The least modulus of a covering system

Bob Hough

DPMMS, Cambridge

July 3, 2013

Covering systems

A covering system of congruences

$$(a_i \bmod m_i), \qquad 1 < m_1 < m_2 < ... < m_k$$

is a collection of arithmetic progressions such that

$$\mathbb{Z} = (a_1 \bmod m_1) \cup (a_2 \bmod m_2) \cup ... \cup (a_k \bmod m_k)$$

For example

$$\ldots, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, \ldots$$

For example

(0 mod 2)

$\ldots, \underline{0}, 1, \underline{2}, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, 9, \underline{10}, 11, \underline{12}, 13, \underline{14}, 15, \underline{16}, 17, \underline{18}, 19, \underline{20}, \ldots$

For example

$(0 \bmod 2) \cup (0 \bmod 3)$

$\ldots, \underline{0}, 1, \underline{2}, \underline{3}, \underline{4}, 5, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, 11, \underline{12}, 13, \underline{14}, \underline{15}, \underline{16}, \underline{17}, \underline{18}, 19, \underline{20}, \ldots$

For example

$(0 \bmod 2) \cup (0 \bmod 3) \cup (5 \bmod 6)$

$\ldots, \underline{0}, 1, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, 13, \underline{14}, \underline{15}, \underline{16}, \underline{17}, \underline{18}, 19, \underline{20}, \ldots$

For example

$(0 \bmod 2) \cup (0 \bmod 3) \cup (5 \bmod 6) \cup (1 \bmod 4)$

$\ldots, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, \underline{13}, \underline{14}, \underline{15}, \underline{16}, \underline{17}, \underline{18}, 19, \underline{20}, \ldots$

For example

$(0 \bmod 2) \cup (0 \bmod 3) \cup (5 \bmod 6) \cup (1 \bmod 4) \cup (7 \bmod 12)$

$\ldots, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, \underline{13}, \underline{14}, \underline{15}, \underline{16}, \underline{17}, \underline{18}, \underline{19}, \underline{20}, \ldots$

Two well-known problems

1. Erdős: For each $M > 1$, is there a cover with

$$M < m_1 < m_2 < \ldots < m_k \qquad ?$$

Two well-known problems

1. Erdős: For each $M > 1$, is there a cover with

$$M < m_1 < m_2 < \dots < m_k \qquad ?$$

2. Erdős, Selfridge: Is there a cover with $m_1, m_2, \dots, m_k$ all odd?

Past results

Some records for m_1

- $m_1 = 9, 18, 20,$ Churchhouse, Krukenberg, Choi (1968-71)

Past results

Some records for m_1

- $m_1 = 9, 18, 20,$ Churchhouse, Krukenberg, Choi (1968-71)
- $m_1 = 24,$ Morikawa, 80s

Past results

Some records for m_1

- $m_1 = 9, 18, 20,$ Churchhouse, Krukenberg, Choi (1968-71)
- $m_1 = 24,$ Morikawa, 80s
- $m_1 = 25,$ Gibson, (2006)

Past results

Some records for m_1

- $m_1 = 9, 18, 20,$ Churchhouse, Krukenberg, Choi (1968-71)
- $m_1 = 24,$ Morikawa, 80s
- $m_1 = 25,$ Gibson, (2006)
- $m_1 = 40,$ Nielsen, (2009)

Past results

Filaseta, Ford, Konyagin, Pomerance, Yu (2007):
As $M \to \infty$, if $M < m_1 < m_2 < \ldots < m_k$ are covering moduli then

$$\sum \frac{1}{m_i} \to \infty$$

as a function of M.

Main theorem

Theorem (H. 2013)

There is an absolute $C > 0$ such that any covering system has $m_1 < C$.

Main theorem

Theorem (H. 2013)

There is an absolute $C > 0$ *such that any covering system has* $m_1 < C$.

Builds on work of FFKPY '07.

Problem set-up

$M =$ large fixed constant.

