The least quadratic non-residue and related problems

Enrique Treviño

Lake Forest College

L-Functions in Analytic Number Theory Collaborative Research Group Seminar
January 18, 2023

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n is either 0,1, or 2 modulo 3.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n is either 0,1, or 2 modulo 3.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n is either 0,1, or 2 modulo 3.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n is either 0,1, or 2 modulo 3.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n is either 0,1, or 2 modulo 3.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Quadratic residues and non-residues

Let n be a positive integer. For $q \in \{1, 2, \ldots, n-1\}$, we call q a quadratic residue $\bmod n$ if there exists an integer x such that $x^2 \equiv q \pmod{n}$. Otherwise we call q a quadratic non-residue.

- For $n = 3$, the quadratic residue is $\{1\}$ and the quadratic non-residue is 2.
- For $n = 5$, the quadratic residues are $\{1, 4\}$ and the quadratic non-residues are $\{2, 3\}$.
- For $n = 7$, the quadratic residues are $\{1, 2, 4\}$ and the quadratic non-residues are $\{3, 5, 6\}$.
- For $n = p$, an odd prime, there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

p	Least quadratic non-residue
7	3
23	5
71	7
311	11
479	13
1559	17
5711	19
10559	23
18191	29
31391	31
422231	37
701399	41
366791	43
3818929	47

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \dots$.

- $\#\{p \le x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \le x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \le x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x) / \log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \le C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x)/\log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \leq C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x)/\log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \leq C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x) / \log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \leq C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x)/\log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \leq C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- If $k = \log \pi(x)/\log 2$ you would expect only one prime satisfying $g(p) = p_k$.
- Choosing $k \approx C \log x$, since $p_k \sim k \log k$ we have $g(x) \leq C \log x \log\log x$.

Theorems on the least quadratic non-residue $\bmod p$

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Our conjecture is

$$g(p) = O(\log p \log \log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$. Soundararajan, Lamzouri and Li improved this to $g(p) \leq \log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log \log \log p$, that is

$$g(p) = \Omega(\log p \log \log \log p).$$

Theorems on the least quadratic non-residue $\bmod p$

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Our conjecture is

$$g(p) = O(\log p \log \log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$. Soundararajan, Lamzouri and Li improved this to $g(p) \leq \log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log \log \log p$, that is

$$g(p) = \Omega(\log p \log \log \log p).$$

Theorems on the least quadratic non-residue $\bmod p$

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Our conjecture is

$$g(p) = O(\log p \log \log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$. Soundararajan, Lamzouri and Li improved this to $g(p) \leq \log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log \log \log p$, that is

$$g(p) = \Omega(\log p \log \log \log p).$$

Theorems on the least quadratic non-residue $\bmod p$

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Our conjecture is

$$g(p) = O(\log p \log\log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$. Soundararajan, Lamzouri and Li improved this to $g(p) \leq \log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log\log\log p$, that is

$$g(p) = \Omega(\log p \log\log\log p).$$

Explicit estimates on the least quadratic non-residue mod p

Norton showed

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET 2015)

Let $p > 3$ be a prime. Let $g(p)$ be the least quadratic non-residue $\bmod p$. Then

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \textit{if } p \equiv 1 \pmod 4, \\ 1.1p^{1/4}\log p & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

Explicit estimates on the least quadratic non-residue mod p

Norton showed

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET 2015)

Let $p > 3$ be a prime. Let $g(p)$ be the least quadratic non-residue $\bmod p$. Then

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \textit{if } p \equiv 1 \pmod 4, \\ 1.1p^{1/4}\log p & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (Burgess 1962)

Let $g(p)$ be the least quadratic non-residue mod p. *Let $\varepsilon > 0$. There exists p_0 such that for all primes $p \geq p_0$ we have $g(p) < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.*

Theorem (ET 2015)

Let $g(p)$ be the least quadratic non-residue mod p. *Let p be a prime greater than 10^{4732}, then $g(p) < p^{1/6}$.*

Theorem (Francis 2021)

Let $g(p)$ be the least quadratic non-residue mod p. *Let p be a prime greater than 10^{3872}, then $g(p) < p^{1/6}$, and if $p > 10^{82}$, $g(p) < p^{1/4}$.*

