Product sets of arithmetic progressions

Yunkun Zhou

Stanford University

SCMS, Dec. 2022

Joint work with Max Wenqiang Xu

Coauthor

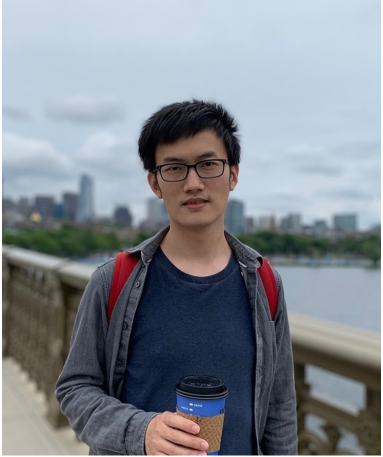

Figure: Max Wenqiang Xu

Contents

Erdős Multiplication table problem

How large is $M(N) := |[N] \cdot [N]|$?

Fact

$$M(N) := o(N^2).$$

Erdős Multiplication table problem

How large is $M(N) := |[N] \cdot [N]|$?

Fact

$$M(N) := o(N^2).$$

Sketch of the proof

Hardy-Ramanujan theorem: all but at most $o(N)$ number of $n \leq N$ have $\log \log N$ number of prime factors (with multiplicities).

Erdős Multiplication table problem

How large is $M(N) := |[N] \cdot [N]|$?

Fact

$$M(N) := o(N^2).$$

Sketch of the proof

Hardy-Ramanujan theorem: all but at most $o(N)$ number of $n \leq N$ have $\log\log N$ number of prime factors (with multiplicities). Thus all but at most $o(N^2)$ elements in the multiplication table have $2\log\log N$ number of prime factors,

Erdős Multiplication table problem

How large is $M(N) := |[N] \cdot [N]|$?

Fact

$$M(N) := o(N^2).$$

Sketch of the proof

Hardy-Ramanujan theorem: all but at most $o(N)$ number of $n \leq N$ have $\log\log N$ number of prime factors (with multiplicities). Thus all but at most $o(N^2)$ elements in the multiplication table have $2\log\log N$ number of prime factors, which is different from typical integers $n \leq N^2$ having $\log\log N^2$ number of prime factors.

Erdős Multiplication table problem

Summary

Let $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086\ldots$.

1. Erdős (1960):
$$M(N) = \frac{N^2}{(\log N)^{\delta+o(1)}}.$$

Erdős Multiplication table problem

Summary

Let $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086\ldots$.

1. Erdős (1960):
$$M(N) = \frac{N^2}{(\log N)^{\delta+o(1)}}.$$
2. Tenenbaum (1984):
$$M(N) \geq \frac{N^2}{(\log N)^{\delta} \exp((\log\log N)^{1/2+\varepsilon})}.$$

Erdős Multiplication table problem

Summary

Let $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086\ldots$.

1. Erdős (1960):
$$M(N) = \frac{N^2}{(\log N)^{\delta+o(1)}}.$$

2. Tenenbaum (1984):
$$M(N) \geq \frac{N^2}{(\log N)^{\delta}\exp((\log\log N)^{1/2+\varepsilon})}.$$

3. Ford (2008):
$$M(N) \asymp \frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}.$$

Elekes-Ruzsa's Conjecture

Elekes-Ruzsa's Conjecture (2003)

Let $A \subset \mathbb{Z}$ be a finite arithmetic progressions of length N. Then

$$|A \cdot A| \gg \frac{N^2}{(\log N)^{\delta + o(1)}}.$$

Elekes-Ruzsa's Conjecture

Elekes-Ruzsa's Conjecture (2003)

Let $A \subset \mathbb{Z}$ be a finite arithmetic progressions of length N. Then

$$|A \cdot A| \gg \frac{N^2}{(\log N)^{\delta+o(1)}}.$$

Theorem 1 (X.-Zhou, 2022+)

The conjecture above is true.

Elekes-Ruzsa's Conjecture

Elekes-Ruzsa's Conjecture (2003)

Let $A \subset \mathbb{Z}$ be a finite arithmetic progressions of length N. Then

$$|A \cdot A| \gg \frac{N^2}{(\log N)^{\delta + o(1)}}.$$

Theorem 1 (X.-Zhou, 2022+)

The conjecture above is true.