Problem set-up

$M =$ large fixed constant.
Assume that $\mathcal{M} \subset \{m \in \mathbb{Z}, m \geq M\}$ is a finite set of moduli. For each $m \in \mathcal{M}$ let congruence a_m mod m be given.

M = large fixed constant.
Assume that $\mathcal{M} \subset \{m \in \mathbb{Z}, m \geq M\}$ is a finite set of moduli. For each $m \in \mathcal{M}$ let congruence $a_m \bmod m$ be given.
Let the unsifted set be

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c .$$

Problem set-up

M = large fixed constant.
Assume that $\mathcal{M} \subset \{m \in \mathbb{Z}, m \geq M\}$ is a finite set of moduli. For each $m \in \mathcal{M}$ let congruence a_m mod m be given.
Let the unsifted set be

$$R = \left(\bigcup_{m\in\mathcal{M}} (a_m \bmod m)\right)^c.$$

We are going to show that it M is sufficiently large then the density of the R is > 0.

Problem set-up

$M =$ large fixed constant.
Assume that $\mathcal{M} \subset \{m \in \mathbb{Z}, m \geq M\}$ is a finite set of moduli. For each $m \in \mathcal{M}$ let congruence $a_m \bmod m$ be given.
Let the unsifted set be

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c .$$

We are going to show that it M is sufficiently large then the density of the R is > 0.
For this talk we assume each $m \in \mathcal{M}$ is squarefree.

Initial ideas

We estimate the density of the unsifted set

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c$$

in stages.

Initial ideas

We estimate the density of the unsifted set

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c$$

in stages.

Set $1 < P_0 < P_1 < P_2 < \ldots$ thresholds, $P_0 = \sqrt{\log M}$, $P_{i+1} = e^{P_i^c}$.

$$Q_i = \prod_{p < P_i} p.$$

Initial ideas

We estimate the density of the unsifted set

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c$$

in stages.
Set $1 < P_0 < P_1 < P_2 < \ldots$ thresholds, $P_0 = \sqrt{\log M}$, $P_{i+1} = e^{P_i^c}$.

$$Q_i = \prod_{p < P_i} p.$$

Evolve the sieve in stages: Let $R_0 \supset R_1 \supset R_2 \supset \ldots$

Initial ideas

We estimate the density of the unsifted set

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m)\right)^c$$

in stages.

Set $1 < P_0 < P_1 < P_2 < \ldots$ thresholds, $P_0 = \sqrt{\log M}$, $P_{i+1} = e^{P_i^c}$.

$$Q_i = \prod_{p < P_i} p.$$

Evolve the sieve in stages: Let $R_0 \supset R_1 \supset R_2 \supset \ldots$

$$R_i = \left(\bigcup_{m | Q_i} (a_m \bmod m)\right)^c$$

Initial ideas

We estimate the density of the unsifted set

$$R = \left(\bigcup_{m \in \mathcal{M}} (a_m \bmod m) \right)^c$$

in stages.
Set $1 < P_0 < P_1 < P_2 < \ldots$ thresholds, $P_0 = \sqrt{\log M}$, $P_{i+1} = e^{P_i^c}$.

$$Q_i = \prod_{p < P_i} p.$$

Evolve the sieve in stages: Let $R_0 \supset R_1 \supset R_2 \supset \ldots$

$$R_i = \left(\bigcup_{m | Q_i} (a_m \bmod m) \right)^c$$

If i is large enough then every $m \in \mathcal{M}$ divides Q_i, so $R = R_i$ eventually.

Initial ideas

Recall R_i is the unsifted set after the ith stage,

$$R_i = \left(\bigcup_{m | Q_i} (a_m \bmod m) \right)^c$$

with $Q_i = \prod_{p < P_i} p$.

