Illinois Number Theory Conference in honor of Harold Diamond at 70

The Pólya–Vinogradov inequality

Carl Pomerance, Dartmouth College

Johann Peter Gustav Lejeune Dirichlet, quite the character ...

What is a (Dirichlet) character?

It is a totally multiplicative function $\chi : \mathbb{Z} \to \mathbb{C}$ that is periodic, such that if the least period is q, then $\chi(m) = 0$ if and only if $(m, q) > 1$.

Thus, by Euler's theorem, if $(m, q) = 1$, then $\chi(m)$ is a $\varphi(q)$-th root of 1.

Some examples:

The characteristic function of the integers coprime to q is a character, called the *principal* character mod q. Usually, we denote it χ_0 with the modulus implied by context.

If q is an odd number, then $\chi(m) = \left(\frac{m}{q}\right)$, the Jacobi symbol, is a character mod q.

If q is an odd prime with primitive root r and ζ is a $(q-1)$-st root of 1 in $\mathbb{C}$, then $\chi(r^j) = \zeta^j$, $\chi(0) = 0$, is a character mod q.

The product of two characters mod q is also a character mod q (the product is as a product of two functions). In fact, the characters mod q form a group under multiplication, with identity χ_0. This group is isomorphic to the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$.

The product of a character mod q_1 and a character mod q_2 is a character with modulus $\text{lcm}[q_1, q_2]$. If a character with minimum modulus can be factored into two characters, one of smaller modulus and the other being principal, then the character is *imprimitive*. Otherwise it is *primitive*.

Every non-principal character to a prime modulus is primitive.

Characters can be used to create characteristic functions.

Example 0: χ_0 is a characteristic function.

Example 1: If $(a, q) = 1$ and $ab \equiv 1 \pmod{q}$, then

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(mb)$$

is 1 if $m \equiv a \pmod{q}$ and is 0 otherwise.

Example 2: If q is prime and $m \mid q-1$, then

$$\frac{1}{m} \sum_{\substack{\chi \bmod q \\ \chi^m = \chi_0}} \chi(a)$$

is 1 if a is an m-th power mod q and is 0 otherwise.

Example 3: If q is prime, then

$$\prod_{p \mid q-1} \left(1 - \frac{1}{p} \sum_{\substack{\chi \bmod q \\ \chi^p = \chi_0}} \chi(a) \right) = \sum_{d \mid q-1} \frac{\mu(d)}{d} \sum_{\substack{\chi \bmod q \\ \chi^d = \chi_0}} \chi(a)$$

is 1 if a is a primitive root mod q and is 0 otherwise.

George Pólya

I. M. vinogradov

Let $S(\chi) = \max_{M,N} \left| \sum_{M \le a \le M+N} \chi(a) \right|$.

The Pólya–Vinogradov inequality (1918):
There is an absolute positive constant c such that for χ mod q non-principal,

$$S(\chi) \le c\sqrt{q} \log q.$$

Corollary: *For q odd, not a square, there is some $a \le q^{1/2+\epsilon}$ with $\left(\frac{a}{q}\right) = -1$ (for each fixed $\epsilon > 0$ and q sufficiently large depending on ϵ).*

How good is it?

It's easy to show via an averaging argument that for χ primitive,

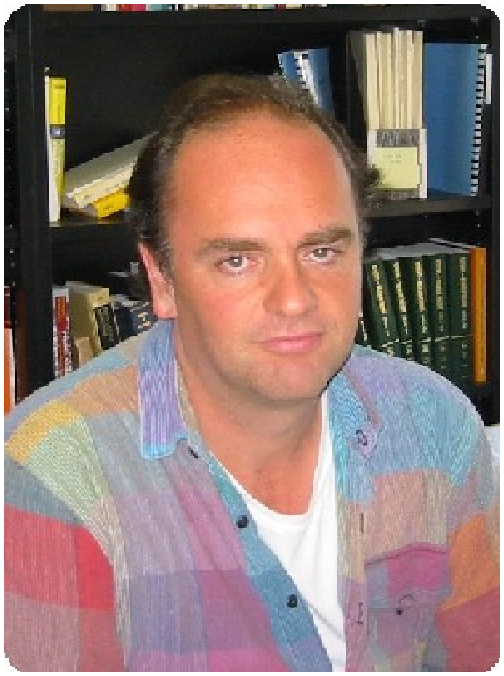
$$S(\chi) \geq \frac{1}{\pi}\sqrt{q}.$$

So, apart from the "$\log q$" factor, the Pólya–Vinogradov inequality is best possible.

