LEAST NONQUADRATIC RESIDUE

BRANDON MULIADI

1. Introduction

A classic fact in elementary number theory is that all squares are congruent to 0 or 1 mod 4. This can be used to get a variety of cute results. For example, if a right triangle has integer sides, at least one of its legs has even length. If both legs had odd length, then the square of the hypotenuse would be 2 mod 4, which is impossible! Similar work can show that there are no squares 2 mod 3, and similar results exist for any modulus. For each n, the *quadratic nonresidues modulo n* are the numbers k such that there is no square congruent to k modulo n. A natural question, then, is to ask: What we can say about the smallest quadratic nonresidue?

2. Preliminaries

Definition 2.1. We say that a is a *quadratic residue modulo n* if there exists an integer b such that

$$b^2 \equiv a \pmod{n}.$$

Definition 2.2. We say that a is a *quadratic nonresidue* modulo n if a is not a quadratic residue modulo n.

We will focus on the case where n is prime, since if a is a quadratic nonresidue for any p dividing n, then a must be a quadratic nonresidue modulo n. For the rest of this paper, p will denote an odd prime number.

Definition 2.3. Let n_p be the least quadratic nonresidue modulo p.

Definition 2.4. Define the *Legendre symbol* function as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a \\ -1 & a \text{ is not a quadratic residue modulo } p \\ 0 & p \mid a \end{cases}$$

The Legendre symbol has a lot of nice properties, like multiplicativity. In fact, it is a Dirichlet character modulo p:

Definition 2.5. Let m be a positive integer. We say that $\chi : \mathbb{Z} \to \mathbb{C}$ is a *Dirichlet character modulo m* if, for all integers a and b:

(1) $\chi(a) = 0$ iff $\gcd(a, m) > 1$.
(2) $\chi(a + m) = \chi(a)$.
(3) $\chi(ab) = \chi(a)\chi(b)$.

It's clear that the Legendre symbol satisfies the first two properties. Showing that the Legendre symbol is multiplicative is more involved, and outside of the scope of this paper.

The simplest Dirichlet character is χ_0, defined as $\chi_0(a) = 0$ if $\gcd(a, m) = 1$ and $\chi(a) = 1$ otherwise. This is called the *principal* Dirichlet character, and any other Dirichlet character is called *nonprincipal*.

3. An Elementary Result

This proof is from [1]. We can get the following upper bound using only the multiplicativity of the Legendre symbol:

Proposition 3.1. *With notation as before, $n_p < \sqrt{p} + 1$.*

Proof. Suppose for the sake of contradiction that $n_p \geq \sqrt{p} + 1$. Let $k = \left\lceil \frac{p}{n_p} \right\rceil$. Since $n_p \geq \sqrt{p} + 1$, we have $k \leq \left\lceil \frac{p}{\sqrt{p}+1} \right\rceil < n_p$, thus k is a quadratic residue. Furthermore, since $p < kn_p < p + n_p$ and n_p is the smallest quadratic nonresidue, kn_p must be a quadratic residue. But by multiplicativity, kn_p must be a quadratic nonresidue, contradiction. ■

It will take a fair bit of work to get something better than this.

4. The Pólya–Vinogradov inequality

One way to bound the least quadratic nonresidue is to bound the character sum

$$\sum_{0<a\leq h} \chi(a).$$

What happens if we take χ to be Legendre symbol? The Legendre symbol takes on values -1 and 1, so if we know the sum is less than h, then at least one of the first h summands must have been -1, which means there was a quadratic nonresidue at most h. Now, let's see what bound we can get on the sum. The goal of this section will be to prove the following:

Theorem 4.1 (Pólya–Vinogradov)**.** *Let χ be a nonprincipal Dirichlet character modulo p, and h be any positive integer. Then*

$$\left| \sum_{0<a<h} \chi(a) \right| \leq \sqrt{p} \log p.$$

We'll need some new tools for this.

Definition 4.2. Let $e(x) = e^{2\pi x}$.