Initial ideas

Recall R_i is the unsifted set after the ith stage,

$$R_i = \left(\bigcup_{m|Q_i} (a_m \bmod m) \right)^c$$

with $Q_i = \prod_{p<P_i} p$.
When M is larger than a fixed constant, for all $i \geq 0$ we will prove:

$$\text{density}(R_i) \geq \exp(-(\log P_i)^2).$$

Initial ideas

Recall R_i is the unsifted set after the ith stage,

$$R_i = \left(\bigcup_{m|Q_i} (a_m \bmod m) \right)^c$$

with $Q_i = \prod_{p<P_i} p$.
When M is larger than a fixed constant, for all $i \geq 0$ we will prove:

$$\text{density}(R_i) \geq \exp(-(\log P_i)^2).$$

This evidently suffices for the theorem.

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i.

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.

The proof now proceeds by induction.

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.

The proof now proceeds by induction.

- View $R_i \subset \mathbb{Z}/Q_i\mathbb{Z}$.

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.
The proof now proceeds by induction.

- View $R_i \subset \mathbb{Z}/Q_i\mathbb{Z}$.
- Think of $\mathbb{Z}/Q_{i+1}\mathbb{Z}$ as fibred over $\mathbb{Z}/Q_i\mathbb{Z}$

Initial ideas

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.

The proof now proceeds by induction.

- View $R_i \subset \mathbb{Z}/Q_i\mathbb{Z}$.
- Think of $\mathbb{Z}/Q_{i+1}\mathbb{Z}$ as fibred over $\mathbb{Z}/Q_i\mathbb{Z}$
- So R_{i+1} exists in fibres over R_i.

Recall that R_i is determined by congruences to moduli dividing Q_i. No sieving happens in the 0th stage, since $Q_0 \approx e^{\sqrt{\log M}} < M$, so the density of R_0 is 1.
The proof now proceeds by induction.

- View $R_i \subset \mathbb{Z}/Q_i\mathbb{Z}$.
- Think of $\mathbb{Z}/Q_{i+1}\mathbb{Z}$ as fibred over $\mathbb{Z}/Q_i\mathbb{Z}$
- So R_{i+1} exists in fibres over R_i.
- We will estimate the density within single fibres.

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10). ($Q_i = 10$)

$$\underline{0} \quad \underline{1} \quad \underline{2} \quad 3 \quad \underline{4} \quad \underline{5} \quad \underline{6} \quad 7 \quad \underline{8} \quad 9$$

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10).

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18)

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10).

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18)

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10).

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18) and (4 mod 15).

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10).

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18) and (4 mod 15). ($Q_{i+1} = 90$).

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m | Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0 | Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$
- If this congruence condition is met, the sieving within fibre r is determined only by $a_m \bmod n$.

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$
- If this congruence condition is met, the sieving within fibre r is determined only by $a_m \bmod n$.

So...

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$
- If this congruence condition is met, the sieving within fibre r is determined only by $a_m \bmod n$.

So... Group moduli according to common n-factor

$$A_{n,r} = \{a_m \bmod n : m = m_0 n, a_m \equiv r \bmod m_0\}$$

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m | Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0 | Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$
- If this congruence condition is met, the sieving within fibre r is determined only by $a_m \bmod n$.

So... Group moduli according to common n-factor

$$A_{n,r} = \{a_m \bmod n : m = m_0 n, a_m \equiv r \bmod m_0\}$$

The set of n's we call $\mathcal{N}_{i+1}$. These n have all their prime factors in the interval $(P_i, P_{i+1}]$.

Initial ideas

R_i is the set that has survived the ith sieving stage, determined modulo Q_i. Let $r \bmod Q_i$ be an element of this set. We consider R_{i+1} fibred over r.

- R_{i+1} in fibre r is determined by congruences to moduli m, $m|Q_{i+1}$, $m \nmid Q_i$.
- Factor such an m as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$.
- The congruence $(a_m \bmod m)$ intersects fibre r iff $a_m \equiv r \bmod m_0$
- If this congruence condition is met, the sieving within fibre r is determined only by $a_m \bmod n$.

