ANTS IX, Nancy, France

Fixed points for discrete logarithms

Carl Pomerance, Dartmouth College

Suppose that G is a group and $g \in G$ has finite order m. Then for each $t \in \langle g \rangle$ the integers n with $g^n = t$ form a residue class mod m. Denote it by

$$\log_g t.$$

The discrete logarithm problem is the computational task of finding a representative of this residue class; that is, finding an integer n with $g^n = t$.

Finding a discrete logarithm can be *very* easy. For example, say $G = \mathbb{Z}/m\mathbb{Z}$ and $g = 1$. More specifically, say $m = 100$ and $t = 17$. We are asking for the number of 1's to add in order to get 17. Hmmm.

Lets make it harder: take g as some other generator of $\mathbb{Z}/m\mathbb{Z}$. But then computing $\log_g t$ is really solving the congruence

$$ng \equiv t \bmod m$$

for n, which we've known how to do easily essentially since Euclid.

The cyclic group of order m:

What does this title mean, especially the key word "The"?

Take $G_1 = \mathbb{Z}/100\mathbb{Z}$ and $G_2 = (\mathbb{Z}/101\mathbb{Z})^\times$. Both are cyclic groups of order 100. Both are generated by 3. And 17 is in both groups.

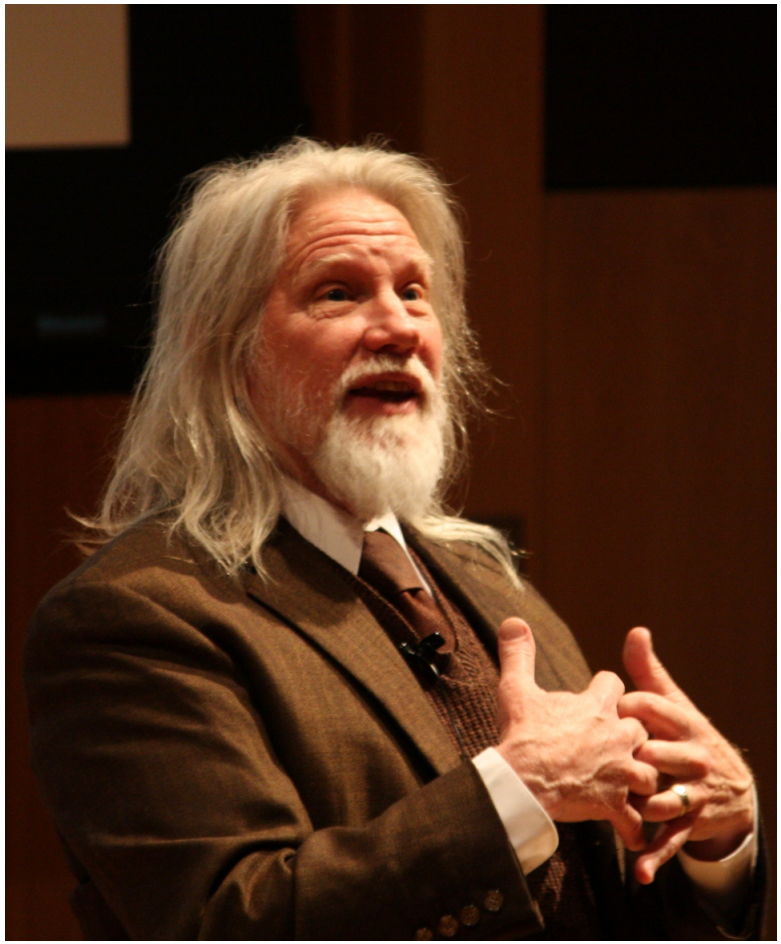
So, there are two versions of computing $\log_3 17$, one in G_1 and one in G_2.

In G_1, we are solving $3n \equiv 17 \bmod 100$. The inverse of 3 is 67, so $n \equiv 17 \cdot 67 \equiv 39 \bmod 100$.