Consecutive quadratic residues or non-quadratic residues

Let $H(p)$ be the largest string of consecutive nonzero quadratic residues or quadratic non-residues modulo p.
For example, with $p = 7$ we have that the nonzero quadratic residues are $\{1, 2, 4\}$ and the quadratic non-residues are $\{3, 5, 6\}$. Therefore $H(7) = 2$.

p	$H(p)$
11	3
13	4
17	3
19	4
23	4
29	4
31	4
37	4
41	5

Burgess proved in 1963 that $H(p) \leq Cp^{1/4} \log p$.

Mathematician	Year	C	Restriction
Norton*	1973	2.5	$p > e^{15}$
Norton*	1973	4.1	None
Preobrazhenskaya	2009	$1.85\ldots + o(1)$	Not explicit
McGown	2012	7.06	$p > 5 \cdot 10^{18}$
McGown	2012	7	$p > 5 \cdot 10^{55}$
ET	2012	1.495...+ o(1)	Not explicit
ET	2012	1.55	$p > 10^{13}$
ET	2017	3.38	None

*Norton didn't provide a proof for his claim.

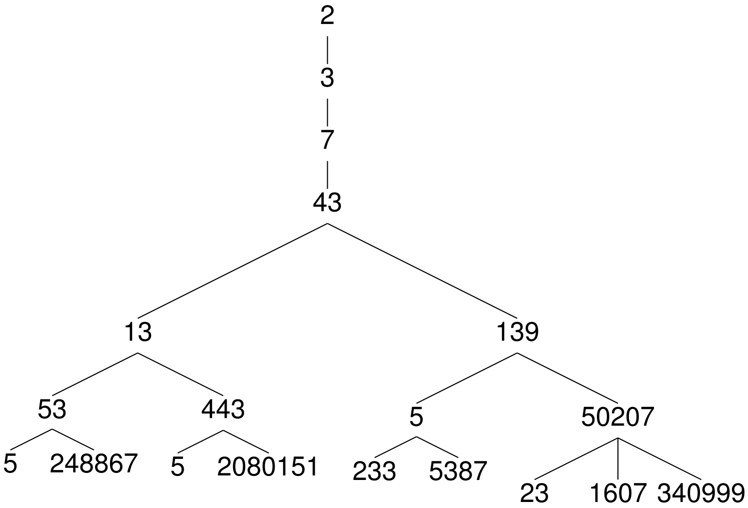
There are infinitely many primes

Start with $q_1 = 2$. Supposing that q_j has been defined for $1 \leq j \leq k$, continue the sequence by choosing a prime q_{k+1} for which

$$q_{k+1} \mid 1 + \prod_{j=1}^{k} q_j.$$

Then 'at the end of the day', the list $q_1, q_2, q_3, \ldots$ is an infinite sequence of distinct prime numbers.

Tree of possibilities



Euclid-Mullin sequences

Since the sequence in the previous slide is not unique, Mullin suggested two possible unique sequences.

- The first is to take $q_1 = 2$, then define recursively q_k to be the **smallest** prime dividing $1 + q_1 q_2 \dots q_{k-1}$.
- i.e. 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, ...
- It is conjectured that the first Mullin sequence touches all the primes eventually.
- Not much is known of this sequence.

Second Euclid-Mullin Sequence

- The second Mullin sequence is to take $q_1 = 2$, then define recursively q_k to be the **largest** prime dividing $1 + q_1 q_2 \dots q_{k-1}$.
- i.e. 2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 4680225641471129, ...
- Cox and van der Poorten (1968) proved 5, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, and 53 are missing from the first Euclid-Mullin sequence.
- Booker in 2012 showed that infinitely many primes are missing from the sequence.
- One of the results used in Booker's proof is the upper bound on $g(p)$.

An elementary bound for $g(p)$

Let $g(p)$ be the least quadratic non-residue $\bmod p$.

Theorem

$g(p) \leq \sqrt{p} + 1$.

Proof.

