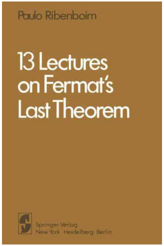
Primes, postdocs and pretentiousness

Andrew Granville

Université de Montréal

Fields-PIMS-CRM prize lecture
20th October 2022

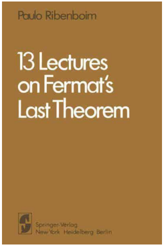


Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

PhD at Queens, 1984-87 with Paulo Ribenboim

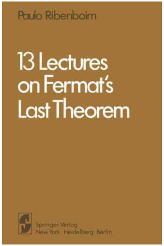


Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

PhD at Queens, 1984-87 with Paulo Ribenboim



Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

- Proved by (Sir) Andrew Wiles in 1994

PhD at Queens, 1984-87 with Paulo Ribenboim

Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

- Proved by (Sir) Andrew Wiles in 1994

PhD at Queens, 1984-87 with Paulo Ribenboim

Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

- Proved by (Sir) Andrew Wiles in 1994

AG 1985: FLT is true for 100% of exponents n.

PhD at Queens, 1984-87 with Paulo Ribenboim

Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

- Proved by (Sir) Andrew Wiles in 1994

AG 1985: FLT is true for 100% of exponents n.

$x^n + y^n = z^n, z \neq 0$ iff $u^n + v^n = 1$ with $u = x/z, v = y/z$

PhD at Queens, 1984-87 with Paulo Ribenboim

Fermat's Last Theorem (FLT):

No integer solutions to

$$x^n + y^n = z^n \text{ with } n > 2 \text{ and } xyz \neq 0.$$

- Proved by (Sir) Andrew Wiles in 1994

AG 1985: FLT is true for 100% of exponents n.

$x^n + y^n = z^n, z \neq 0$ iff $u^n + v^n = 1$ with $u = x/z, v = y/z$

Faltings' 1983 Theorem – proof of Mordell's conjecture

Any curve, defined in $\mathbb{Q}$, of genus > 1, contains only finitely many rational points. This includes $u^n + v^n = 1$ when $n > 3$

FLT is true for 100% of exponents n

Corollary to Faltings' Theorem

For each prime $p > 3$ there exists a bound B_p such that if $x^p + y^p = z^p$ with $x, y, z > 0$ then $z \leq B_p$.

FLT is true for 100% of exponents n

Corollary to Faltings' Theorem

For each prime $p > 3$ there exists a bound B_p such that if $x^p + y^p = z^p$ with $x, y, z > 0$ then $z \leq B_p$.

Suppose $a^n + b^n = c^n$ where $n = mp$ with p prime

FLT is true for 100% of exponents n

Corollary to Faltings' Theorem

For each prime $p > 3$ there exists a bound B_p such that if $x^p + y^p = z^p$ with $x, y, z > 0$ then $z \leq B_p$.

Suppose $a^n + b^n = c^n$ where $n = mp$ with p prime

Then $(a^m)^p + (b^m)^p = (c^m)^p$, so $2^m \leq c^m = z \leq B_p$,

FLT is true for 100% of exponents n

Corollary to Faltings' Theorem

For each prime $p > 3$ there exists a bound B_p such that if $x^p + y^p = z^p$ with $x, y, z > 0$ then $z \leq B_p$.

Suppose $a^n + b^n = c^n$ where $n = mp$ with p prime

Then $(a^m)^p + (b^m)^p = (c^m)^p$, so $2^m \leq c^m = z \leq B_p$,

Therefore if prime $p > 3$ divides n then $n = pm \leq b_p := p \log_2 B_p$.

FLT is true for 100% of exponents n

Corollary to Faltings' Theorem

For each prime $p > 3$ there exists a bound B_p such that if $x^p + y^p = z^p$ with $x, y, z > 0$ then $z \leq B_p$.

Suppose $a^n + b^n = c^n$ where $n = mp$ with p prime

Then $(a^m)^p + (b^m)^p = (c^m)^p$, so $2^m \leq c^m = z \leq B_p$,

Therefore if prime $p > 3$ divides n then $n = pm \leq b_p := p \log_2 B_p$.

"Easy" sieve result: A proportion $1 - \epsilon_y$ of the integers have a prime factor in $[5, y]$, where $\epsilon_y \to 0$ as $y \to \infty$.

This implies FLT is true for 100% of exponents n. □

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

Wieferich (1909): FLTI false implies $2^{p-1} \equiv 1 \pmod{p^2}$.

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

Wieferich (1909): FLTI false implies $2^{p-1} \equiv 1 \pmod{p^2}$.
Holds only for $p = 1093$ and 3511 of all primes $p < 3 \times 10^{18}$

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

Wieferich (1909): FLTI false implies $2^{p-1} \equiv 1 \pmod{p^2}$.
Holds only for $p = 1093$ and 3511 of all primes $p < 3 \times 10^{18}$

Thesis work (1985-6): Found a way to show
"FLTI false implies $q^{p-1} \equiv 1 \pmod{p^2}$" for arbitrary q,
depending on linear algebra / large (symbolic) matrices calculation.

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

Wieferich (1909): FLTI false implies $2^{p-1} \equiv 1 \pmod{p^2}$.
Holds only for $p = 1093$ and 3511 of all primes $p < 3 \times 10^{18}$

Thesis work (1985-6): Found a way to show
"FLTI false implies $q^{p-1} \equiv 1 \pmod{p^2}$" for arbitrary q,
depending on linear algebra / large (symbolic) matrices calculation.

Too large for technology of that time!

Invited to Maple (Waterloo) to help design their "large linear algebra" package.

The First Case of FLT (FLTI): $x^p + y^p = z^p$ where $p \nmid xyz$

Wieferich (1909): FLTI false implies $2^{p-1} \equiv 1 \pmod{p^2}$.
Holds only for $p = 1093$ and 3511 of all primes $p < 3 \times 10^{18}$

Thesis work (1985-6): Found a way to show
"FLTI false implies $q^{p-1} \equiv 1 \pmod{p^2}$" for arbitrary q,
depending on linear algebra / large (symbolic) matrices calculation.
Too large for technology of that time!
Invited to Maple (Waterloo) to help design their "large linear algebra" package.

AG-Monagan (1988)

The first case of Fermat's last theorem is true for all prime exponents up to $714,591,416,091,389$.

We showed: FLTI false implies $q^{p-1} \equiv 1 \pmod{p^2}$ for all $q \leq 89$.

FLT and ABC

How to generalize $x^n + y^n = z^n$? Part of a family of curves?

FLT and ABC

How to generalize $x^n + y^n = z^n$? Part of a family of curves?
Or a special example of

$$a + b = c \text{ with } a, b, c \in \mathbb{Z}_{\geq 1}, (a, b, c) = 1$$

where a, b, c are divisible by higher powers of primes.

FLT and ABC

How to generalize $x^n + y^n = z^n$? Part of a family of curves?
Or a special example of

$$a + b = c \text{ with } a, b, c \in \mathbb{Z}_{\geq 1}, (a, b, c) = 1$$

where a, b, c are divisible by higher powers of primes.
Perhaps we can bound a, b, c in terms of the distinct prime factors?

