum_{\substack{q_m\le x\\ q_m-q_{m-1}>\frac{1}{2}\log x}} (q_m - q_{m-1})^2 \ll \sum_{q_m\le x} (q_m - q_{m-1})^2 \ll x.$$

Consequently we expect that (clearly this is not the best possible upper bound since we estimated crudely at each step)

$$\sum_{\substack{n\le x\\ i_f(n)>\log n}} 1 \ll \frac{x}{\log x}.$$

2 Proof of Theorems 1,2 and 3

Before presenting the proofs let us start with an observation which reduces most of the arguments to the case where $f(z)$ is a newform. Henceforth we may assume in some of the proofs without loss of generality that $f(z)$ is a newform. Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is an integer weight form in $S_k(\Gamma_0(N), \chi)$ with weight $k \ge 2$ which is not a linear combination of forms with complex multiplication. If p is prime, then the Hecke operators T_p are defined by

$$T_p \mid f(z) = \sum_{n=1}^{\infty} \big(a_f(pn) + \chi(p)p^{k-1}a_f(n/p)\big)\, q^n.$$

Let $g_1(z), g_2(z), \dots, g_s(z)$ be a list of all weight k newforms with levels dividing N. Also let

$$g_i(z) = \sum_{n=1}^{\infty} b_i(n)q^n$$

be the Fourier expansion of $g_i(z)$. Note that if p is a prime not dividing N, then we have

$$T_p \mid g_i(z) = b_i(p)g_i(z).$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

By the principle of multiplicity one, we can find infinitely many primes p such that $b_i(p) \neq b_j(p)$ when $i \neq j$. Since newforms span the whole space we have

$$0 \neq f(z) = \sum_{i=1}^{s} \sum_{\delta | N} \alpha_{i,\delta}\, g_i(\delta z).$$

Without loss of generality we may assume that $\alpha_{1,\delta_1} \neq 0$ where δ_1 is the smallest such divisor of N (*i.e.*, we are assuming that $g_1(z)$ is a nonzero newform). Next we choose p_1 prime not dividing N such that $b_1(p_1) \neq b_2(p_1)$. Then we have

$$(T_{p_1} \mid f(z)) - b_2(p_1) f(z) = \sum_{i=1}^{s} (b_i(p_1) - b_2(p_1)) \sum_{\delta | N} \alpha_{i,\delta}\, g_i(\delta z).$$

This clearly eliminates all terms involving $g_2(\delta z)$. In this way we get

$$f_1(z) = \sum_{n=1}^{\infty} a_1(n) q^n$$

where

$$a_1(n) = a_f(p_1 n) + \chi(p_1) p_1^{k-1} a_f(n/p_1) - b_2(p_1) a_f(n).$$

Continuing in this way we can remove all newform components $g_i(\delta z)$ for $2 \leq i \leq s$ to get

$$F(z) = \sum_{n=1}^{\infty} A(n) q^n = \sum_{\delta | N} \alpha_{1,\delta}\, g_1(\delta z)$$

in $S_k(\Gamma_0(N), \chi)$ where

$$A(n) = \sum_{\delta | N} \alpha_{1,\delta}\, b_1\left(\frac{n}{\delta}\right) = \sum_{j} \beta_j a_f(\omega_j n).$$

In the above formula for $A(n)$ the sum on j is a finite sum and for each j, β_j is an algebraic number and ω_j is a rational number. Applying the shift operator U_{δ_1} we get

$$U_{\delta_1} F(z) = F^*(z) = \sum_{n=1}^{\infty} A^*(n) q^n \in S_k(\Gamma_0(N), \chi)$$

where $A^*(n) = A(\delta_1 n)$. Let S_1 be the set of primes dividing N together with the set of primes p such that $b_1(p) = 0$. Let N_{S_1} be the set of square-free numbers with no prime divisors in S_1. If $n \in N_{S_1}$, then by minimality of δ_1 we get

$$A^*(n) = \alpha_{1,\delta_1} b_1(n) = \sum_{j} \beta_j\, a_f(\omega_j \delta_1 n)$$

so that $b_1(n) \neq 0$ implies $a_f(\omega_j \delta_1 n) \neq 0$ for some j. This establishes a finite-to-one correspondence between nonvanishing Fourier coefficients of $g_1(z)$ and $f(z)$. Note that reduction to newforms in this way will effect only the constants in our asymptotic estimates and will be harmless.

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

Proof of Theorem 1 Without loss of generality we may assume that

$$f(z)=\sum_{n=1}^{\infty} a_f(n)q^n$$

is a newform. If n is square-free, then

$$a_f(n)=\prod_{p|n} a_f(p)$$

so that $a_f(n)\neq 0$ when n is square-free and B-free where B is defined as in (3). Let A be the set of primes in B together with squares of primes not in B. Consider

$$\sum_{\substack{n-M<m\leq n\\ m \text{ is } A\text{-free}}} 1 \geq \sum_{\substack{n-M<m\leq n\\ m\not\equiv 0 \pmod{b_s}\\ \text{for all } s\leq r}} 1 - \sum_{\substack{n-M<m\leq n\\ b_r<b_s\leq M\\ m\equiv 0 \pmod{b_s}\\ \text{for some } s>r}} 1 - \sum_{\substack{n-M<m\leq n\\ M<b_s\leq n\\ m\equiv 0 \pmod{b_s}\\ \text{for some } s>r}} 1 \tag{5}$$

where $b_1, b_2, \dots$ are elements of A in increasing order. The value of the parameter r in (5) will be fixed soon. The number of $n-M<m\leq n$ that are divisible by b_s is

$$\left[\frac{n}{b_s}\right]-\left[\frac{n-M}{b_s}\right]=\frac{M}{b_s}+r_{b_s}(n,M)$$

where $r_{b_s}(n,M)$ is a remainder term and $|r_{b_s}(n,M)|\leq 1$. By the Inclusion-Exclusion principle

$$\sum_{\substack{n-M<m\leq n\\ m\not\equiv 0 \pmod{b_s}\\ \text{for all } s\leq r}} 1 = M\prod_{s=1}^{r}\Bigl(1-\frac{1}{b_s}\Bigr)+R_A(n,M)$$

where $R_A(n,M)$ is the sum of 2^r remainder terms so that $|R_A(n,M)|\leq 2^r$. It is known from [12] that $\sum_{p\in B}\frac{1}{p}$ is finite. Hence $\sum_{s=1}^{\infty}\frac{1}{b_s}$ is finite and we may put $C_A=\prod_{s=1}^{\infty}\bigl(1-\frac{1}{b_s}\bigr)>0$. Next we note that

$$\sum_{\substack{n-M<m\leq n\\ b_r<b_s\leq M\\ m\equiv 0 \pmod{b_s}\\ \text{for some } s>r}} 1 \leq 2M\sum_{s=r+1}^{\infty}\frac{1}{b_s}. \tag{6}$$