Assuming the GRH: $S(\chi) \ll \sqrt{q} \log\log q$.

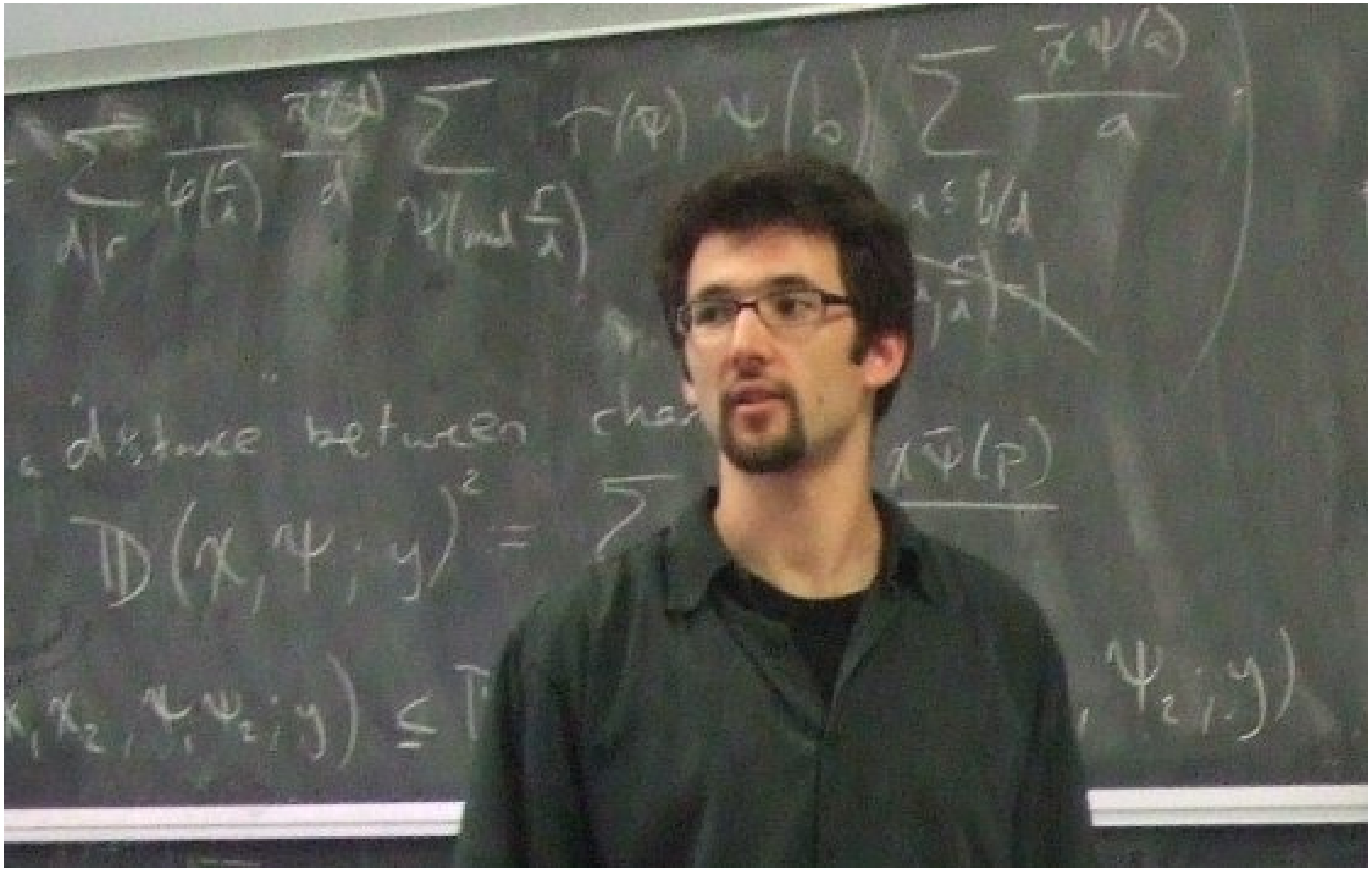
Paley (1932): *For infinitely many quadratic characters,* $S(\chi) \gg \sqrt{q} \log\log q$.

