

The least quadratic non-residue and related problems

Enrique Treviño

Lake Forest College

California State University, Chico Colloquium
April 17, 2015



Squares

Consider the sequence

$$2, 5, 8, 11, \dots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories:
 $n \equiv 0, 1$ or $2 \pmod{3}$.
- 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

$$2, 5, 8, 11, \dots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories:
 $n \equiv 0, 1$ or $2 \pmod{3}$.
- 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

$$2, 5, 8, 11, \dots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories:
 $n \equiv 0, 1$ or $2 \pmod{3}$.
- 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

$$2, 5, 8, 11, \dots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories:
 $n \equiv 0, 1$ or $2 \pmod{3}$.
- 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

$$2, 5, 8, 11, \dots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories:
 $n \equiv 0, 1$ or $2 \pmod{3}$.
- 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 $q \in \{0, 1, 2, \dots, n-1\}$, we call q a quadratic residue mod 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 residues are $\{0, 1\}$ and the quadratic non-residue is 2.
- For $n = 5$, the quadratic residues are $\{0, 1, 4\}$ and the quadratic non-residues are $\{2, 3\}$.
- For $n = 7$, the quadratic residues are $\{0, 1, 2, 4\}$ 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 quadratic non-residue

How big can the least quadratic non-residue be?

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

p	Least quadratic non-residue
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2
31	3

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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p . Let p_i be the i -th prime, i.e, $p_1 = 2, p_2 = 3, \dots$

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{\pi(x)}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{\pi(x)}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.
- 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 mod p

Let $g(p)$ be the least quadratic non-residue mod 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 $g(p) \gg \log p \log \log p$, that is

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

Theorems on the least quadratic non-residue mod p

Let $g(p)$ be the least quadratic non-residue mod 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 $g(p) \gg \log p \log \log p$, that is

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

Theorems on the least quadratic non-residue mod p

Let $g(p)$ be the least quadratic non-residue mod 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 $g(p) \gg \log p \log \log p$, that is

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

Theorems on the least quadratic non-residue mod p

Let $g(p)$ be the least quadratic non-residue mod 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 mod p . Then

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

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 mod p . Then

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

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
$$g(p) < p^{\frac{1}{4\sqrt{\varepsilon}} + \varepsilon}.$$

Theorem (ET)

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

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

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	$1.85 \dots + o(1)$	Not explicit
McGown	2012	7.06	$p > 5 \cdot 10^{18}$
McGown	2012	7	$p > 5 \cdot 10^{55}$
ET	2012	$1.495 \dots + o(1)$	Not explicit
ET	2012	1.55	$p > 10^{13}$
ET	2012	3.64	None

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

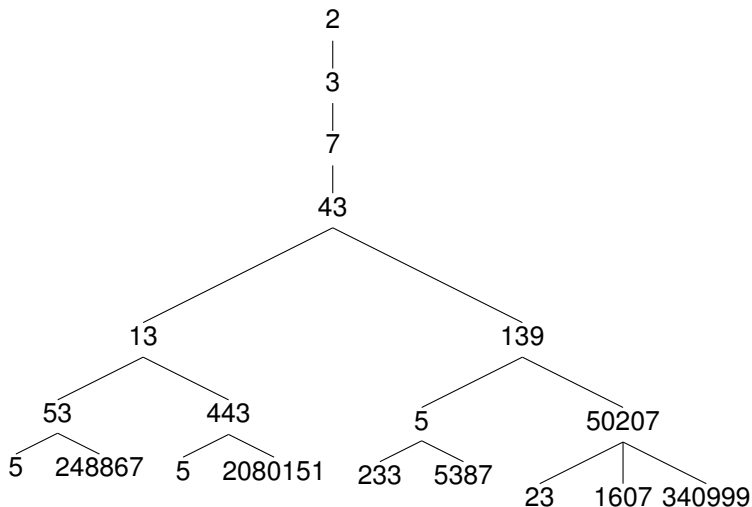
There are infinitely many primes

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, \dots 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 mod 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 $kq \equiv a \pmod{p}$ 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! □

An elementary bound for $H(p)$

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

- The largest string of quadratic non-residues is $< 2\sqrt{p}$.
- Suppose $\{a + 1, a + 2, \dots, a + H\}$ are all quadratic residues mod p .
- For n a non-residue, $na + n, \dots, na + Hn$ 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 $H(p) < 2\sqrt{p}$.

