Research Statement

Enrique Treviño

My research interests lie in elementary analytic number theory. Most of my work concerns finding explicit estimates for character sums. While these estimates are interesting in their own right, they also are very useful to answer some questions from elementary number theory. For example, I have used these estimates to bound the least quadratic nonresidue $\bmod p$ and to bound the least inert prime in a real quadratic field.

Let χ be a character mod q and let N, M be integers. Consider

$$S_\chi(N,M) = \sum_{M<n\leq N+M} \chi(n).$$

The first important upper bound on $S_\chi(N,M)$ came in 1918 in what we now call the Pólya–Vinogradov inequality (proven independently). The inequality states that there is a universal constant c such that $|S_\chi(N,M)| \leq c\sqrt{q}\log q$ for χ a non-principal Dirichlet character $\bmod q$. Note that, surprisingly, the upper bound does not depend on N, it only depends on the modulus of the character. It is useful to note that $|\chi(n)| = 1$ or $\chi(n) = 0$ whenever χ is a Dirichlet character. From this it is trivial to see that $|S_\chi(N,M)| \leq N$. Now if N is small compared to q then the Pólya–Vinogradov inequality is not a good improvement on the trivial bound.

Mathematicians have worked out upper bounds for c, for example Pomerance proved the following in [18]:

Theorem 1. *For χ a primitive character to the modulus $q > 1$, we have*

$$|S_\chi(N,M)| \leq \begin{cases} \frac{2}{\pi^2}\sqrt{q}\log q + \frac{4}{\pi^2}\sqrt{q}\log\log q + \frac{3}{2}\sqrt{q} & , \quad \chi(-1) = 1, \\ \frac{1}{2\pi}\sqrt{q}\log q + \frac{1}{\pi}\sqrt{q}\log\log q + \sqrt{q} & , \quad \chi(-1) = -1. \end{cases}$$

An application of the Pólya–Vinogradov inequality is to put an upper bound on the least quadratic non-residue mod p a prime. The reason we can do this, is that the function that gives 1 if it is a quadratic residue, -1 if it is not a quadratic residue and 0 if the number is not coprime to the modulus is a Dirichlet character (this function is written $\left(\frac{\cdot}{p}\right)$ and it is called the Legendre symbol). If we show that the sum of this character is small compared to the number of things we summed, it means that χ must have been -1 at some point, giving us a quadratic non-residue. Using the Pólya–Vinogradov inequality and a bit of sieving we can get that the least quadratic non-residue is bounded by $q^{\frac{1}{2\sqrt{e}}+\epsilon}$ for any real $\epsilon > 0$. We conjecture that the least quadratic non-residue is much smaller than that, in fact, Bach [2] proved that under the Generalized Riemann Hypothesis (GRH), the least quadratic non-residue is $\leq 2(\log q)^2$ (this was recently improved on by Li, Lamzouri and Soundararajan in [7] to $\leq \log q^2$).

That the Pólya–Vinogradov inequality is sharp follows from the existence of M and N such that $S_\chi(N,M) \gg \sqrt{q}$. In a sense, the inequality is only "off" by $\log q$. In this direction, we have other nice results. Paley [17] showed that there exists an absolute constant c such that there exist infinitely many quadratic characters $\chi \pmod q$ such that for some integers N_q and M_q (depending on q), $S_\chi(N_q, M_q) \geq c\sqrt{q}\log\log q$. Montgomery and Vaughan [13] proved that under GRH $S_\chi(N,M) \ll \sqrt{q}\log\log q$, hence making the Paley result best possible (up to a constant). This analysis works for quadratic characters, but what about characters of odd order? Work of Granville and Soundararajan [5] led to the following theorem of Goldmakher [3]:

Theorem 2. *For each fixed odd number $g > 1$, for $\chi \pmod q$ of order g,*

$$S_\chi(N,M) \ll_g \sqrt{q}(\log q)^{\Delta_g + o(1)}, \quad \Delta_g = \frac{g}{\pi}\sin\frac{\pi}{g}, \quad q \to \infty.$$

Moreover, under GRH

$$S_\chi(N,M) \ll_g \sqrt{q}(\log\log q)^{\Delta_g + o(1)}.$$

Furthermore, there exists an infinite family of characters $\chi \pmod q$ of order g and integers N_q, M_q satisfying

$$S_\chi(N_q, M_q) \gg_{\epsilon,g} \sqrt{q}(\log\log q)^{\Delta_g - \epsilon}.$$

Recently, in [8], Levin, Pomerance and Soundararajan considered a "smoothed" version of the Pólya-Vinogradov inequality. Instead of considering the sum of character values, they consider the sum of weighted character values

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

The theorem they proved is the following:

Theorem 3. *Let χ be a primitive Dirichlet character to the modulus $q > 1$ and let M, N be real numbers with $0 < N \leq q$. Then*

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

The remarkable thing about this inequality is that it is very tight. As a lower bound, in [1], I proved:

Theorem 4. *Let χ be a primitive Dirichlet character to the modulus $q > 1$. Then, there exist integers M and N such that*

$$\left|S^*_\chi(M,N)\right| > \frac{2}{\pi^2}\sqrt{q}.$$

This theorem shows us that the smoothed Pólya–Vinogradov inequality is best possible up to a constant.