Now we may fix r large enough so that $C=C_A-2\sum_{s=r+1}^{\infty}\frac{1}{b_s}>0$. Note that this choice of r depends on B and hence on $f(z)$. We will estimate the last error term in (5) where $M<b_s\leq n$ on the average. To this end we consider

$$\sum_{T<n<2T}\ \sum_{\substack{n-M<m\leq n\\ M<b_s\leq n\\ m\equiv 0 \pmod{b_s}\\ \text{for some } s>r}} 1$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

where T is a large enough parameter. Changing the order of summation, this double sum is easily seen to be $\ll MT\sum_{b_s>M}\frac{1}{b_s}$, so that

$$\sum_{\substack{n-M<m\leq n\\ M<b_s\leq n\\ m\equiv 0 \pmod{b_s}\\ \text{for some } s>r}} 1 \;\leq \frac{C}{2}M \tag{7}$$

except for a subset of $(T,2T)$ of cardinality $O\bigl(T\sum_{b_s>M}\frac{1}{b_s}\bigr)$. Using a dyadic argument, the total number of exceptions $\leq T$ is again $O\bigl(T\sum_{b_s>M}\frac{1}{b_s}\bigr)$. Hence combining (5), (6) and (7) we get that

$$\sum_{\substack{n-M<m\leq n\\ m \text{ is } A\text{-free}}} 1 \geq \frac{C}{2}M + R_A(n,M)$$

where $|R_A(n,M)| \leq 2^r$ independently of M and the number of exceptions in $(1,x)$ is at most $O\bigl(x\sum_{b_s>M}\frac{1}{b_s}\bigr)$. Finally choosing $M = M(\epsilon, f)$ large enough the number of exceptions is $\leq \epsilon x$ and

$$\#\Bigl\{ n\leq x : \sum_{\substack{n-M<m\leq n\\ m \text{ is } A\text{-free}}} 1 \;>\; 0\Bigr\} \geq (1-\epsilon)x.$$

This completes the proof of Theorem 1. ■

Proof of Theorem 2 Let B be defined as in (3) and let q_s be the sequence of square-free and B-free numbers. Note that if $q_{s-1} < n \leq q_s$ and $i_f(n) = \phi(n)$ then $\phi(q_{s-1}) < \phi(n) = i_f(n) \leq q_s - q_{s-1}$ since $a_f(q_s) \neq 0$. Moreover $i_f(n+j) = i_f(n) - j < \phi(n) < \phi(n+j)$ for $1 \leq j \leq \phi(n)$. Hence for each $q_{s-1} < n \leq q_s$ such that $i_f(n) = \phi(n)$ there are at least $\phi(n)$ consecutive numbers u such that $i_f(u) \neq \phi(u)$. It follows that

$$\begin{aligned}\sum_{\substack{n\leq x\\ i_f(n)=\phi(n)}} 1 &\ll \sqrt{x} + \sum_{\sqrt{x}<q_{s-1}<q_s\leq x}\; \sum_{\substack{q_{s-1}<n\leq q_s\\ i_f(n)=\phi(n)}} 1 \\ &\ll \sqrt{x} + \sum_{\substack{\sqrt{x}<q_{s-1}<q_s\leq x\\ q_s-q_{s-1}>\phi(q_{s-1})}} \frac{q_s-q_{s-1}}{\phi(q_{s-1})} \\ &\ll_\phi \sqrt{x} + \frac{1}{\phi(\sqrt{x})} \sum_{\substack{q_s\leq x\\ q_s-q_{s-1}>\phi(\sqrt{x})}} (q_s-q_{s-1})\end{aligned} \tag{8}$$

by the fact that ϕ is increasing. By the sieve of Eratosthenes, for some $0<c<1$, there are at most $c(q_s-q_{s-1})$ numbers in (q_{s-1},q_s) which are not divisible either

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

by p^2, p prime and $p \leq \log \phi(\sqrt{x})$ or by $r \in B$ and $r \leq \log \phi(\sqrt{x})$. Since there are no square-free and B-free numbers in (q_{s-1}, q_s), it follows that there are at least $(1-c)(q_s - q_{s-1})$ numbers in (q_{s-1}, q_s) divisible either by p^2 and $p > \log \phi(\sqrt{x})$ or $r \in B$ and $r > \log \phi(\sqrt{x})$. This gives

$$\sum_{\substack{q_s \leq x \\ q_s - q_{s-1} > \phi(\sqrt{x})}} (q_s - q_{s-1}) \ll \Big(\sum_{p > \log \phi(\sqrt{x})} \frac{1}{p^2} + \sum_{r > \log \phi(\sqrt{x})} \frac{1}{r} \Big) x. \tag{9}$$

Clearly we have

$$\sum_{p > \log \phi(\sqrt{x})} \frac{1}{p^2} \ll \frac{1}{\log \phi(\sqrt{x})} \tag{10}$$

and if r_m is the mth prime in B, then we know from D. Wan's work on the Lang–Trotter Conjecture [17] that $r_m \gg_{f,\epsilon} m(\log m)^{2-\epsilon}$ where $\epsilon > 0$ can be arbitrarily small (one can alternatively use an improvement of K. Murty [11] on r_m to obtain a slightly better result). This gives

$$\begin{aligned} \sum_{r > \log \phi(\sqrt{x})} \frac{1}{r} &\ll_{f,\phi,\epsilon} \sum_{m \gg \frac{\log \phi(\sqrt{x})}{(\log \log \phi(\sqrt{x}))^{2-\epsilon}}} \frac{1}{m(\log m)^{2-\epsilon}} + \sum_{m \ll \frac{\log \phi(\sqrt{x})}{(\log \log \phi(\sqrt{x}))^{2-\epsilon}}} \frac{1}{\log \phi(\sqrt{x})} \\ &\ll_{f,\phi,\epsilon} \frac{1}{(\log \log \phi(\sqrt{x}))^{1-\epsilon}}. \end{aligned} \tag{11}$$

