Bounded gaps between products of special primes

Ping Ngai (Brian) Chung (MIT),

Shiyu Li (UC Berkeley)

January 17, 2014

Bounded gaps between primes

Let p_n be the n^{th} prime.

Theorem (Goldston, Pintz, Yıldırım)

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

Bounded gaps between primes

Let p_n be the n^{th} prime.

Theorem (Goldston, Pintz, Yıldırım)

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

Theorem (Zhang)

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \le C.$$

Bounded gaps between primes

Let p_n be the n^{th} prime.

Theorem (Goldston, Pintz, Yıldırım)

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

Theorem (Zhang)

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq C.$$

- Zhang: $C \leq 7 \times 10^7$,

Bounded gaps between primes

Let p_n be the n^{th} prime.

Theorem (Goldston, Pintz, Yıldırım)

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

Theorem (Zhang)

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq C.$$

- Zhang: $C \leq 7 \times 10^7$,
- Maynard-Tao: $C \leq 600$,

Bounded gaps between primes

Let p_n be the n^{th} prime.

Theorem (Goldston, Pintz, Yıldırım)

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

Theorem (Zhang)

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq C.$$

- Zhang: $C \leq 7 \times 10^7$,
- Maynard-Tao: $C \leq 600$,
- Polymath: $C \leq 270$.

Generalizations

Generalizations:

- Bounded gaps between E_r numbers (product of r distinct primes) for $r \geq 2$?
- Restrict to a "nice" subset of primes $\mathcal{P}$?

Work of Thorne

Let $\mathcal{P}$ be a "well-distributed" subset of primes,
q_n be the n^{th} E_r number with all prime factors in $\mathcal{P}$.

Theorem (Thorne)

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

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

Applications

Thorne's main result leads to several corollaries:

Bounded gaps between integers n with special properties:

1. The class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-n}))$ contains order 4 elements.
2. Given an elliptic curve $E/\mathbb{Q}$, the quadratic twist $E(n)$ has rank 0 and $L(E(n), 1) \neq 0$.

Our observation

We observe that in Thorne's applications, without a restriction on the number of prime factors, much improved bounds are possible.

Our observation

We observe that in Thorne's applications, without a restriction on the number of prime factors, much improved bounds are possible.

Let $\mathcal{P}$ be a "well-distributed" subset of primes,

q_n be the n^{th} square-free number with all prime factors in $\mathcal{P}$.

Theorem (C., Li)

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

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

Our observation

We observe that in Thorne's applications, without a restriction on the number of prime factors, much improved bounds are possible.

Let $\mathcal{P}$ be a "well-distributed" subset of primes,

q_n be the n^{th} square-free number with all prime factors in $\mathcal{P}$.

Theorem (C., Li)

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

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

Here, the constant $C(\mathcal{P})$ is smaller than $C(r, \mathcal{P})$ for all $r \geq 2$.

Our observation

We observe that in Thorne's applications, without a restriction on the number of prime factors, much improved bounds are possible.

Let $\mathcal{P}$ be a "well-distributed" subset of primes,
q_n be the n^{th} square-free number with all prime factors in $\mathcal{P}$.

Theorem (C., Li)

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

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

Here, the constant $C(\mathcal{P})$ is smaller than $C(r, \mathcal{P})$ for all $r \geq 2$.

We will make the statement precise. Then we revisit Thorne's examples and give better bounds on gaps.

Regularity condition on $\mathcal{P}$

Following Thorne, we require that

- $\mathcal{P}$ is a set of primes with positive "nice" density.

Regularity condition on $\mathcal{P}$

Following Thorne, we require that

- $\mathcal{P}$ is a set of primes with positive "nice" density.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a Siegel-Walfisz condition $SW(M)$,

Regularity condition on $\mathcal{P}$

Following Thorne, we require that

- $\mathcal{P}$ is a set of primes with positive "nice" density.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a Siegel-Walfisz condition $SW(M)$,
- where M is an exceptional modulus: we allow bad distribution modulo q for $(q, M) > 1$.

Regularity condition on $\mathcal{P}$

Following Thorne, we require that

- $\mathcal{P}$ is a set of primes with positive "nice" density.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a Siegel-Walfisz condition $SW(M)$,
- where M is an exceptional modulus: we allow bad distribution modulo q for $(q, M) > 1$.

$E_{\mathcal{P}}$ number: a square-free number with all prime factors in $\mathcal{P}$.