In G_2, we are solving $3^n \equiv 17 \bmod 101$. And this seems much harder.

The moral: when someone talks about *the* cyclic group of a given order, they are not concerned with computational issues.

The algorithmic question of computing discrete logarithms is venerable and also important. Why important?



Whitfield Diffie

Martin Hellman

The Diffie–Hellman key-exchange protocol:

Say we have a cyclic group generated by g, which everyone knows. Alice has a secret integer a and "publishes" g^a. Similarly, Bob has a secret integer b and publishes g^b.

Alice and Bob want to set up a secure session with a secret key that only they know, yet they want to set this up over a public line. Here's how they do it: Alice takes Bob's group element g^b and raises it to her secret exponent a, getting $(g^b)^a = g^{ab}$. Bob arrives at the same group element via a different method, namely $(g^a)^b = g^{ab}$.

Eve (an eavesdropper) knows something's afoot and knows g^a and g^b, but apparently cannot easily compute g^{ab} without finding either a or b, that is without solving the dl problem.

So, a group that is well-suited for cryptographic purposes is one where

- it is easy to apply the group operation;
- it is difficult (in practice) to solve the discrete logarithm problem.

However, our topic in this talk is not crypto, nor dl algorithms, but fixed points, the equation

$$\log_g x = x.$$

First note that the equation $\log_g x = x$ doesn't make complete sense, since the first "x" is an element of the cyclic group $\langle g \rangle$ and the second x is an integer (or residue class modulo the order of g).

We can make sense by the conflation of integers with residue classes, as we have already been doing. In particular, in the group $(\mathbb{Z}/p\mathbb{Z})^\times$ with generator g, the equation $\log_g x = x$ could be taken to mean that x is an integer in $[1, p-1]$ with $g^x \equiv x \pmod{p}$.

Lets see if such fixed points exist for small primes p:

For $p = 2$, we have $g = 1$, $x = 1$, and yes, $g^x \equiv x \pmod{p}$.

For $p = 3$, we have $g = 2$, and $2^1 \not\equiv 1 \pmod 3$, $2^2 \not\equiv 2 \pmod 3$, so no, there is no fixed point.

For $p = 5$, there are two primitive roots (i.e., cyclic generators for $(\mathbb{Z}/p\mathbb{Z})^\times$), namely 2 and 3. One quickly checks that with the base 3, there are no fixed points, but $2^3 \equiv 3 \pmod 5$.

For $p = 7$, the primitive roots are 3 and 5, and we have

$$3^2 \equiv 2 \pmod 7, \quad 3^4 \equiv 4 \pmod 7, \quad 3^5 \equiv 5 \pmod 7.$$

Richard Guy

In Guy, section F9, it is mentioned that D. Brizolis conjectured that for every prime $p > 3$ there is a primitive root g and an integer x in $[1, p-1]$ with $\log_g x = x$.

Lemma. *Yes for p, 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 $g^x = x^{xy} \equiv x \pmod{p}$. □

More generally, a necessary and sufficient condition: *Suppose $x \in [1, p-1]$ has multiplicative order $(p-1)/d$. There is a primitive root g for p with $\log_g x = x$ if and only if $\gcd(x, p-1) = d$.*

Let us say that a prime p has the "Brizolis property" if there is a primitive root g in the range $[1, p-1]$ that is coprime to $p-1$.

How many such primitive roots do we expect? Well, there are exactly $\varphi(p-1)$ primitive roots in $[1, p-1]$ and exactly $\varphi(p-1)$ integers in this range coprime to $p-1$. If these are "independent events", then we would expect

$$\left(\frac{\varphi(p-1)}{p-1}\right)^2 (p-1) = \frac{\varphi(p-1)^2}{p-1}$$

such numbers. Since $\varphi(n) > cn/\log\log n$, the above expression is at least of order $p/(\log\log p)^2$, which is positive for all large p.

How might we try and prove this?

Lets begin with characteristic functions.