Suppose $g(p) = q$ with $q > \sqrt{p} + 1$. Let k be the ceiling of p/q. Then $p < kq < p + q$, so $kq \equiv a \bmod p$ for some $0 < a < q$, and therefore kq is a quadratic residue modulo p. Since $q > \sqrt{p} + 1$, then $p/q < \sqrt{p}$, so k is at most the ceiling of $\sqrt{p} < \sqrt{p} + 1 < q$. Therefore k is a quadratic residue modulo p. But if k and kq are quadratic residues modulo p, then q is a square modulo p. Contradiction! $\square$

An elementary bound for $H(p)$

Sketch of a proof that $H(p) < 2\sqrt{p}$.

- Suppose $\{a+1, a+2, \ldots, a+H\}$ are all quadratic residues mod p.
- For n a non-residue, $na+n, \ldots, na+Hn$ are non-residues.
- If $Hn > p$, then $H(p) \leq n-1$. Therefore $H(p) \leq \max\{p/n, n-1, 2\sqrt{p}\}$.
- If $n \in (\sqrt{p}/2, 2\sqrt{p}]$ we have $H(p) < 2\sqrt{p}$.
- Let k be the largest integer such that $k^2 g(p) \leq \sqrt{p}/2$.
- $(k+1)^2 g(p) > 2\sqrt{p} \geq 4k^2 g(p)$ implies $(2k+1) > 3k^2$ which is false for each $k \geq 1$. Therefore there is a non-residue in the interval $(\sqrt{p}/2, 2\sqrt{p}]$, yielding $H(p) < 2\sqrt{p}$.

$\square$

An elementary bound for $H(p)$

Sketch of a proof that $H(p) < 2\sqrt{p}$.

- Suppose $\{a+1, a+2, \ldots, a+H\}$ are all quadratic residues mod p.
- For n a non-residue, $na+n, \ldots, na+Hn$ are non-residues.
- If $Hn > p$, then $H(p) \leq n-1$. Therefore $H(p) \leq \max\{p/n, n-1, 2\sqrt{p}\}$.
- If $n \in (\sqrt{p}/2, 2\sqrt{p}]$ we have $H(p) < 2\sqrt{p}$.
- Let k be the largest integer such that $k^2 g(p) \leq \sqrt{p}/2$.
- $(k+1)^2 g(p) > 2\sqrt{p} \geq 4k^2 g(p)$ implies $(2k+1) > 3k^2$ which is false for each $k \geq 1$. Therefore there is a non-residue in the interval $(\sqrt{p}/2, 2\sqrt{p}]$, yielding $H(p) < 2\sqrt{p}$.

An elementary bound for $H(p)$

Sketch of a proof that $H(p) < 2\sqrt{p}$.

- Suppose $\{a+1, a+2, \ldots, a+H\}$ are all quadratic residues mod p.
- For n a non-residue, $na+n, \ldots, na+Hn$ are non-residues.
- If $Hn > p$, then $H(p) \le n-1$. Therefore $H(p) \le \max\{p/n, n-1, 2\sqrt{p}\}$.
- If $n \in (\sqrt{p}/2, 2\sqrt{p}]$ we have $H(p) < 2\sqrt{p}$.
- Let k be the largest integer such that $k^2 g(p) \le \sqrt{p}/2$.
- $(k+1)^2 g(p) > 2\sqrt{p} \ge 4k^2 g(p)$ implies $(2k+1) > 3k^2$ which is false for each $k \ge 1$. Therefore there is a non-residue in the interval $(\sqrt{p}/2, 2\sqrt{p}]$, yielding $H(p) < 2\sqrt{p}$.

An elementary bound for $H(p)$

Sketch of a proof that $H(p) < 2\sqrt{p}$.

- Suppose $\{a+1, a+2, \ldots, a+H\}$ are all quadratic residues mod p.
- For n a non-residue, $na+n, \ldots, na+Hn$ are non-residues.
- If $Hn > p$, then $H(p) \leq n-1$. Therefore $H(p) \leq \max\{p/n, n-1, 2\sqrt{p}\}$.
- If $n \in (\sqrt{p}/2, 2\sqrt{p}]$ we have $H(p) < 2\sqrt{p}$.
- Let k be the largest integer such that $k^2 g(p) \leq \sqrt{p}/2$.
- $(k+1)^2 g(p) > 2\sqrt{p} \geq 4k^2 g(p)$ implies $(2k+1) > 3k^2$ which is false for each $k \geq 1$. Therefore there is a non-residue in the interval $(\sqrt{p}/2, 2\sqrt{p}]$, yielding $H(p) < 2\sqrt{p}$.