Regularity condition on $\mathcal{P}$

Following Thorne, we require that

- $\mathcal{P}$ is a set of primes with positive "nice" density.
- $\mathcal{P}$ is well-distributed in arithmetic progressions: $\mathcal{P}$ satisfies a Siegel-Walfisz condition $SW(M)$,
- where M is an exceptional modulus: we allow bad distribution modulo q for $(q, M) > 1$.

$E_{\mathcal{P}}$ number: a square-free number with all prime factors in $\mathcal{P}$.

Goal: Prove bounded gaps between $E_{\mathcal{P}}$ numbers.

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

For our purpose, we often take $a_1 = \cdots = a_k = M$.

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

For our purpose, we often take $a_1 = \cdots = a_k = M$.

Density δ_i = the proportion of $E_{\mathcal{P}}$ numbers represented by $a_i n + b_i$.

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

For our purpose, we often take $a_1 = \cdots = a_k = M$.

Density δ_i = the proportion of $E_{\mathcal{P}}$ numbers represented by $a_i n + b_i$.
Minimum density δ = minimum of δ_i.

M-admissible k-tuples

An M-admissible k-tuple is a set of linear forms

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

that

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

For our purpose, we often take $a_1 = \cdots = a_k = M$.

Density δ_i = the proportion of $E_{\mathcal{P}}$ numbers represented by $a_i n + b_i$.
Minimum density δ = minimum of δ_i.

Strategy: If at least two $Mn + b_i$ represent $E_{\mathcal{P}}$ numbers infinitely often, our k-tuple gives bounded gaps (bounded by $b_k - b_1$).

Precise Statement

Let $\mathcal{P}$ be a set of prime with density $\alpha > 0$ that satisfies $SW(M)$, $\{a_i n + b_i\}$ be an M-admissible k-tuple with minimum density δ.

Precise Statement

Let $\mathcal{P}$ be a set of prime with density $\alpha > 0$ that satisfies $SW(M)$, $\{a_i n + b_i\}$ be an M-admissible k-tuple with minimum density δ.

Theorem (C., Li)

There are at least $\nu + 1$ forms among them which infinitely often simultaneously represent $E_{\mathcal{P}}$ numbers, provided that

$$k > \nu \frac{4^{1-\alpha}}{\delta\phi(M)} \frac{\mathfrak{b}(0,\alpha)\mathfrak{b}(1,\alpha)}{\mathfrak{b}(k,\alpha)} (1-\alpha)^2 \Gamma(\alpha)\Gamma(1-\alpha),$$

where

$$\mathfrak{b}(k,\alpha) := \frac{\Gamma(1-\alpha)\Gamma(k(1-\alpha)+1)}{\Gamma((k+1)(1-\alpha)+1)}.$$

Precise Statement (twin-prime type)

As a corollary (for $\nu = 1$, $k = 2$), we have a twin-prime type result.

Precise Statement (twin-prime type)

As a corollary (for $\nu = 1$, $k = 2$), we have a twin-prime type result.

Let $\mathcal{P}$ be a set of prime with density $\alpha > 0$ that satisfies $SW(M)$, δ be the minimum density of the pair $(Mn, Mn + d)$.

Corollary

For any even number d, assume that $\delta\phi(M) > F(\alpha)$, where

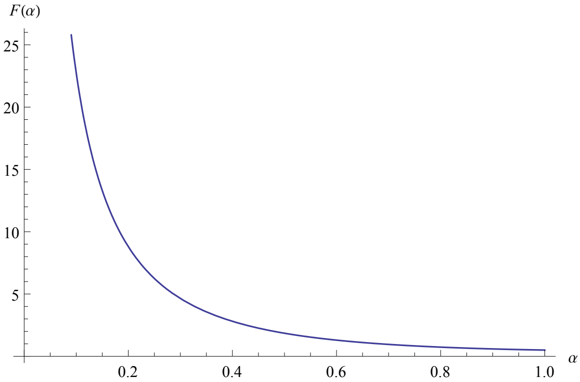
$$F(\alpha) = 2^{1-2\alpha} \frac{\mathfrak{b}(0,\alpha)\mathfrak{b}(1,\alpha)}{\mathfrak{b}(2,\alpha)} (1-\alpha)^2 \Gamma(\alpha)\Gamma(1-\alpha).$$

Then there are infinitely many n for which n and $n + d$ are simultaneously $E_{\mathcal{P}}$ numbers.