FLT and ABC

How to generalize $x^n + y^n = z^n$? Part of a family of curves?
Or a special example of

$$a + b = c \text{ with } a, b, c \in \mathbb{Z}_{\geq 1}, (a, b, c) = 1$$

where a, b, c are divisible by higher powers of primes.
Perhaps we can bound a, b, c in terms of the distinct prime factors?

$$a, b, c \text{ bound by a function of } \prod_{p|abc} p \text{ ?}$$

Easy to prove the analogy for polynomials a, b, c

FLT and ABC

How to generalize $x^n + y^n = z^n$? Part of a family of curves?
Or a special example of

$$a + b = c \text{ with } a, b, c \in \mathbb{Z}_{\geq 1}, (a, b, c) = 1$$

where a, b, c are divisible by higher powers of primes.
Perhaps we can bound a, b, c in terms of the distinct prime factors?

$$a, b, c \text{ bound by a function of } \prod_{p|abc} p \text{ ?}$$

Easy to prove the analogy for polynomials a, b, c

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if
$a + b = c$ with $a, b, c > 0$ and $(a, b) = 1$

$$c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

FLT and ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if

$$a + b = c \text{ with } a, b, c \geq 1 \text{ and } (a, b) = 1,$$

$$\text{then } c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

Now if $x^n + y^n = z^n$ then let $a = x^n, b = y^n, c = z^n$.

FLT and ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if

$$a + b = c \text{ with } a, b, c \geq 1 \text{ and } (a, b) = 1,$$

$$\text{then } c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

Now if $x^n + y^n = z^n$ then let $a = x^n, b = y^n, c = z^n$.We have

$$\prod_{p|abc} p = \prod_{p|xyz} p \leq xyz = (abc)^{1/n} \leq c^{3/n}$$

FLT and ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if

$$a + b = c \text{ with } a, b, c \geq 1 \text{ and } (a, b) = 1,$$

$$\text{then } c \leq \kappa_\epsilon \Bigl(\prod_{p|abc} p \Bigr)^{1+\epsilon}.$$

Now if $x^n + y^n = z^n$ then let $a = x^n, b = y^n, c = z^n$.We have

$$\prod_{p|abc} p = \prod_{p|xyz} p \leq xyz = (abc)^{1/n} \leq c^{3/n}$$

So for $n \geq 4$ the *abc*-conjecture with $\epsilon = 1/7$ and $\kappa = \kappa_{1/7}$ implies

$$c \leq \kappa \left(c^{3/n} \right)^{8/7} = \kappa c^{6/7}$$

so $c \leq \kappa^7$

FLT and ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if

$$a + b = c \text{ with } a, b, c \geq 1 \text{ and } (a, b) = 1,$$

$$\text{then } c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

Now if $x^n + y^n = z^n$ then let $a = x^n, b = y^n, c = z^n$.We have

$$\prod_{p|abc} p = \prod_{p|xyz} p \leq xyz = (abc)^{1/n} \leq c^{3/n}$$

So for $n \geq 4$ the *abc*-conjecture with $\epsilon = 1/7$ and $\kappa = \kappa_{1/7}$ implies

$$c \leq \kappa \left(c^{3/n} \right)^{8/7} = \kappa c^{6/7}$$

so $c \leq \kappa^7 \implies$ **Bounded number of FLT solns with $n \geq 4$.**

Applicability of ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if $a + b = c$ with $a, b, c > 0$ and $(a, b) = 1$

$$a, b, c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

- Fermat 1637: $x^n + y^n = z^n$ with $(x, y) = 1$ and $n > 3$;

Applicability of ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if $a + b = c$ with $a, b, c > 0$ and $(a, b) = 1$

$$a, b, c \leq \kappa_\epsilon \Bigg(\prod_{p|abc} p \Bigg)^{1+\epsilon}.$$

- Fermat 1637: $x^n + y^n = z^n$ with $(x, y) = 1$ and $n > 3$;
- Catalan 1844: $x^p - y^q = 1$ with $(x, y) = 1$ and $p, q > 1$;

Applicability of ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if $a + b = c$ with $a, b, c > 0$ and $(a, b) = 1$

$$a, b, c \leq \kappa_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

- Fermat 1637: $x^n + y^n = z^n$ with $(x, y) = 1$ and $n > 3$;
- Catalan 1844: $x^p - y^q = 1$ with $(x, y) = 1$ and $p, q > 1$;
- $x^p + y^q = z^n$ with $(x, y) = 1$ and $\frac{1}{p} + \frac{1}{q} + \frac{1}{n} < 1$;

Applicability of ABC

The *abc*-conjecture (Masser-Oesterlé, 1985)

For each fixed $\epsilon > 0$ there exists a constant κ_ϵ such that if $a + b = c$ with $a, b, c > 0$ and $(a, b) = 1$

$$a, b, c \leq \kappa_\epsilon \Bigg(\prod_{p \mid abc} p \Bigg)^{1+\epsilon}.$$

- Fermat 1637: $x^n + y^n = z^n$ with $(x, y) = 1$ and $n > 3$;
- Catalan 1844: $x^p - y^q = 1$ with $(x, y) = 1$ and $p, q > 1$;
- $x^p + y^q = z^n$ with $(x, y) = 1$ and $\frac{1}{p} + \frac{1}{q} + \frac{1}{n} < 1$;
- $F(x, y) = z^n$ with $(x, y) = 1$ and $2/d + 1/n < 1$ where $F(\cdot, \cdot)$ is a binary form of degree d.

Another generalization: Sophie Germain and me

Sophie Germain (≈ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Another generalization: Sophie Germain and me

Sophie Germain ($\approx$ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Idea: If $q \nmid x$ then $(x^p)^k = x^{q-1} \equiv 1 \pmod{q}$ and so x^p is a kth root of unity mod q.

Another generalization: Sophie Germain and me

Sophie Germain ($\approx$ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Idea: If $q \nmid x$ then $(x^p)^k = x^{q-1} \equiv 1 \pmod{q}$ and so x^p is a kth root of unity mod q. Thus $x^p + y^p = z^p, q \nmid xyz$ yields $\zeta_1 + \zeta_2 + \zeta_3 \equiv 0 \pmod{q}$, each ζ_j is a kth root of unity mod q.

Another generalization: Sophie Germain and me

Sophie Germain ($\approx$ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Idea: If $q \nmid x$ then $(x^p)^k = x^{q-1} \equiv 1 \pmod{q}$ and so x^p is a kth root of unity mod q. Thus $x^p + y^p = z^p, q \nmid xyz$ yields $\zeta_1 + \zeta_2 + \zeta_3 \equiv 0 \pmod{q}$, each ζ_j is a kth root of unity mod q. So q divides $\mathrm{Norm}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_1 + \zeta_2 + \zeta_3)$, which is non-zero if $3 \nmid k$.

Another generalization: Sophie Germain and me

Sophie Germain (≈ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Idea: If $q \nmid x$ then $(x^p)^k = x^{q-1} \equiv 1 \pmod{q}$ and so x^p is a kth root of unity mod q. Thus $x^p + y^p = z^p, q \nmid xyz$ yields $\zeta_1 + \zeta_2 + \zeta_3 \equiv 0 \pmod{q}$, each ζ_j is a kth root of unity mod q. So q divides $\mathrm{Norm}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_1 + \zeta_2 + \zeta_3)$, which is non-zero if $3 \nmid k$.

Generalization: Let $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$. Are there integer solutions $\ell_1, \ldots, \ell_m$ to

$$F(\ell_1^n, \ldots, \ell_m^n) = 0? \qquad (1)$$

Another generalization: Sophie Germain and me

Sophie Germain ($\approx$ 1805)

For any even integer k with $3 \nmid k$, if p is a sufficiently large prime and $q = kp + 1$ is also prime then FLTI is true for exponent p.