The primes that Euclid forgot

Theorem

Let $Q_1, Q_2, \ldots Q_r$ be the smallest r primes omitted from the second Euclid-Mullin sequence, where $r \geq 0$. Then there is another omitted prime smaller than

$$24^2 \left(\prod_{i=1}^{r} Q_i \right)^2 .$$

Using the deep results of Burgess, Booker showed that the exponent can be replaced with any real number larger than $\dfrac{1}{4\sqrt{e}-1} = 0.178734\ldots$, provided that 24^2 is also replaced by a possibly larger constant.

Proof Sketch

Let $X = 24^2(\prod_{i=1}^{r} Q_i)^2$. Assume there is no prime missing from $[2, X]$ besides $Q_1, \ldots, Q_r$. Let p be the prime in $[2, X]$ that is last to appear in the sequence $\{q_i\}$. Let n be such that $q_n = p$.
Then $1 + q_1 \ldots q_{n-1} = Q_1^{e_1} \ldots Q_r^{e_r} p^e$.
Let d be the smallest number satisfying the following conditions:

(i) $d \equiv 1 \pmod 4$,

(ii) $d \equiv -1 \pmod{Q_1 \ldots Q_r}$

(iii) $\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)$.

- Using the Chinese Remainder Theorem and the bound on $H(p)$ yields that $d \leq X$.
- Given the conditions on d and using that $d \leq X$ shows that d is both a quadratic residue and a non-residue mod $1 + q_1 q_2 \ldots q_{n-1}$. Contradiction!

Legendre Symbol

$$Let \left(\frac{a}{p}\right) = \begin{cases} 0 & , \quad \text{if } a \equiv 0 \mod p, \\ 1 & , \quad \text{if } a \text{ is a square } \mod p \\ -1 & , \quad \text{if } a \text{ is a quadratic non-residue } \mod p. \end{cases}$$

$\left(\frac{a}{p}\right)$ has the following important properties:

- $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$ for all a.
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ for all a, b.
- $\left(\frac{a}{p}\right) \neq 0$ if and only if $\gcd(a, p) = 1$.

Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character $\bmod n$ if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) \neq 0$ if and only if $\gcd(a, n) = 1$.

The Legendre symbol is an example of a Dirichlet character.

A simple but powerful idea

Let $g(p) = m$ be the least quadratic non-residue modulo p.

Suppose $\chi(a) = \left(\frac{a}{p}\right)$ Then $\chi(n) = 1$ for $n = 1, 2, 3, ..., m - 1$ and $\chi(m) = -1$. Therefore

$$\sum_{i=1}^{m} \chi(i) = m - 2 < m,$$

and

$$\sum_{i=1}^{k} \chi(i) = k \text{ for all } k < m.$$

Therefore bounding $\sum_{i=1}^{n} \chi(i)$ can give an upper bound for $g(p)$.

Pólya–Vinogradov

Let χ be a Dirichlet character to the modulus $q > 1$. Let

$$S(\chi) = \max_{M,N} \left| \sum_{n=M+1}^{M+N} \chi(n) \right|$$

The Pólya–Vinogradov inequality (1918) states that there exists an absolute universal constant c such that for any Dirichlet character $S(\chi) \leq c\sqrt{q}\log q$.

Under GRH, Montgomery and Vaughan showed that $S(\chi) \ll \sqrt{q}\log\log q$.

Paley showed in 1932 that there are infinitely many quadratic characters such that $S(\chi) \gg \sqrt{q}\log\log q$.

