The least quadratic non-residue modulo a prime and related problems

Enrique Treviño

Lake Forest College

Number Theory in Illinois: A conference in honor of the Batemans and Halberstam
June 3, 2014

LAKE FOREST COLLEGE

Squares

Consider the sequence

$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots$$

Can it contain any squares?

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

$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots$$

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

$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots$$

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

$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots$$

Can it contain any squares?

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

$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0, 1 \text{ or } 2 \pmod 3$.
- 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 $q \in \{0, 1, 2, \ldots, n-1\}$, 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 non-residue is 2.
- For $n = 5$, the quadratic residues are $\{0, 1, 4\}$ and the non-residues are $\{2, 3\}$.
- For $n = 7$, the quadratic residues are $\{0, 1, 2, 4\}$ and the non-residues are $\{3, 5, 6\}$.
- For $n = p$, an odd prime, there are $\frac{p+1}{2}$ quadratic residues and $\frac{p-1}{2}$ non-residues.

Least non-residue

p	Least non-residue
3	2
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, $p_1 = 2, p_2 = 3, \ldots$.

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

Heuristics

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

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

Heuristics

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

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

Heuristics

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

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

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 $g(p) = p_k$.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log \log x$.

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 $g(p) = p_k$.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log\log x$.

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 $g(p) \leq 2\log^2 p$.
- 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 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 $g(p) \le 2\log^2 p$.
- 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 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 $g(p) \leq 2\log^2 p$.
- 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 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 $g(p) \leq 2 \log^2 p$.
- 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

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

The first breakthrough came in 1914 with some clever ideas from I.M. Vinogradov. Consider the function χ where $\chi(a)$ is 1 if a is a nonzero quadratic residue mod p, -1 if its a non-residue and 0 for $a = 0$. χ is then a primitive Dirichlet character mod p.

- Vinogradov noted that if $\sum_{1 \leq a \leq n} \chi(a) < n$, then $g(p) \leq n$.
- He then proved $\sum_{1 \leq a \leq n} \chi(a) < \sqrt{p} \log p$, which shows that $g(p) \leq \sqrt{p} \log p$.
- Then using that $\chi(ab) = \chi(a)\chi(b)$ he was able to improve this to show the asymptotic inequality $g(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}$.

History

The first breakthrough came in 1914 with some clever ideas from I.M. Vinogradov. Consider the function χ where $\chi(a)$ is 1 if a is a nonzero quadratic residue mod p, -1 if its a non-residue and 0 for $a = 0$. χ is then a primitive Dirichlet character mod p.

- Vinogradov noted that if $\sum_{1 \leq a \leq n} \chi(a) < n$, then $g(p) \leq n$.
- He then proved $\sum_{1 \leq a \leq n} \chi(a) < \sqrt{p} \log p$, which shows that $g(p) \leq \sqrt{p} \log p$.
- Then using that $\chi(ab) = \chi(a)\chi(b)$ he was able to improve this to show the asymptotic inequality $g(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}$.

History

The first breakthrough came in 1914 with some clever ideas from I.M. Vinogradov. Consider the function χ where $\chi(a)$ is 1 if a is a nonzero quadratic residue mod p, -1 if its a non-residue and 0 for $a = 0$. χ is then a primitive Dirichlet character mod p.

- Vinogradov noted that if $\sum_{1 \leq a \leq n} \chi(a) < n$, then $g(p) \leq n$.
- He then proved $\sum_{1 \leq a \leq n} \chi(a) < \sqrt{p} \log p$, which shows that $g(p) \leq \sqrt{p} \log p$.
- Then using that $\chi(ab) = \chi(a)\chi(b)$ he was able to improve this to show the asymptotic inequality $g(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}$.

History

The first breakthrough came in 1914 with some clever ideas from I.M. Vinogradov. Consider the function χ where $\chi(a)$ is 1 if a is a nonzero quadratic residue mod p, -1 if its a non-residue and 0 for $a = 0$. χ is then a primitive Dirichlet character mod p.

- Vinogradov noted that if $\sum_{1 \le a \le n} \chi(a) < n$, then $g(p) \le n$.
- He then proved $\sum_{1 \le a \le n} \chi(a) < \sqrt{p} \log p$, which shows that $g(p) \le \sqrt{p} \log p$.
- Then using that $\chi(ab) = \chi(a)\chi(b)$ he was able to improve this to show the asymptotic inequality $g(p) \ll p^{\frac{1}{2\sqrt{e}} + \varepsilon}$.

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

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

Explicit estimates on the least k-th power non-residue

Let $p > 3$ be a prime. Let $g_k(p)$ be the least k-th power non-residue mod p.
Norton showed in the late 60's that

$$g_k(p) \le \begin{cases} 4.7p^{1/4}\log p & \text{if } k = 2 \text{ and } p \equiv 3 \pmod 4, \\ 3.9p^{1/4}\log p & \text{otherwise.} \end{cases}$$

Theorem (ET)

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

Explicit estimates on the least k-th power non-residue

Let $p > 3$ be a prime. Let $g_k(p)$ be the least k-th power non-residue $\bmod p$.
Norton showed in the late 60's that

$$g_k(p) \leq \begin{cases} 4.7p^{1/4}\log p & \text{if } k = 2 \text{ and } p \equiv 3 \pmod 4, \\ 3.9p^{1/4}\log p & \text{otherwise.} \end{cases}$$

Theorem (ET)

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

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*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

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*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

A Corollary

Theorem (ET)

Let $g(p)$ *be the least quadratic nonresidue* mod p*. Let* p *be a prime greater than* 10^{4685}*, then* $g(p) < p^{1/6}$*.*

Other Applications of the Explicit Estimates

- 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 and Pomerance 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, $g^x \equiv x \pmod{p}$.

Other Applications of the Explicit Estimates

- 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 and Pomerance 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, $g^x \equiv x \pmod{p}$.

Other Applications of the Explicit Estimates

- 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 and Pomerance 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, $g^x \equiv x \pmod{p}$.

Vinogradov's Trick

Lemma

Let $x \geq 259$ be a real number, and let $y = x^{1/\sqrt{e}+\delta}$ for some $\delta > 0$. Let χ be a non-principal Dirichlet character mod *p for some prime p. If $\chi(n) = 1$ for all $n \leq y$, then*

$$\sum_{n \leq x} \chi(n) \geq x \left(2 \log \left(\delta \sqrt{e} + 1 \right) - \frac{4}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x} - \frac{2}{\log x} \right).$$

Proof.

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

where the sum ranges over q prime. Therefore we have

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

□

Proof of Main Corollary

Let $x \geq 259$ be a real number and let $y = x^{\frac{1}{\sqrt{e}}+\delta} = p^{1/6}$ for some $\delta > 0$. Assume that $\chi(n) = 1$ for all $n \leq y$. Now we have

$$2.71 x^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}} \geq x \left(2 \log\left(\delta\sqrt{e}+1\right) - \frac{4}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x} - \frac{2}{\log x} \right).$$

Now, letting $x = p^{\frac{1}{4}+\frac{1}{2r}}$ we get

$$2.71 p^{\frac{\log\log p}{r \log p} - \frac{1}{4r^2}} \geq 2 \log\left(\delta\sqrt{e}+1\right) - \frac{4}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x} - \frac{2}{\log x}. \quad (1)$$

Picking $r = 22$, one finds that $\delta = 0.00458\ldots$. For $p \geq 10^{4685}$, the right hand side of (1) is bigger than the left hand side.

Thank you!