BOUNDED GAPS BETWEEN PRODUCTS OF PRIMES WITH APPLICATIONS TO ELLIPTIC CURVES AND MODULAR L-FUNCTIONS

FRANK THORNE (INTRODUCTION; PRELIMINARY)

Abstract. In the recent papers [9, 10], Goldston, Graham, Pintz, and Yıldırım use a variant of the Selberg sieve to prove the existence of small gaps between E_2 numbers; that is, squarefree numbers with exactly two prime factors. We apply their techniques to prove similar bounds for E_r numbers for any $r \geq 3$, where these numbers are required to have all of their prime factors in a set of primes $\mathcal{P}$. Our result holds for any $\mathcal{P}$ of positive density that satisfies a Siegel-Walfisz condition regarding distribution in arithmetic progressions. We also prove a stronger result in the case that $\mathcal{P}$ satisfies a Bombieri-Vinogradov condition. In addition, using results of Ono [17] and Soundararajan [20], we give applications to divisibility of class numbers, critical values of L-functions, and ranks of elliptic curves.

1. Introduction and Statement of Results

In a recent series of papers [8, 9, 10], Goldston, Graham, Pintz, and Yıldırım considered the problem of bounding gaps between primes and almost primes. Goldston, Pintz, and Yıldırım proved in [8] that

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0, \tag{1.1}$$

and Goldston, Graham, Pintz, and Yıldırım gave an alternate proof [9] of (1.1) based on the Selberg sieve. The latter authors also observed that their method could be successively applied to E_2 numbers, that is, squarefree numbers with exactly two prime factors. In [10] these authors proved that

$$\liminf_{n\to\infty} \big(q_{n+1} - q_n\big) \leq 6,$$

where q_n denotes the nth E_2 number.

The GGPY sieve is interesting not only on account of these results, but also because of its adaptability. As these authors observe in [10], their method can, for example, bound gaps between nonconsecutive almost-primes q_n and $q_{n+\nu}$ for any ν, or between E_2 numbers whose prime factors are both congruent to 1 modulo 4.

2000 *Mathematics Subject Classification.* 11N25, 11N36.

As an illustrative example, we consider the straightforward proof (see [10]) of this latter fact. In general, one considers a sum of the shape

$$S = \sum_{n=N}^{2N} \left(\sum_{h \in \mathcal{H}} \beta(n+h) - 1 \right) \left(\sum_{d | P(n;\mathcal{H})} \lambda_d \right)^2,$$

where

$$P(n;\mathcal{H}) := \prod_{h \in \mathcal{H}} (n+h),$$

and $\beta(n+h)$ is the characteristic function of E_2 numbers. The positive and negative contributions are estimated separately, and if $S > 0$ for a given choice of $\mathcal{H}$, then it follows that there are infinitely many n for which $n+h \in E_2$ for at least two $h \in \mathcal{H}$.

To restrict attention to E_2 numbers with both prime factors congruent to 1 modulo 4, one observes that by Dirichlet's theorem, these represent a quarter of all E_2 numbers. The analysis of the quantity S shows that the contribution of such E_2 numbers is the expected one fourth of the total contribution, and so it suffices to simply choose a larger set $\mathcal{H}$.

This methodology differs from the most successful approaches to problems of this sort, which use weighted sieves to prove approximations to the twin prime conjecture. The strongest result in this direction is due to Chen [4], who proved that there are infinitely many primes p for which $p+2$ is a P_2 number; that is, $p+2$ has at most two prime factors. As a simpler example we cite the result of Bombieri ([2]; see also [5]) that for infinitely many primes p, one has $p+2 \in P_4$. The proof of this proceeds by considering a sum

$$\sum_{p \leq x} \left(2 - \sum_{\substack{q \leq x^{1/4} \log^B x \\ q \neq 2 \\ q | (p+2)}} 1 \right) \left(\sum_{\substack{d \leq x^{1/8} \log^{-B} x \\ 2 \nmid d; \mu^2(d) = 1 \\ d | (p+2)}} \lambda_d \right)^2$$

which one shows is asymptotically positive. This shows, then, that for infinitely many p, $p+2$ has at most one prime factor less than $x^{1/4} \log^B x$, thereby establishing the result.