Plot

Corollary

For any even number d, assume that $\delta\phi(M) > F(\alpha)$, then there are infinitely many n for which n and $n+d$ are simultaneously $E_{\mathcal{P}}$ numbers.



Sketch of the proof

Following the same idea as GPY/GGPY and Thorne, consider

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

where

- $\chi_{\mathcal{P}}$ is the characteristic function of $E_{\mathcal{P}}$ numbers,
- λ_d is any real numbers.

Sketch of the proof

Following the same idea as GPY/GGPY and Thorne, consider

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

where

- $\chi_{\mathcal{P}}$ is the characteristic function of $E_{\mathcal{P}}$ numbers,
- λ_d is any real numbers.

If $S > 0$ for all large N, the theorem is true.

Sketch of the proof

Following the same idea as GPY/GGPY and Thorne, consider

$$S = \sum_{n=N}^{2N} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(a_i n + b_i) - \nu \right) \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2 ,$$

where

- $\chi_{\mathcal{P}}$ is the characteristic function of $E_{\mathcal{P}}$ numbers,
- λ_d is any real numbers.

If $S > 0$ for all large N, the theorem is true.

Remark: The additional requirement that $p \nmid d$ for all $p \in \mathcal{P}$ gives a bigger sieve weight to those n for which $\prod_i (a_i n + b_i)$ is divisible by many primes in $\mathcal{P}$.

Sketch of the proof

Break S up into

$$S_0 := \sum_{n=N}^{2N} \left(\sum_{\substack{d | \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2,$$

and

$$S_{1,j} = \sum_{n=N}^{2N} \chi_{\mathcal{P}}(a_j n + b_j) \left(\sum_{\substack{d | \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2.$$

Sketch of the proof

Break S up into

$$S_0 := \sum_{n=N}^{2N} \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2,$$

and

$$S_{1,j} = \sum_{n=N}^{2N} \chi_{\mathcal{P}}(a_j n + b_j) \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2.$$

Then $S = \sum_{j=1}^{k} S_{1,j} - \nu S_0$.

Sketch of the proof

Break S up into

$$S_0 := \sum_{n=N}^{2N} \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2 ,$$

and

$$S_{1,j} = \sum_{n=N}^{2N} \chi_{\mathcal{P}}(a_j n + b_j) \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2 .$$

Then $S = \sum_{j=1}^{k} S_{1,j} - \nu S_0$.
Choose the sieve weights λ_d so that S_0 is small and $S_{1,j}$ is big.

Sketch of the proof

Break S up into

$$S_0 := \sum_{n=N}^{2N} \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2 ,$$

and

$$S_{1,j} = \sum_{n=N}^{2N} \chi_{\mathcal{P}}(a_j n + b_j) \left(\sum_{\substack{d \mid \prod_i (a_i n + b_i) \\ p \nmid d \forall p \in \mathcal{P}}} \lambda_d \right)^2 .$$

Then $S = \sum_{j=1}^{k} S_{1,j} - \nu S_0$.
Choose the sieve weights λ_d so that S_0 is small and $S_{1,j}$ is big.
Estimate $S_{1,j}$, S_0: use BV estimate and Selberg diagonalization.

Applications

We now revisit two of Thorne's applications:

Bounded gaps between integers n with special properties:

1. The class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-n}))$ contains order 4 elements.
2. Given an elliptic curve $E/\mathbb{Q}$, the quadratic twist $E(n)$ has rank 0 and $L(E(n),1) \neq 0$.

Ideal class groups with order 4 elements

Thorne's main result leads to the corollary:

Corollary

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

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

Ideal class groups with order 4 elements

Our main result yields:

Corollary

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

$$|m - n| \leq 8.$$

Ideal class groups with order 4 elements

Theorem (Soundararajan)

For any positive square-free number $d \equiv 1 \bmod 8$ whose prime factors $\equiv \pm 1 \bmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

Ideal class groups with order 4 elements

Theorem (Soundararajan)

For any positive square-free number $d \equiv 1 \bmod 8$ whose prime factors $\equiv \pm 1 \bmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

$\mathcal{P}$:= the set of primes $\equiv \pm 1 \bmod 8$,

Ideal class groups with order 4 elements

Theorem (Soundararajan)

For any positive square-free number $d \equiv 1 \bmod 8$ whose prime factors $\equiv \pm 1 \bmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

$\mathcal{P} :=$ the set of primes $\equiv \pm 1 \bmod 8$, $\quad \delta = 1/2$, $\alpha = 1/2$, $M = 8$.