So... Group moduli according to common n-factor

$$A_{n,r} = \{a_m \bmod n : m = m_0 n, a_m \equiv r \bmod m_0\}$$

The set of n's we call $\mathcal{N}_{i+1}$. These n have all their prime factors in the interval $(P_i, P_{i+1}]$. This control of the size of prime factors is critical.

Heuristic

To recap: within the fibre $r \in R_i$, the $i+1$st stage of the sieve is determined by congruences only to moduli $n \in \mathcal{N}_{i+1}$, which have all of their prime factors in $(P_i, P_{i+1}]$. The set of congruences for a given n we denote by $A_{n,r}$.

Heuristic

To recap: within the fibre $r \in R_i$, the $i+1$st stage of the sieve is determined by congruences only to moduli $n \in \mathcal{N}_{i+1}$, which have all of their prime factors in $(P_i, P_{i+1}]$. The set of congruences for a given n we denote by $A_{n,r}$.

Heuristic: Size of $|A_{n,r}|$ is key.

- When varying r in the whole set $\mathbb{Z}/Q_i\mathbb{Z}$: the distribution of $|A_{n,r}|$ is easy (mean is $\approx \log P_i$)

Heuristic

To recap: within the fibre $r \in R_i$, the $i+1$st stage of the sieve is determined by congruences only to moduli $n \in \mathcal{N}_{i+1}$, which have all of their prime factors in $(P_i, P_{i+1}]$. The set of congruences for a given n we denote by $A_{n,r}$.

Heuristic: Size of $|A_{n,r}|$ is key.

- When varying r in the whole set $\mathbb{Z}/Q_i\mathbb{Z}$: the distribution of $|A_{n,r}|$ is easy (mean is $\approx \log P_i$)
- If $(n_1, n_2) = 1$ then sieving by $A_{n_1,r}$, $A_{n_2,r}$ is independent (Chinese Remainder Theorem)

Heuristic

To recap: within the fibre $r \in R_i$, the $i+1$st stage of the sieve is determined by congruences only to moduli $n \in \mathcal{N}_{i+1}$, which have all of their prime factors in $(P_i, P_{i+1}]$. The set of congruences for a given n we denote by $A_{n,r}$.

Heuristic: Size of $|A_{n,r}|$ is key.

- When varying r in the whole set $\mathbb{Z}/Q_i\mathbb{Z}$: the distribution of $|A_{n,r}|$ is easy (mean is $\approx \log P_i$)
- If $(n_1, n_2) = 1$ then sieving by $A_{n_1,r}$, $A_{n_2,r}$ is independent (Chinese Remainder Theorem)

Total independence would give density in fibre r

$$\prod_{n \in \mathcal{N}_{i+1}} \left(1 - \frac{|A_{n,r}|}{n}\right) \approx \prod_{n \in \mathcal{N}_{i+1}} \left(1 - \frac{\log P_i}{n}\right) \approx P_{i+1}^{-O(1)}$$

which would easily give our lower bound for the density of R_{i+1}.

Difficulties

Two PROBLEMS:

Difficulties

Two PROBLEMS:

1. For most $n_1, n_2 \in \mathcal{N}_{i+1}$, $(n_1, n_2) > 1 \Rightarrow$ sieving by the sets $A_{n_1,r}$ and $A_{n_2,r}$ is not independent.

Difficulties

Two PROBLEMS:

1. For most $n_1, n_2 \in \mathcal{N}_{i+1}$, $(n_1, n_2) > 1 \Rightarrow$ sieving by the sets $A_{n_1,r}$ and $A_{n_2,r}$ is not independent.
2. We vary $r \in R_i$, which is much smaller than $\mathbb{Z}/Q_i\mathbb{Z}$, so we don't know the typical behaviour: $|A_{n,r}| \sim ??$

Lemma (Lovász Local Lemma)

