Bounded Gaps Between Products of Primes with Applications to Elliptic Curves and Modular L-functions

Frank Thorne

University of Wisconsin - Madison

May 16, 2007

Work of Goldston, Graham, Pintz, Yıldırım

Notation:
$p_n := n^{\text{th}}$ prime
$q_n := n^{\text{th}}$ E_2 number (product of two primes)

Theorem (Goldston, Pintz, Yıldırım)

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

Theorem (Goldston, Graham, Pintz, Yıldırım)

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

Natural Questions

Natural generalizations:

Natural Questions

Natural generalizations:

- Can a similar bound be proved for E_r numbers, for any $r \geq 3$?

Natural Questions

Natural generalizations:

- Can a similar bound be proved for E_r numbers, for any $r \geq 3$?
- Can a similar bound be proved when the prime factors are required to lie in some "nice" set of primes $\mathcal{P}$?

Natural Questions

Natural generalizations:

- Can a similar bound be proved for E_r numbers, for any $r \geq 3$?
- Can a similar bound be proved when the prime factors are required to lie in some "nice" set of primes $\mathcal{P}$?

Yes.

Main Theorem

Notation:

$\mathcal{P} :=$ subset of the primes; must be "fairly well distributed".

$q_n := n^{\text{th}}$ E_r number with all prime factors in $\mathcal{P}$.

Main Theorem

Notation:
$\mathcal{P}$:= subset of the primes; must be "fairly well distributed".
$q_n := n^{\text{th}}$ E_r number with all prime factors in $\mathcal{P}$.

Theorem (T.)

For any such $\mathcal{P}$ and $r \geq 2$ there exists an explicit constant $C(r, \mathcal{P})$ such that

$$\liminf_{n \to \infty} (q_{n+1} - q_n) \leq C(r, \mathcal{P}).$$

Main Theorem

Notation:
$\mathcal{P}$:= subset of the primes; must be "fairly well distributed".
$q_n := n^{\text{th}}$ E_r number with all prime factors in $\mathcal{P}$.

Theorem (T.)

For any such $\mathcal{P}$ and $r \geq 2$ there exists an explicit constant $C(r, \mathcal{P})$ such that

$$\liminf_{n \to \infty} (q_{n+1} - q_n) \leq C(r, \mathcal{P}).$$

We will describe our result more explicitly, and give some applications.

Conditions on $\mathcal{P}$

- $\mathcal{P}$ = a set of primes with a natural density > 0.

Conditions on $\mathcal{P}$

- $\mathcal{P}$ = a set of primes with a natural density > 0.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a *Bombieri-Vinogradov* or *Siegel-Walfisz condition.*

Conditions on $\mathcal{P}$

- $\mathcal{P}$ = a set of primes with a natural density > 0.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a *Bombieri-Vinogradov* or *Siegel-Walfisz condition.*
- An exceptional modulus M is allowed: we can allow bad distribution modulo q when $(q, M) > 1$.

Admissible k-tuples

An *M-admissable k-tuple* is a set

$$\{a_1 n + b_1, \ldots, a_k n + b_k\}$$

which:

Admissible k-tuples

An *M-admissable k-tuple* is a set

$$\{a_1 n + b_1, \ldots, a_k n + b_k\}$$

which:

- never simultaneously represents all residue classes modulo p, for any prime p.

Admissible k-tuples

An *M-admissable k-tuple* is a set

$$\{a_1 n + b_1, \ldots, a_k n + b_k\}$$

which:

- never simultaneously represents all residue classes modulo p, for any prime p.
- satisfies $a_i | M$ and $(M, a_i/M) = 1$ for each i.

Admissible k-tuples, cont.

Goal: Infinitely often, two or more $a_i n + b_i$ represent E_r numbers.
If $a_1 = \cdots = a_k = M$, our k-tuple gives bounded gaps.

Admissible k-tuples, cont.

Goal: Infinitely often, two or more $a_i n + b_i$ represent E_r numbers.
If $a_1 = \cdots = a_k = M$, our k-tuple gives bounded gaps.

To each linear form, associate a *density* δ_i: the proportion of E_r numbers represented by $a_i n + b_i$ which are products of primes in $\mathcal{P}$.

Admissible k-tuples, cont.

Goal: Infinitely often, two or more $a_i n + b_i$ represent E_r numbers.
If $a_1 = \cdots = a_k = M$, our k-tuple gives bounded gaps.

To each linear form, associate a *density* δ_i: the proportion of E_r numbers represented by $a_i n + b_i$ which are products of primes in $\mathcal{P}$.

Write δ for the minimum of the δ_i.