Definition 4.3. Let χ be a Dirichlet character modulo n. The *Gauss sum* of χ is

$$\tau(\chi) = \sum_{0<a<n} \chi(a) e(a/n).$$

Lemma 4.4. *If χ is a non-principal Dirichlet character modulo p, then*

$$|\tau(\chi)| = \sqrt{p}.$$

Proof. Equivalently, we show that $|\tau(\chi)|^2 = p$. We can write this as a product of two sums:

$$\begin{aligned}|\tau(\chi)|^2 &= \tau(\chi)\overline{\tau(\chi)}\\ &= \left(\sum_{0<a<p} \chi(a)e(a/n)\right)\left(\sum_{0<b<p} \chi(b^{-1})e(-b/n)\right)\end{aligned}$$

We split this into two sums based on whether $a = b$ or not.

$$= \sum_{0<a<p} 1 + \sum_{0<a<p} \sum_{\substack{0<b<p\\ b\neq a}} \chi(ab^{-1})e\left(\frac{a-b}{n}\right)$$

The first sum is clearly just $p-1$. As for the second, we sum over $c = ab^{-1}$:

$$= p - 1 + \left(\sum_{1<c<p} \chi(c)\right)\left(\sum_{0<b<p} e\left(\frac{b(c-1)}{n}\right)\right)$$

The sum $\sum_{1<c<p} \chi(c)$ would be 0 if it included $c = 1$. Since it doesn't, $\sum_{1<c<p} \chi(c) = -1$. Similarly, the sum $\sum_{0<b<p} e\left(\frac{b(c-1)}{n}\right)$ would be 0 if it included $b = 0$, since then we'd have the sum of the n-th roots of unity, which is 0. But the sum starts from $b = 1$, so $\sum_{0<b<p} e\left(\frac{b(c-1)}{n}\right) = -1$. We get

$$p - 1 + (-1)(-1) = p$$

as desired. ■

Lemma 4.5.

$$\frac{1}{p}\sum_{0\le a<p} e(ax/p)e(-an/p) = \begin{cases} 1 & \textit{if } x \equiv n \bmod p\\ 0 & \textit{otherwise}\end{cases}$$

Proof. If $x \equiv n \pmod p$, then the summand is 1 for every a, so the sum equals p. Otherwise, we're summing all the p-th roots of unity, and their sum is 0. ■

Now we're ready to prove the Pólya–Vinogradov inequality.

Theorem 4.6 (Pólya–Vinogradov)**.** *Let χ be a nonprincipal Dirichlet character modulo p, and h be any positive integer. Then*

$$\left|\sum_{0<a<h} \chi(a)\right| \le \sqrt{p}\log p.$$

Proof. Here is the approach of [1]. First, we use Lemma 4.5 to rewrite the sum.

$$\sum_{0<n<h} \chi(n) = \sum_{0<n<h} \sum_{0\le x<p} \chi(x)\left(\frac{1}{p}\sum_{0\le a<p} e(ax/p)e(-an/p)\right)$$

What we're doing is that, for each n, we add $\chi(x)$ iff $x \equiv n \pmod p$, which means we're just adding $\chi(n)$.

Now, we swap the sums.

$$\sum_{0<n<h}\sum_{0\leq x<p}\chi(x)\left(\frac{1}{p}\sum_{0\leq a<p}e(ax/p)e(-an/p)\right)=\frac{1}{p}\sum_{0\leq a<p}\sum_{0\leq x<p}\chi(x)e(ax/p)\sum_{0<n<h}e(-an/p)$$

The sum $\sum_{0\leq x<p}\chi(x)e(ax/p)$ is not too bad. If $a\neq 0$, then since $\chi(x)e(ax/p)=\chi(a^{-1})\chi(ax)e(ax/p)$, and ax runs over $\{1,2,\dots p-1\}$, then

$$\sum_{0\leq x<p}\chi(x)e(ax/p)=\sum_{0\leq x<p}\chi(a^{-1})\chi(ax)e(ax/p)=\chi(a^{-1})\tau(x).$$