What this argument does not establish, however, is the number of prime factors of $p+2$, or any information about these prime factors. Suppose, for example, that one wanted to prove the existence of P_r numbers $p+2$, whose prime factors were all congruent to 1 modulo 4. One would then be obliged to attach a negative weight to all other primes, and the level of support on the innermost sum would not be limited to $x^{1/4} \log^B x$. This sum would then fail to be positive by a large margin.

The sieve of Goldston, Graham, Pintz, and Yıldırım has the advantage that positive contributions to S can easily be broken up, and it is the objective of this paper to exploit this advantage and prove several generalizations of their results. We shall be interested in bounding gaps between E_r numbers, for any $r \geq 2$, whose prime factors

are required to lie in an arbitrary well-distributed set $\mathcal{P}$. In the case of E_2 numbers, the analysis is carried out in [10], and we state the following mild generalization of ([10], Theorem XX):

Theorem 1.1. *Let $\mathcal{P}$ be an infinite set of primes of density δ satisfying condition $BV(\vartheta, \Delta)$ (see Section **??**), with $\vartheta \leq 1/2$, and let $L_i(x)(1 \leq i \leq k)$ be an admissable k-tuple of linear forms. Then there are $\nu + 1$ forms among them which take simultaneously E_2 numbers as values, each with both prime factors in $\mathcal{P}$, if*

$$k \geq \frac{4e^{-\gamma}(1 + o(1))}{B} e^{B\nu/4\delta^2}.$$

In the case of E_r numbers for $r \geq 3$, we will prove the following bound:

Theorem 1.2. *Let $\mathcal{P}$ be an infinite set of primes of density δ satisfying the Bombieri-Vinogradov condition $BV(\vartheta, \Delta)$, and let $L_i(x)(1 \leq i \leq k)$ be an admissable k-tuple of linear forms. For any $r \geq 3$, there are $\nu + 1$ forms among them which infinitely often take simultaneously E_r numbers as values, each with all prime factors in $\mathcal{P}$, if*

$$k > 3\exp\big(\big[\frac{29B\nu(r-1)!}{\delta^r}\big]^{\frac{1}{r-1}}\big)+2,$$

where

$$B := \max\left(\frac{2}{\vartheta}, r + 2\right).$$

We will also show that uniquely in the case $r \geq 3$, we can avoid the use of a Bombieri-Vinogradov theorem for the set $\mathcal{P}$, substituting instead a weaker Siegel-Walfisz condition. In this case we will prove the following bound:

Theorem 1.3. *With the same notation as in Theorem 1.2, if $\mathcal{P}$ instead satisfies a Siegel-Walfisz condition for an integer Δ (see Section **??**), then we may take*

$$k > 3\exp\big(\big[\frac{29\nu(r+4)(r-2)!}{\delta^r}\big]^{\frac{1}{r-2}}\big)+2.$$

Remark. We have stated our results for almost-primes whose prime factors are all required to be in the same set $\mathcal{P}$, but using an appropriate generalization of Lemma **??**, the above results generalize to the case of E_r numbers $n = p_1 p_2 \dots p_r$, with $p_1 < p_2 < \dots < p_r$, and $p_i \in \mathcal{P}_i$ for each i. In such a situation, δ^r would be replaced with the product of the δ_i. This allows us to prove similar bounds for almost-primes with a larger variety of conditions. In particular, if some multiplicative function f is defined on squarefree numbers, we could consider those almost primes n so that $f(n)$ takes a fixed value. If the density of such numbers is δ, then under appropriate assumptions we could replace the δ^r of any of the above theorems with δ.

To motivate our work, we consider several applications suggested by the work of Ono [17] and Balog and Ono [1] regarding elliptic curves and non-vanishing of modular L-functions. We start by recalling some notation (see, e.g., [11, 19] for definitions).