Bounded gaps between E_2 numbers

Theorem

Suppose $\mathcal{P}$ satisfies BV with a level of distribution ϑ. Let $\{L_i(n)\}$ be an M-admissable k-tuple of linear forms. There are $\nu + 1$ forms among them which simultaneously represent E_2 numbers with prime factors in $\mathcal{P}$ infinitely often, provided

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

Very similar to a result proved in [GGPY2].
We may take

$$o_k(1) = \frac{1}{3}\left(\frac{5}{k} + \frac{1}{\sqrt{k}}\right).$$

Bounded gaps between E_r numbers ($r \geq 3$)

Theorem

Suppose $\mathcal{P}$ satisfies BV with a level of distribution ϑ, and let $\{L_i(n)\}$ be an admissable k-tuple. There are $\nu + 1$ forms among them which simultaneously represent E_r numbers with prime factors in $\mathcal{P}$ infinitely often, provided

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

where

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

Bounded gaps between E_r numbers ($r \geq 3$), II

For the weaker Siegel-Walfisz condition:

Theorem

Suppose $\mathcal{P}$ satisfies SW, and let $\{L_i(n)\}$ be an M-admissable k-tuple. There are $\nu + 1$ forms which simultaneously represent E_r numbers with prime factors in $\mathcal{P}$ infinitely often, provided

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

Sketch of the proof

Follow the same idea as GPY/GGPY. Consider

$$S = \sum_{n=N}^{2N} \left(\sum_{i=1}^{k} \beta_r(a_i n + b_i) - \nu \right) \left(\sum_{d \mid \prod_i (a_i n + b_i)} \lambda_d \right)^2,$$

where
$\beta_r(n)$ = characteristic function of "good" E_r's,
λ_d = any real numbers.

Sketch of the proof

Follow the same idea as GPY/GGPY. Consider

$$S = \sum_{n=N}^{2N} \left(\sum_{i=1}^{k} \beta_r(a_i n + b_i) - \nu \right) \left(\sum_{d \mid \prod_i (a_i n + b_i)} \lambda_d \right)^2,$$

where

$\beta_r(n) =$ characteristic function of "good" E_r's,

$\lambda_d =$ any real numbers.

Goal: Prove $S > 0$.

Sketch of the proof (cont.)

Break S up:

$$S^- = \sum_{N<n\leq 2N} \left(\sum_{d \mid \prod_i (a_i n + b_i)} \lambda_d \right)^2$$

and

$$S_j^+ = \sum_{N<n\leq 2N} \beta_r(a_j n + b_j) \left(\sum_{d \mid \prod_i (a_i n + b_i)} \lambda_d \right)^2 .$$

Choose λ_d so S^- is small and S_j^+ is large.
Our choice of λ_d will be as in the Selberg sieve.

Sketch of the proof (cont.)

- Change the order of summation, use BV estimates and Selberg diagonalization.

Sketch of the proof (cont.)

- Change the order of summation, use BV estimates and Selberg diagonalization.
- Write our sums as nonnegative Stieltjes integrals, and approximate by integrals of smooth functions.

Sketch of the proof (cont.)

- Change the order of summation, use BV estimates and Selberg diagonalization.
- Write our sums as nonnegative Stieltjes integrals, and approximate by integrals of smooth functions.
- Bound these integrals from below (or evaluate them numerically.)

Applications

Bound gaps interesting integers n that satisfy interesting properties, such as:

- The class number $h(\mathbb{Q}(\sqrt{-n}))$ is divisible or indivisible by some fixed integer k.

Applications

Bound gaps interesting integers n that satisfy interesting properties, such as:

- The class number $h(\mathbb{Q}(\sqrt{-n}))$ is divisible or indivisible by some fixed integer k.
- For a fixed elliptic curve $E/\mathbb{Q}$, the quadratic twist $E(n)$ has rank 0.

Applications

Bound gaps interesting integers n that satisfy interesting properties, such as:

- The class number $h(\mathbb{Q}(\sqrt{-n}))$ is divisible or indivisible by some fixed integer k.
- For a fixed elliptic curve $E/\mathbb{Q}$, the quadratic twist $E(n)$ has rank 0.
- As above, and moreover, the Shafarevich-Tate group of $E(n)$ has an element of order $\ell > 1$.

Applications

Bound gaps interesting integers n that satisfy interesting properties, such as:

- The class number $h(\mathbb{Q}(\sqrt{-n}))$ is divisible or indivisible by some fixed integer k.
- For a fixed elliptic curve $E/\mathbb{Q}$, the quadratic twist $E(n)$ has rank 0.
- As above, and moreover, the Shafarevich-Tate group of $E(n)$ has an element of order $\ell > 1$.

We apply works of Ono, Balog-Ono, Murty-Murty, and Soundararajan to address some of these applications.

