PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 6, June 2016, Pages 2301–2305
http://dx.doi.org/10.1090/proc/12887
Article electronically published on October 1, 2015

A NOTE ON SMALL GAPS BETWEEN NONZERO FOURIER COEFFICIENTS OF CUSP FORMS

SOUMYA DAS AND SATADAL GANGULY

(Communicated by Kathrin Bringmann)

Abstract. It is shown that there are infinitely many primitive cusp forms f of weight 2 with the property that for all X large enough, every interval $(X, X + cX^{1/4})$, where $c > 0$ depends only on the form, contains an integer n such that the n-th Fourier coefficient of f is nonzero.

1. Introduction

The question about the lacunarity of the sequence of Fourier coefficients of a nonzero elliptic cusp form seems to have originated in Serre's seminal paper [Se81]. Following his notation, given a modular form

$$f = \sum_{n=1}^{\infty} a_f(n) e^{2\pi i n z},$$

which is not a linear combination of forms with complex multiplication, one defines for any positive integer n, the quantity $i_f(n)$ by,

$$i_f(n) := \max\{i \mid a_f(n+j) = 0, \quad 0 < j \leq i\},$$

and the question is to estimate the magnitude of this quantity as n grows; expecting it to be small most of the time. For example, Serre [Se81] showed that

$$i_f(n) \ll_f n,$$

and asked the question whether one has

$$i_f(n) \ll_f n^{\delta}, \quad \text{for some } \delta < 1. \tag{1.1}$$

From the Rankin-Selberg theory, one knows that (1.1) holds with $\delta = 3/5$. Several results on this topic have appeared in the literature in recent years. For example A. Balog and K. Ono [BO01] prove for a cusp form on $\Gamma_0(N)$, not a linear combination of CM-forms, that for any $\varepsilon > 0$,

$$i_f(n) \ll_{f,\varepsilon} n^{17/41+\varepsilon}.$$

E. Alkan has many interesting results in this direction; see, e.g., the works [Al03], [Al05], [AZ08] where he proves (among many other related results) that for almost all n or for n is a set of positive natural density,

$$i_f(n) \ll_f \phi(n),$$

Received by the editors January 25, 2015 and, in revised form, June 29, 2015.
2010 *Mathematics Subject Classification.* Primary 11F30; Secondary 11F11, 11G05.
Key words and phrases. Fourier coefficients of cusp forms, elliptic curves, sums of two squares.

where $\phi(n)$ is any monotonically increasing function satisfying $\phi(2n) \ll \phi(n)$. If f arises from an elliptic curve $E/\mathbb{Q}$, he proves the bound

$$i_f(n) \ll_{E,\varepsilon} n^{69/169+\varepsilon}, \tag{1.2}$$

for any $\varepsilon > 0$, by exploiting a result of N. Elkies [Elk92] on distribution of supersingular primes.

For holomorphic nonCM cusp forms f on general congruence groups the bound due to Kowalski, Robert and Wu [KRW07] is currently the strongest result uniform for all n and gives

$$i_f(n) \ll_f n^{7/17+\varepsilon}.$$

Almost all of the works cited above use some variant of the machinery of $\mathscr{B}$-free numbers, sieve techniques, bounds on exponential sums and the result of Serre which states that for any $\varepsilon > 0$ and f a newform on $\Gamma_0(N)$ without CM, one has

$$\#\{p \leq x \mid a_f(p) = 0\} \ll_{f,\varepsilon} \frac{x}{\log(x)^{3/2-\varepsilon}},$$

which follows by considering the 2-dimensional Galois representations attached to f and an effective Chebotarev's density theorem; for more details see [Se81].

In a recent work [DG14], it was shown that if f is a holomorphic cusp form for the modular group $SL(2,\mathbb{Z})$ of weight $k \geq 12$, one has the bound

$$i_f(n) \ll_k n^{1/4}.$$

This result was proved by utilizing certain congruences due to Hatada [Hat79] for Hecke eigenvalues of cusp forms for the group $SL(2,\mathbb{Z})$; and is simpler in the sense that it avoids all of the aforementioned methods in the previous paragraphs. It is not clear to us whether one can prove similar congruences for forms on congruence groups of higher levels and use them to improve on the bound of Kowalski, Robert and Wu in full generality.

The purpose of this note is to prove that the bound $i_f(n) = O(n^{1/4})$ holds for an infinite family of cusp forms that are *not* of level one. This family comes from certain elliptic curves over $\mathbb{Q}$.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve having a rational point of exact order 4. Then the associated primitive form f_E satisfies the bound*

$$i_{f_E}(n) \ll_E n^{1/4}.$$

By showing that there are infinitely many distinct isogeny classes of such elliptic curves, we obtain the following corollary.

Corollary 1. *There are infinitely many primitive forms f of weight 2 and level larger than one that satisfies the bound*

$$i_f(n) \ll_f n^{1/4}.$$

Note that $69/169 \approx 0.41$, so our result also improves upon that of Alkan in (1.2) for those elliptic curves which have a point of order 4 over $\mathbb{Q}$.