Vinogradov's Trick: Showing $g(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}$

- Suppose $\sum_{n \le x} \chi(n) = o(x)$.
- Let $y = x^{1/\sqrt{e}+\delta}$ for some $\delta > 0$. So $\log\log x - \log\log y = \log\left(1/\sqrt{e}+\delta\right) < 1/2$
- Suppose $g(p) > y$.

$$\sum_{n \le x} \chi(n) = \sum_{n \le x} 1 - 2 \sum_{\substack{y < q \le x \\ \chi(q) = -1}} \sum_{n \le \frac{x}{q}} 1,$$

where the sum ranges over q prime. Therefore we have

$$\sum_{n \le x} \chi(n) \ge \lfloor x \rfloor - 2 \sum_{y < q \le x} \left\lfloor \frac{x}{q} \right\rfloor \ge x - 1 - 2x \sum_{y < q \le x} \frac{1}{q} - 2 \sum_{y < q \le x} 1.$$

It took almost 50 years before the next breakthrough. It came from the following theorem of Burgess:

Theorem (Burgess, 1962)

Let χ be a primitive character $\bmod q$, where $q > 1$, r is a positive integer and $\epsilon > 0$ is a real number. Then

$$|S_\chi(M,N)| = \left| \sum_{M<n\leq M+N} \chi(n) \right| \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon}$$

for $r = 1, 2, 3$ and for any $r \geq 1$ if q is cubefree, the implied constant depending only on ϵ and r.

Consider

$$\left|\sum_{n\le N}\chi(n)\right|.$$

By Burgess

$$\left|\sum_{n\le N}\chi(n)\right| \ll N^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\epsilon}.$$

However, if $\chi(n)=1$ for all $n\le N$, then

$$N\le\left|\sum_{n\le N}\chi(n)\right| \ll N^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\epsilon},$$

so

$$N^{\frac{1}{r}} \ll q^{\frac{r+1}{4r^2}+\epsilon}.$$

Hence

$$N \ll q^{\frac{1}{4}+\frac{1}{4r}+\epsilon r}$$

Now we know why

$$g(p) \ll p^{\frac{1}{4\sqrt{e}}+\varepsilon},$$

but how do we go from there to be able to figure out the theorems:

Theorem (ET 2015)

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p be a prime greater than 10^{4732}, then $g(p) < p^{1/6}$.

Theorem (Francis 2021)

Let $g(p)$ be the least quadratic non-residue $\bmod p$. Let p be a prime greater than 10^{3872}, then $g(p) < p^{1/6}$, and if $p > 10^{82}$, $g(p) < p^{1/4}$.

Explicit Burgess

Theorem (Iwaniec-Kowalski-Friedlander)

Let χ be a non-principal Dirichlet character mod p (a prime). Let M and N be non-negative integers with $N \geq 1$ and let $r \geq 2$, then

$$|S_\chi(M,N)| \leq 30 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Theorem (ET, 2015)

Let p be a prime. Let χ be a non-principal Dirichlet character $\bmod$ p. Let M and N be non-negative integers with $N \geq 1$ and let r be a positive integer. Then for $p \geq 10^7$, we have

$$|S_\chi(M,N)| \leq 2.74 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Explicit Burgess

Theorem (Iwaniec-Kowalski-Friedlander)

Let χ be a non-principal Dirichlet character mod p (a prime). Let M and N be non-negative integers with $N \geq 1$ and let $r \geq 2$, then

$$|S_\chi(M,N)| \leq 30 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Theorem (ET, 2015)

Let p be a prime. Let χ be a non-principal Dirichlet character $\bmod p$. Let M and N be non-negative integers with $N \geq 1$ and let r be a positive integer. Then for $p \geq 10^7$, we have

$$|S_\chi(M,N)| \leq 2.74 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Some Applications of the Explicit Estimates

- Booker (2006) computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved (2012) that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$. Recently (2017) improved to no Norm-Euclidean fields with discriminant $> 10^{100}$
- Levin, Pomerance and Soundararajan proved a conjecture of Brizolis that for every prime $p > 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$.
- Explicit bound on the least prime primitive root done by Cohen, Oliveira e Silva and Trudgian (2016).

Some Applications of the Explicit Estimates

- Booker (2006) computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved (2012) that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$. Recently (2017) improved to no Norm-Euclidean fields with discriminant $> 10^{100}$
- Levin, Pomerance and Soundararajan proved a conjecture of Brizolis that for every prime $p > 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$.
- Explicit bound on the least prime primitive root done by Cohen, Oliveira e Silva and Trudgian (2016).