Combining (8), (9), (10) and (11) we complete the proof of Theorem 2. ■

Proof of Theorem 3 We proceed similarly as in the proof of Theorem 2. The number of integers in (q_{s-1}, q_s) which are divisible either by p^2, p prime and $p \leq c\,\phi(\sqrt{x}) \log \phi(\sqrt{x})$ or $r \in B$, $r \leq c\phi(\sqrt{x}) \log \phi(\sqrt{x})$ $(0 < c < 1)$ is at most

$$\begin{aligned} \pi\big(c\phi(\sqrt{x}) \log \phi(\sqrt{x})\big) &+ \sum_{p \leq c\phi(\sqrt{x}) \log \phi(\sqrt{x})} \frac{(q_s - q_{s-1})}{p^2} \\ &+ B\big(c\,\phi(\sqrt{x}) \log \phi(\sqrt{x})\big) + \sum_{r \leq c\ \phi(\sqrt{x}) \log \phi(\sqrt{x})} \frac{(q_s - q_{s-1})}{r} \end{aligned} \tag{12}$$

where $\pi(x)$ is the number of primes $\leq x$ and $B(x)$ is defined as in (4). Note that $\pi(x) = O\big(\frac{x}{\log x}\big)$ and $B(x) = o\big(\frac{x}{\log x}\big)$. Hence if x is large and c is small enough we have

$$B(c\,\phi(\sqrt{x}) \log \phi(\sqrt{x})) = o(\phi(\sqrt{x}))$$

and

$$\pi(c\,\phi(\sqrt{x}) \log \phi(\sqrt{x})) < \eta\phi(\sqrt{x})$$

where

$$\eta < 1 - \sum_p \frac{1}{p^2} - \sum_{r \in B} \frac{1}{r}.$$

Note that such an $\eta > 0$ exists since it is easy to check that

$$\sum_p \frac{1}{p^2} < \frac{3}{4}$$

and by assumption

$$\sum_{r \in B} \frac{1}{r} \leq \frac{1}{4}.$$

Again using the estimate for r_m from [17] we see for every $\epsilon > 0$ that

$$\left(\sum_{p > c\ \phi(\sqrt{x}) \log \phi(\sqrt{x})} \frac{1}{p^2} + \sum_{r > c\ \phi(\sqrt{x}) \log \phi(\sqrt{x})} \frac{1}{r} \right) x \ll_{f,\phi,\epsilon} \frac{x}{(\log \phi(\sqrt{x}))^{1-\epsilon}}. \tag{13}$$

Combining (12) and (13) and summing over all $q_s \leq x$ such that $q_s - q_{s-1} > \phi(\sqrt{x})$ completes the proof of Theorem 3. ■

3 Proof of Theorems 4, 5 and 6

Proof of Theorem 4 (i) Let

$$f_E(z) = \sum_{n=1}^{\infty} a_E(n) q^n$$

be the weight 2 newform associated to $E/\mathbb{Q}$ without complex multiplication. Recall that a prime p not dividing the conductor N_E of $E/\mathbb{Q}$ is a supersingular prime if and only if $a_E(p) = 0$. Elkies [6] proved that

$$\#\{p \leq x : a_E(p) = 0\} \ll_E x^{\frac{3}{4}}.$$

As before $a_E(n) \neq 0$ when n is square-free and B_E-free where B_E is defined as in (2). Hence it suffices to show that

$$\#\{x - y < n \leq x : n \text{ is } A\text{-free }\} \gg_{E,\epsilon} y$$

for $y = x^\theta, \theta > \frac{51}{134}$ where A is the set of primes in B_E together with squares of primes not in B_E. We define

$$M = M(x, \delta_1, \mu) = \{x^{\delta_1} < m < x^{\delta_1 + \mu} : p | m \text{ is prime then } p \geq x^\eta\}$$

and

$$P = P(x, \delta_2, \mu) = \{x^{\delta_2} < p < x^{\delta_2 + \mu} : p \text{ is prime}\}$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

where $\delta_2 + \mu < \delta_1$, $\delta_1 + 2\mu < \theta$ and $\mu > 0$, $\eta > 0$ can be arbitrarily small. For $n \le x$, we use the sieving weight

$$w(n) = \sum_{m \in M} \sum_{p \in P} \sum_{n \equiv 0 \pmod{pm}} 1$$

which was introduced by Wu [18] for detecting B-free numbers in short intervals. Our improvement here is due to the fact that in one of the error terms below we can get better estimates since the set of primes B that we are sieving is a very thin subset by Elkies' estimate on the number of supersingular primes mentioned above. Observe that $w(n) \le C(\delta_2, \eta)$ independently of x. Hence it is enough to show that

$$\sum_{\substack{x-y<n\le x \\ n \text{ is } A\text{-free}}} w(n) \gg y.$$

Consider

$$\begin{aligned} \sum_{\substack{x-y<n\le x \\ n \text{ is } A\text{-free}}} w(n) \ \ge \ & \sum_{\substack{x-y<n\le x \\ n\not\equiv 0 \pmod{b_s} \\ \text{for all } s\le k}} w(n) \ - \sum_{\substack{x-y<n\le x \\ b_k<b_s\le x^{\frac{\eta}{2}} \\ n\equiv 0 \pmod{b_s} \\ \text{for some } s>k}} w(n) \\ & - \sum_{\substack{x-y<n\le x \\ x^{\frac{\eta}{2}}<b_s\le y \\ n\equiv 0 \pmod{b_s} \\ \text{for some } s>k}} w(n) \ - \sum_{\substack{x-y<n\le x \\ y<b_s\le x \\ n\equiv 0 \pmod{b_s} \\ \text{for some } s>k}} w(n) \end{aligned} \tag{14}$$