Since $|\chi(a^{-1})|=1$ and $|\tau(x)|=\sqrt{p}$ by Lemma 4.4, we find

$$\left|\sum_{0\leq x<p}\chi(x)e(ax/p)\right|=\sqrt{p}$$

for $a\leq 0$. On the other hand, if $a=0$, then we just have

$$\sum_{0\leq x<p}\chi(x)=0.$$

We conclude

$$\left|\sum_{0\leq x<p}\chi(x)e(ax/p)\right|\leq\sqrt{p}. \tag{4.1}$$

The other sum, $\sum_{0<n<h}e(-an/p)$, is just the sum of a geometric sequence, so applying the formula for the sum of a geometric sequence, we have

$$\left|\sum_{0<n<h}e(-an/p)\right|=\left|\frac{e(-ah/p)-e(-a/p)}{1-e(-a/p)}\right|\leq\frac{2}{|1-e(-a/p)|}. \tag{4.2}$$

Applying both (4.1) and (4.2), we have

$$\begin{aligned}\left|\sum_{0<n<h}\chi(n)\right|&\leq\frac{1}{p}\sum_{0<a<p}\sqrt{p}\left(\frac{2}{|1-e(-a/p)|}\right)\\&=\frac{2}{\sqrt{p}}\sum_{0<a<p}\frac{1}{|1-e(-a/p)|}\end{aligned}$$

Note that $e(-a/p)=\overline{e(-(p-a)/p)}$, so $|1-e(-a/p)|=|\overline{1-e(-(p-a)/p)}|=|1-e(-(p-a)/p)|$. Thus we have

$$\left|\sum_{0<n<h}\chi(n)\right|\leq\frac{4}{\sqrt{p}}\sum_{0<a\leq(p-1)/2}\frac{1}{|1-e(-a/p)|}.$$

Now, we use the inequality $|1-e(x)|\geq 4x$ for $x\in[0,1/2]$ to get

$$\frac{1}{|1-e(-a/p)|}\leq\frac{p}{4a}.$$

Substituting this in gives

$$\sum_{0<n<h} \chi(n) \leq \sqrt{p} \sum_{0<a\leq(p-1)/2} \frac{1}{a}.$$

To finish, we show $\sum_{0<a\leq(p-1)/2} \frac{1}{a} < \log p$. We have

$$\sum_{n=1}^{m} \frac{1}{n} < \log m + \gamma$$

where γ is the Euler-Mascheroni constant. It follows that

$$\sum_{a=1}^{(p-1)/2} \frac{1}{n} < \log(p-1) - \log 2 + \gamma \leq \log p$$

as desired. ■

Now, let's extract an upper bound on the least quadratic nonresidue. Taking $\chi(a) = \left(\frac{a}{p}\right)$ and $h = \lceil\sqrt{p}\log p\rceil + 1$ in the Pólya–Vinogradov inequality, we have

$$\left|\sum_{a=1}^{\lceil\sqrt{p}\log p\rceil} \left(\frac{a}{p}\right)\right| \leq \sqrt{p}\log p.$$

We see that at least one of $\chi(1), \chi(2), \ldots \chi(\lceil\sqrt{p}\log p\rceil)$ must be -1, because each is -1 or 1 and if they're all 1 then the LHS would be $\lceil\sqrt{p}\log p\rceil > \sqrt{p}\log p$, a contradiction. Thus we conclude $n_p < \sqrt{p}\log p + 1$.

We still haven't beaten the bound obtained with elementary methods, but we've added a useful tool to our belt. Onward!

5. Vinogradov's Trick

Theorem 5.1 (Vinogradov's Trick). *For any $\varepsilon > 0$, for sufficiently large p we have*

$$n_p \leq p^{\frac{1}{2\sqrt{e}}+\varepsilon}.$$

How do we do this? Well, we've already done most of the work by proving the Pólya–Vinogradov inequality. We just need to make a more sophisticated argument to extract a bound, using the multiplicativity of χ to our advantage. Before, we used the fact that every $n \leq n_p$ satisfies $\left(\frac{n}{p}\right) = 1$, so if n_p is too large then the Pólya–Vinogradov inequality would be contradicted. But we can do better, since really every n is that $(n_p - 1)$-smooth - that is, every prime dividing n is less than n_p - satisfies $\left(\frac{n}{p}\right) = 1$.