Say $f_1(g)$ is 1 if $\gcd(g, p-1) = 1$ and 0 otherwise, and $f_2(g)$ is 1 if g is a primitive root for p and 0 otherwise.

Let $N(p)$ be the number of integers in $[1, p-1]$ that are both primitive roots for p and coprime to $p-1$. Then

$$N(p) = \sum_{g=1}^{p-1} f_1(g) f_2(g).$$

To use this, we need explicit representations for these characteristic functions. Being coprime to $p-1$ is easy, it is essentially a combinatorial inclusion-exclusion over common divisors of g and $p-1$. We have

$$f_1(g) = \sum_{d \mid \gcd(g,p-1)} \mu(d),$$

where μ is the Möbius function.

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

A combinatorially similar idea works for $f_2(g)$, the characteristic function for primitive roots for p, but here we need to introduce characters. Let g_0 be some primitive root for p and let $\zeta = e^{2\pi i/(p-1)}$, a primitive $(p-1)$st root of 1 in $\mathbb{C}$. There is a natural isomophism χ from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\langle\zeta\rangle$ where $\chi(g_0^j) = \zeta^j$. Then

$$f_2(g) = \sum_{m|p-1} \frac{\mu(m)}{m} \sum_{j=1}^{m} \chi(g)^{j(p-1)/m}.$$

This can be seen by noting that the inner sum is m if $g^{(p-1)/m} \equiv 1 \pmod{p}$ and 0 otherwise.

So for $N(p)$, the number of integers in $[1, p-1]$ that satisfy the Brizolis property for p,

$$N(p) = \sum_{g=1}^{p-1} \sum_{d \mid \gcd(g,p-1)} \mu(d) \sum_{m \mid p-1} \frac{\mu(m)}{m} \sum_{j=1}^{m} \chi(g)^{j(p-1)/m}.$$

Fine, but are we making any progress? It is perhaps natural to write $g = dh$, use $\chi(g) = \chi(d)\chi(h)$ and rearrange a bit. We have

$$N(p) = \sum_{d,m \mid p-1} \frac{\mu(d)\mu(m)}{m} \sum_{j=1}^{m} \chi(d)^{j(p-1)/m} \sum_{h=1}^{(p-1)/d} \chi(h)^{j(p-1)/m}.$$

Note that the terms in this triple sum with $j = m$ are

$$\sum_{d,m \mid p-1} \frac{\mu(d)\mu(m)}{m} \frac{p-1}{d} = \frac{\varphi(p-1)^2}{p-1}.$$

We have proved that

$$\left|N(p)-\frac{\varphi(p-1)^2}{p-1}\right|\le\sum_{d,m|p-1}\frac{|\mu(d)\mu(m)|}{m}\sum_{j=1}^{m-1}\left|\sum_{h=1}^{(p-1)/d}\chi(h)^{j(p-1)/m}\right|.$$

Let

$$S\left(\chi^{j(p-1)/m}\right)=\max_n\left|\sum_{h=1}^{n}\chi(h)^{j(p-1)/m}\right|,$$

when $1\le j\le m-1$. Thus,

$$\left|N(p)-\frac{\varphi(p-1)^2}{p-1}\right|\le\sum_{d,m|p-1}\frac{|\mu(d)\mu(m)|}{m}\sum_{j=1}^{m-1}S\left(\chi^{j(p-1)/m}\right).$$

George Pólya

I. M. vinogradov

The Pólya–Vinogradov inequality

In 1918, Pólya and Vinogradov independently showed that for a nonprincipal character ψ modulo q, we have

$$S(\psi) := \max_n \left| \sum_{h=1}^{n} \psi(h) \right| < cq^{1/2} \log q,$$

for a universal positive constant c. Here, ψ is a non-principal character with modulus q. Thus,

$$\sum_{d,m|p-1} \frac{|\mu(d)\mu(m)|}{m} \sum_{j=1}^{m-1} S\left(\chi^{j(p-1)/m}\right) = O(4^{\omega(p-1)} p^{1/2} \log p),$$

and since $\omega(n) = o(\log n)$, we have the above expression being of magnitude at most $p^{1/2+\epsilon}$.