Remark

The strongest version we can prove is, for some $c > 0$

$$|A \cdot A| \gg \frac{N^2}{(\log N)^{\delta} (\log \log N)^{c}}.$$

Sum-Product conjecture

Sum-Product Conjecture (Erdős-Szemerédi, 1983)

Let $A \subset \mathbb{Z}$ ($\subset \mathbb{R}$) be a finite set. Then,

$$\max\{|A+A|, |A\cdot A|\} \geq |A|^{2-o(1)}.$$

Sum-Product conjecture

Sum-Product Conjecture (Erdős-Szemerédi, 1983)

Let $A \subset \mathbb{Z}$ ($\subset \mathbb{R}$) be a finite set. Then,

$$\max\{|A+A|, |A \cdot A|\} \geq |A|^{2-o(1)}.$$

Record (Rudnev-Stevens, 2020)

$$\max\{|A+A|, |A \cdot A|\} \geq |A|^{\frac{4}{3}+\frac{2}{1167}-o(1)}.$$

Extremal Sum-Product Conjecture

Extremal cases

Let $A \subset \mathbb{Z}$ be a finite set.

1. Chang's Theorem (2003): $|A \cdot A| \ll |A| \implies |A + A| \gg |A|^2$.

Extremal Sum-Product Conjecture

Extremal cases

Let $A \subset \mathbb{Z}$ be a finite set.

1. Chang's Theorem (2003): $|A \cdot A| \ll |A| \implies |A + A| \gg |A|^2$.
2. $|A + A| \ll |A| \implies |A \cdot A| \gg ?$

Extremal Sum-Product Conjecture

Extremal cases

Let $A \subset \mathbb{Z}$ be a finite set.

1. Chang's Theorem (2003): $|A \cdot A| \ll |A| \implies |A + A| \gg |A|^2$.
2. $|A + A| \ll |A| \implies |A \cdot A| \gg ?$

Progress on the case with small sumset

1. Chang (unpublished notes): $|A + A| \ll |A| \implies |A \cdot A| \gg |A|^{2-o(1)}$.

Extremal Sum-Product Conjecture

Extremal cases

Let $A \subset \mathbb{Z}$ be a finite set.

1. Chang's Theorem (2003): $|A \cdot A| \ll |A| \implies |A+A| \gg |A|^2$.
2. $|A+A| \ll |A| \implies |A \cdot A| \gg ?$

Progress on the case with small sumset

1. Chang (unpublished notes): $|A+A| \ll |A| \implies |A \cdot A| \gg |A|^{2-o(1)}$.
2. Elekes-Ruzsa (2003): $|A+A| \ll |A| \implies |A \cdot A| \gg \frac{|A|^2}{\log |A|}$.

Extremal Sum-Product Conjecture

Extremal cases

Let $A \subset \mathbb{Z}$ be a finite set.

1. Chang's Theorem (2003): $|A \cdot A| \ll |A| \implies |A + A| \gg |A|^2$.
2. $|A + A| \ll |A| \implies |A \cdot A| \gg ?$

Progress on the case with small sumset

1. Chang (unpublished notes): $|A + A| \ll |A| \implies |A \cdot A| \gg |A|^{2-o(1)}$.
2. Elekes-Ruzsa (2003): $|A + A| \ll |A| \implies |A \cdot A| \gg \frac{|A|^2}{\log |A|}$.
3. Solymosi (2009): $|A \cdot A||A + A|^2 \gg \frac{|A|^4}{\log |A|}$

Elekes-Ruzsa's Conjecture

Do we expect better bounds than $|A \cdot A| \gg \frac{|A|^2}{\log |A|}$ when $|A + A| \ll |A|$?

Elekes-Ruzsa's Conjecture

Do we expect better bounds than $|A \cdot A| \gg \frac{|A|^2}{\log |A|}$ when $|A + A| \ll |A|$?

Elekes-Ruzsa's Conjecture (2003)

Let $A \subset \mathbb{Z}$ be a finite set. If $|A + A| \ll |A|$, then

$$|A \cdot A| \gg \frac{|A|^2}{(\log A)^{2 \log 2 - 1 + o(1)}}.$$

Here $2 \log 2 - 1 \approx 0.39$.

Elekes-Ruzsa's Conjecture

Do we expect better bounds than $|A \cdot A| \gg \frac{|A|^2}{\log |A|}$ when $|A + A| \ll |A|$?

Elekes-Ruzsa's Conjecture (2003)

Let $A \subset \mathbb{Z}$ be a finite set. If $|A + A| \ll |A|$, then

$$|A \cdot A| \gg \frac{|A|^2}{(\log A)^{2 \log 2 - 1 + o(1)}}.$$

Here $2 \log 2 - 1 \approx 0.39$.

The conjecture is based on a special case: $A \subset [N]$ with $|A| \gg N$, proved by Pomerance-Sárkőzy (1987).

Why $2\log 2 - 1$?

Simple case: $A \subset [N]$ with $|A| \gg N$. How small can $|A \cdot A|$ be?

Why $2\log 2 - 1$?

Simple case: $A \subset [N]$ with $|A| \gg N$. How small can $|A \cdot A|$ be?
Heuristic: Let $A' \subset A$ be the subset of typical numbers n, where each n has $\omega(n) \approx \Omega(n) \approx \log\log N$.

Why $2\log 2 - 1$?