Class numbers

Theorem (Soundararajan)

Suppose $d \equiv 1 \mod 8$ *is positive and square-free with all prime factors* $\equiv \pm 1 \mod 8$*. Then* $Cl(\mathbb{Q}(\sqrt{-d}))$ *has an element of order 4.*

Class numbers

Theorem (Soundararajan)

Suppose $d \equiv 1 \mod 8$ *is positive and square-free with all prime factors* $\equiv \pm 1 \mod 8$*. Then* $Cl(\mathbb{Q}(\sqrt{-d}))$ *has an element of order 4.*

Corollary

There are infinitely many pairs of E_2 *numbers, say* m *and* n*, such that the class groups* $Cl(\mathbb{Q}(\sqrt{-m}))$ *and* $Cl(\mathbb{Q}(\sqrt{-n}))$ *each have elements of order 4, with*

$$|m - n| \leq 64.$$

Class numbers: the proof

Consider the 6-tuple

$$\mathcal{L} = \{8n + 49, 8n + 65, 8n + 73, 8n + 89, 8n + 97, 8n + 113\}.$$

Half of the E_2 numbers represented will meet Soundararajan's condition. So our density δ is $1/2$.

Class numbers: the proof

Consider the 6-tuple

$$\mathcal{L} = \{8n + 49, 8n + 65, 8n + 73, 8n + 89, 8n + 97, 8n + 113\}.$$

Half of the E_2 numbers represented will meet Soundararajan's condition. So our density δ is $1/2$.
This is a lot better than $1/8$.

Class numbers: the proof

Consider the 6-tuple

$$\mathcal{L} = \{8n + 49, 8n + 65, 8n + 73, 8n + 89, 8n + 97, 8n + 113\}.$$

Half of the E_2 numbers represented will meet Soundararajan's condition. So our density δ is $1/2$.
This is a lot better than $1/8$.
Check: our E_2 theorem allows $k = 6$.

Elliptic curves: background

Given an elliptic curve

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

If D is a fundamental discriminant, the *D-quadratic twist* is

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

Question

How do the ranks of $E(D)$ vary with D?

Elliptic curves: background

Given an elliptic curve

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

If D is a fundamental discriminant, the *D-quadratic twist* is

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

Question

How do the ranks of $E(D)$ vary with D?

Conjecture (Goldfeld)

$$\sum_D \mathrm{ord}_{s=1}(L(E(D), s)) \sim \frac{1}{2} \sum_D 1.$$

Ono's result

Theorem (Ono)

Suppose E does not have a $\mathbb{Q}$-torsion point of order 2. Then

$$\#\{D : |D| \leq X, L(E(D), 1) \neq 0\} \gg \frac{X}{\log^{1-\alpha} X},$$

where α is the density of a Chebotarev set of primes S_E.

Ono's result

Theorem (Ono)

Suppose E does not have a $\mathbb{Q}$-torsion point of order 2. Then

$$\#\{D : |D| \leq X, L(E(D), 1) \neq 0\} \gg \frac{X}{\log^{1-\alpha} X},$$

where α is the density of a Chebotarev set of primes S_E.
The D are constructed as products

$$Np_1 p_2 \ldots p_{2j},$$

for primes $p_i \in S_E$.

Bounded gaps for elliptic curves

Theorem (Murty-Murty)

Chebotarev sets satisfy BV.

Bounded gaps for elliptic curves

Theorem (Murty-Murty)

Chebotarev sets satisfy BV.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. There is $C_E > 0$ and infinitely many pairs of square-free integers m and n for which:
(i) $L(E(m), 1) \cdot L(E(n), 1) \neq 0$,
(ii) $\mathit{rank}(E(m)) = \mathit{rank}(E(n)) = 0$,
(iii) $|m - n| < C_E$.

Bounded gaps for elliptic curves

Theorem (Murty-Murty)

Chebotarev sets satisfy BV.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. There is $C_E > 0$ and infinitely many pairs of square-free integers m and n for which:
(i) $L(E(m), 1) \cdot L(E(n), 1) \neq 0$,
(ii) $\mathit{rank}(E(m)) = \mathit{rank}(E(n)) = 0$,
(iii) $|m - n| < C_E$.

This can be made effective for particular examples.

Question on Shafarevich-Tate Groups

Look at D such that $E(D)$ has rank 0 and an element of order $\ell \in \{3, 5, 7\}$ in the Shafarevich-Tate group. Can we say anything?

Question on Shafarevich-Tate Groups

Look at D such that $E(D)$ has rank 0 and an element of order $\ell \in \{3, 5, 7\}$ in the Shafarevich-Tate group. Can we say anything? By work of Balog and Ono, we should find solutions to an equation

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

with $p_i \in S_E$.

Question on Shafarevich-Tate Groups

Look at D such that $E(D)$ has rank 0 and an element of order $\ell \in \{3, 5, 7\}$ in the Shafarevich-Tate group. Can we say anything? By work of Balog and Ono, we should find solutions to an equation

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

with $p_i \in S_E$.
Get a simultaneous multiplicative and additive question. Can one prove bounded gaps? We would be interested to see a proof.