Proof. The only n that could possibly satisfy $\left(\frac{n}{p}\right) = -1$ are the n divisible by a prime $q > n_p$, so we write

$$\begin{aligned}\sum_{0<n\leq x} \chi(n) &\geq \sum_{0<n\leq x} 1 - \sum_{n_p\leq q\leq x} \sum_{\substack{0<n\leq x\\ q|n}} 2 \\ &= \lfloor x \rfloor - 2\sum_{n_p\leq q\leq x} \left\lfloor \frac{x}{q} \right\rfloor .\end{aligned}$$

Now, let's break out some asymptotic notation. We have

$$\lfloor x \rfloor = x + O(1) = x + o(x)$$

and

$$\sum_{n_p\leq q\leq h} \left\lfloor \frac{x}{q} \right\rfloor = \sum_{n_p\leq q\leq x} \left(\frac{x}{q} + O(1) \right) = x \sum_{n_p\leq q\leq x} \frac{1}{q} + O\left(\frac{x}{\log x} \right) = x \sum_{n_p\leq q\leq x} \frac{1}{q} + o(x)$$

where we used the Prime Number Theorem on the sum $\sum_{n_p\leq p\leq x} O(1)$. So we have

$$\sum_{0<a\leq x} \chi(a) \geq x - 2x \sum_{n_p<q\leq x} \frac{1}{q} + o(x).$$

Now, we apply the asymptotic $\sum_{n\leq x} \frac{1}{n} = \log\log x + C + o(1)$, which gives us

$$\sum_{0<a\leq x} \chi(a) \geq x - 2x \log\left(\frac{\log x}{\log n_p} \right) + o(x) = x \left[1 - 2\log\left(\frac{\log x}{\log n_p} \right) + o(1) \right].$$

If we take x to be some function of p such that $\sqrt{p}\log p = o(x)$, then the term in brackets has to go to 0 as p grows large, otherwise the LHS grows as fast as x up to a constant factor, which means it will exceed $\sqrt{p}\log p$, contradicting the Pólya–Vinogradov inequality. So n_p cannot be too large - more specifically, for any $\varepsilon > 0$, $n_p \geq x^{\frac{1}{\sqrt{e}}+\varepsilon}$ cannot hold for arbitrarily large p, otherwise

$$1 - 2\log\left(\frac{\log x}{\log n_p} \right) \geq 1 + 2\log\left(\frac{1}{\sqrt{e}} + \varepsilon \right) = 2\left(\log\left(\frac{1}{\sqrt{e}} + \varepsilon \right) - \log\left(\frac{1}{\sqrt{e}} \right) \right) > 0$$

thus $1-2\log\left(\frac{\log x}{\log n_p}\right)+o(1)$ is bounded above by some positive constant K for sufficiently large p. But it cannot be true that $\sum_{0<n\leq x} \chi(n) \geq Kx$ for arbitrarily large p, since $\sqrt{p}\log p = o(x)$ and $\sum_{0<n\leq x} \chi(n) \leq \sqrt{p}\log p$, so we have a contradiction to the Pólya–Vinogradov inequality. Thus, it must be the case that for every $\varepsilon > 0$, $n_p \leq x^{\frac{1}{\sqrt{e}}+\varepsilon}$ for large enough p. To finish, take $x = \sqrt{p}(\log p)^2$, which satisfies $\sqrt{p}\log p = o(x)$ as required. Then

$$n_p \leq x^{\frac{1}{\sqrt{e}}+\frac{\varepsilon}{2}} \leq p^{\frac{1}{2\sqrt{e}}+\varepsilon}$$

for sufficiently large p. ■

6. Improvements

The bound $n_p \leq p^{\frac{1}{2\sqrt{e}}+\varepsilon}$ is not the best one can do. There is in fact a stronger inequality than the Pólya–Vinogradov inequality [2]:

Theorem 6.1 (Burgess inequality)**.** *Let χ be a nonprincipal Dirichlet character modulo p, and r be any positive integer. Then*

$$\left|\sum_{0<n\leq N} \chi(n)\right| \leq CN^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}+\varepsilon}(\log p)^{1/r}$$

for some constant C only depending on ε and r.

Using Vinogradov's trick gives [1]:

$$n_p \leq p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

This is the best known unconditional bound.

References

[1] Kevin McGown and Enrique Trevino. "The least quadratic non-residue". In: *Preprint, July* 18 (2019).

[2] Enrique Treviño. "The Burgess inequality and the least kth power non-residue". In: *International Journal of Number Theory* 11.05 (2015), pp. 1653–1678.