Simple case: $A \subset [N]$ with $|A| \gg N$. How small can $|A \cdot A|$ be?
Heuristic: Let $A' \subset A$ be the subset of typical numbers n, where each n has $\omega(n) \approx \Omega(n) \approx \log\log N$. We have

$$|A \cdot A| \gg |A' \cdot A'|.$$

Each product $ab \in A' \cdot A'$ has approximately $\omega(n) \approx \Omega(n) \approx 2\log\log N$.

Why $2\log 2 - 1$?

Simple case: $A \subset [N]$ with $|A| \gg N$. How small can $|A \cdot A|$ be?
Heuristic: Let $A' \subset A$ be the subset of typical numbers n, where each n has $\omega(n) \approx \Omega(n) \approx \log\log N$. We have

$$|A \cdot A| \gg |A' \cdot A'|.$$

Each product $ab \in A' \cdot A'$ has approximately $\omega(n) \approx \Omega(n) \approx 2\log\log N$. One might expect that $|A' \cdot A'|$ is comparable to

$$\#\{n \leq N^2 : \omega(n) = (2 + o(1))\log\log N\}.$$

as $|A'| \asymp N$.

Why $2\log 2 - 1$?

We use the classical formula due to Sathe-Selberg (Landau, Delange etc.) in the range when $k = (2 + o(1)) \log\log x$,

$$\pi_k(x) := \#\{n \le x : \omega(n) = k\} \asymp \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!}$$

Why $2\log 2 - 1$?

We use the classical formula due to Sathe-Selberg (Landau, Delange etc.) in the range when $k = (2 + o(1)) \log\log x$,

$$\pi_k(x) := \#\{n \leq x : \omega(n) = k\} \asymp \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!} \asymp \frac{x}{(\log x)^{2\log 2 - 1 + o(1)}}.$$

Why δ?

Using the same method, we could also analyze the value of δ.
Let $N_k(x) = \#\{n \le x : \Omega(n) = k\}$. Then one has

$$\begin{aligned} |[N] * [N]| &\le \sum_{k_1,k_2} \min\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\} \\ &\ll (\log\log N)^2 \max_{k_1,k_2}\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\} \end{aligned}$$

Why δ?

Using the same method, we could also analyze the value of δ.
Let $N_k(x) = \#\{n \le x : \Omega(n) = k\}$. Then one has

$$\begin{aligned} |[N] * [N]| &\le \sum_{k_1,k_2} \min\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\} \\ &\ll (\log\log N)^2 \max_{k_1,k_2}\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\} \end{aligned}$$

When $k_1 + k_2 < (2-\epsilon)\log\log N$, we have the asymptotics

$$N_{k_i}(N) \ll \frac{N}{\log N}\frac{(\log\log N)^{k_i-1}}{(k_i-1)!};\, N_{k_1+k_2}(N^2) \ll \frac{N^2}{\log N}\frac{(\log\log N)^{k_1+k_2-1}}{(k_1+k_2-1)!}$$

Why δ?

Using the same method, we could also analyze the value of δ.
Let $N_k(x) = \#\{n \le x : \Omega(n) = k\}$. Then one has

$$|[N] * [N]| \le \sum_{k_1,k_2} \min\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\}$$
$$\ll (\log\log N)^2 \max_{k_1,k_2}\{N_{k_1}(N)N_{k_2}(N), N_{k_1+k_2}(N^2)\}$$

When $k_1 + k_2 < (2-\epsilon)\log\log N$, we have the asymptotics

$$N_{k_i}(N) \ll \frac{N}{\log N}\frac{(\log\log N)^{k_i-1}}{(k_i-1)!}; N_{k_1+k_2}(N^2) \ll \frac{N^2}{\log N}\frac{(\log\log N)^{k_1+k_2-1}}{(k_1+k_2-1)!}$$

This is optimized at $k_1 = k_2 = \left(\frac{1}{\log 4} + o(1)\right)\log\log N$, and

$$N_k(N)^2 \approx N_{2k}(N^2) = \frac{N^2}{(\log N)^{\delta+o(1)}}.$$

Constant doubling number

Summary

Suppose $|A + A| < C|A|$, where $A \subset \mathbb{Z}$ is finite.

1. $C = 2 \implies A$ is an arithmetic progression.

Constant doubling number

Summary

Suppose $|A+A| < C|A|$, where $A \subset \mathbb{Z}$ is finite.

1. $C = 2 \implies A$ is an arithmetic progression.
2. $C \approx 3 \implies A \subset \mathcal{P}$ with $|A| \asymp |\mathcal{P}|$ where $\mathcal{P}$ is an A.P. (Freiman's $3k-4$ theorem).

Constant doubling number

Summary

Suppose $|A+A| < C|A|$, where $A \subset \mathbb{Z}$ is finite.