Idea: If $q \nmid x$ then $(x^p)^k = x^{q-1} \equiv 1 \pmod q$ and so x^p is a kth root of unity mod q. Thus $x^p + y^p = z^p, q \nmid xyz$ yields $\zeta_1 + \zeta_2 + \zeta_3 \equiv 0 \pmod q$, each ζ_j is a kth root of unity mod q. So q divides $\mathrm{Norm}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_1 + \zeta_2 + \zeta_3)$, which is non-zero if $3 \nmid k$.

Generalization: Let $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$. Are there integer solutions $\ell_1, \ldots, \ell_m$ to

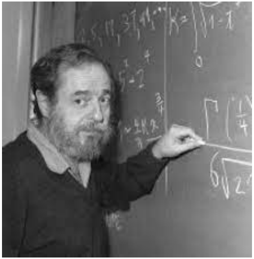
$$F(\ell_1^n, \ldots, \ell_m^n) = 0? \qquad (1)$$

AG: If there are no solutions to $F(\zeta_1, \ldots, \zeta_m) = 0$ in roots of unity, then $\exists$ integer solns to (1) for very "few" exponents n.

Gauss's letter to Sophie Germain, 1807

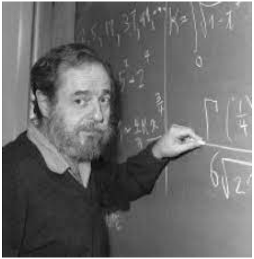
"A taste for the abstract sciences in general and above all the mysteries of numbers is excessively rare. One is not astonished by it for the enchanting charms of this sublime science are revealed only to those who have the courage to go deeply into it. However, when a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents and superior genius. Indeed nothing could prove to me in so flattering and unequivocal manner that the attractions of this science, which have enriched my life with so many joys, are not illusory, than the attention with which you have honored it."

Postdoc at Toronto, 1987-89 with John Friedlander

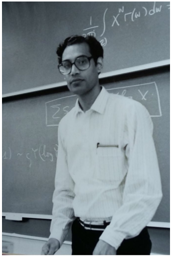


John Friedlander

Postdoc at Toronto, 1987-89 with John Friedlander

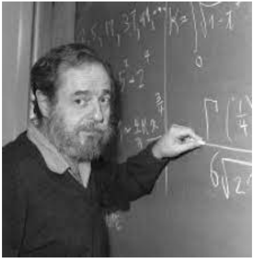


John Friedlander

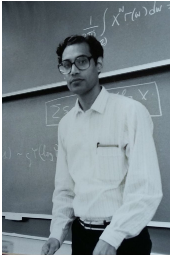


Kumar Murty

Postdoc at Toronto, 1987-89 with John Friedlander



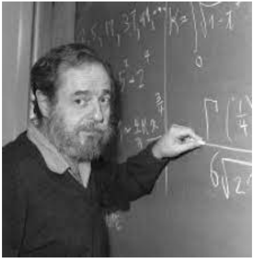
John Friedlander



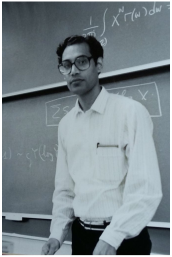
Kumar Murty

Cem Yildirim

Postdoc at Toronto, 1987-89 with John Friedlander



John Friedlander



Kumar Murty

Cem Yildirim

If $(a, q) = 1$ then

$$\pi(x; q, a) = \#\{ \text{ primes } p \le x : p \equiv a \pmod q\} \sim \frac{\pi(x)}{\phi(q)}$$

where $\pi(x) = \#\{\text{primes } p \le x\}$ and
$\phi(q) = \#\{a \in [1, q] : \ (a, q) = 1\}$.

(Prime Number Theorem for Arithmetic Progressions – PNT4APs)

Prime numbers

PNT4APs:
$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^{\epsilon}}$.

Prime numbers

PNT4APs:
$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \qquad (2)$$

holds for $x \geq e^{q^{\epsilon}}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Prime numbers

$$\text{PNT4APs:} \qquad \pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^\epsilon}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Bombieri-Vinogradov Theorem ($\approx$ 1965)

(2) holds for "almost all" $x \geq q^2(\log q)^{1+\epsilon}$, for all $(a, q) = 1$.

Prime numbers

PNT4APs:
$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^{\epsilon}}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Bombieri-Vinogradov Theorem ($\approx$ 1965)

(2) holds for "almost all" $x \geq q^2(\log q)^{1+\epsilon}$, for all $(a, q) = 1$.

Exponent "2" a barrier to progress.

Prime numbers

$$\text{PNT4APs:} \qquad \pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^\epsilon}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Bombieri-Vinogradov Theorem ($\approx$ 1965)

(2) holds for "almost all" $x \geq q^2(\log q)^{1+\epsilon}$, for all $(a, q) = 1$.

Exponent "2" a barrier to progress. Can exponent "1" hold always?

Prime numbers

PNT4APs:
$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^\epsilon}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Bombieri-Vinogradov Theorem ($\approx$ 1965)

(2) holds for "almost all" $x \geq q^2(\log q)^{1+\epsilon}$, for all $(a, q) = 1$.

Exponent "2" a barrier to progress. Can exponent "1" hold always?

Friedlander-AG, 1989 – disproof of Elliott-Halberstam conj

(2) does not hold for "almost all" q with $x = q(\log q)^A$, for some $(a, q) = 1$.

Prime numbers

PNT4APs:
$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)} \tag{2}$$

holds for $x \geq e^{q^\epsilon}$. And for $x \geq q^2(\log q)^{2+\epsilon}$ assuming GRH.

Bombieri-Vinogradov Theorem ($\approx$ 1965)

(2) holds for "almost all" $x \geq q^2(\log q)^{1+\epsilon}$, for all $(a, q) = 1$.

Exponent "2" a barrier to progress. Can exponent "1" hold always?

Friedlander-AG, 1989 – disproof of Elliott-Halberstam conj

(2) does not hold for "almost all" q with $x = q(\log q)^A$, for some $(a, q) = 1$.

Elliott-Halberstam conj, II: (2) holds for "almost all" q, for all $x \geq q^{1+\epsilon}$, for all $(a, q) = 1$.

Postdoc at IAS Princeton, 1989-91 with Enrico Bombieri

Enrico Bombieri

Postdoc at IAS Princeton, 1989-91 with Enrico Bombieri

Enrico Bombieri

Atle Selberg

Postdoc at IAS Princeton, 1989-91 with Enrico Bombieri

Enrico Bombieri

Atle Selberg

Riemann Hypotheses (GRH), 1859+

- $L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$ for $\text{Re}(s) > 1$, with $\chi(\cdot)$ a character.

Postdoc at IAS Princeton, 1989-91 with Enrico Bombieri

Enrico Bombieri

Atle Selberg

Riemann Hypotheses (GRH), 1859+

- $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$ for $\mathrm{Re}(s) > 1$, with $\chi(\cdot)$ a character.
- Analytically continue it to all of $\mathbb{C}$ (except perhaps at $s = 1$).