The basic idea of the proof is that by considering the mod 4 Galois representation associated to E as above, we obtain certain congruences satisfied by the coefficients a_p of the modular form f_E at primes p that are coprime to the conductor N_E of E. Using these congruences we are able to prove that $a_n \neq 0$ if n is a sum of two squares and $(n, 2N_E) = 1$. The rest of the proof is to show that such n can be found in reasonably short intervals; namely, between X and $X + cX^{1/4}$ for all X

sufficiently large, c being a positive constant depending on E. The possibility of extending the idea of this proof to forms of higher weights remains to be explored.

2. Proofs

2.1. **Proof of the theorem.** We follow the notation of [Sil86]. We first recall that the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set $E[N]$ of N-torsion points of E and gives rise to a representation

$$\rho_{E,N} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}/N\mathbb{Z}).$$

The proof begins with the following observation that was pointed out to the authors by B. Gross. If an elliptic curve $E/\mathbb{Q}$ has a rational point of exact order N, then the image of the associated Galois representation $\rho_{E,N}$ is contained in a Borel subgroup. This can be seen as follows. Suppose $P \in E(\mathbb{Q})$ is of exact order N. Since $E[N] \cong (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$, we can find another point $Q \in E[N]$ such that $\{P, Q\}$ is a basis for $E[N]$. Since $\sigma(P) = P$ for any $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, if we represent $\rho(\sigma)$ for some $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ as a matrix with respect to the ordered basis (P, Q), it will look like $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.

Remark 1. In fact there is a necessary and sufficient condition for the image of $\rho_{E,N}$ to be contained in a Borel subgroup; see [Rid10, Prop. 2.1].

Now we apply this observation to the case $N = 4$ and $\sigma = \sigma_p$, the Frobenius element at an odd prime p. We shall see later that the choice $N = 4$ is admissible; i.e., there are elliptic curves over $\mathbb{Q}$ that admit rational points of exact order 4. Thus we have,

$$\rho_{E,4}(\sigma_p) = \begin{pmatrix} 1 & * \\ 0 & \beta_p \end{pmatrix},$$

where β_p and $*$ are elements in $\mathbb{Z}/4\mathbb{Z}$. There is a primitive form (i.e., a newform) f_E of weight 2 and level N_E associated to the elliptic curve E. Suppose a_n denotes the n-th normalized (i.e. $a_1 = 1$) Hecke eigenvalue of f_E. We know that $a_n \in \mathbb{Z}$ for all n and from the theory of ℓ-adic representations (see, e.g., [Sil86, §5]), we also know that the Hecke eigenvalues a_p of f_E at odd primes p satisfy the congruences

$$1 + \beta_p \equiv a_p \pmod 4$$

and

$$\beta_p \equiv p^{2-1} \pmod 4.$$

Therefore, we obtain the relation

$$a_p \equiv p + 1 \pmod 4. \tag{2.1}$$

Next, as in [DG14], we observe that $a_n \neq 0$ for all odd integers n that are sums of two squares and are coprime to N_E. We sketch an argument below. See [DG14] for more details.

For showing $a_n \neq 0$, it is enough to show that $a_{p^\alpha} \neq 0$ for all prime factors p of n, where α is the exponent of p occurring in the prime factorization of n. Now, if n is a sum of two squares, then the prime factors of n that are $\equiv 3 \pmod 4$ must occur with an even exponent. From (2.1) it follows using Hecke's recurrence relation that $a_{p^n} \equiv 1 \pmod 4$ for $p \equiv 3 \pmod 4$ and n even. For primes $p \equiv 1 \pmod 4$ that divide n, we see, again from (2.1), that $a_p \equiv 2 \pmod 4$. Now, a lemma in the paper by Kowalski, Robert and Wu (see [KRW07, Lemma 2.2]) applied

to our situation (modular form with integer coefficients and with trivial nebentypus) implies that if $a_p \neq 0$, then $a_{p^m} \neq 0$ for all $m \geq 1$ as long as $(p, N_E) = 1$.

Now we come to the last part of the proof. An elementary technique stated in [BC47] allows us to show that every interval of the form $(X, X + 7X^{1/4})$ contains a sum of two squares as soon as $X \geq 1154$. We can modify this technique (see, for example, the proof of Thm. 1 in [DG14]) to ensure that we can also obtain an integer that is coprime to $2N_E$ and is a sum of two squares in an interval of type $(X, X + cX^{1/4})$, where $X \geq 1154$ and $c > 0$ is a constant that depends only on N_E.

2.2. **Proof of the corollary.** We have shown that if an elliptic curve $E/\mathbb{Q}$ has a rational point of exact order 4, then we have the bound $i_{f_E}(n) \ll n^{1/4}$. Now, by the famous Modularity Theorem, every isogeny class of elliptic curves over $\mathbb{Q}$ with conductor N (and it is necessary that $N > 1$) corresponds to a primitive cusp form of weight 2 and level N. Moreover, this primitive form is uniquely determined since, according to a theorem of Faltings [Fa83], the L-function of an elliptic curve determines the curve up to isogeny. Therefore, the corollary will follow once we show that there are infinitely many isogeny classes of elliptic curves, each containing a rational point of exact order 4.