$A_1, A_2, \ldots, A_n$ are events in a probability space. $D = ([n], E)$ is a dependency graph, such that, for each $1 \le i \le n$, event A_i is independent of the sigma-algebra generated by the events $\{A_j : (i,j) \notin E\}$. Let real numbers $x_1, x_2, \ldots, x_n$ satisfy $0 < x_i < 1$, and for each $1 \le i \le n$,

$$\mathbf{P}(A_i) \le x_i \prod_{(i,j)\in E} (1 - x_j).$$

Then for any $1 \le m \le n$

$$\mathbf{P}\left(\bigcap_{i=1}^{n} A_i^c\right) \ge \mathbf{P}\left(\bigcap_{i=1}^{m} A_i^c\right) \cdot \prod_{j=m+1}^{n} (1 - x_j).$$

Solution idea

Recall that we've fixed a fibre $r \in R_i$ in which we're sieving, and we think of the sieve as happening to moduli in $\mathcal{N}_{i+1}$.

To address problem 1:
Truncation. We write $\mathcal{N}_{i+1} = \mathcal{N}_{small} \sqcup \mathcal{N}_{large}$

$$\mathcal{N}_{small} = \{n \in \mathcal{N}_{i+1} : P_i < n \leq e^{P_i^\gamma}\}$$

$$\mathcal{N}_{large} = \{n \in \mathcal{N}_{i+1} : e^{P_i^\gamma} < n\}$$

Solution idea

Recall that we've fixed a fibre $r \in R_i$ in which we're sieving, and we think of the sieve as happening to moduli in $\mathcal{N}_{i+1}$.

To address problem 1:
Truncation. We write $\mathcal{N}_{i+1} = \mathcal{N}_{small} \sqcup \mathcal{N}_{large}$

$$\mathcal{N}_{small} = \{n \in \mathcal{N}_{i+1} : P_i < n \leq e^{P_i^\gamma}\}$$

$$\mathcal{N}_{large} = \{n \in \mathcal{N}_{i+1} : e^{P_i^\gamma} < n\}$$

On $\mathcal{N}_{small}$ usually $(n_1, n_2) = 1$, approximate independence $\Rightarrow$ Lovász Local Lemma gives a product approximation.

Solution idea

Recall that we've fixed a fibre $r \in R_i$ in which we're sieving, and we think of the sieve as happening to moduli in $\mathcal{N}_{i+1}$.

To address problem 1:
Truncation. We write $\mathcal{N}_{i+1} = \mathcal{N}_{small} \sqcup \mathcal{N}_{large}$

$$\mathcal{N}_{small} = \{n \in \mathcal{N}_{i+1} : P_i < n \le e^{P_i^\gamma}\}$$

$$\mathcal{N}_{large} = \{n \in \mathcal{N}_{i+1} : e^{P_i^\gamma} < n\}$$

On $\mathcal{N}_{small}$ usually $(n_1, n_2) = 1$, approximate independence $\Rightarrow$ Lovász Local Lemma gives a product approximation.
For $\mathcal{N}_{large}$: Use that smooth numbers are sparse to cover the error with a union bound.

Solution idea

Recall that we've fixed a fibre $r \in R_i$ in which we're sieving, and we think of the sieve as happening to moduli in $\mathcal{N}_{i+1}$.

To address problem 1:
Truncation. We write $\mathcal{N}_{i+1} = \mathcal{N}_{small} \sqcup \mathcal{N}_{large}$

$$\mathcal{N}_{small} = \{n \in \mathcal{N}_{i+1} : P_i < n \leq e^{P_i^\gamma}\}$$

$$\mathcal{N}_{large} = \{n \in \mathcal{N}_{i+1} : e^{P_i^\gamma} < n\}$$

On $\mathcal{N}_{small}$ usually $(n_1, n_2) = 1$, approximate independence $\Rightarrow$ Lovász Local Lemma gives a product approximation.
For $\mathcal{N}_{large}$: Use that smooth numbers are sparse to cover the error with a union bound.

Control of size of prime factors is the key. We're able to get approximate independence in a range which is almost exponential in P_i. ($e^{P_i^\gamma}$).