Given an elliptic curve $E/\mathbb{Q}$, we denote by $L(E,s)$ its Hasse-Weil L-function, and we define the Mordell-Weil rank $\mathrm{rk}(E) := \mathrm{rk}(E,\mathbb{Q})$ to be the rank of the (abelian) group of rational points on E. By Kolyvagin's work [12] on the Birch and Swinnerton-Dyer conjecture, we have $\mathrm{rk}(E) = 0$ for any E for which $L(E,1) \neq 0$.

If E is given by the equation

$$E: \quad y^2 = x^3 + ax^2 + bx + c$$

we define, for a fundamental discriminant D, the *D-quadratic twist* $E(D)$ by the equation

$$E(D): \quad Dy^2 = x^3 + ax^2 + bx + c.$$

It is natural to consider the set of D for which $L(E(D),1)) \neq 0$. We have the following conjecture of Goldfeld [7]:

Conjecture 1 (Goldfeld)**.** *If $E/\mathbb{Q}$ is an elliptic curve with conductor N, we have*

$$\sum_{\substack{|D|\leq X,\\ \gcd(D,N)=1}} \mathrm{ord}_{s=1}(L(E(D),s)) \sim \frac{1}{2} \sum_{\substack{|D|\leq X,\\ \gcd(D,N)=1}} 1. \tag{1.2}$$

where D ranges over all fundamental discriminants D with $-X \leq D \leq X$.

The strongest known result in this direction is due to Ono and Skinner [18]:

Theorem 1.4 (Ono-Skinner)**.** *For any elliptic curve E with conductor N we have the lower bound*

$$\#\{|D| \leq X \ : \ L(E(D),1) \neq 0 \text{ and } \gcd(D,N) = 1\} \gg \frac{X}{\log X}. \tag{1.3}$$

Moreover, for elliptic curves $E/\mathbb{Q}$ without a $\mathbb{Q}$-rational torsion point of order 2, Ono [17] improves (1.3) to

$$\#\{|D| \leq X \ : \ L(E(D),1) \neq 0 \text{ and } \gcd(D,N) = 1\} \gg \frac{X}{\log^{1-\alpha} X} \tag{1.4}$$

where α is the density of a certain set of primes S_F. Although these results are strong, they do not imply Corollary 1.6.

However, Ono proves (1.4) by giving an explicit description of a set of D satisfying the above conditions; essentially, such D come from products of primes in S_F, and we will then be able to apply Theorem 1.1 to the set S_F. To state Ono's result, we recall that a set of primes S has *Frobenius density* if there is a Galois extension $K/\mathbb{Q}$ with the property that those primes $p \in S$, up to finitely many exceptions, are distinguished as those primes for which the $\mathrm{Frob}(p)$ constitute a fixed conjugacy class or a union of conjugacy classes in $\mathrm{Gal}(K/\mathbb{Q})$. A Siegel-Walfisz condition for such an S is given by the Chebotarev Density Theorem [13], and in fact the stronger condition $BV(\vartheta,\Delta)$ is given by work of Murty and Murty [14].

We can now state Ono's result:

Theorem 1.5 (Ono [17]). *Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. Then there exists a number N and a set of primes S_F with positive Frobenius density with the property that for every positive integer j we have*

$$L(E(Np_1p_2\dots p_{2j}),1)\neq 0$$

and

$$\mathrm{rk}(E(Np_1p_2\dots p_{2j}),\mathbb{Q})=0$$

whenever $p_1,p_2,\dots,p_{2j}\in S_F$ are distinct primes not dividing N.

Taking $j=1$, Theorem 1.1 immediately implies the existence of bounded gaps:

Corollary 1.6. *Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. Then there exist a constant C_E and infinitely many pairs of squarefree integers m and n with*

$$L(E(m),1),\ L(E(n),1)\neq 0,$$
$$\mathrm{rk}(E(m))=\mathrm{rk}(E(n))=0,$$

and

$$|m-n|<C_E.$$

The constant C_E can be explicitly computed, and in Section **??** we do so for the elliptic curve $X_0(11)$.