Postdoc at IAS Princeton, 1989-91 with Enrico Bombieri

Enrico Bombieri

Atle Selberg

Riemann Hypotheses (GRH), 1859+

- $L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$ for $\text{Re}(s) > 1$, with $\chi(\cdot)$ a character.
- Analytically continue it to all of $\mathbb{C}$ (except perhaps at $s = 1$).
- Guess: If $L(\rho, \chi) = 0$ with $0 < \text{Re}(\rho) < 1$ then $\text{Re}(\rho) = \frac{1}{2}$.

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\operatorname{Re}(s) > 1$

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\mathrm{Re}(s) > 1$

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

Suppose $L(\rho, \chi) = 0$ with $\rho = \beta + i\gamma$ where $0 < \beta < 1$ then

GRH: $\beta = \frac{1}{2}$

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\text{Re}(s) > 1$

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

Suppose $L(\rho, \chi) = 0$ with $\rho = \beta + i\gamma$ where $0 < \beta < 1$ then

GRH: $\beta = \frac{1}{2}$ — Too hard!

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\mathrm{Re}(s) > 1$

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

Suppose $L(\rho,\chi) = 0$ with $\rho = \beta + i\gamma$ where $0 < \beta < 1$ then

GRH: $\beta = \frac{1}{2}$ — Too hard!

Bombieri-Vinogradov Theorem: $\beta > \frac{1}{2} + \epsilon$ is rare.

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\text{Re}(s) > 1$

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

Suppose $L(\rho, \chi) = 0$ with $\rho = \beta + i\gamma$ where $0 < \beta < 1$ then

GRH: $\beta = \frac{1}{2}$ — Too hard!

Bombieri-Vinogradov Theorem: $\beta > \frac{1}{2} + \epsilon$ is rare.

Strong PNT4APs (Siegel): If χ is real and $\gamma = 0$ then we need to show that $\beta \leq 1 - \frac{1}{\log q}$

A more moderate ambition than the Riemann Hypothesis

Let $\chi(\cdot)$ be a Dirichlet character mod q. Define for $\text{Re}(s) > 1$

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

and analytically continue to all of $\mathbb{C}$.

Suppose $L(\rho, \chi) = 0$ with $\rho = \beta + i\gamma$ where $0 < \beta < 1$ then

GRH: $\beta = \frac{1}{2}$ — Too hard!

Bombieri-Vinogradov Theorem: $\beta > \frac{1}{2} + \epsilon$ is rare.

Strong PNT4APs (Siegel): If χ is real and $\gamma = 0$ then we need to show that $\beta \leq 1 - \frac{1}{\log q}$

Life goal – Prove there are no "Siegel zeros"!

($L(\beta, \chi) \neq 0$ whenever $\beta > 1 - \frac{1}{\log q}$ for real characters χ)

Proving there are no Siegel zeros

AG-Stark, 2000

If the "uniform" *abc*-conjecture holds in "Hilbert class fields" then there are no Siegel zeros for $L(s, (\frac{D}{\cdot}))$ where $D < 0$.

That is, if $L(\beta, (\frac{D}{\cdot})) = 0$ with $\beta \in \mathbb{R}$ and $D < 0$ then

$$\beta < 1 - \frac{1}{\log |D|}.$$

Proving there are no Siegel zeros

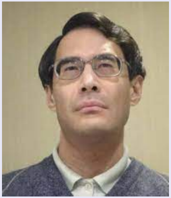
AG-Stark, 2000

If the "uniform" *abc*-conjecture holds in "Hilbert class fields" then there are no Siegel zeros for $L(s, (\frac{D}{\cdot}))$ where $D < 0$.

That is, if $L(\beta, (\frac{D}{\cdot})) = 0$ with $\beta \in \mathbb{R}$ and $D < 0$ then

$$\beta < 1 - \frac{1}{\log |D|}.$$

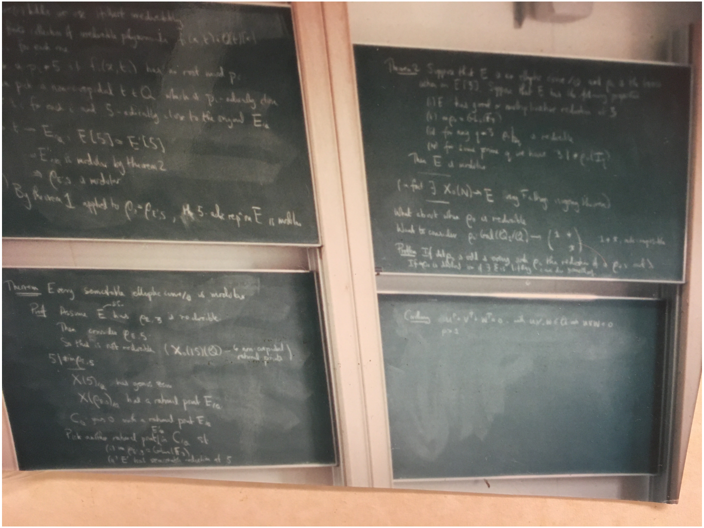
Mochizuki-Fesenko-Hoshi-Minamide-Porowski, Nov 2020



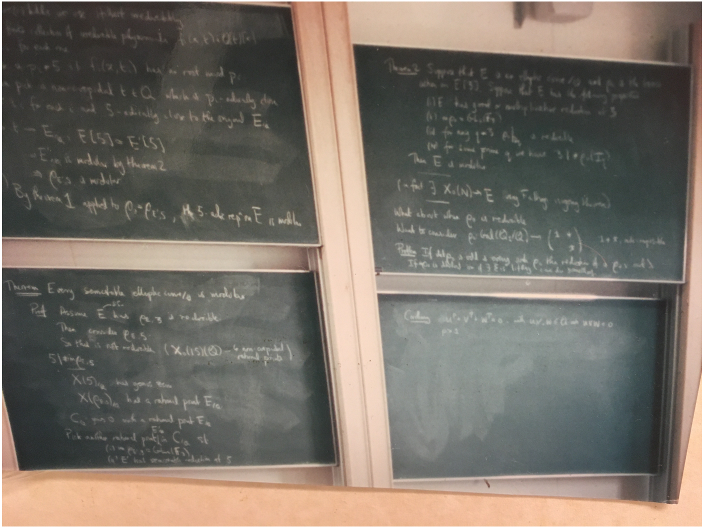
A modification of this version of *abc* can be proved unconditionally!

"Proof" gives bounds on solns to Fermat equation in number fields.

At a meeting at the Isaac Newton Institute, June 23,1993



At a meeting at the Isaac Newton Institute, June 23,1993



Corollary: $u^p + v^p + w^p = 0$ $(p > 2)$ with $u, v, w \in \mathbb{Q} \implies uvw = 0$.

Back to $x^p + y^q = z^r$

Darmon-AG, 1995

For fixed integers p, q, r with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1.$$

A much more subtle Corollary to Faltings' Theorem.

Back to $x^p + y^q = z^r$

Darmon-AG, 1995

For fixed integers p, q, r with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1.$$

A much more subtle Corollary to Faltings' Theorem.
Techniques also apply to

$$z^m = F(x, y) \text{ with } (x, y) = 1$$

Back to $x^p + y^q = z^r$

Darmon-AG, 1995

For fixed integers p, q, r with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1.$$

A much more subtle Corollary to Faltings' Theorem.
Techniques also apply to

$$z^m = F(x, y) \text{ with } (x, y) = 1$$

The Fermat-Catalan conjecture

There are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1 \text{ and } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

Back to $x^p + y^q = z^r$

Darmon-AG, 1995

For fixed integers p, q, r with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1.$$

A much more subtle Corollary to Faltings' Theorem.
Techniques also apply to

$$z^m = F(x, y) \text{ with } (x, y) = 1$$

The Fermat-Catalan conjecture

There are only finitely many integer solutions to

$$x^p + y^q = z^r \text{ with } (x, y) = 1 \text{ and } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

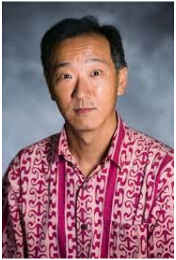
Perhaps none with $p, q, r \geq 3$?