where b_s denote the elements of A in increasing order. We will denote the right side of (14) by $M_0 - E_1 - E_2 - E_3$. Next we estimate each sum on the right side of (14). For the main term, using the definition of $w(n)$ and the Inclusion-Exclusion principle, we have

$$M_0 = \sum_{\substack{x-y<n\le x \\ n\not\equiv 0 \pmod{b_s} \\ \text{for all } s\le k \\ n\equiv 0 \pmod{pm} \\ p\in P, m\in M}} 1 = \sum_{\omega} (-1)^{|\omega|} \sum_{p\in P, m\in M} \sum_{\substack{x-y<n\le x \\ n\equiv 0 \pmod{d_\omega} \\ n\equiv 0 \pmod{pm}}} 1 \tag{15}$$

where ω runs through all subsets of $\{s : 1 \le s \le k\}$ and $d_\omega = \prod_{s\in\omega} b_s$ (empty products are taken to be 1). Note that once the parameter k is fixed and x is large enough then we have $\gcd(d_\omega, pm) = 1$ for all subsets ω. Let us define the remainder terms $r_d(x, y)$ with

$$r_d(x,y) = \left[\frac{x}{d}\right] - \left[\frac{x-y}{d}\right] - \frac{y}{d}$$

so that

$$\sum_{\substack{x-y<n\le x \\ n\equiv 0 \pmod{pmd_\omega}}} 1 = \frac{y}{pmd_\omega} + r_{pmd_\omega}(x,y).$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

Combining this with (15) we get

$$M_0 = y \sum_{p\in P} \frac{1}{p} \sum_{m\in M} \frac{1}{m} \prod_{s\le k} \Bigl(1 - \frac{1}{b_s}\Bigr) + R(x, y)$$

where

$$R(x, y) = \sum_{\omega} (-1)^{|\omega|} \sum_{p\in P, m\in M} r_{pm}\Bigl(\frac{x}{d_\omega}, \frac{y}{d_\omega}\Bigr).$$

Note that

$$\sum_{p\in P} \frac{1}{p} = \log\Bigl(1 + \frac{\mu}{\delta_2}\Bigr) + O\Bigl(\frac{1}{\log x}\Bigr) \ge \mu$$

when x is large enough. As before, $\sum_{s=1}^{\infty} \frac{1}{b_s}$ is finite and we may put

$$C_A = \prod_{s=1}^{\infty} \Bigl(1 - \frac{1}{b_s}\Bigr) > 0.$$

Hence for the main term we get

$$M_0 \ge C_A \mu y \sum_{m\in M} \frac{1}{m} + R(x, y). \tag{16}$$

We also have

$$E_1 \le \frac{1}{\delta_2} \sum_{m\in M} \sum_{\substack{x-y<n\le x\\ b_k<b_s\le x^{\eta/2}\\ n\equiv 0 \pmod{mb_s}}} 1 \le \frac{2y}{\delta_2} \sum_{s=k+1}^{\infty} \frac{1}{b_s} \sum_{m\in M} \frac{1}{m} \tag{17}$$

since $mb_s \le x^{\delta_1+2\mu} < y$ and $\gcd(m, b_s) = 1$ when $b_s \le x^{\frac{\eta}{2}}$. Next we fix k such that

$$\sum_{s=k+1}^{\infty} \frac{1}{b_s} < \frac{C_A \mu \delta_2}{4}$$

so that combining (16) and (17) we get

$$M_0 - E_1 \ge \frac{C_A \mu y}{2} \sum_{m\in M} \frac{1}{m} + R(x, y).$$

Using the asymptotic formula for the number of integers whose prime factors are all $\ge x^{\eta}$, and partial summation, Wu obtained (see [18, Lemma 13]) the estimate

$$\sum_{m\in M} \frac{1}{m} \ge \frac{\mu}{2\eta}.$$

Hence we get

$$M_0 - E_1 \geq \left(\frac{C_A \mu^2}{4\eta}\right) y + R(x, y).$$

Improving on the work of Fouvry and Iwaniec [7] about estimates of exponential sums with monomials, Wu obtained (see [18, Lemma 10])

$$|R(x, y)| \leq C_1(\mu) 2^k \left(\frac{e^{-s \log s}}{\eta} + x^{-\frac{\eta}{2}}\right) y$$

for $s \geq 3$ where $C_1(\mu)$ is a constant depending only on μ. Here we get the following restrictions (see [18] for details)

$$s\eta < \frac{\mu}{2},\ \delta_2 < \frac{19\theta - 6}{11} \quad \text{and} \quad \delta_1 + \delta_2 < \frac{1+\theta}{2}. \tag{18}$$

It is easy to see that $E_2 = o(y)$. Finally we estimate E_3. Using definition of $w(n)$, we have

$$E_3 = \sum_{y < v^2 \leq x} \sum_{p \in P} \sum_{m \in M} \sum_{\substack{x - y < n \leq x \\ n \equiv 0 \ (\mathrm{mod}\ v^2) \\ n \equiv 0 \ (\mathrm{mod}\ pm)}} 1 + \sum_{y < r \leq x} \sum_{p \in P} \sum_{m \in M} \sum_{\substack{x - y < n \leq x \\ n \equiv 0 \ (\mathrm{mod}\ r) \\ n \equiv 0 \ (\mathrm{mod}\ pm)}} 1, \tag{19}$$

where v denotes a prime not in B_E and r denotes a prime in B_E. Note that there is at most one n with $x - y < n \leq x$ satisfying either $n \equiv 0 \pmod{v^2}$ or $n \equiv 0 \pmod{r}$. Moreover for any such n there are at most finitely many (independent of x) pairs (p, m) with $p \in P$ and $m \in M$ satisfying $n \equiv 0 \pmod{pm}$. Hence

$$V = \sum_{p \in P} \sum_{m \in M} \sum_{\substack{x - y < n \leq x \\ n \equiv 0 \ (\mathrm{mod}\ v^2) \\ n \equiv 0 \ (\mathrm{mod}\ pm)}} 1 = O(1) \tag{20}$$

and

$$R = \sum_{p \in P} \sum_{m \in M} \sum_{\substack{x - y < n \leq x \\ n \equiv 0 \ (\mathrm{mod}\ r) \\ n \equiv 0 \ (\mathrm{mod}\ pm)}} 1 = O(1), \tag{21}$$

where the implied constants are independent of v, r and x. It follows from (19), (20) and (21) that

$$E_3 \ll \sum_{\substack{V > 0 \\ y < v^2 \leq x}} 1 + \sum_{\substack{R > 0 \\ y < r \leq x}} 1.$$