The smoothed Pólya–Vinogradov inequality was used by Levin, Pomerance and Soundararajan to settle a conjecture of Brizolis regarding fixed points of discrete logarithms. I used the smoothed Pólya–Vinogradov inequality to make an improvement on a theorem of Granville, Mollin and Williams. In [4], they proved that the least inert prime of a real quadratic field with discriminant $D > 3705$ is smaller than $\sqrt{D}/2$. In [19], I improved this to:

Theorem 5. *The least inert prime of a real quadratic field with discriminant $D > 1596$ is smaller than $D^{0.45}$*

The proof of the theorem consists of three parts, when D is small ($D \leq 2.6 \times 10^{17}$ for D odd and $D \leq 1.04 \times 10^{18}$ for D even), when D is huge ($D \geq 10^{24}$) and when D is neither small nor huge. To check D small, a special computer called the Manitoba Scalable Sieving Unit (MSSU, see [9]) was used. It ran for about 5 months. Recent developments in sieving machines (see [23]) suggests that a sieving machine could check up to about 10^{24}, which would allow us to improve the upper bound in the theorem to $D^{3/7}$ or better instead of $D^{0.45}$. One of the difficulties in the problem is the fact that D need not be prime. When D is prime we can get much stronger results, indeed, Norton [14] showed that the least inert prime is at most $4.7p^{1/4}\log p$. In [22], I improved Norton's estimate to $1.1p^{1/4}\log p$. To be able to prove this, strong explicit estimates of the Burgess inequality were needed.

The Burgess inequality is the best estimate we have for character sums, the theorem is the following:

Theorem 6 (D. Burgess)**.** *Let χ be a primitive character* mod q*, where $q > 1$, r is a positive integer and $\epsilon > 0$ is a real number. Then*

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

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

Note that Pólya–Vinogradov works for any non-principal character while Burgess works for primitive characters and the modulus must be cubefree. Norton [16] has extended it to all moduli by adding an extra term that depends on the number of prime powers in the factorization of q. I'd like to point out that using Burgess instead of Pólya–Vinogradov allows us to get that the least quadratic non-residue mod p is bounded above by $p^{\frac{1}{4\sqrt{e}}+\epsilon}$ for large enough p.

As mentioned earlier, to be able to use the inequality in applications, we need to work out an explicit version of the Burgess inequality. In their analytic number theory book [6], Iwaniec and Kowalski give a sketch of a proof for the following explicit estimate (they credit Friedlander and Iwaniec for this argument):

Theorem 7. *Let χ be a primitive character* mod p*, where p is a large enough prime. Let r be a positive integer, and let M and N be non-negative reals with $N \geq 1$. Then*

$$|S_\chi(M, N)| = \left| \sum_{M < n \leq M+N} \chi(n) \right| \leq 30 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Iwaniec and Kowalski were not looking for the best possible constant. In [21], with an eye towards getting the best possible constant, I improved this to

Theorem 8. *Let p be a prime such that $p \geq 10^7$. Let χ be a non-principal Dirichlet character* mod p*. Let r be a positive integer, and let M and N be non-negative reals with $N \geq 1$. Then*

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

A nice corollary (proved in [21]) that follows from this theorem is

Theorem 9. *Let $p > 10^{4732}$, then the least quadratic non-residue modulo p is less than or equal to $p^{1/6}$.*

To prove Theorem 8 I used the following inequality (which I proved in [22]):

Theorem 10. *Let p be a prime. Let w, h and k be integers such that $w \leq 9h$, $h \leq p$, $k \geq 2$ and $k \mid p-1$. Let χ be a character $\pmod p$ of order k. Then*

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

The inequality also allowed me to improve results on explicit estimates for the least k-th power non-residue (see [22]). The inequality has other uses, for example one could use it to have good explicit bounds on the second least k-th power non-residue and to bound H, the largest integer such that there exists an integer N such that $\chi(N+1) = \chi(N+2) = \ldots = \chi(N+H)$. In [11], McGown proved that $H < 7.06p^{1/4}\log p$ whenever $p > 5 \cdot 10^{18}$ and $H < 7p^{1/4}\log p$ when $p > 5 \cdot 10^{55}$. Norton claimed stronger results without proof (see [15]). In [20] I was able to improve both McGown's results and Norton's claims by showing that $H < 3.64p^{1/4}\log p$ for all odd p and $H < 1.55p^{1/4}\log p$ whenever $p > 2.5 \cdot 10^9$.