Univ of Georgia: Students and Postdocs

Anitha Srinivasan

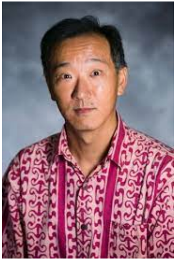
Univ of Georgia: Students and Postdocs

Anitha Srinivasan



Ken Ono

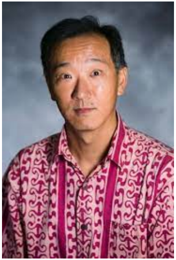
Univ of Georgia: Students and Postdocs



Anitha Srinivasan   Ken Ono   Ernie Croot

Univ of Georgia: Students and Postdocs

Anitha Srinivasan



Ken Ono

Ernie Croot

Ernie Croot 2003 – The Erdős-Graham coloring conjecture

There exists a constant $b > 0$ such that if we r-color the integers then there exists a monochromatic subset S of $[2, b^r]$ such that

$$\sum_{n \in S} \frac{1}{n} = 1.$$

Negative mean values of multiplicative functions

K Soundararajan

Negative mean values of multiplicative functions

K Soundararajan

If $n = p_1 \cdots p_k$ then let $f(n) = f(p_1) \cdots f(p_k)$.

Negative mean values of multiplicative functions

K Soundararajan

If $n = p_1 \cdots p_k$ then let $f(n) = f(p_1) \cdots f(p_k)$.
Assume each $f(n) = -1$ or 1.

Negative mean values of multiplicative functions

K Soundararajan

If $n = p_1 \cdots p_k$ then let $f(n) = f(p_1) \cdots f(p_k)$.
Assume each $f(n) = -1$ or 1.
They can all be 1, but they cannot all be -1 since if $f(2) = f(3) = -1$ then $f(6) = f(2)f(3) = 1$.

Negative mean values of multiplicative functions

K Soundararajan

If $n = p_1 \cdots p_k$ then let $f(n) = f(p_1) \cdots f(p_k)$.
Assume each $f(n) = -1$ or 1.
They can all be 1, but they cannot all be -1 since if $f(2) = f(3) = -1$ then $f(6) = f(2)f(3) = 1$.
What is the most -1's one can get up to x?

Negative mean values of multiplicative functions

K Soundararajan

If $n = p_1 \cdots p_k$ then let $f(n) = f(p_1) \cdots f(p_k)$.
Assume each $f(n) = -1$ or 1.
They can all be 1, but they cannot all be -1 since if $f(2) = f(3) = -1$ then $f(6) = f(2)f(3) = 1$.
What is the most -1's one can get up to x?

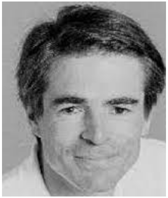
AG-Soundararajan, 2001

The number of -1's is always $\leq \{c + o(1)\}x$ where

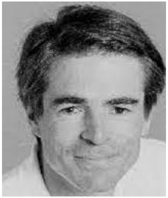
$$c = \log(1 + \sqrt{e}) - 2\int_1^{\sqrt{e}} \frac{\log t}{t+1}\, dt = .828499\ldots$$

Attained if $f(p) = 1$ for $p < x^{1/(1+\sqrt{e})}$ and $f(p) = -1$ otherwise.

Université de Montréal (2002–): Primes and pretentions

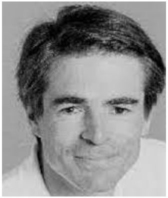
Université de Montréal (2002–): Primes and pretentions

PRIME PATTERNS

Are there infinitely many prime *twins*, $p, p+2$?

Université de Montréal (2002–): Primes and pretentions




PRIME PATTERNS

Are there infinitely many prime *twins*, $p, p+2$?

Celebrity Twin Prime Video

Prime patterns and pretentiousness

$$p, p+2$$

Prime patterns and pretentiousness

$$p, p + 2$$

$$p, p + 4$$

Prime patterns and pretentiousness

$$p, p+2$$

$$p, p+4 \text{ or } p+6 \text{ or } \ldots$$

Prime patterns and pretentiousness

$$p, p + 2$$

$$p, p + 4 \text{ or } p + 6 \text{ or } \ldots$$

$$p, 2p + 1$$

Prime patterns and pretentiousness

$$p, p+2$$

$$p, p+4 \text{ or } p+6 \text{ or } \ldots$$

$$p, 2p+1$$

$$2p+1, 4p+1 \text{ and } 6p+5$$

Prime patterns and pretentiousness

$$p, p + 2$$

$$p, p + 4 \text{ or } p + 6 \text{ or } \ldots$$

$$p, 2p + 1$$

$$2p + 1, 4p + 1 \text{ and } 6p + 5$$

$$p, p + d, p + 2d, \ldots, p + kd$$

Any pattern except if obvious reason why not, like $n, n + 1$.

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

$$\text{Average}_{p_n \leq x} p_{n+1} - p_n \approx \log x,$$

Up to 2000, best result known $< \frac{1}{4} \log x$.

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

$$\text{Average}_{p_n \le x} p_{n+1} - p_n \approx \log x,$$

Up to 2000, best result known $< \frac{1}{4} \log x$.

Goldston-Yildirim 2003 – novel approach (new sieve wts) *claiming*

$$\liminf_{p_n \le x} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

$\text{Average}_{p_n \leq x} p_{n+1} - p_n \approx \log x$,

Up to 2000, best result known $< \frac{1}{4} \log x$.

Goldston-Yildirim 2003 – novel approach (new sieve wts) *claiming*

$$\liminf_{p_n \leq x} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Proof based on certain believable lemmas with sketched proofs

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

$$\text{Average}_{p_n \le x} p_{n+1} - p_n \approx \log x,$$

Up to 2000, best result known $< \frac{1}{4} \log x$.

Goldston-Yildirim 2003 – novel approach (new sieve wts) *claiming*

$$\liminf_{p_n \le x} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Proof based on certain believable lemmas with sketched proofs

AG-Soundararajan: Assuming these lemmas, inf many n with $p_{n+1} - p_n \le 16$.

The GPY story, I

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes.

Wts, Inf many n such that $p_{n+1} - p_n = 2$.

$\text{Average}_{p_n \leq x} p_{n+1} - p_n \approx \log x$,

Up to 2000, best result known $< \frac{1}{4} \log x$.

Goldston-Yildirim 2003 – novel approach (new sieve wts) *claiming*

$$\liminf_{p_n \leq x} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Proof based on certain believable lemmas with sketched proofs

AG-Soundararajan: Assuming these lemmas, inf many n with

$p_{n+1} - p_n \leq 16$.

Found the mistake in one of those lemmas!:

High dimensional geometry is not like low-dimensional geometry.