Granville, Soundararajan (2007), Goldmakher (2009): *For χ primitive of odd order h, $S(\chi) \ll_h \sqrt{q}(\log q)^{(h/\pi)\sin(\pi/h)+o(1)}$, as $q \to \infty$.*



Andrew Granville

K. Soundararajan



Leo Goldmakher

Back to $S(\chi) \leq c\sqrt{q}\log q$:

What's "c"? Various proofs of the Pólya–Vinogradov inequality are effective in principle, and for the simpler proofs, it is not hard to actually put some numbers behind the argument.

For example, the argument in Davenport (due to Schur) can rather easily be used to show that

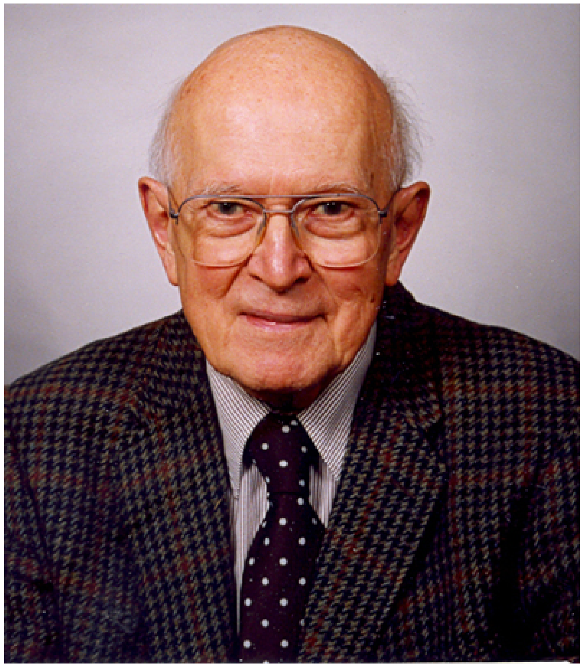
$$S(\chi) \leq \frac{2}{\pi}\sqrt{q}\log q + 0.16\sqrt{q}.$$

There are some papers dealing with a numerically explicit version of the Pólya–Vinogradov inequality:

Qiu (1991): $S(\chi) \le \dfrac{4}{\pi^2}\sqrt{q}\log q + 0.5\sqrt{q}$.

Bachman, Rachakonda (2001): $S(\chi) \le \dfrac{1}{3\log 3}\sqrt{q}\log q + 6.5\sqrt{q}$.

Pomerance (2010): $S(\chi) \le \dfrac{2}{\pi^2}\sqrt{q}(\log q + 2\log\log q) + 1.5\sqrt{q}$
and if χ is odd, "$2/\pi^2$" changes to $1/(2\pi)$ and "1.5" to 1.



Edmund Landau

Paul T. Bateman

My proof borrows heavily from Landau and Bateman.

Hildebrand (1988) has a result with a small leading coefficient, but with an inexplicit secondary term. His proof is based on an approach of Landau (1918), an unpublished improvement of Bateman, and work of Montgomery, Vaughan.

It seems difficult to make the Montgomery, Vaughan ideas numerically explicit, but the earlier stuff was very doable.

And I did it.

A. J. Hildebrand

A “smoothed” Pólya–Vinogradov inequality:

Let $S_N(\chi) = \max_M \left| \sum_{M \le a \le M+2N} \chi(a) \left(1 - \left| \frac{a-M}{N} - 1 \right| \right) \right|$.

Say what?

The ugly-looking factor with $\chi(a)$ is merely a “tent” that rises linearly from $a = M$, where it is 0, to $a = M + N$, where it is 1, and then falls back to 0 at $a = M + 2N$.

So, the formula for it is a bit off-putting, but it is just a simple “tent”.

Levin, Pomerance, Soundararajan (2010): *For χ primitive and $N \le q$, we have $S_N(\chi) \le \sqrt{q} - \frac{N}{\sqrt{q}}$.*

Mariana Levin

The result is nearly best possible.

Treviño (2010): *For* χ *primitive*, $\max_{N \le q} S_N(\chi) \ge \frac{2}{\pi^2}\sqrt{q}$.