Let us assume that

$$\delta_1 + \delta_2 + \frac{4\theta}{3} > 1 \tag{22}$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

(so that in particular $\delta_1 + \delta_2 + 2\theta > 1$). If $y^2 < v^2 \le x$ and $V > 0$, then v is not in P or M so that $n \equiv 0 \pmod{pmv^2}$ for some n with $x - y < n \le x$. But from (22), we get that $pmv^2 > x$ which is a contradiction. Hence

$$\sum_{\substack{V>0\\ y<v^2\le x}} 1 \le \sum_{y<v^2\le y^2} 1 = O\Big(\frac{y}{\log y}\Big) = o(y).$$

Similarly if

$$\frac{x^{\frac{4\theta}{3}}}{\log x} < r \le x$$

and $R > 0$ then we get a contradiction, so that

$$\sum_{\substack{R>0\\ y<r\le x}} 1 \le \sum_{y<r\le \frac{x^{\frac{4\theta}{3}}}{\log x}} 1 \ll \frac{x^{\theta}}{(\log x)^{\frac{3}{4}}} = o(y)$$

using Elkies' estimate. It follows that $E_3 = o(y)$. Note that the choice of k depends on A and μ (the dependence on δ_2 is minor). We may assume that

$$C(A,\mu) = C_1(\mu)2^k > \frac{8}{C_A\mu^2} > 16$$

and we choose

$$\eta = \min\Big(\frac{\mu^2}{5}, \frac{1}{C(A,\mu)}\Big),$$

so that taking $s = \eta^{-\frac{1}{2}}$ we satisfy $s\eta < \frac{\mu}{2}$. Finally using the fact that

$$s \log s \ge \frac{1}{2}\sqrt{C(A,\mu)} \log C(A,\mu),$$

we get that

$$C(A,\mu)e^{-s\log s} \le \frac{1}{C(A,\mu)} < \frac{C_A\mu^2}{8}.$$

After arranging all the parameters as above we obtain

$$M_0 - E_1 - E_2 - E_3 \ge \Big(\frac{C_A\mu^2}{8\eta}\Big) y + o(y).$$

The compatibility of the conditions (18) and (22) on θ gives that $\theta > \frac{51}{134}$. This completes the proof of (i). The proof of (ii) for a newform $f(z)$ without complex multiplication is identical. Just note that from [12] we know

$$\#\{p \le x : a_f(p) = 0\} \ll_f x^{\frac{3}{4}}$$

assuming the Generalized Riemann Hypothesis for Dedekind Zeta functions. The general case follows from the argument at the beginning of Section 2. ■

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

Proof of Theorem 5 Let A be the set of primes in B together with squares of primes not in B where B is defined as in (3). If $f(z)$ is a newform without complex multiplication, then we know unconditionally from [12] that

$$B(x) \ll_{f,\epsilon} \frac{x}{(\log x)^{\frac{3}{2}-\epsilon}}$$

where $\epsilon > 0$ can be arbitrarily small and $B(x)$ is defined as in (4). It follows that

$$\sum_{b_s \in A} \frac{1}{b_s}$$

is convergent. Now a special case of [14, Theorem 11] gives that

$$\sum_{\substack{x-y<n\leq x \\ n \text{ is } A\text{-free}}} 1 \gg_\epsilon y$$

for $x^{\frac{40}{97}+\epsilon} \leq y$. The proof then proceeds exactly as before. ■

Proof of Theorem 6 Given an elliptic curve $E(a,b)/\mathbb{Q}$ without complex multiplication, let $\pi_{E(a,b)}(X)$ be the number of supersingular primes for $E(a,b)$ up to X. In proving the Lang–Trotter Conjecture on the average, David and Pappalardi [3] obtained the following estimate

$$\frac{1}{4AD} \sum_{|a|\leq A, |b|\leq D} \Big| \pi_{E(a,b)}(X) - c_0 \int_2^X \frac{1}{2\sqrt{t}\log t}\, dt \Big|^2 = O\Big(\frac{X}{(\log X)^c} + \Big(\frac{1}{A} + \frac{1}{D}\Big) X^3 + \frac{1}{AD} X^5 \Big)$$

for every $c > 0$ and $A, D > X^{1+\lambda}$ for $\lambda > 0$ where the O constant depends only on c. In particular if $A, D > X^{2+\lambda}$, then since

$$\int_2^X \frac{1}{2\sqrt{t}\log t}\, dt$$

is about $\frac{\sqrt{X}}{\log X}$, we get that

$$\pi_{E(a,b)}(X) \ll_{E(a,b)} \sqrt{X}$$

when X is large enough with at most

$$O\Big(\frac{AD}{(\log X)^c}\Big)$$

exceptions of $E(a,b)$. This means that if

$$B_{E(a,b)}(x) = \#\{p \leq x : p \text{ is prime and } a_{E(a,b)}(p) = 0\},$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

then

$$B_{E(a,b)}(x) \ll_{E(a,b)} \sqrt{x}$$

with the number of exceptional $E(a,b)$ stated as above. The conclusion of Theorem 6 now follows when we recall a result obtained in [1].