The GPY story, II

In 2004, Ben Green (postdoc at UBC) came to U de M for a visit. Working on his first project with Terry Tao on prime patterns

$$p, p+d, p+2d, p+3d.$$

The GPY story, II

In 2004, Ben Green (postdoc at UBC) came to U de M for a visit. Working on his first project with Terry Tao on prime patterns

$$p, p+d, p+2d, p+3d.$$

Stuck on one issue, which he explained to me ... Sieve weights
After some experimenting, I found that Selberg weights might work, and then ...

The GPY story, II

In 2004, Ben Green (postdoc at UBC) came to U de M for a visit. Working on his first project with Terry Tao on prime patterns

$$p, p+d, p+2d, p+3d.$$

Stuck on one issue, which he explained to me ... Sieve weights After some experimenting, I found that Selberg weights might work, and then ... the sieve weights of Goldston and Yildirim provided all the technical details Green and Tao needed.

The GPY story, II

In 2004, Ben Green (postdoc at UBC) came to U de M for a visit. Working on his first project with Terry Tao on prime patterns

$$p, p + d, p + 2d, p + 3d.$$

Stuck on one issue, which he explained to me ... Sieve weights
After some experimenting, I found that Selberg weights might work, and then ... the sieve weights of Goldston and Yildirim provided all the technical details Green and Tao needed.
Three days later ...

Ben Green and Terry Tao, 2005

There are infinitely many k-term arithmetic progressions of primes.

The GPY story, III

Dan Goldston, Janos Pintz and Cem Yildirim, 2009

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq \sqrt{\log p_n}.$$

The GPY story, III

Dan Goldston, Janos Pintz and Cem Yildirim, 2009

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq \sqrt{\log p_n}.$$

Proof uses Bombieri-Vinogradov Thm (with $x \geq q^{2+\epsilon}$)

The GPY story, III

Dan Goldston, Janos Pintz and Cem Yildirim, 2009

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq \sqrt{\log p_n}.$$

Proof uses Bombieri-Vinogradov Thm (with $x \geq q^{2+\epsilon}$)

Yitang Zhang, 2014

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq 7 \times 10^7.$$

The GPY story, III

Dan Goldston, Janos Pintz and Cem Yildirim, 2009

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq \sqrt{\log p_n}.$$

Proof uses Bombieri-Vinogradov Thm (with $x \geq q^{2+\epsilon}$)

Yitang Zhang, 2014

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq 7 \times 10^7.$$

Proof uses GPY sieve weights but a *version* of the Bombieri-Vinogradov Thm (with $x \geq q^{5/3}$) Very very tough stuff

The GPY story, IV

James Maynard
(CRM-ISM postdoc 2013-14)

Perhaps we can modify the GPY sieve to obtain Zhang's result, and only use Bombieri-Vinogradov? It would be simpler.

The GPY story, IV

James Maynard
(CRM-ISM postdoc 2013-14)

Perhaps we can modify the GPY sieve to obtain Zhang's result, and only use Bombieri-Vinogradov? It would be simpler.

James Maynard, 2015

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq 600.$$

The GPY story, IV

James Maynard
(CRM-ISM postdoc 2013-14)

Perhaps we can modify the GPY sieve to obtain Zhang's result, and only use Bombieri-Vinogradov? It would be simpler.

James Maynard, 2015

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq 600.$$

Also infinitely many primes p_n with

$$p_{n+m} - p_n \leq m^3 e^{3m}.$$

The GPY story, IV

James Maynard
(CRM-ISM postdoc 2013-14)

Perhaps we can modify the GPY sieve to obtain Zhang's result, and only use Bombieri-Vinogradov? It would be simpler.

James Maynard, 2015

There are infinitely many primes p_n with

$$p_{n+1} - p_n \leq 600.$$

Also infinitely many primes p_n with

$$p_{n+m} - p_n \leq m^3 e^{3m}.$$

Very similar results proved at the same time by Terry Tao.

The GPY story, V

And then towards the end of James's year in Montreal:

The GPY story, V

And then towards the end of James's year in Montreal:
We believe if x is suff large then

$$\max_{p_n \le x} p_{n+1} - p_n \ge (\log x)^2.$$

The GPY story, V

And then towards the end of James's year in Montreal:

We believe if x is suff large then

$$\max_{p_n \leq x} p_{n+1} - p_n \geq (\log x)^2.$$

Erdős-Rankin (1930s-60s) proved

$$\max_{p_n \leq x} p_{n+1} - p_n \geq c \log x \frac{\log \log x \log \log \log \log x}{(\log \log \log x)^2}$$

Erdős: \$ 10,000 to prove that one can let $c \to \infty$ as $x \to \infty$.

The GPY story, V

And then towards the end of James's year in Montreal:

We believe if x is suff large then

$$\max_{p_n \leq x} p_{n+1} - p_n \geq (\log x)^2.$$

Erdős-Rankin (1930s-60s) proved

$$\max_{p_n \leq x} p_{n+1} - p_n \geq c \log x \frac{\log\log x \log\log\log\log x}{(\log\log\log x)^2}$$

Erdős: $ 10,000 to prove that one can let $c \to \infty$ as $x \to \infty$.

James Maynard, 2016 + Ford, Green, Konyagn & Tao

$$\max_{p_n \leq x} p_{n+1} - p_n \geq c \log x \frac{\log\log x \log\log\log\log x}{\log\log\log x}$$

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Let $\Omega(n) = \#\{$ prime powers p^e divides $n\}$.

PNT true $\iff$ $\Omega(n)$ is even as often as it is odd.

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Let $\Omega(n) = \#\{$ prime powers p^e divides $n\}$.

PNT true $\iff$ $\Omega(n)$ is even as often as it is odd.

Define

$$\lambda(n) = (-1)^{\Omega(n)} \text{ a multiplicative function.}$$

PNT $\iff$ $\frac{1}{x}\sum_{n\le x}\lambda(n) \to 0$ as $x \to \infty$.

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Let $\Omega(n) = \#\{$ prime powers p^e divides $n\}$.

PNT true $\iff$ $\Omega(n)$ is even as often as it is odd.

Define

$$\lambda(n) = (-1)^{\Omega(n)} \text{ a multiplicative function.}$$

PNT $\iff$ $\frac{1}{x}\sum_{n\leq x}\lambda(n) \to 0$ as $x \to \infty$.

RH $\iff$ $\left|\sum_{n\leq x}\lambda(n)\right| < x^{1/2+\epsilon}$ if x suff large.

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Let $\Omega(n) = \#\{$ prime powers p^e divides $n\}$.

PNT true $\iff$ $\Omega(n)$ is even as often as it is odd.

Define

$$\lambda(n) = (-1)^{\Omega(n)} \text{ a multiplicative function.}$$

PNT $\iff$ $\frac{1}{x}\sum_{n\leq x}\lambda(n) \to 0$ as $x \to \infty$.

RH $\iff$ $\left|\sum_{n\leq x}\lambda(n)\right| < x^{1/2+\epsilon}$ if x suff large.

Can we prove PNT like this without zeros?

Pretentious I

How many primes there are up to x is an elementary question – why does it involve zeros of the *analytic continuation* of $\zeta(s)$?

$\exists$ "ad hoc" proofs of the PNT which do not use zeros, but no coherent theory.

Let $\Omega(n) = \#\{$ prime powers p^e divides $n\}$.

PNT true $\iff$ $\Omega(n)$ is even as often as it is odd.