Some Applications of the Explicit Estimates

- Booker (2006) computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved (2012) that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$. Recently (2017) improved to no Norm-Euclidean fields with discriminant $> 10^{100}$
- Levin, Pomerance and Soundararajan proved a conjecture of Brizolis that for every prime $p > 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$.
- Explicit bound on the least prime primitive root done by Cohen, Oliveira e Silva and Trudgian (2016).

Some Applications of the Explicit Estimates

- Booker (2006) computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved (2012) that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$. Recently (2017) improved to no Norm-Euclidean fields with discriminant $> 10^{100}$
- Levin, Pomerance and Soundararajan proved a conjecture of Brizolis that for every prime $p > 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$.
- Explicit bound on the least prime primitive root done by Cohen, Oliveira e Silva and Trudgian (2016).

Key Inequality to prove Burgess Inequality

Theorem (Burgess, Booker, ET)

Let h and w be positive integers. Let χ be a primitive Dirichlet character $\bmod p$, then

$$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} < (2w-1)!!p\,h^{w} + (2w-1)\sqrt{p}\,h^{2w}.$$

Sketch of a Proof

- $$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} = \sum_{l_1,l_2,\ldots,l_{2w}}\sum_{x \bmod p}\chi(q(x)),$$

  where

  $$q(x) = \frac{(x+l_1)(x+l_2)\ldots(x+l_w)}{(x+l_{w+1})(x+l_{w+2})\ldots(x+l_{2w})}.$$

- If $q(x)$ is not a k-th power (where k is the order of χ), then

  $$\left|\sum_{x \bmod p}\chi(q(x))\right| \leq (r-1)\sqrt{p},$$

  where r is the number of distinct roots of $q(x)$.

Sketch of a Proof

- $$\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} = \sum_{l_1,l_2,\ldots,l_{2w}}\sum_{x \bmod p}\chi(q(x)),$$
  where
  $$q(x) = \frac{(x+l_1)(x+l_2)\ldots(x+l_w)}{(x+l_{w+1})(x+l_{w+2})\ldots(x+l_{2w})}.$$
- If $q(x)$ is not a k-th power (where k is the order of χ), then
  $$\left|\sum_{x \bmod p}\chi(q(x))\right| \le (r-1)\sqrt{p},$$
  where r is the number of distinct roots of $q(x)$.

Applications

Theorem (ET 2015)

Let $p > 3$ be a prime and k be a positive integer that divides $p-1$. Let $g(p,k)$ be the least k-th power non-residue $\bmod p$. Then

$$g(p,k) \leq \begin{cases} 1.1p^{1/4}\log p & \text{if } p \equiv 3 \bmod 4 \text{ and } k = 2, \\ 0.9p^{1/4}\log p & \text{otherwise.} \end{cases}$$

Theorem (ET 2012, 2017)

If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then

$$H \leq \begin{cases} 3.38p^{1/4}\log p, & \text{for all odd } p, \\ 1.55p^{1/4}\log p, & \text{for } p \geq 10^{13}. \end{cases}$$

Applications

Theorem (ET 2015)

Let $p > 3$ be a prime and k be a positive integer that divides $p-1$. Let $g(p,k)$ be the least k-th power non-residue $\bmod p$. Then

$$g(p,k) \leq \begin{cases} 1.1p^{1/4}\log p & \text{if } p \equiv 3 \bmod 4 \text{ and } k = 2, \\ 0.9p^{1/4}\log p & \text{otherwise.} \end{cases}$$

Theorem (ET 2012, 2017)

If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then

$$H \leq \begin{cases} 3.38p^{1/4}\log p, & \text{for all odd } p, \\ 1.55p^{1/4}\log p, & \text{for } p \geq 10^{13}. \end{cases}$$

Quadratic fields and inert primes

- Let d be a squarefree integer.
- Then $\mathbb{Q}(\sqrt{d})$ is a quadratic field.
- A prime $p \in \mathbb{Z}$ is inert if it remains prime when it is lifted to the quadratic field.
- For example $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. In this field, the inert primes are the primes $p \equiv 3 \pmod 4$.
- Note that 5 is not prime in $\mathbb{Q}(i)$ because $(1+2i)(1-2i) = 5$. Similarly any prime $p \equiv 1 \pmod 4$ is not prime in $\mathbb{Q}(i)$ since p can be written as $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and hence $p = (a+bi)(a-bi)$.