1. $C = 2 \implies A$ is an arithmetic progression.
2. $C \approx 3 \implies A \subset \mathcal{P}$ with $|A| \asymp |\mathcal{P}|$ where $\mathcal{P}$ is an A.P. (Freiman's $3k-4$ theorem).
3. In general, $A \subset$ GAP (Freiman-Ruzsa theorem).

Constant doubling number

Summary

Suppose $|A+A| < C|A|$, where $A \subset \mathbb{Z}$ is finite.

1. $C = 2 \implies A$ is an arithmetic progression.
2. $C \approx 3 \implies A \subset \mathcal{P}$ with $|A| \asymp |\mathcal{P}|$ where $\mathcal{P}$ is an A.P. (Freiman's $3k-4$ theorem).
3. In general, $A \subset$ GAP (Freiman-Ruzsa theorem).
4. $|A-A| \leq (4-\varepsilon)|A| \implies A \subset \mathcal{P}$ with $|A| \asymp |\mathcal{P}|$ where $\mathcal{P}$ is an A.P. (Eberhard-Green-Manners)

Product sets of dense subsets of Arithmetic Progressions

Theorem 2 (X. Zhou, 2022+)

Let $A \subset \mathcal{P} \subset \mathbb{Z}$ be a finite set with $|A| \asymp |\mathcal{P}|$, where $\mathcal{P}$ is an arithmetic progression. Then,

$$|A \cdot A| \gg \frac{|A|^2}{(\log |A|)^{2\log 2 - 1 + o(1)}}.$$

Multiplicative energies

Definition (Multiplicative energy)

Let A, B be two finite subsets of integers. The multiplicative energy between A, B is defined as

$$E_\times(A, B) := \left|\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2\}\right|.$$

When $A = B$, we write $E_\times(A) := E_\times(A, A)$.

Multiplicative energies

Definition (Multiplicative energy)

Let A, B be two finite subsets of integers. The multiplicative energy between A, B is defined as

$$E_\times(A,B) := \left|\{(a_1,a_2,b_1,b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2\}\right|.$$

When $A = B$, we write $E_\times(A) := E_\times(A,A)$.

1. $|A \cdot B| \geq \frac{|A|^2|B|^2}{E_\times(A,B)} \implies$ suffice to give good upper bounds on $E_\times(A)$.

Multiplicative energies

Definition (Multiplicative energy)

Let A, B be two finite subsets of integers. The multiplicative energy between A, B is defined as

$$E_\times(A, B) := \left|\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2\}\right|.$$

When $A = B$, we write $E_\times(A) := E_\times(A, A)$.

1. $|A \cdot B| \geq \frac{|A|^2|B|^2}{E_\times(A,B)} \implies$ suffice to give good upper bounds on $E_\times(A)$.
2. $E_\times(A, B) \leq \sqrt{E_\times(A)E_\times(B)} \implies$ Theorem 1,2 have asymmetric extensions.

Main results restated

Theorem 1'(X.-Zhou, 2022+)

Let A be a finite arithmetic progression. Then there exists a subset $A' \subset A$ with $|A'| \gg |A|(\log |A|)^{-\delta/2-o(1)}$ such that

$$E_\times(A') \ll |A'|^2.$$

Main results restated

Theorem 1'(X.-Zhou, 2022+)

Let A be a finite arithmetic progression. Then there exists a subset $A' \subset A$ with $|A'| \gg |A|(\log|A|)^{-\delta/2-o(1)}$ such that

$$E_\times(A') \ll |A'|^2.$$

Theorem 2'(X.-Zhou, 2022+)

Let $A \subset \mathcal{P}$ with $|A| \asymp |\mathcal{P}|$ where $\mathcal{P}$ is an arithmetic progression. Then there exists $A' \subset A$ with $|A'| \asymp |A|$ such that

$$E_\times(A') \ll |A|^2(\log|A|)^{2\log 2-1+o(1)}.$$

Main ideas in the proof of Theorem 2'

As indicated in the heuristic argument, we may want to chose $A' \subset A$ to be the set of typical numbers!

Main ideas in the proof of Theorem 2'

As indicated in the heuristic argument, we may want to chose $A' \subset A$ to be the set of typical numbers! Then use "Sathe-Selberg's formula" to get the $2\log 2 - 1$.

Main ideas in the proof of Theorem 2'

As indicated in the heuristic argument, we may want to chose $A' \subset A$ to be the set of typical numbers! Then use "Sathe-Selberg's formula" to get the $2\log 2 - 1$. This might require us to understand the quantity: number of elements in $\mathcal{P}$ with a given number of (distinct) prime factors (uniformly for all arithmetic progressions with a given length).

Main ideas in the proof of Theorem 2'

As indicated in the heuristic argument, we may want to chose $A' \subset A$ to be the set of typical numbers! Then use "Sathe-Selberg's formula" to get the $2\log 2 - 1$. This might require us to understand the quantity: number of elements in $\mathcal{P}$ with a given number of (distinct) prime factors (uniformly for all arithmetic progressions with a given length).