Theorem 2.3 of **[1]** *Let B be a subset of primes such that $B(x) \ll \sqrt{x}$. If $y = x^\theta$ and $\theta > \frac{1}{3}$, then the number of square-free and B-free integers in $(x-y,x)$ is $\gg y$.*

■

4 Proof of Theorem 7 and Corollary 8

Proof of Theorem 7 Our method here is inspired by the classical work of Selberg [13]. Since $B(x) \ll x^\rho$ for some $\frac{1}{2} \le \rho < 1$, we get that

$$\prod_{p\in B}\Big(1+\frac{1}{p^s}\Big)$$

is defined for all complex s with $\mathrm{Re}(s) > \rho$. Consider the multiplicative function $\mu_B(n)$ which is defined as $\mu(n)$ (μ is the Möbius function) when n is square-free and B-free and $\mu_B(n) = 0$ otherwise. We will work with the counting function

$$\theta_B(x) = \sum_{n\le x} |\mu_B(n)|\,.$$

By Perron's Inversion formula,

$$\theta_{B,1}(x) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{s}\Big(\sum_{n=1}^{\infty}\frac{|\mu_B(n)|}{n^s}\Big)\,ds$$

where

$$\theta_{B,1}(x) = \frac{\theta_B(x+)+\theta_B(x-)}{2}.$$

Here $x+$ and $x-$ denote the limits from right and left respectively, and the integral is taken as the Cauchy principal value. Note that

$$\sum_{n=1}^{\infty}\frac{|\mu_B(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}\prod_{p\in B}\Big(1+\frac{1}{p^s}\Big)^{-1}$$

for $\mathrm{Re}(s) > 1$. First we move the line of integration to the left of $\mathrm{Re}(s) = 1$, say to $\mathrm{Re}(s) = \sigma_0$ for some $\rho < \sigma_0 < 1$. This can be justified by using standard results such as $|\zeta(s)| \ll \sqrt{|t|}\log|t|$ for $|t| \ge 2$ and the inequalities

$$\Big|\frac{1}{\zeta(2s)}\Big| \le \frac{\zeta(2\sigma)}{\zeta(4\sigma)} \le \zeta(2\sigma)$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

which is Theorem 8.7 of [15] and

$$\Big|\prod_{p\in B}\Big(1+\frac{1}{p^{s}}\Big)\Big| \geq \prod_{p\in B}\Big(1-\frac{1}{p^{\sigma_0}}\Big)$$

where $s = \sigma + it$ and $\frac{1}{2} \leq \rho < \sigma_0 \leq \sigma \leq 2$. Applying the Residue Theorem we get

$$\theta_{B,1}(x) - cx = \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{x^{\sigma_0+it}}{(\sigma_0+it)} \frac{\zeta(\sigma_0+it)}{\zeta(2\sigma_0+i2t)} \prod_{p\in B}\Big(1+\frac{1}{p^{\sigma_0+it}}\Big)^{-1} dt \tag{23}$$

where the residue at $s = 1$ is computed to be

$$c = \frac{6}{\pi^2}\prod_{p\in B}\Big(1+\frac{1}{p}\Big)^{-1}.$$

Next we put $e^{\delta} = 1 + \frac{1}{T}$ for $T > 0$ and from (23) we obtain

$$\frac{\theta_{B,1}(e^{\delta+\tau}) - \theta_{B,1}(e^{\tau}) - c\frac{e^{\tau}}{T}}{e^{\sigma_0\tau}} = \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{(e^{\delta(\sigma_0+it)}-1)}{\sigma_0+it}\, e^{i\tau t}\, I(\sigma_0,t)\, dt \tag{24}$$

for $\tau > 0$ (indeed (24) also holds when $\tau \leq 0$, but as t tends to $-\infty$, both $\theta_{B,1}(e^{\delta+\tau}) = 0$ and $\theta_{B,1}(e^{\tau}) = 0$ so that the left side of (24) simplifies considerably) where

$$I(\sigma_0,t) = \frac{\zeta(\sigma_0+it)}{\zeta(2\sigma_0+i2t)}\prod_{p\in B}\Big(1+\frac{1}{p^{\sigma_0+it}}\Big)^{-1}.$$

Let us now show that the integrand in (24) is in $L^2(-\infty,\infty)$. Clearly it is enough to show that the integrand is in $L^2(0,\infty)$ (since all of the estimates are symmetric, the norm estimate for $(0,\infty)$ will be true for the norm estimate for $(-\infty,0)$ up to constants). We put $\sigma_0 = \rho + \eta$ where $\eta > 0$ and $\frac{1}{2} \leq \rho < 1$. Note that

$$\Big|\frac{1}{\zeta(2s)}\Big| = O\Big(\frac{1}{2\rho+2\eta-1}\Big) \tag{25}$$

independently of t. To estimate

$$\int_0^{\infty}\Big|\frac{e^{\delta(\sigma_0+it)}-1}{\sigma_0+it}\Big|^2 |I(\sigma_0,t)|^2\, dt$$

consider the series of inequalities for $k \geq 1$,

$$\begin{aligned}
&\int_{(2^k-1)T}^{(2^{k+1}-1)T}\Big|\frac{e^{\delta(\sigma_0+it)}-1}{\sigma_0+it}\Big|^2 |I(\sigma_0,t)|^2\, dt \qquad (26)\\
&\ll \frac{1}{(2\rho+2\eta-1)^2 2^{2k}T^2}\int_{(2^k-1)T}^{(2^{k+1}-1)T}|\zeta(\sigma_0+it)|^2\, dt\\
&\ll \frac{1}{(2\rho+2\eta-1)^2 2^{2k}T}\,\frac{(2^{k+1}-1)}{(2^{k+1}-1)T}\int_0^{(2^{k+1}-1)T}|\zeta(\sigma_0+it)|^2\, dt\\
&\ll \frac{\zeta(2\sigma_0)(2^{k+1}-1)}{(2\rho+2\eta-1)^2 2^{2k}T} \ll \frac{(2^{k+1}-1)}{(2\rho+2\eta-1)^3 2^{2k}T}
\end{aligned}$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

where we have used Theorem 7.2 of [15] on the mean square of the Riemann Zeta function and the fact that

$$\zeta(2\sigma_0) = \sum_{n=1}^{\infty} \frac{1}{n^{2\rho+2\eta}} = O\Big(\frac{1}{2\rho+2\eta-1}\Big)$$

since $2\rho + 2\eta > 1$. Similarly we can show that

$$\int_0^T \Big|\frac{e^{\delta(\sigma_0+it)}-1}{\sigma_0+it}\Big|^2 \, |I(\sigma_0,t)|^2 \, dt \ll \frac{1}{(2\rho+2\eta-1)^3 T} \tag{27}$$

(besides the presence of the term $\frac{1}{(2\rho+2\eta-1)^3}$, the implied constants in (26) and (27) still depend on ρ and η because of the term

$$\Big|\prod_{p\in B}\Big(1+\frac{1}{p^{\sigma_0+it}}\Big)^{-1}\Big|^2$$

which will be estimated more precisely when we choose η specifically). It follows from (26) and (27) that the integrand is in $L^2(-\infty,\infty)$. We recall the following result from [16] on the Parseval–Plancherel Theory of Fourier transforms.