This comes from the theory of modular curves, in particular, from considering modular curves as moduli spaces classifying elliptic curves with some extra structures up to isomorphism. We first recall (see [Sil86, §13, Appendix C]) that there is a bijection between points on the complex curve $Y_1(N) = \mathbb{H}/\Gamma_1(N)$ and isomorphism classes of pairs (E, P) of elliptic curves $E/\mathbb{C}$ and a point $P \in E(\mathbb{C})$ of exact order N. This moduli interpretation can be extended to elliptic curves over number fields as well if $N \geq 4$. A theorem (see [DI95, Thm. 8.2.1]) says that for $N \geq 4$, $Y_1(N)$ is a fine moduli space for the moduli problem of classifying isomorphism classes of pairs (E, P) where $P \in E(\mathbb{Q})$ is of exact order N. This means, in particular, that the rational points on the modular curve $Y_1(N)$ are in bijection with the isomorphism classes of pairs (E, P) where E is an elliptic curve over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ is of exact order N. See [DI95, §8.2] for a discussion on this result. Now, it is known that $X_1(4)$ is a smooth algebraic curve of genus zero and hence is rational and that it has a rational point. Therefore, $X_1(4)$ has infinitely many rational points and hence so does $Y_1(4)$ and, by the above result, there are infinitely many isomorphism classes of pairs (E, P), where $P \in E(\mathbb{Q})$ is of exact order 4. Now we recall the fact (see [Sil86, §IX.6, Cor. 6.2]) that given an elliptic curve E over $\mathbb{Q}$ there can be only finitely many elliptic curves over $\mathbb{Q}$ that are isogenous to E. Since on a fixed elliptic curve there can be only a finite number of rational points of exact order 4, we see from the infinitude of isomorphism classes of pairs (E, P) described above that there are infinitely many isogeny classes of elliptic curves $E/\mathbb{Q}$, each of which contains a rational point of exact order 4.

Acknowledgements

It is a pleasure to thank Arijit Dey, Benedict Gross, Emmanuel Kowalski, Souradip Mazumdar and C. S. Rajan for helpful remarks. The first author also acknowledges financial support from IISc Bangalore, UGC centre for advanced studies and DST(India).

References

[Al03] Emre Alkan, *Nonvanishing of Fourier coefficients of modular forms*, Proc. Amer. Math. Soc. **131** (2003), no. 6, 1673–1680 (electronic), DOI 10.1090/S0002-9939-02-06758-8. MR1953571 (2003k:11068)

[Al05] Emre Alkan, *On the sizes of gaps in the Fourier expansion of modular forms*, Canad. J. Math. **57** (2005), no. 3, 449–470, DOI 10.4153/CJM-2005-019-7. MR2134398 (2006a:11056)

[AZ08] Emre Alkan and Alexandru Zaharescu, *On the gaps in the Fourier expansion of cusp forms*, Ramanujan J. **16** (2008), no. 1, 41–52, DOI 10.1007/s11139-007-9091-z. MR2407238 (2009c:11061)

[BO01] Antal Balog and Ken Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, J. Number Theory **91** (2001), no. 2, 356–371, DOI 10.1006/jnth.2001.2694. MR1876282 (2003h:11145)

[BC47] R. P. Bambah and S. Chowla, *On numbers which can be expressed as a sum of two squares*, Proc. Nat. Inst. Sci. India **13** (1947), 101–103. MR0022879 (9,273a)

[DG14] Soumya Das and Satadal Ganguly, *Gaps between nonzero Fourier coefficients of cusp forms*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3747–3755, DOI 10.1090/S0002-9939-2014-12164-2. MR3251716

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR1357209 (97g:11044)

[Elk92] Noam D. Elkies, *Distribution of supersingular primes*, Astérisque **198-200** (1991), 127–132 (1992). Journées Arithmétiques, 1989 (Luminy, 1989). MR1144318 (93b:11070)

[Fa83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German), Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432. MR718935 (85g:11026a)

[Hat79] Kazuyuki Hatada, *Eigenvalues of Hecke operators on* SL(2, **Z**), Math. Ann. **239** (1979), no. 1, 75–96, DOI 10.1007/BF01420494. MR516060 (80b:10037)

[KRW07] Emmanuel Kowalski, Olivier Robert, and Jie Wu, *Small gaps in coefficients of L-functions and $\mathfrak{B}$-free numbers in short intervals*, Rev. Mat. Iberoam. **23** (2007), no. 1, 281–326, DOI 10.4171/RMI/496. MR2351136 (2008m:11100)

[Rid10] Penny C. Ridgdill, *On the frequency of finitely anomalous elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2010. Thesis (Ph.D.)–University of Massachusetts Amherst. MR2941460

[Se81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev* (French), Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559 (83k:12011)

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

Department of Mathematics, Indian Institute of Science, Bangalore 560012, India
E-mail address: soumya.u2k@gmail.com

Theoretical Statistics and Mathematics Unit, Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata 700108, India
E-mail address: sgisical@gmail.com