1. Short intervals: What if $\mathcal{P} \subset [x, x+y]$ with y very small comparing to x?

Main ideas in the proof of Theorem 2'

As indicated in the heuristic argument, we may want to chose $A' \subset A$ to be the set of typical numbers! Then use "Sathe-Selberg's formula" to get the $2\log 2 - 1$. This might require us to understand the quantity: number of elements in $\mathcal{P}$ with a given number of (distinct) prime factors (uniformly for all arithmetic progressions with a given length).

1. Short intervals: What if $\mathcal{P} \subset [x, x+y]$ with y very small comparing to x?
2. Sparsity: Suppose $\mathcal{P}$ is contained in an interval $\mathcal{I}$, what if $|\mathcal{P}|/|\mathcal{I}|$ very small?

Two reduction steps

We show the following two lemmas to deduce our problem to only considering a "good" $\mathcal{P}$. Let $\mathcal{P} = \{a + id : 1 \leq i \leq L\}$.

Two reduction steps

We show the following two lemmas to deduce our problem to only considering a "good" $\mathcal{P}$. Let $\mathcal{P} = \{a + id : 1 \leq i \leq L\}$.

Lemma (Dyadic interval)

We may assume that $a \geq dL$, i.e. $\mathcal{P} \subset [x, 2x]$ for some x.

Two reduction steps

We show the following two lemmas to deduce our problem to only considering a "good" $\mathcal{P}$. Let $\mathcal{P} = \{a + id : 1 \le i \le L\}$.

Lemma (Dyadic interval)

We may assume that $a \ge dL$, i.e. $\mathcal{P} \subset [x, 2x]$ for some x.

Sketch of the proof.

Dyadically decompose $[a, a + dL]$ into sub-intervals $\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_t$ and consider the intersections $\mathcal{P} \cap \mathcal{I}_j$. Then apply Pigeonhole Principle. The density change roughly from δ to $\frac{\delta}{\log \delta^{-1}}$. □

Two reduction steps

We show the following two lemmas to deduce our problem to only considering a "good" $\mathcal{P}$. Let $\mathcal{P} = \{a + id : 1 \leq i \leq L\}$.

Lemma (Dyadic interval)

We may assume that $a \geq dL$, i.e. $\mathcal{P} \subset \mathcal{I} = [a, 2a]$.

Lemma (Density)

We may further assume that $ad \leq L \log L$, i.e. $\mathcal{P}$ has density in $\mathcal{I}$ at least (roughly)

$$1/\sqrt{\log a}.$$

.

Two reduction steps

We now prove the "density" Lemma.

Lemma (density lemma)

Let $\mathcal{P} = \{a + id : 0 \le i < L\}$ be an arithmetic progression with $\gcd(a, d) = 1$ and $a > 0, d > 0$. For any $A \subseteq \mathcal{P}$, we have

$$E_\times(A) \le 2|A|^2 + 4\frac{L^3}{a}(1 + \log L).$$

Two reduction steps

We now prove the "density" Lemma.

Lemma (density lemma)

Let $\mathcal{P} = \{a + id : 0 \le i < L\}$ be an arithmetic progression with $\gcd(a, d) = 1$ and $a > 0, d > 0$. For any $A \subseteq \mathcal{P}$, we have

$$E_\times(A) \le 2|A|^2 + 4\frac{L^3}{a}(1 + \log L).$$

We begin with parametrization to off diagonal solutions to the equation

$$n_1 n_2 = n_3 n_4.$$

Two reduction steps

We now prove the "density" Lemma.

Lemma (density lemma)

Let $\mathcal{P} = \{a + id : 0 \le i < L\}$ be an arithmetic progression with $\gcd(a, d) = 1$ and $a > 0, d > 0$. For any $A \subseteq \mathcal{P}$, we have

$$E_\times(A) \le 2|A|^2 + 4\frac{L^3}{a}(1 + \log L).$$

We begin with parametrization to off diagonal solutions to the equation

$$n_1 n_2 = n_3 n_4.$$

Write $x_1 = \gcd(n_1, n_3)$, then we have 4 parameters x_1, x_2, y_1, y_2 such that

$$n_1 = x_1 y_1, \quad n_2 = x_2 y_2, \quad n_3 = x_1 y_2, \quad n_4 = x_2 y_1.$$

Continue to prove the reduction steps

Fix x_1. WLOG assume $x_2 \geq x_1$.