Theorem *Let $f(x)$ be a (real or complex) function in $L^2(-\infty,\infty)$ and let*

$$F(x,a) = \frac{1}{\sqrt{2\pi}} \int_{-a}^{a} f(y)e^{ixy}\, dy.$$

Then as $a > 0$ tends to infinity, $F(x,a)$ converges in mean over $(-\infty,\infty)$ to a function $F(x)$ in $L^2(-\infty,\infty)$. Moreover we have

$$\int_{-\infty}^{\infty} |F(x)|^2\, dx \le \int_{-\infty}^{\infty} |f(x)|^2\, dx.$$

The function on the left side of (24) is the Fourier transform of

$$\frac{\big(e^{\delta(\sigma_0+it)}-1\big)}{\sigma_0+it} I(\sigma_0,t)$$

which was shown to be in $L^2(-\infty,\infty)$ above. Hence by the theorem just mentioned, we can conclude that

$$\int_{-a}^{a} \frac{\big(e^{\delta(\sigma_0+it)}-1\big)}{\sigma_0+it}\, e^{i\tau t}\, I(\sigma_0,t)\, dt$$

converges in mean to a function $f(\tau) \in L^2(-\infty,\infty)$. It is well known that mean convergence implies the convergence of a subsequence almost everywhere. But in our case any such subsequence converges to the function on the left side of (24), so that the function on the left side of (24) and $f(\tau)$ agree almost everywhere and their

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

L^2 norms are equal. Again by the same theorem, the norm of $f(\tau)$ is $\leq$ the norm of the integrand. Hence making the change of variable $y = e^\tau$, $1 \leq y < \infty$ we get that (note that since $\theta_{B,1}(x)$ has a countable number of jump discontinuities we can use $\theta_B(x)$ in all of the integrals)

$$\int_1^\infty \frac{\left|\theta_B\left(y + \frac{y}{T}\right) - \theta_B(y) - c\frac{y}{T}\right|^2}{y^{1+2\sigma_0}}\, dy \ll \int_{-\infty}^\infty \left|\frac{e^{\delta(\sigma_0+it)} - 1}{\sigma_0 + it}\right|^2 |I(\sigma_0, t)|^2\, dt \tag{28}$$

$$\ll \frac{1}{(2\rho + 2\eta - 1)^3 T} \sum_{k=0}^\infty \frac{\left(2^{k+1} - 1\right)}{2^{2k}}$$

$$\ll \frac{1}{(2\rho + 2\eta - 1)^3 T}.$$

Next we choose $\eta = \frac{1}{\log\log T}$, so that

$$\sigma_0 = \rho + \frac{1}{\log\log T} \tag{29}$$

and

$$\left|\prod_{p \in B}\left(1 + \frac{1}{p^{\sigma_0+it}}\right)^{-1}\right|^2 \ll (\log T)^2.$$

Note that if $\rho > \frac{1}{2}$, then $\frac{1}{(2\rho+2\eta-1)^3}$ is harmless to our estimates and if $\rho = \frac{1}{2}$, then $\frac{1}{(2\rho+2\eta-1)^3}$ is about $(\log\log T)^3$. In any case we obtain from (28) and (29) that

$$\int_1^{T^4} \left|\frac{\theta_B(y + \frac{y}{T}) - \theta_B(y) - c\frac{y}{T}}{y}\right|^2 dy \ll \frac{e^{\frac{8\log T}{\log\log T}} (\log T)^2 (\log\log T)^3}{T^{5-8\rho}} \ll \frac{e^{\frac{8\log T}{\log\log T}}}{T^{5-8\rho}}. \tag{30}$$

For $0 < H \leq x^{\frac{3}{4}}$ we put $T = \frac{2x}{H}$. Using this in (30) we get

$$\int_1^x \left|\frac{\theta_B\left(y + \frac{Hy}{2x}\right) - \theta_B(y) - c\frac{Hy}{2x}}{y}\right|^2 dy \ll \frac{\exp\left(\frac{8\log(\frac{2x}{H})}{\log\log(\frac{2x}{H})}\right)}{\left(\frac{2x}{H}\right)^{5-8\rho}}. \tag{31}$$

Let q_n be the sequence of square-free and B-free numbers. Our next goal is to estimate a sum of the form

$$\sum_{\substack{q_n \leq x \\ q_n - q_{n-1} \geq \frac{H}{x} q_n}} (q_n - q_{n-1}).$$

To this end, note that if q_{n-1} and q_n are consecutive square-free and B-free numbers $\leq x$ such that $q_n - q_{n-1} \geq \frac{H}{x} q_n$, then (31) gives that

$$\int_{q_{n-1}}^{q_n - \frac{H}{2x}q_n} \left|\frac{\theta_B\left(y + \frac{Hy}{2x}\right) - \theta_B(y) - c\frac{Hy}{2x}}{y}\right|^2 dy = c^2 \int_{q_{n-1}}^{q_n - \frac{H}{2x}q_n} \frac{H^2}{4x^2}\, dy$$

$$\gg \frac{H^2}{x^2}(q_n - q_{n-1})$$

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press

and summing over all such $q_n \le x$ we get

$$\sum_{\substack{q_n \le x \\ q_n - q_{n-1} \ge \frac{H}{x} q_n}} (q_n - q_{n-1}) \ll \left(\frac{x}{H}\right)^{8\rho-3} \exp\left(\frac{8\log\left(\frac{2x}{H}\right)}{\log\log\left(\frac{2x}{H}\right)}\right) \tag{32}$$