Thus,

$$N(p) = \frac{\varphi(p-1)^2}{p-1} + O(p^{1/2+\epsilon}).$$

Since as we have seen, the main term is at least of order $p/(\log\log p)^2$, this shows that all sufficiently large primes p have $N(p) > 0$.

But is it true for all primes $p > 3$?

Questions like this pose a computational challenge, since it involves putting explict constants on all of the inequalities involved. And challenges can remain, since the point at which $N(p) > 0$ is proved to be true may be too large to do a case study up to that point.

Some history: W.-P. Zhang in 1995 gave essentially the above argument but did not work out a starting point for when it is true.

C. Cobelli and A. Zaharescu in 1999 gave a somewhat different proof, showing that $N(p) > 0$ for all $p > 10^{2070}$. They said that a reorganization of their estimates would likely support a bound near 10^{50}.

So, can we do better? And how good is the Pólya–Vinogradov inequality?

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

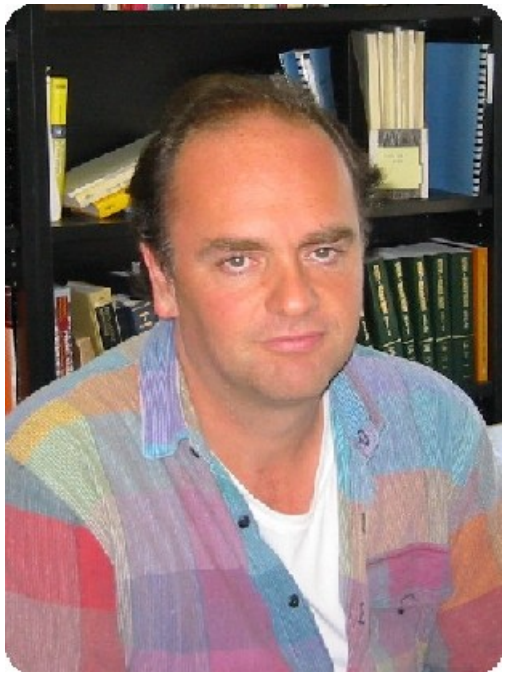
$$S(\chi) \geq \frac{1}{\pi}\sqrt{q}.$$

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

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

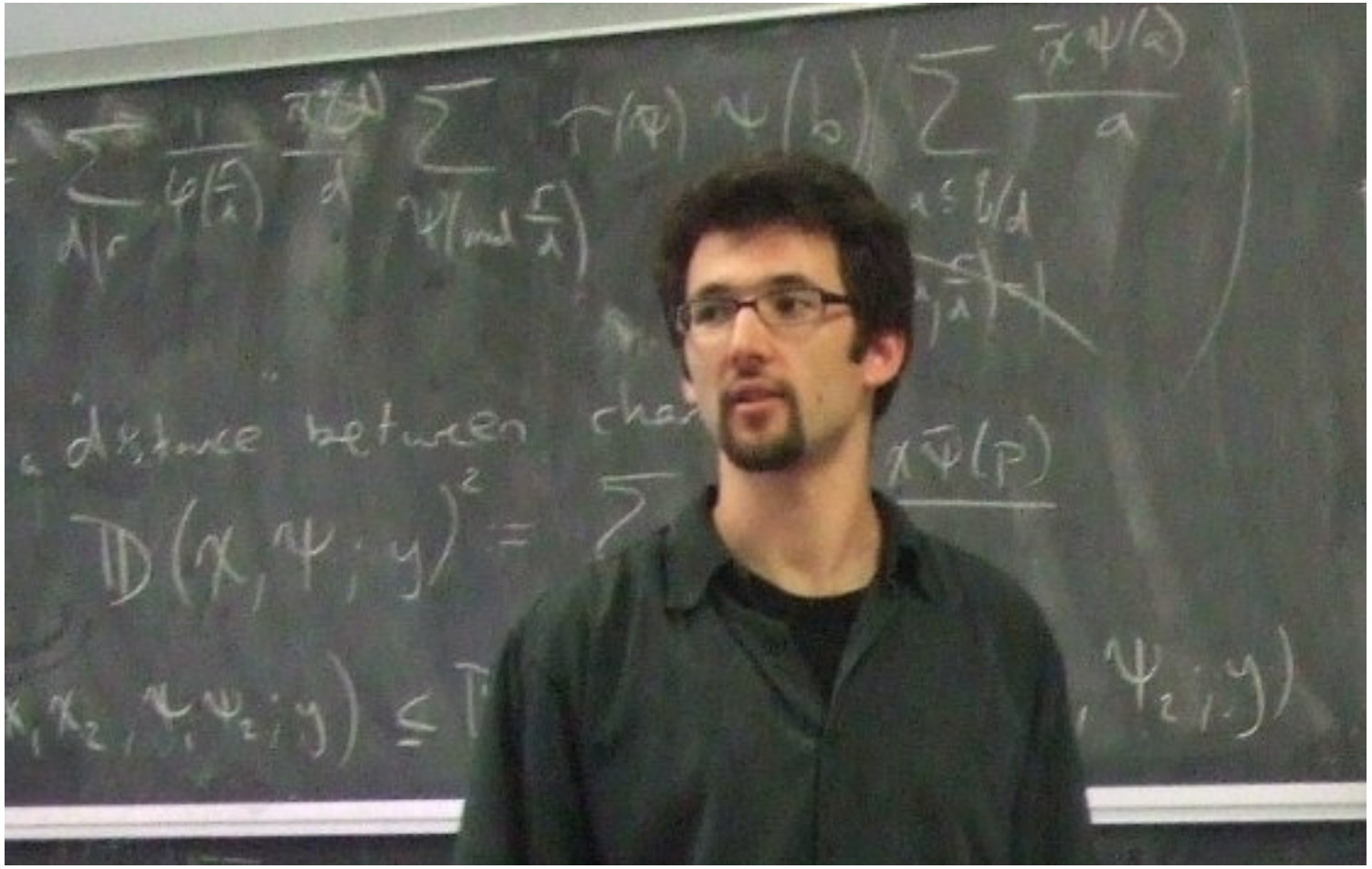
Paley (1932): *For infinitely many quadratic characters,* $S(\chi) \gg \sqrt{q}\log\log q$.

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



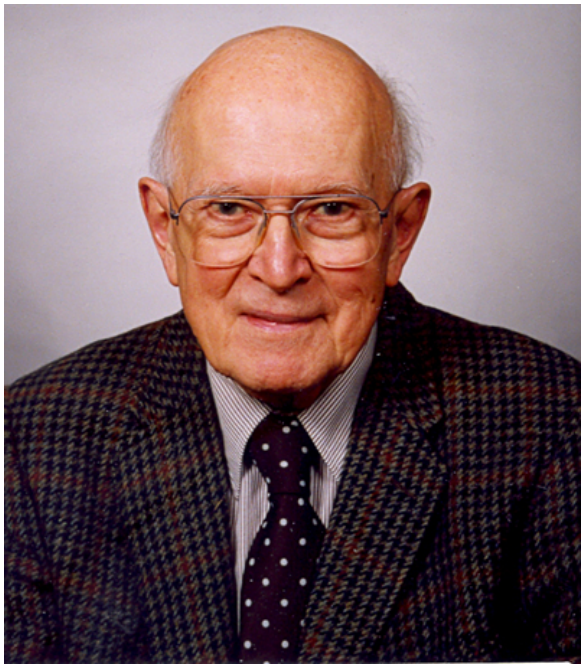
Leo Goldmakher

Recently I proved that for ψ a primitive Dirichlet character modulo q, we have

$$S(\psi) = \max_n \left| \sum_{h=1}^{n} \psi(h) \right| \leq q^{1/2} \left(\frac{1}{2\pi} (\log q + 2 \log \log q) + 1 \right).$$

My proof used some classical Fourier series arguments, a paper of Landau from 1918, and an idea of Bateman as reported in a paper of Hildebrand. (There are other explicit versions of this inequality in the literature, but they are not as sharp.)