Ideal class groups with order 4 elements

Theorem (Soundararajan)

For any positive square-free number $d \equiv 1 \bmod 8$ whose prime factors $\equiv \pm 1 \bmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

$\mathcal{P}$:= the set of primes $\equiv \pm 1$ mod 8, $\delta = 1/2$, $\alpha = 1/2$, $M = 8$.
Check that $\delta\phi(M) > F(\alpha)$, therefore

Ideal class groups with order 4 elements

Theorem (Soundararajan)

For any positive square-free number $d \equiv 1 \bmod 8$ whose prime factors $\equiv \pm 1 \bmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

$\mathcal{P}$:= the set of primes $\equiv \pm 1 \bmod 8$, $\delta = 1/2$, $\alpha = 1/2$, $M = 8$.
Check that $\delta\phi(M) > F(\alpha)$, therefore

Corollary

There are infinitely many square-free numbers n such that the class groups $\mathrm{Cl}(\mathbb{Q}(\sqrt{-n}))$ and $\mathrm{Cl}(\mathbb{Q}(\sqrt{-n-8}))$ each contain elements of order 4.

Quadratic twists of Elliptic curves

Thorne's main result leads to the corollary:

Corollary

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) $rank(E(m)) = rank(E(n)) = 0$,

(iii) $|m - n| \leq C_E$.

Quadratic twists of Elliptic curves

Thorne's main result leads to the corollary:

Corollary

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) $rank(E(m)) = rank(E(n)) = 0$,

(iii) $|m - n| \leq C_E$.

For $E := X_0(11)$, Thorne calculated that $C_E \leq 6152146$.

Quadratic twists of Elliptic curves

Thorne's main result leads to the corollary:

Corollary

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) $rank(E(m)) = rank(E(n)) = 0$,

(iii) $|m-n| \leq C_E$.

For $E := X_0(11)$, Thorne calculated that $C_E \leq 6152146$.
Our result yields that $C_E \leq 48$.

Quadratic twists of Elliptic curves

Thorne's main result leads to the corollary:

Corollary

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) $rank(E(m)) = rank(E(n)) = 0$,

(iii) $|m - n| \leq C_E$.

For $E := X_0(11)$, Thorne calculated that $C_E \leq 6152146$.
Our result yields that $C_E \leq 48$.
The proof uses results by Ono and Murty-Murty.

Further improvement

Recall the main result:

Corollary

For any even number d, assume that $\delta\phi(M) > F(\alpha)$, where

$$F(\alpha) = 2^{1-2\alpha}\frac{\mathfrak{b}(0,\alpha)\mathfrak{b}(1,\alpha)}{\mathfrak{b}(2,\alpha)}(1-\alpha)^2\Gamma(\alpha)\Gamma(1-\alpha).$$

Then there are infinitely many n for which n and $n+d$ are simultaneously $E_{\mathcal{P}}$ numbers.

Further improvement

Recall the main result:

Corollary

For any even number d, assume that $\delta\phi(M) > F(\alpha)$, where

$$F(\alpha) = 2^{1-2\alpha}\frac{\mathfrak{b}(0,\alpha)\mathfrak{b}(1,\alpha)}{\mathfrak{b}(2,\alpha)}(1-\alpha)^2\Gamma(\alpha)\Gamma(1-\alpha).$$

Then there are infinitely many n for which n and $n+d$ are simultaneously $E_{\mathcal{P}}$ numbers.

J. Thorner has recently applied Maynard's method to obtain stronger results in these applications (if we consider only primes with the special properties).

Further improvement

Recall the main result:

Corollary

For any even number d, assume that $\delta\phi(M) > F(\alpha)$, where

$$F(\alpha) = 2^{1-2\alpha}\frac{\mathfrak{b}(0,\alpha)\mathfrak{b}(1,\alpha)}{\mathfrak{b}(2,\alpha)}(1-\alpha)^2\Gamma(\alpha)\Gamma(1-\alpha).$$

Then there are infinitely many n for which n and $n+d$ are simultaneously $E_{\mathcal{P}}$ numbers.

J. Thorner has recently applied Maynard's method to obtain stronger results in these applications (if we consider only primes with the special properties).

Using Maynard's new sieve method may improve our main result.