Recently, I started working on the problem of bounding the least primitive root modulo p. Working with Kevin McGown and Timothy Trudgian, assuming GRH, we settled a conjecture by Grosswald that states that for $p > 409$, the least primitive root modulo p is smaller than $\sqrt{p} - 2$. The main result in our paper ([12]) is the following explicit estimate:

Theorem 11. *Assume GRH and $p \geq 10^9$. The least prime primitive root $\hat{g}(p)$ satisfies*

$$\hat{g}(p) \leq \left(\frac{8}{5}(2^{\omega(p-1)-1} - 1)\log(p) \right)^2.$$

I'm currently working (or planning to work) on the following projects:

- Together with Kevin McGown, we're working on explicit bounds for Siegel zeros.
- Together with Kevin McGown and Timothy Trudgian, we're working on improving our bounds for least primitive roots assuming GRH.
- Together with Kevin McGown and Timothy Trudgian, we're working on improving our bounds for least primitive roots unconditionally.
- Together with Kevin McGown we're planning on trying to classify Norm-Euclidean cubic cyclic fields. Mcgown has classified them assuming GRH in [10].

References

[1] K. Adamczewski and E. Treviño. The smoothed Pólya-Vinogradov inequality. *Integers*, 15:Paper No. A20, 11, 2015.

[2] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[3] L. I. Goldmakher. *Multiplicative mimicry and improvements of the Pólya–Vinogradov inequality.* ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–University of Michigan.

[4] A. Granville, R. A. Mollin, and H. C. Williams. An upper bound on the least inert prime in a real quadratic field. *Canad. J. Math.*, 52(2):369–380, 2000.

[5] A. Granville and K. Soundararajan. Large character sums: pretentious characters and the Pólya-Vinogradov theorem. *J. Amer. Math. Soc.*, 20(2):357–384 (electronic), 2007.

[6] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 2004.

[7] Y. Lamzouri, X. Li, and K. Soundararajan. Conditional bounds for the least quadratic non-residue and related problems. *Math. Comp.*, 84(295):2391–2412, 2015.

[8] M. Levin, C. Pomerance, and K. Soundararajan. Fixed points for discrete logarithms. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 6–15. 2010.

[9] R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Math. Comp.*, 65(213):361–372, S25–S27, 1996.

[10] K. J. McGown. Norm-Euclidean Galois fields and the generalized Riemann hypothesis. *J. Théor. Nombres Bordeaux*, 24(2):425–445, 2012.

[11] K. J. McGown. On the constant in Burgess' bound for the number of consecutive residues or non-residues. *Funct. Approx. Comment. Math.*, 46(part 2):273–284, 2012.

[12] K. J. McGown, E. Treviño, and T. Trudgian. Resolving Grosswald's conjecture on GRH. To appear in *Funct. Approx. Comment. Math.*

[13] H. L. Montgomery and R. C. Vaughan. Exponential sums with multiplicative coefficients. *Invent. Math.*, 43(1):69–82, 1977.

[14] K. K. Norton. *Numbers with small prime factors, and the least kth power non-residue.* Memoirs of the American Mathematical Society, No. 106. American Mathematical Society, Providence, R.I., 1971.

[15] K. K. Norton. Bounds for sequences of consecutive power residues. I. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 213–220. Amer. Math. Soc., Providence, R.I., 1973.

[16] K. K. Norton. A character-sum estimate and applications. *Acta Arith.*, 85(1):51–78, 1998.

[17] R. Paley. A theorem on characters. *J. Lond. Math. Soc.*, 7:28–32, 1932.

[18] C. Pomerance. Remarks on the Pólya–Vinogradov inequality. *Proceedings of the Integers Conference*, October 2009, to appear.

[19] E. Treviño. The least inert prime in a real quadratic field. In preparation.

[20] E. Treviño. On the maximum number of consecutive integers on which a character is constant. *Mosc. J. Comb. Number Theory*, 2(1):56–72, 2012.

[21] E. Treviño. The Burgess inequality and the least kth power non-residue. *Int. J. Number Theory*, 11(5):1653–1678, 2015.

[22] E. Treviño. The least k-th power non-residue. *J. Number Theory*, 149:201–224, 2015.

[23] K. Wooding. *The sieve problem in one- and two-dimensions.* 2010. Thesis (Ph.D.)–University of Calgary.