Edmund Landau



Paul T. Bateman

A. J. Hildebrand

Armed with this fairly strong and explcit version of the Pólya–Vinogradov inequality, it is possible to close the gap on the Brizolis problem.

Levin, Pomerance (2010): *For each prime $p \neq 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $g^x \equiv x \pmod{p}$.*

We had written up a draft of this paper this past winter, and mentioned it to Soundararajan. Since our proof was fairly lengthy, with much computation still needed, he suggested a simpler approach.

Mariana Levin

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 $S_N(\chi) \le \sqrt{q} - \frac{N}{\sqrt{q}}$.*

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. (A similar result for prime moduli is due to Hua in 1942.)

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 $\sqrt{q} - N/\sqrt{q}$.

Using the smoothed Pólya–Vinogradov inequality makes the proof of the fixed point theorem much simpler.

Using just our smoothed Pólya–Vinogradov inequality gets us that the property holds 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 proved that $N(p) > 0$ if both $s < 1/2$, 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

Is the smoothed Pólya–Vinogradov inequality a "one-hit wonder"?

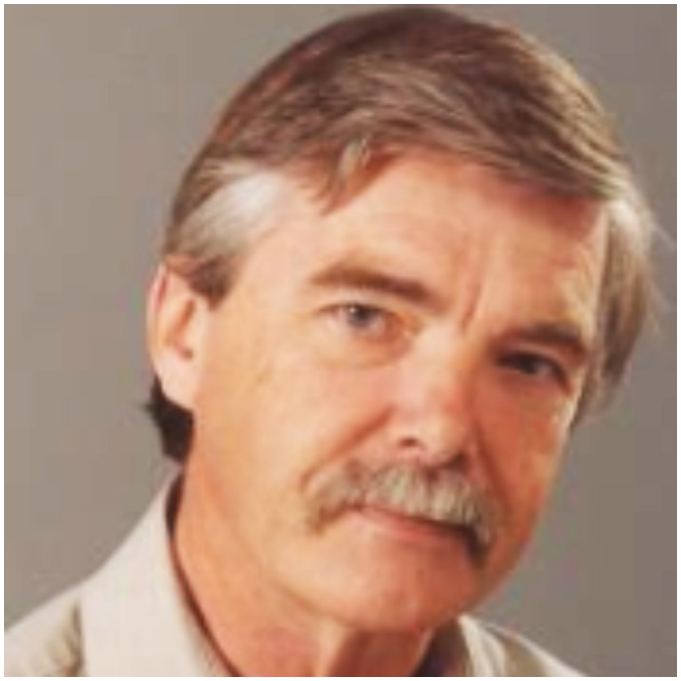
Another possible application:

Let $B(\chi)$ be the smallest positive integer n with $\chi(n) \neq 0, 1$.

Ankeny, Oesterlé, Bach: *Assuming the GRH, if χ is a nonprincipal character modulo q, then $B(\chi) < 3 \log^2 q$.*

Vinogradov, Burgess: *Unconditionally, $B(\chi) < q^{1/4\sqrt{e}+\epsilon}$.*

Eric Bach



Hugh Williams

Computational problem: Choose some target function $T(q)$, like $q^{1/2}$ or smaller, and find all examples of a character χ modulo q, with $B(\chi) > T(q)$.

Granville, Mollin, Williams (2000): *For χ the quadratic character to a positive fundamental discriminant q, if $B(\chi) > \sqrt{q}/2$, then $q \leq 3705$.*

Treviño is working on improving this result, both by improving the bound $T(q)$ and dealing with all primitive characters.

So, it is expected that the smoothed Pólya–Vinogradov inequality will become another arrow in our quiver for attacking computational problems.