Solution idea

To address problem 2 we need to be able to estimate means over the set R_i, as opposed to $\mathbb{Z}/Q_i\mathbb{Z}$. To do so:
Declare fibre $r \in R_i$ is GOOD if well-balanced:

Solution idea

To address problem 2 we need to be able to estimate means over the set R_i, as opposed to $\mathbb{Z}/Q_i\mathbb{Z}$. To do so:
Declare fibre $r \in R_i$ is GOOD if well-balanced:
$\forall n \in \mathcal{N}_{small}$, $\forall a \bmod n$

$$\text{density } R_{i+1} \text{ in fibre } r \cap (a \bmod n) \lesssim \text{ density } R_{i+1} \text{ in fibre } r$$

Solution idea

To address problem 2 we need to be able to estimate means over the set R_i, as opposed to $\mathbb{Z}/Q_i\mathbb{Z}$. To do so:
Declare fibre $r \in R_i$ is GOOD if well-balanced:
$\forall n \in \mathcal{N}_{small}$, $\forall a \bmod n$

$$\text{density } R_{i+1} \text{ in fibre } r \cap (a \bmod n) \lesssim \text{ density } R_{i+1} \text{ in fibre } r$$

At each stage, evolve R_{i+1} only over GOOD fibres $\Rightarrow$ distribution over $R_i \approx$ distribution over $\mathbb{Z}/Q_i\mathbb{Z}$

Solution idea

To address problem 2 we need to be able to estimate means over the set R_i, as opposed to $\mathbb{Z}/Q_i\mathbb{Z}$. To do so:
Declare fibre $r \in R_i$ is GOOD if well-balanced:
$\forall n \in \mathcal{N}_{small}$, $\forall a \bmod n$

$$\text{density } R_{i+1} \text{ in fibre } r \cap (a \bmod n) \lesssim \text{ density } R_{i+1} \text{ in fibre } r$$

At each stage, evolve R_{i+1} only over GOOD fibres $\Rightarrow$ distribution over $R_i \approx$ distribution over $\mathbb{Z}/Q_i\mathbb{Z}$
Use Lovász Local Lemma again: most fibres are good!

In practice, one must balance being able to truncate (problem 1) against making fibres from previous stages be well behaved (problem 2).

In practice, one must balance being able to truncate (problem 1) against making fibres from previous stages be well behaved (problem 2).

Removing the squarefree assumption is technical but ugly.

Thanks

Thanks for coming!

References

References

1. Filaseta, M., K. Ford, S. Konyagin, C. Pomerance, and G. Yu. "Sieving by large integers and covering systems of congruences." JAMS, 20(2): 495–519, 2007.
2. Nielsen, P. "A covering system whose smallest modulus is 40." J. Num. Thy. 129: 640–666, 2009.

Application of LLL to GOOD fibres

Recall we want the bound

$$\text{density}(R_{i+1}) \text{ in fibre } r \cap (a \bmod n) \lesssim \text{density}(R_{i+1}) \text{ in fibre } r.$$

Applying LLL:

$$LHS \le \mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}} A_{n,r}^c \middle| (a \bmod n) \right) \le \mathbf{P}\left(\bigcap_{\substack{n' \in \mathcal{N}_{i+1} \\ (n',n)=1}} A_{n,r}^c \middle| (a \bmod n) \right)$$

$$= \mathbf{P}\left(\bigcap_{\substack{n' \in \mathcal{N}_{i+1} \\ (n',n)=1}} A_{n,r}^c \right) \approx \mathbf{P}\left(\bigcap_{\substack{n' \in \mathcal{N}_{i+1} \\ (n',n)=1}} A_{n,r}^c \right) \prod_{\substack{n' \in \mathcal{N}_{i+1} \\ (n',n)>1}} (1 - x_n)$$

$$\lesssim \mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}} A_{n,r}^c \right) \lesssim RHS.$$