Continue to prove the reduction steps

Fix x_1. WLOG assume $x_2 \geq x_1$.Then

$$\frac{x_2}{x_1} = \frac{n_4}{n_1} \leq \frac{a + dL}{a}.$$

Continue to prove the reduction steps

Fix x_1. WLOG assume $x_2 \geq x_1$. Then

$$\frac{x_2}{x_1} = \frac{n_4}{n_1} \leq \frac{a + dL}{a}.$$

Also $x_2 \equiv x_1 \equiv a y_1^{-1} \mod d$. Thus, # of choices for x_2 is at most $\frac{x_1 L}{a}$.

Continue to prove the reduction steps

Fix x_1. WLOG assume $x_2 \geq x_1$.Then

$$\frac{x_2}{x_1} = \frac{n_4}{n_1} \leq \frac{a + dL}{a}.$$

Also $x_2 \equiv x_1 \equiv a y_1^{-1} \mod d$. Thus, # of choices for x_2 is at most $\frac{x_1 L}{a}$. Note $y_i \in [\frac{a}{x_1}, \frac{a+dL}{x_1}]$. To guarantee off diagonal solutions exist, we require $y_1 \neq y_2$ and it implies $x_1 \leq L$ and # of choices for each y_i is at most $L/x_1 + 1$.

Continue to prove the reduction steps

Fix x_1. WLOG assume $x_2 \geq x_1$. Then

$$\frac{x_2}{x_1} = \frac{n_4}{n_1} \leq \frac{a + dL}{a}.$$

Also $x_2 \equiv x_1 \equiv a y_1^{-1} \mod d$. Thus, $\#$ of choices for x_2 is at most $\frac{x_1 L}{a}$. Note $y_i \in [\frac{a}{x_1}, \frac{a+dL}{x_1}]$. To guarantee off diagonal solutions exist, we require $y_1 \neq y_2$ and it implies $x_1 \leq L$ and $\#$ of choices for each y_i is at most $L/x_1 + 1$. Thus $\#\{(n_1, n_2, n_3, n_4) : \text{off-diag solution to } n_1 n_2 = n_3 n_4\}$ is

$$\sum_{\substack{x_1 \neq x_2, y_1 \neq y_2 \\ x_i y_j \in A}} 1 \ll \sum_{x_1 \leq L} \frac{x_1 L}{a} \cdot \left(\frac{L}{x_1}\right)^2.$$

Finish the proof of Theorem 2'

We now focus on a "nice" $\mathcal{P}$ and A has constant density in $\mathcal{P}$. As discussed in "Heuristic", we choose

$$A' = \{a \in A : \omega(a) \leq (1 + o(1)) \log\log(a + dL), a \text{ square-free}\}.$$

Finish the proof of Theorem 2'

We now focus on a "nice" $\mathcal{P}$ and A has constant density in $\mathcal{P}$. As discussed in "Heuristic", we choose

$$A' = \{a \in A : \omega(a) \leq (1+o(1)) \log\log(a+dL), a \text{ square-free}\}.$$

Two tasks:

1. $|A'| = (1+o(1))|A|$.
2. $E_\times(A') \ll |A|^2(\log|A|)^{2\log 2 - 1 + o(1)}$.

Finish the proof of Theorem 2'

Proof of (2).

We do the same parametrization as before: having x_1, x_2, y_1, y_2.

Finish the proof of Theorem 2'

Proof of (2).

We do the same parametrization as before: having x_1, x_2, y_1, y_2. The quantity we are interested in now is

$$\sum_{\substack{x_1, x_2, y_1, y_2 \\ x_i y_j \in A' \\ \omega(x_i y_j) \leq (1+o(1)) \log\log(a+dL)}} 1.$$

Finish the proof of Theorem 2'

Proof of (2).

We do the same parametrization as before: having x_1, x_2, y_1, y_2. The quantity we are interested in now is

$$\sum_{\substack{x_1,x_2,y_1,y_2 \\ x_i y_j \in A' \\ \omega(x_i y_j) \le (1+o(1)) \log\log(a+dL)}} 1.$$

Let $k = (1 + o(1)) \log\log(a + dL)$

Finish the proof of Theorem 2'

Proof of (2).

We do the same parametrization as before: having x_1, x_2, y_1, y_2. The quantity we are interested in now is

$$\sum_{\substack{x_1,x_2,y_1,y_2 \\ x_i y_j \in A' \\ \omega(x_i y_j) \le (1+o(1)) \log\log(a+dL)}} 1.$$

Let $k = (1 + o(1)) \log\log(a + dL)$ and we use the classical trick: for any $\lambda > 1$,

$$1 \le \lambda^{k - \omega(x_i y_j)}.$$

$\square$

Finish the proof of Theorem 2'

Proof of (2) continue.

Thus we have following upper bounds for any $\lambda > 1$,

$$\sum_{x_i y_j \in A'} \lambda^{4k-\omega(x_1y_1)-\omega(x_1y_2)-\omega(x_2y_1)-\omega(x_2y_2)}$$
$$\leq \sum_{x_i y_j \in \mathcal{P}} \lambda^{4k} \lambda^{-2\omega(x_1)} \lambda^{-2\omega(x_2)} \lambda^{-2\omega(y_1)} \lambda^{-2\omega(y_2)}.$$

Finish the proof of Theorem 2'

Proof of (2) continue.