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square} \mod p, \\ -1 & \text{if } a \text{ is a non-square} \mod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square } \bmod p, \\ -1 & \text{if } a \text{ is a non-square } \bmod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square } \bmod p, \\ -1 & \text{if } a \text{ is a non-square } \bmod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The least inert prime in a real quadratic field

Theorem (Granville, Mollin and Williams, 2000)

For any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$.

Theorem (ET, 2010)

For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$.

The least inert prime in a real quadratic field

Theorem (Granville, Mollin and Williams, 2000)

For any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$.

Theorem (ET, 2010)

For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$.

Elements of the Proof

- Use a computer to check the “small” cases. Granville, Mollin and Williams used the Manitoba Scalable Sieving Unit.
- Use analytic techniques to prove it for the “infinite case”, i.e. the very large D. The tool used by Granville et al. was the Pólya–Vinogradov inequality. I used a “smoothed” version of it.
- Use Pólya–Vinogradov plus a bit of clever computing to fill in the gap.

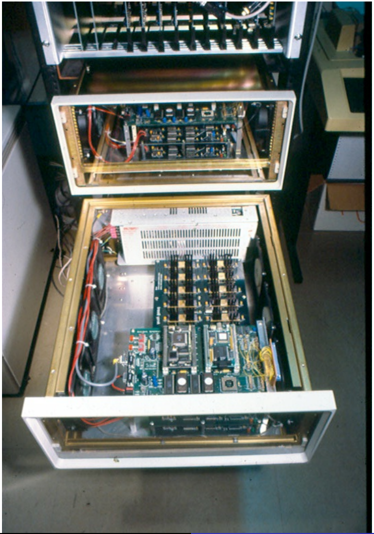
Elements of the Proof

- Use a computer to check the “small” cases. Granville, Mollin and Williams used the Manitoba Scalable Sieving Unit.
- Use analytic techniques to prove it for the “infinite case”, i.e. the very large D. The tool used by Granville et al. was the Pólya–Vinogradov inequality. I used a “smoothed” version of it.
- Use Pólya–Vinogradov plus a bit of clever computing to fill in the gap.

Elements of the Proof

- Use a computer to check the “small” cases. Granville, Mollin and Williams used the Manitoba Scalable Sieving Unit.
- Use analytic techniques to prove it for the “infinite case”, i.e. the very large D. The tool used by Granville et al. was the Pólya–Vinogradov inequality. I used a “smoothed” version of it.
- Use Pólya–Vinogradov plus a bit of clever computing to fill in the gap.

Manitoba Scalable Sieving Unit



Smoothed Pólya–Vinogradov

Let M, N be real numbers with $0 < N \le q$, then define $S^*(\chi)$ as follows:

$$S^*(\chi) = \max_{M,N} \left| \sum_{M \le n \le M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right|.$$

Theorem (Levin, Pomerance, Soundararajan, 2009)

Let χ be a primitive character to the modulus $q > 1$, and let M, N be real numbers with $0 < N \le q$, then

$$S^*(\chi) \le \sqrt{q} - \frac{N}{\sqrt{q}}.$$

Lower bound for the smoothed Pólya–Vinogradov

Theorem (ET, 2010)

Let χ be a primitive character to the modulus $q > 1$, and let M, N be real numbers with $0 < N \leq q$, then

$$S^*(\chi) \geq \frac{2}{\pi^2}\sqrt{q}.$$

Therefore, the order of magnitude of $S^*(\chi)$ is $\sqrt{q}$.