We also consider the work of Balog and Ono [1]. For a large class of elliptic curves E, Balog and Ono prove lower bounds on the number of quadratic twists $E(n)$ with nonzero rank, with the additional property that their Shafarevich-Tate groups contain an element of order $\ell\in\{3,5,7\}$. For "good" curves E, they prove that these properties hold for the quadratic twists $E(-Mp_1\dots p_{2\ell})$, whenever there is a solution to the Diophantine equation

$$Mcp_1\dots p_{2\ell}=m^{2\ell}-n^2 \tag{1.5}$$

for certain values M and c, where the primes p_i are restricted to a set $\mathcal{P}$ satisfying a Siegel-Walfisz condition. Balog and Ono then use the circle method to prove a lower bound for the number of solutions of (1.5). It is natural to ask whether a result similar to Corollary 1.6 can be proved in this situation. Such a result would follow immediately if we could extend the result of Theorem 1.3 to the situation where we impose the additional condition (1.5). This problem is more difficult, and it suggests a potential application of bounding gaps between E_r numbers for larger values of r.

Although we do not currently have a proof, we can apply our methods to a related question concerning divisibility of class groups of quadratic fields. Balog and Ono's proof in [1] proceeds by using a result of Soundararajan [20], which shows that for any integer $g\geq 3$, the ideal class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$ contains an element of order g for any d satisfying a condition similar to (1.5). In the case $g=4$, Soundararajan gives a simple classification of such d, which establishes the following:

Proposition 1.7 (Soundararajan)**.** *Suppose $d \equiv 1 (\mod 8)$ is a squarefree integer whose prime factors are all congruent to $\pm 1 (\mod 8)$. Then the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$ contains an element of order 4.*

We may then apply Theorem 1.1, with the density $\frac{1}{8}$ in place of δ^2. Theorem 1.1 allows $k = 1675$, and choosing an appropriate 1675-tuple (see Section **??**) yields the following bound:

Corollary 1.8. *There exist infinitely many pairs of squarefree integers m and n, such that the class groups $\mathrm{Cl}(\mathbb{Q}(\sqrt{m}))$ and $\mathrm{Cl}(\mathbb{Q}(\sqrt{n}))$ each contain elements of order 4, with*

$$|m - n| \leq 15070.$$

Moreover, this bound may be improved by considering E_r numbers for multiple r. Subject to potential numerical imprecision, we were able to improve the bound 15070 to 94; a brief account is in Section **??**.

References

[1] A. Balog and K. Ono, *Elements of class groups and Shafarevich-Tate groups of elliptic curves*, Duke Math J. **120** (2003), 35-63.

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, 2nd ed., Astérisque 18. Société Mathématique de France, Paris, 1987.

[3] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in progression to large moduli*, Acta Math., **156** (1986), 203-251.

[4] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica, **16** (1973), 157-176.

[5] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and their Applications*, Cambridge University Press, Cambridge, 2005.

[6] T. J. Engelsma, *k-tuple permissible patterns*, http://www.opertech.com/primes/k-tuples.html.

[7] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108-118.

[8] D. A. Goldston, J. Pintz, and C.Y. Yıldırım, *Primes in Tuples I*, preprint.

[9] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım, *Small gaps between primes or almost primes*, preprint.

[10] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım, *Small gaps between products of two primes*, preprint.

[11] N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer-Verlag, New York, 1993.

[12] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Sha_{E/\mathbb{Q}}$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk., USSR, ser. Matem. **52** (1988), 522-540.

[13] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev Density Theorem*. Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 409-464. Academic Press, London, 1977.

[14] M. R. Murty and V. K. Murty, *A variant of the Bombieri-Vinogradov theorem*, Canadian Math. Soc. Conf. Proc., Vol. 7 (1987), 243-272.

[15] Y. Motohashi, *An induction principle for the generalization of Bombieri's prime number theorem*, Proc. Japan Acad., **52** (1976), 273-275.

[16] K. Ono, *Twists of elliptic curves*, Compositio Math., **106** (1997), 349-360.
[17] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. math., **533** (2001), 81-97.
[18] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math. **134**, 1998, 651-660.
[19] J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.
[20] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc., **61** (2000), 681-690.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: thorne@math.wisc.edu