Thus we have following upper bounds for any $\lambda > 1$,

$$\sum_{x_i y_j \in A'} \lambda^{4k-\omega(x_1y_1)-\omega(x_1y_2)-\omega(x_2y_1)-\omega(x_2y_2)}$$

$$\leq \sum_{x_i y_j \in \mathcal{P}} \lambda^{4k} \lambda^{-2\omega(x_1)} \lambda^{-2\omega(x_2)} \lambda^{-2\omega(y_1)} \lambda^{-2\omega(y_2)}.$$

We need to take sum of multiplicative function over an AP. We have classical tool, e.g. Shiu's lemma to deal with it.

Finish the proof of Theorem 2'

Proof of (2) continue.

Thus we have following upper bounds for any $\lambda > 1$,

$$\sum_{x_i y_j \in A'} \lambda^{4k-\omega(x_1y_1)-\omega(x_1y_2)-\omega(x_2y_1)-\omega(x_2y_2)}$$
$$\leq \sum_{x_i y_j \in \mathcal{P}} \lambda^{4k} \lambda^{-2\omega(x_1)} \lambda^{-2\omega(x_2)} \lambda^{-2\omega(y_1)} \lambda^{-2\omega(y_2)}.$$

We need to take sum of multiplicative function over an AP. We have classical tool, e.g. Shiu's lemma to deal with it. Apply Shiu's result, we end up geting a function in λ. Optimize it and $\lambda = \sqrt{2}$ gives the desired bound. $\square$

Shiu's Lemma

Shiu's Lemma: a vague version

Let $f(n)$ be a non-negative multiplicative function, not growing too fast.

Shiu's Lemma

Shiu's Lemma: a vague version

Let $f(n)$ be a non-negative multiplicative function, not growing too fast. Suppose $\gcd(a, d) = 1$, then as $x \to \infty$ we have

$$\sum_{\substack{x-y\leq n<x \\ n\equiv a \pmod{d}}} f(n) \ll \frac{y}{\phi(d)} \frac{1}{\log x} \exp\left(\sum_{p\leq x, p\nmid d} \frac{f(p)}{p}\right),$$

Shiu's Lemma

Shiu's Lemma: a vague version

Let $f(n)$ be a non-negative multiplicative function, not growing too fast. Suppose $\gcd(a, d) = 1$, then as $x \to \infty$ we have

$$\sum_{\substack{x-y \le n < x \\ n \equiv a \pmod{d}}} f(n) \ll \frac{y}{\phi(d)} \frac{1}{\log x} \exp\left(\sum_{p \le x, p \nmid d} \frac{f(p)}{p} \right),$$

provided that the A.P. is not too sparse the interval is not too short.

Shiu's Lemma

Shiu's Lemma

Let $f(n)$ be a non-negative multiplicative function such that $f(p^\ell) \leq A_1^\ell$ for some positive constant A_1 and for any $\varepsilon > 0$, $f(n) \leq A_2 n^\varepsilon$ for some $A_2 = A_2(\varepsilon)$.

Shiu's Lemma

Shiu's Lemma

Let $f(n)$ be a non-negative multiplicative function such that $f(p^\ell) \le A_1^\ell$ for some positive constant A_1 and for any $\varepsilon > 0$, $f(n) \le A_2 n^\varepsilon$ for some $A_2 = A_2(\varepsilon)$. Let $\alpha, \beta \in (0, 1/2)$, integer a satisfying $\gcd(a, d) = 1$. Then as $x \to \infty$ we have

$$\sum_{\substack{x-y \le n < x \\ n \equiv a \pmod{d}}} f(n) \ll \frac{y}{\phi(d)} \frac{1}{\log x} \exp\left(\sum_{p \le x, p \nmid d} \frac{f(p)}{p} \right),$$

provided that $d < y^{1-\alpha}$ and $x^\beta < y < x$, where the implicit constant depends only on A_1, A_2, α, β and the summation on the right hand side is taken over prime p.

h-fold product Conjecture

We may naturally extend the Elekes-Ruzsa's conjecture to the following.

Conjecture (X.-Zhou, 2022)

Let A be a set of integers and $A^h := \{a_1 a_2 \cdots a_h : a_i \in A, \forall\ 1 \leq i \leq h\}$. If $|A+A| \ll |A|$, then

$$|A^h| \geq |A|^h (\log |A|)^{-h \log h + h - 1 - o(1)}.$$

One way to achieve this lower bound is by choosing $A = \{1 \leq n \leq N : \omega(n) = (1+o(1)) \log \log N\}$.

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P.