Define

$$\lambda(n) = (-1)^{\Omega(n)} \text{ a multiplicative function.}$$

PNT $\iff$ $\frac{1}{x}\sum_{n\leq x}\lambda(n) \to 0$ as $x \to \infty$.

RH $\iff$ $\left|\sum_{n\leq x}\lambda(n)\right| < x^{1/2+\epsilon}$ if x suff large.

Can we prove PNT like this without zeros?

Use properties of multiplicative functions!

Pretentious II: Averages of a multiplicative function

A multiplicative function: $f(mn) = f(m)f(n)$.
If each $|f(n)| = 1$, when does average $\to 0$?

Pretentious II: Averages of a multiplicative function

A multiplicative function: $f(mn) = f(m)f(n)$.
If each $|f(n)| = 1$, when does average $\to 0$?

The average does not $\to 0$, for $f(n) = 1$, or $f(n) = n^{it}$:

$$\frac{1}{N}\sum_{n=1}^{N} n^{it} \approx \frac{1}{N}\int_{u=0}^{N} u^{it}du = \frac{1}{N}\cdot\frac{N^{1+it}}{1+it} = \frac{N^{it}}{1+it}$$

Size $\to \frac{1}{|1+it|}$; rotates round the circle of this radius as N increases!

Pretentious II: Averages of a multiplicative function

A multiplicative function: $f(mn) = f(m)f(n)$.
If each $|f(n)| = 1$, when does average $\to 0$?

The average does not $\to 0$, for $f(n) = 1$, or $f(n) = n^{it}$:

$$\frac{1}{N}\sum_{n=1}^{N} n^{it} \approx \frac{1}{N}\int_{u=0}^{N} u^{it} du = \frac{1}{N} \cdot \frac{N^{1+it}}{1+it} = \frac{N^{it}}{1+it}$$

Size $\to \frac{1}{|1+it|}$; rotates round the circle of this radius as N increases!

Other examples: Functions $f(n)$ that are "close" to n^{it} .

Pretentious II: Averages of a multiplicative function

A multiplicative function: $f(mn) = f(m)f(n)$.
If each $|f(n)| = 1$, when does average $\to 0$?

The average does not $\to 0$, for $f(n) = 1$, or $f(n) = n^{it}$:

$$\frac{1}{N}\sum_{n=1}^{N} n^{it} \approx \frac{1}{N}\int_{u=0}^{N} u^{it} du = \frac{1}{N}\cdot\frac{N^{1+it}}{1+it} = \frac{N^{it}}{1+it}$$

Size $\to \frac{1}{|1+it|}$; rotates round the circle of this radius as N increases!

Other examples: Functions $f(n)$ that are "close" to n^{it} .

Gábor Halász (1968)

The only multiplicative function with "large" mean values are those that are "close" to n^{it} for some real t.

Pretentious III – Applying Halász's Theorem

Gábor Halász (1968)

The only multiplicative function with "large" mean values are those that are "close" to n^{it} for some real t.

Remember: PNT $\iff \frac{1}{x}\sum_{n\leq x}\lambda(n)\to 0$ as $x\to\infty$.

Pretentious III – Applying Halász's Theorem

Gábor Halász (1968)

The only multiplicative function with "large" mean values are those that are "close" to n^{it} for some real t.

Remember: PNT $\iff \frac{1}{x}\sum_{n\le x}\lambda(n) \to 0$ as $x \to \infty$.

If PNT does not hold then the mean value of $\lambda(n)$ is "large" and so $\lambda(n)$ is "close" to n^{it} for some real t.

Pretentious III – Applying Halász's Theorem

Gábor Halász (1968)

The only multiplicative function with "large" mean values are those that are "close" to n^{it} for some real t.

Remember: PNT $\iff \frac{1}{x}\sum_{n\leq x}\lambda(n) \to 0$ as $x \to \infty$.

If PNT does not hold then the mean value of $\lambda(n)$ is "large" and so $\lambda(n)$ is "close" to n^{it} for some real t.

But then $1 = \lambda(n)^2$ is "close" to n^{2it}, and so $t = 0$.
This implies $\lambda(n)$ is "close" to $n^{it} = 1$; "obviously" impossible:

Pretentious III – Applying Halász's Theorem

Gábor Halász (1968)

The only multiplicative function with "large" mean values are those that are "close" to n^{it} for some real t.

Remember: PNT $\iff \frac{1}{x}\sum_{n\leq x}\lambda(n) \to 0$ as $x \to \infty$.

If PNT does not hold then the mean value of $\lambda(n)$ is "large" and so $\lambda(n)$ is "close" to n^{it} for some real t.

But then $1 = \lambda(n)^2$ is "close" to n^{2it}, and so $t = 0$.
This implies $\lambda(n)$ is "close" to $n^{it} = 1$; "obviously" impossible:

If $\lambda(n) = (-1)^{\Omega(n)} = 1$ for most n, then $\lambda(2n) = -1$, a contradiction!

Linnik's Theorem (1944)

YURI LINNIK: *There exists a constant L such that any arithmetic progression*

$$a, a+d, a+2d, \ldots$$

with $\gcd(a,d)=1$ *contains a prime* $p = a + nd$ *with* $p \leq d^L$.

Bombieri's 1974 Fields' medal:
Partly for improvement and development of Linnik's proof by developing the "Large sieve".

Linnik's Theorem (1944)

Yuri Linnik: *There exists a constant L such that any arithmetic progression*

$$a, a+d, a+2d, \ldots$$

with $gcd(a, d) = 1$ *contains a prime* $p = a + nd$ *with* $p \leq d^L$.

Bombieri's 1974 Fields' medal:
Partly for improvement and development of Linnik's proof by developing the "Large sieve".

AG-Soundararajan (2009)

20 pg pf of Linnik's Theorem using the "pretentious large sieve".

Linnik's Theorem (1944)

YURI LINNIK: *There exists a constant L such that any arithmetic progression*

$$a, a+d, a+2d, \ldots$$

with $gcd(a, d) = 1$ contains a prime $p = a + nd$ with $p \leq d^L$.

Bombieri's 1974 Fields' medal:
Partly for improvement and development of Linnik's proof by developing the "Large sieve".

AG-Soundararajan (2009)

20 pg pf of Linnik's Theorem using the "pretentious large sieve".

"Repulsion principles": Zeros of polynomials, and of L-functions cannot be close together.

Pretentious IV: AG-Soundararajan: *A pretentious dream*

From 1859 to 2010 the only coherent approach to analytic number theory came through Riemann's zeros.

Could we possibly avoid them?

Pretentious IV: AG-Soundararajan: *A pretentious dream*

From 1859 to 2010 the only coherent approach to analytic number theory came through Riemann's zeros.

Could we possibly avoid them?

Can we prove all the basic theorems of analytic number theory, with no zeros?!

Pretentious IV: AG-Soundararajan: *A pretentious dream*

From 1859 to 2010 the only coherent approach to analytic number theory came through Riemann's zeros.

Could we possibly avoid them?

Can we prove all the basic theorems of analytic number theory, with no zeros?!

Would a new coherent approach be useful?

Pretentious IV: AG-Soundararajan: *A pretentious dream*

From 1859 to 2010 the only coherent approach to analytic number theory came through Riemann's zeros.

Could we possibly avoid them?

Can we prove all the basic theorems of analytic number theory, with no zeros?!

Would a new coherent approach be useful?