- The largest string of quadratic non-residues is $< 2\sqrt{p}$.
- Suppose $\{a + 1, a + 2, \dots, a + H\}$ are all quadratic residues mod p .
- For n a non-residue, $na + n, \dots, na + Hn$ 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 $H(p) < 2\sqrt{p}$.

- The largest string of quadratic non-residues is $< 2\sqrt{p}$.
- Suppose $\{a + 1, a + 2, \dots, a + H\}$ are all quadratic residues mod p .
- For n a non-residue, $na + n, \dots, na + Hn$ 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 $H(p) < 2\sqrt{p}$.

- The largest string of quadratic non-residues is $< 2\sqrt{p}$.
- Suppose $\{a + 1, a + 2, \dots, a + H\}$ are all quadratic residues mod p .
- For n a non-residue, $na + n, \dots, na + Hn$ 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 $H(p) < 2\sqrt{p}$.

- The largest string of quadratic non-residues is $< 2\sqrt{p}$.
- Suppose $\{a + 1, a + 2, \dots, a + H\}$ are all quadratic residues mod p .
- For n a non-residue, $na + n, \dots, na + Hn$ 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, \dots, 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 $\frac{1}{4\sqrt{e}-1} = 0.178734\dots$, provided that 24^2 is also replaced by a possibly larger constant.

Proof Sketch

Let $X = 24^2 \left(\prod_{i=1}^r Q_i \right)^2$. Assume there is no prime missing from $[2, X]$ besides Q_1, \dots, 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 $1 + q_1 \dots q_{n-1} = Q_1^{e_1} \dots Q_r^{e_r} p^e$.

Let d be the smallest number satisfying the following conditions:

- (i) $d \equiv 1 \pmod{4}$,
- (ii) $d \equiv -1 \pmod{Q_1 \dots Q_r}$
- (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 $1 + q_1 q_2 \dots q_{n-1}$. Contradiction!

Legendre Symbol

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

$\left(\frac{a}{p}\right)$ 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.

$\chi : \mathbb{Z} \rightarrow \mathbb{C}$ is a Dirichlet character mod 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 $n = 1, 2, 3, \dots, m-1$
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 $\sum_{n \leq x} \chi(n) = o(x)$.
- Let $y = x^{1/\sqrt{e} + \delta}$ for some $\delta > 0$. So $\log \log x - \log \log y = \log(1/\sqrt{e} + \delta) < 1/2$
- Suppose $g(p) > y$.

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

where the sum ranges over q prime. Therefore we have

$$\sum_{n \leq x} \chi(n) \geq [x] - 2 \sum_{y < q \leq x} \left\lfloor \frac{x}{q} \right\rfloor \geq x - 1 - 2x \sum_{y < q \leq x} \frac{1}{q} - 2 \sum_{y < q \leq x} 1.$$

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 mod 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

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

By Burgess

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

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

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

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 theorem:

Theorem (ET)

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

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)

Let p be a prime. Let χ be a non-principal Dirichlet character mod 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)

Let p be a prime. Let χ be a non-principal Dirichlet character mod 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

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$.
- 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, $g^x \equiv x \pmod{p}$.
- I used similar explicit estimates of character sums to bound the least inert prime in a real quadratic field.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$.
- 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, $g^x \equiv x \pmod{p}$.
- I used similar explicit estimates of character sums to bound the least inert prime in a real quadratic field.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$.
- 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, $g^x \equiv x \pmod{p}$.
- I used similar explicit estimates of character sums to bound the least inert prime in a real quadratic field.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$.
- 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, $g^x \equiv x \pmod{p}$.
- I used similar explicit estimates of character sums to bound the least inert prime in a real quadratic field.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{140}$.
- 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, $g^x \equiv x \pmod{p}$.
- I used similar explicit estimates of character sums to bound the least inert prime in a real quadratic field.

Thank you!