in the range $0 < H \le x^{\frac{3}{4}}$. Moreover using the well-known fact $q_n - q_{n-1} \ll \sqrt{q_n}$ (in fact sharper bounds are known by the work of Sargos and Wu [14]) we will show that (32) holds for the full range $0 < H \le x$. Indeed combining $q_n - q_{n-1} \ll \sqrt{q_n}$ with the condition $\frac{H}{x} q_n \le q_n - q_{n-1}$ of the summation, we get that $q_n \ll \left(\frac{x}{H}\right)^2$. Hence if H is close to $x^{\frac{3}{4}}$, then q_n's can go up to a bound which is about $\sqrt{x}$. Using (32) with x replaced by $\sqrt{x}$ and H replaced by $\frac{H}{\sqrt{x}}$, we get that (32) is valid when $\frac{H}{\sqrt{x}} \le (\sqrt{x})^{\frac{3}{4}} = x^{\frac{3}{8}}$ *i.e.,* when $0 < H \le x^{\frac{7}{8}}$. Continuing in this way, we get that (32) is valid for $0 < H \le x$. Integrating with respect to H we get

$$\begin{aligned} \sum_{q_n \le x} (q_n - q_{n-1})^2 &\le x \sum_{q_n \le x} \frac{(q_n - q_{n-1})^2}{q_n} \\ &= \int_1^x \Bigg(\sum_{\substack{q_n \le x \\ q_n - q_{n-1} \ge \frac{H}{x} q_n}} (q_n - q_{n-1}) \Bigg) \, dH \\ &\ll x^{8\rho-3} \int_1^x \frac{\exp\left(\frac{8\log\left(\frac{2x}{H}\right)}{\log\log\left(\frac{2x}{H}\right)}\right)}{H^{8\rho-3}} \, dH \ll x^{8\rho-3} e^{\frac{8\log x}{\log\log x}}. \end{aligned} \tag{33}$$

If

$$f(z) = \sum_{n=1}^{\infty} a_f(n) q^n$$

is a newform, then $a_f(q_s) \ne 0$ for every q_s, so that by the definition of $i_f(n)$ we have

$$i_f(n) \le q_s - n$$

when $q_{s-1} < n \le q_s$. It follows that

$$\sum_{q_{s-1} < n \le q_s} i_f(n) \ll \sum_{q_{s-1} < n \le q_s} (q_s - n) \ll (q_s - q_{s-1})^2$$

and finally, using (33),

$$\sum_{n \le x} i_f(n) \ll \sum_{q_s \le 2x} \sum_{q_{s-1} < n \le q_s} i_f(n) \ll \sum_{q_s \le 2x} (q_s - q_{s-1})^2 \ll x^{8\rho-3} e^{\frac{8\log x}{\log\log x}}.$$

This completes the proof of Theorem 7. ■

Proof of Corollary 8 Let us recall that by the result of David and Pappalardi [3] (see proof of Theorem 6) we get

$$\pi_{E(a,b)}(X) \ll \sqrt{X}$$

with at most

$$O\Big(\frac{AD}{(\log X)^c}\Big)$$

exceptions of $E(a, b)$ where $A, D > X^{2+\lambda}$ and $\lambda > 0$. It follows that

$$B_{E(a,b)}(x) \ll \sqrt{x}$$

with this many exceptions and Corollary 8 is a consequence of Theorem 7 by taking $\rho = \frac{1}{2}$. ■

Acknowledgment I would like to thank the referee for helpful comments and suggestions on an earlier version of the paper.

References

[1] E. Alkan, *Nonvanishing of Fourier coefficients of modular forms.* Proc. Amer. Math. Soc. **131**(2003), 1673–1680.

[2] A. Balog and K. Ono, *The Chebotarev density theorem in short intervals and some questions of Serre.* J. Number Theory **91**(2001), 356–371.

[3] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves.* Internat. Math. Res. Notices **4**(1999), 165–183.

[4] P. Erdős, *On the difference of consecutive terms of sequences defined by divisibility properties.* Acta Arith. **12**(1966), 175–182.

[5] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$. Invent. Math. **89**(1987), 561–567.

[6] ———, *Distribution of supersingular primes.* Astérisque **198-200**(1992), 127–132.

[7] E. Fouvry and H. Iwaniec, *Exponential sums with monomials.* J. Number Theory **33**(1989), 311–333.

[8] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers II.* J. London Math. Soc. **45**(1992), 215–221.

[9] A. Granville, *ABC allows us to count squarefrees.* Internat. Math. Res. Notices **19**(1998), 991–1009.

[10] H. Iwaniec, *Topics in Classical Automorphic Forms.* Graduate Studies in Mathematics 17, American Mathematical Society, Providence, RI, 1997.

[11] V. K. Murty, *Modular forms and the Chebotarev density theorem II.* In: Analytic Number Theory, London Math. Soc. Lecture Note Ser. 247, 1997, pp. 287–308.

[12] J. P. Serre, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. **54**(1981), 323–401.

[13] A. Selberg, *On the normal density of primes in small intervals, and the difference between consecutive primes.* Arch. Math. Naturvid. **47**(1943), 87–105.

[14] P. Sargos and J. Wu, *Multiple exponential sums with monomials and their applications in number theory.* Acta Math. Hungar. **87**(2000), 333–354.

[15] E C. Titchmarsh, *The Theory of the Riemann Zeta-Function.* Clarendon Press, Oxford, 1951.

[16] ———, *Introduction to the theory of Fourier Integrals.* Third edition. Chelsea Publishing Company, New York, 1986

[17] D. Wan, *On the Lang-Trotter conjecture.* J. Number Theory **35**(1990), 247–268.

[18] J. Wu, *Nombres B-libres dans les petits intervalles.* Acta Arith. **65**(1993), 97–116.

Department of Mathematics
University of Illinois at Urbana-Champaign
61801, USA
e-mail: alkan@math.uiuc.edu

https://doi.org/10.4153/CJM-2005-019-7 Published online by Cambridge University Press