Soundararajan (2010) – pretentious subconvexity for L-function values

Quantum unique ergodicity for $SL_2(\mathbb{Z}) \setminus \mathbb{H}$.
(Completed Lindenstrauss's program – 2010 Fields' medal)

Pretentious IV: AG-Soundararajan: *A pretentious dream*

From 1859 to 2010 the only coherent approach to analytic number theory came through Riemann's zeros.

Could we possibly avoid them?

Can we prove all the basic theorems of analytic number theory, with no zeros?!

Would a new coherent approach be useful?

Soundararajan (2010) – pretentious subconvexity for L-function values

Quantum unique ergodicity for $SL_2(\mathbb{Z}) \setminus \mathbb{H}$.
(Completed Lindenstrauss's program – 2010 Fields' medal)

AG-Sound (2011): First draft of a "book" with the new theory

Pretentious shortfalls, # 1

Pretentious shortfalls, # 1

AG-Sound (2011): Theory for all mult functions f with $|f(n)| \leq 1$.

Pretentious shortfalls, # 1

AG-Sound (2011): Theory for all mult functions f with $|f(n)| \leq 1$.

Quantitative problem: Unable to prove strong results for specific f, like error term in PNT.

Pretentious shortfalls, $\#$ 1

AG-Sound (2011): Theory for all mult functions f with $|f(n)| \leq 1$.
Quantitative problem: Unable to prove strong results for specific f, like error term in PNT.

Dimitris Koukoulopoulos
(CRM-ISM postdoc 2010-12)

Determined for which f one can prove sharper results.
Recovered all classical quantitativity.
Koukoulopoulos converse Theorem

Pretentious shortfalls, # 1

AG-Sound (2011): Theory for all mult functions f with $|f(n)| \leq 1$.
Quantitative problem: Unable to prove strong results for specific f, like error term in PNT.

Dimitris Koukoulopoulos
(CRM-ISM postdoc 2010-12)

Determined for which f one can prove sharper results.
Recovered all classical quantitativity.
Koukoulopoulos converse Theorem

Koukoulopoulos, 2013 – Strongest known unconditional PNT

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| \leq c\, x \exp\left(- c' \frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)$$

Pretentious shortfalls, # 2

AG-Sound (2011): Hard to motivate pf of Halász's key Thm.

Pretentious shortfalls, # 2

AG-Sound (2011): Hard to motivate pf of Halász's key Thm.

Adam Harper
(CRM-ISM postdoc 2012-13)

Different, more motivated proof. Ties in better with other modern theoretical developments.

Pretentious shortfalls, # 2

AG-Sound (2011): Hard to motivate pf of Halász's key Thm.

Adam Harper
(CRM-ISM postdoc 2012-13)

Different, more motivated proof. Ties in better with other modern theoretical developments.

Compelled us to rewrite our book from scratch!

Pretentious shortfalls, # 2

AG-Sound (2011): Hard to motivate pf of Halász's key Thm.

Adam Harper
(CRM-ISM postdoc 2012-13)

Different, more motivated proof. Ties in better with other modern theoretical developments.

Compelled us to rewrite our book from scratch!

AG-Harper-Sound, 2019

Explains new theory in 35 pages, including the pretentious large sieve, and proofs of Linnik's Theorem and Hoheisel's Theorem.

Annals of Mathematics **184** (2016), 1–42

Multiplicative functions in short intervals

By Kaisa Matomäki and Maksym Radziwiłł

Dedicated to Andrew Granville

Abstract

We introduce a general result relating "short averages" of a multiplicative function to "long averages" which are well understood. This result has several consequences. First, for the Möbius function we show that there are cancellations in the sum of $\mu(n)$ in almost all intervals of the form $[x, x+\psi(x)]$ with $\psi(x) \to \infty$ arbitrarily slowly. This goes beyond what was

Kaisa Matomäki and Maksym Radziwiłł
(CRM thematic postdocs 2014-15)

Annals of Mathematics **184** (2016), 1–42

Multiplicative functions in short intervals

By Kaisa Matomäki and Maksym Radziwiłł

Dedicated to Andrew Granville

Abstract

We introduce a general result relating "short averages" of a multiplicative function to "long averages" which are well understood. This result has several consequences. First, for the Möbius function we show that there are cancellations in the sum of $\mu(n)$ in almost all intervals of the form $[x, x+\psi(x)]$ with $\psi(x) \to \infty$ arbitrarily slowly. This goes beyond what was

Kaisa Matomäki and Maksym Radziwiłł
(CRM thematic postdocs 2014-15)

2019 *New Horizons in Mathematics* Prize

Pretentious V: The Erdos discrepancy problem, 2015

Paul Erdős and Terry Tao

Let $a_1, a_2, \ldots$ be a sequence of 1's and -1's. The sums

$$a_d + a_{2d} + \ldots + a_{Nd}$$

get arbitrarily big (any d, any N).

Pretentious V: The Erdos discrepancy problem, 2015

Paul Erdős and Terry Tao

Let $a_1, a_2, \ldots$ be a sequence of 1's and -1's. The sums

$$a_d + a_{2d} + \ldots + a_{Nd}$$

get arbitrarily big (any d, any N).
Tao reduces this, via Fourier analysis, to

For any multiplicative f with each $|f(n)| = 1$ prove that

$$f(N+1) + f(N+2) + \ldots + f(N+m)$$

get arbitrarily large "on average".

Pretentious V: The Erdos discrepancy problem, 2015

Paul Erdős and Terry Tao

Let $a_1, a_2, \ldots$ be a sequence of 1's and -1's. The sums

$$a_d + a_{2d} + \ldots + a_{Nd}$$

get arbitrarily big (any d, any N). *Tao reduces this, via Fourier analysis, to*

For any multiplicative f with each $|f(n)| = 1$ prove that

$$f(N+1) + f(N+2) + \ldots + f(N+m)$$

get arbitrarily large "on average".

Using Matomäki-Radziwiłł: If such sums stay small then

f must be n^{it}-pretentious!

Pretentious VI: Tao's question

If f is n^{it}-pretentious, can we get good estimates for

$$f(N+1) + f(N+2) + \ldots + f(N+m) \quad ?$$

Pretentious VI: Tao's question

If f is n^{it}-pretentious, can we get good estimates for

$$f(N+1)+f(N+2)+\ldots+f(N+m) \quad ?$$

Oleksiy Klurman
(U de M PhD student 2014-17)

Uses old-fashioned techniques of Delange from the book to resolve Tao's question

Pretentious VI: Tao's question

If f is n^{it}-pretentious, can we get good estimates for

$$f(N+1)+f(N+2)+\ldots+f(N+m) \quad ?$$

Oleksiy Klurman
(U de M PhD student 2014-17)

Uses old-fashioned techniques of Delange from the book to resolve Tao's question

The subject of multiplicative functions is "out of control". New fantastic preprints every month or two.

Pretentious VI: Tao's question

If f is n^{it}-pretentious, can we get good estimates for

$$f(N+1) + f(N+2) + \ldots + f(N+m) \quad ?$$

Oleksiy Klurman
(U de M PhD student 2014-17)

Uses old-fashioned techniques of Delange from the book to resolve Tao's question

The subject of multiplicative functions is "out of control". New fantastic preprints every month or two.
The main work has been on their correlations, due to Klurman, Mangerel, Matomäki, Radziwiłł, Shao, Tao, Teräväinen, Ziegler, ...

Noblest courage, extraordinary talents and superior genius