Actually, he has a slightly larger constant here, but he favors this one, which has a neat proof. For the value of N that he uses, which is near $q/2$, the upper bound in the LPS theorem is a bit more than twice the Treviño lower bound.

Does the GRH have anything to say here? What if χ has odd order? Are there special quadratic characters?

Enrique Treviño

The proof of the smoothed version of Pólya–Vinogradov is based on Poisson summation and Gauss sums, and is almost immediate.

Let $H(t) = \max\{0, 1 - |t|\}$. We wish to estimate

$$S = \sum_{a \in \mathbb{Z}} \chi(a) H\left(\frac{a - M}{N} - 1\right).$$

Use the Gauss-sum trick, so that

$$S = \frac{1}{\tau(\bar{\chi})} \sum_{j=1}^{q-1} \bar{\chi}(j) \sum_{a \in \mathbb{Z}} e(aj/q) H\left(\frac{a - M}{N} - 1\right).$$

If one then applies Poisson summation to the inner sum and then estimates trivially through the triangle inequality, one gets (since the Fourier transform $\widehat{H}$ is nonnegative)

$$|S| \leq \frac{N}{\sqrt{q}} \sum_{k \in \mathbb{Z} \setminus q\mathbb{Z}} \widehat{H}\left(\frac{kN}{q}\right).$$

Via another call to Poisson summation, this last quantity is at most $\sqrt{q} - N/\sqrt{q}$.

An application: The following problem of Brizolis has been mentioned in Guy, *Unsolved problems in number theory*. For a prime $p > 3$ must there be a primitive root g and an integer x in $[1, p-1]$ with $g^x \equiv x \pmod{p}$?

Lemma. *Yes, if there is a primitive root x in $[1, p-1]$ that is coprime to $p-1$.*

Proof. If such x exists, say $xy \equiv 1 \pmod{p-1}$ and let $g = x^y$. Then g is a primitive root for p and $g^x = x^{xy} \equiv x \pmod{p}$. $\square$

Setting things up with characters: Let $N(p)$ be the number of primitive roots for p in $[1, p-1]$ that are coprime to $p-1$. Then

$$
\begin{aligned}
N(p) &= \sum_{(g,p-1)=1} \sum_{d|p-1} \frac{\mu(d)}{d} \sum_{\chi^d=\chi_0} \chi(g) \\
&= \frac{\varphi(p-1)}{p-1} \sum_{(g,p-1)=1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \text{ of order } d} \chi(g) \\
&= \frac{\varphi(p-1)}{p-1} \sum_{d,j|p-1} \frac{\mu(d)\mu(j)}{\varphi(d)} \sum_{\chi \text{ of order } d} \sum_{h=1}^{(p-1)/j} \chi(jh).
\end{aligned}
$$

The contribution from $d = 1$, that is, $\chi = \chi_0$, is $\dfrac{\phi(p-1)^2}{p-1}$.

The Pólya–Vinogradov inequality shows that all of the $d > 1$ terms together have absolute value at most $c\dfrac{\varphi(p-1)}{p-1}4^{\omega(p-1)}\sqrt{p}\log p$.

Thus, $N(p) > 0$ for all sufficiently large p. In fact ...

Zhang (1995), Cobeli, Zaharescu (1999):
$N(p) = \dfrac{\varphi(p-1)^2}{p-1} + O(p^{1/2+\epsilon})$.

Cobeli, Zaharescu: $N(p) > 0$ for $p > 10^{2080}$ (and probably can be improved to 10^{50}).

Levin, Pomerance, Soundararajan (2010): $N(p) > 0$ *for all primes* $p > 3$.

Using just our smoothed Pólya–Vinogradov inequality gets us $N(p) > 0$ for $p > 10^{25}$. To bring the story down to a computable level, we let uv be the largest squarefree divisor of $p-1$, with u having the "small" primes and v the "large" primes. Using our inequality we then proved that $N(p) > 0$ if $s < 1/2$, where s is the reciprocal sum of the primes in v, and

$$\sqrt{p} > \frac{4^{\omega(u)}}{\varphi(u)} \cdot \frac{1 + 2\omega(v)}{1 - 2s}.$$

Using this criterion with v the product of the largest 6 primes in $p-1$, we handled all the cases with $\omega(p-1) \geq 10$. In the remaining cases we handled every p with $p > 1.25 \times 10^9$. We then checked each prime to this level. QED

Happy Birthday Harold!