Tighter smoothed PV

Theorem (ET, 2010)

Let χ be a primitive character to the modulus $q > 1$, let M, N be real numbers with $0 < N \leq q$. Then

$$\left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right| \leq \frac{\phi(q)}{q}\sqrt{q} + 2^{\omega(q)-1}\frac{N}{\sqrt{q}}.$$

Applying smoothed PV to the least inert prime problem

Let $\chi(p) = \left(\frac{D}{p}\right)$. Since D is a fundamental discriminant, χ is a primitive character of modulus D. Consider

$$S_\chi(N) = \sum_{n \leq 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right).$$

By smoothed PV, we have

$$|S_\chi(N)| \leq \frac{\phi(D)}{D}\sqrt{D} + 2^{\omega(D)-1}\frac{N}{\sqrt{D}}.$$

Now,

$$S_\chi(N) = \sum_{\substack{n \le 2N \\ (n,D)=1}} \left(1 - \left|\frac{n}{N} - 1\right|\right) - 2 \sum_{\substack{B < p \le 2N \\ \chi(p)=-1}} \sum_{\substack{n \le \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

- Therefore,

$$\frac{\phi(D)}{D}\sqrt{D} + 2^{\omega(D)-1}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N - 2^{\omega(D)-2} - 2\sum_{\substack{n \le \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

- Now, letting $N = c\sqrt{D}$ for some constant c we get

$$0 \ge c - 1 - 2^{\omega(D)}\left(\frac{c}{2} + \frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n \le \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right)$$

Now,

$$S_\chi(N) = \sum_{\substack{n\le 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) - 2\sum_{\substack{B<p\le 2N\\ \chi(p)=-1}} \sum_{\substack{n\le \frac{2N}{p}\\(n,D)=1}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Therefore,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Now, letting $N = c\sqrt{D}$ for some constant c we get

$$0 \ge c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

Now,

$$S_\chi(N) = \sum_{\substack{n\le 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) - 2\sum_{\substack{B<p\le 2N\\ \chi(p)=-1}}\ \sum_{\substack{n\le \frac{2N}{p}\\(n,D)=1}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Therefore,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}}\ \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

- Now, letting $N = c\sqrt{D}$ for some constant c we get

$$0 \ge c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}}\ \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

Eventually we have,

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2c}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p \mid D}} \frac{p}{p-1}.$$

For $D \geq 10^{24}$ this is a contradiction.

Hybrid Case

We have as in the previous case

$$0 \geq c - 1 - 2^{\omega(D)}\left(\frac{c}{2} + \frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}}\sum_{B < p \leq \frac{2N}{n}}\left(1 - \left|\frac{np}{N} - 1\right|\right)$$

In this case, since we don't have to worry about the infinite case, we can have a messier version of

$$\sum_{B < p \leq \frac{2N}{n}}\left(1 - \left|\frac{np}{N} - 1\right|\right).$$

The idea is to consider 2^{13} cases, one for each possible value of $\gcd(D, M)$ where $M = \prod_{p \leq 41} p$.

- We consider the odd values and the even values separately. For odd values, the strategy of checking all the cases proves the theorem for $21853026051351495 = 2.2\ldots \times 10^{16}$.
- For even values we get the theorem for $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Here we need a little extra work, we find that there are 12 outstanding cases and we deal with them one at a time.
- QED.

- We consider the odd values and the even values separately. For odd values, the strategy of checking all the cases proves the theorem for $21853026051351495 = 2.2\ldots \times 10^{16}$.
- For even values we get the theorem for $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Here we need a little extra work, we find that there are 12 outstanding cases and we deal with them one at a time.
- QED.

- We consider the odd values and the even values separately. For odd values, the strategy of checking all the cases proves the theorem for $21853026051351495 = 2.2\ldots \times 10^{16}$.
- For even values we get the theorem for $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Here we need a little extra work, we find that there are 12 outstanding cases and we deal with them one at a time.
- QED.

- We consider the odd values and the even values separately. For odd values, the strategy of checking all the cases proves the theorem for $21853026051351495 = 2.2\ldots \times 10^{16}$.
- For even values we get the theorem for $1707159924755154870 = 1.71\ldots \times 10^{18}$.
- Here we need a little extra work, we find that there are 12 outstanding cases and we deal with them one at a time.
- QED.

Thank you!