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P. Following the strategy towards multiplication table problem, we choose the following subset (taking both global and local information into account).

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P. Following the strategy towards multiplication table problem, we choose the following subset (taking both global and local information into account).

Subset A'

$$\mathcal{N}_k(A;\alpha,\beta) := \{n \in A : \omega(n) = k, \log\log p_j(n) \geq \alpha j - \beta,\ 1 \leq j \leq k\},$$

where $k = \left\lfloor \frac{\log\log L}{\log 4} - 5\sqrt{\log\log L} \right\rfloor - 4, \alpha = \log 4, \beta = 1$, and $p_j(n)$ is the j-th prime factor.

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P. Following the strategy towards multiplication table problem, we choose the following subset (taking both global and local information into account).

Subset A'

$$\mathcal{N}_k(A; \alpha, \beta) := \{n \in A : \omega(n) = k, \log\log p_j(n) \geq \alpha j - \beta,\ 1 \leq j \leq k\},$$

where $k = \left\lfloor \frac{\log\log L}{\log 4} - 5\sqrt{\log\log L} \right\rfloor - 4, \alpha = \log 4, \beta = 1$, and $p_j(n)$ is the j-th prime factor.

Remark: A similar set has been considered by Ford (2018).

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P. Following the strategy towards multiplication table problem, we choose the following subset (taking both global and local information into account).

Subset A'

$$\mathcal{N}_k(A;\alpha,\beta) := \{n \in A : \omega(n) = k, \log\log p_j(n) \geq \alpha j - \beta,\ 1 \leq j \leq k\},$$

where $k = \left\lfloor \frac{\log\log L}{\log 4} - 5\sqrt{\log\log L} \right\rfloor - 4, \alpha = \log 4, \beta = 1$, and $p_j(n)$ is the j-th prime factor.

Remark: A similar set has been considered by Ford (2018).

1. Show the size of $\mathcal{N}_k(A;\alpha,\beta)$ is actually large (Smirnov statistics).

Strategy of proving Theorem 1': local information

We need to pick a subset $A' \subset A$ where A can be assumed as a "nice" A.P. Following the strategy towards multiplication table problem, we choose the following subset (taking both global and local information into account).

Subset A'

$$\mathcal{N}_k(A; \alpha, \beta) := \{n \in A : \omega(n) = k, \log\log p_j(n) \geq \alpha j - \beta,\ 1 \leq j \leq k\},$$

where $k = \left\lfloor \frac{\log\log L}{\log 4} - 5\sqrt{\log\log L} \right\rfloor - 4, \alpha = \log 4, \beta = 1$, and $p_j(n)$ is the j-th prime factor.

Remark: A similar set has been considered by Ford (2018).

1. Show the size of $\mathcal{N}_k(A; \alpha, \beta)$ is actually large (Smirnov statistics).
2. Show the multiplicative energy of $\mathcal{N}_k(A; \alpha, \beta)$ is small.

Strategy of proving Theorem 1': large subset

To complete Task 1, the reduction steps are necessary, e.g. we need to count primes in A.P. (Siegel-Walfisz) which requires the moduli are small.

Strategy of proving Theorem 1': One more parameter

$\mathcal{N}_k(A; \alpha, \beta)$ **has small multiplicative energy.**

Strategy of proving Theorem 1': One more parameter

$\mathcal{N}_k(A; \alpha, \beta)$ **has small multiplicative energy.** In the proof of Theorem 2', we studied average value of multiplicative function $f = \lambda^{k-\omega(x_i y_j)}$.

Strategy of proving Theorem 1': One more parameter

$\mathcal{N}_k(A;\alpha,\beta)$ **has small multiplicative energy.** In the proof of Theorem 2', we studied average value of multiplicative function $f = \lambda^{k-\omega(x_i y_j)}$. Now to further detect the local information, we write

$$\omega(n,t) \leq g(t) := \frac{\log\log t}{\log 4} + \beta,$$

where

$$\omega(n,t) := \#\{\text{distinct } p : p|n, p \leq t\}.$$

Strategy of proving Theorem 1': One more parameter

$\mathcal{N}_k(A;\alpha,\beta)$ **has small multiplicative energy.** In the proof of Theorem 2', we studied average value of multiplicative function $f = \lambda^{k-\omega(x_i y_j)}$. Now to further detect the local information, we write

$$\omega(n,t) \leq g(t) := \frac{\log\log t}{\log 4} + \beta,$$

where

$$\omega(n,t) := \#\{\text{distinct } p : p|n, p \leq t\}.$$

Apply Shiu's Lemma to sums of terms of the form

$$\lambda_1^{k-\omega(x_i y_j)} \lambda_2^{g(t)-\omega(x_i y_j, t)}$$

and optimize the two parameters ($\lambda_1 = \sqrt{\log 4}, \lambda_2 = \sqrt{2}$).

Thank You !