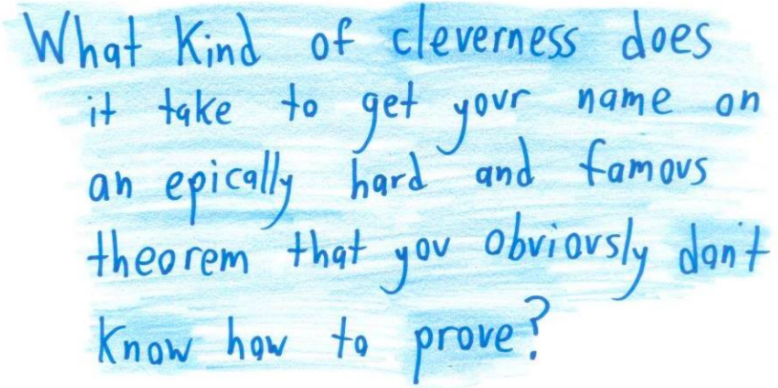
Impact of Women in Number Theory

Allysa Lumley

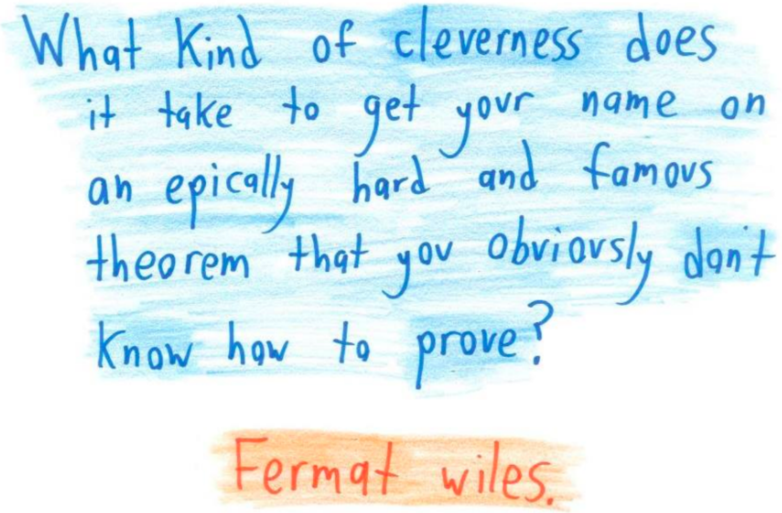
Impact of Women Mathematicians on Research and Education in Mathematics
BIRS 2018

March 17, 2018

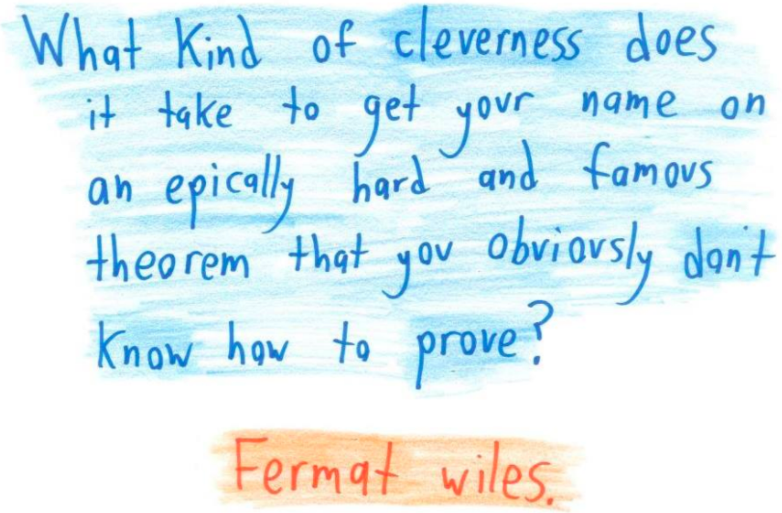
Introduction



Introduction



Introduction



Credit: Math With Bad Drawings

Fermat's Last Theorem

Theorem (1630 ?)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Fermat's Last Theorem

Theorem (1630 ?)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

'Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.'

Pierre de Fermat, ~1630

translated: " It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into two powers of like degree. I have discovered a truly remarkable proof which this margin is too small to contain."

Fermat's Last Theorem (FLT)

Theorem (Wiles 1995)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Fermat's Last Theorem (FLT)

Theorem (Wiles 1995)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Some well known Mathematicians who worked on this 1600's-1900's century:

Fermat's Last Theorem (FLT)

Theorem (Wiles 1995)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Some well known Mathematicians who worked on this 1600's-1900's century:
Fermat, Euler, Legendre, Gauss, Abel, Dirichlet, Kummer and Cauchy.

Fermat's Last Theorem (FLT)

Theorem (Wiles 1995)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Some well known Mathematicians who worked on this 1600's-1900's century:
Fermat, Euler, Legendre, Gauss, Abel, Dirichlet, Kummer and Cauchy.
In 1770, Euler published a proof for the case $n = 3$.

Fermat's Last Theorem (FLT)

Theorem (Wiles 1995)

There are no positive integer solutions to

$$x^n + y^n = z^n, \text{ for all } n > 2.$$

Some well known Mathematicians who worked on this 1600's-1900's century:
Fermat, Euler, Legendre, Gauss, Abel, Dirichlet, Kummer and Cauchy.
In 1770, Euler published a proof for the case $n = 3$.
In 1630's, Fermat himself did prove this for the case $n = 4$.

Progress

Fermat's Last Theorem was eventually broken into two cases: Let p be and odd prime

1. $x^p + y^p = z^p$ has no solutions for which $p \nmid xyz$.

Progress

Fermat's Last Theorem was eventually broken into two cases: Let p be and odd prime

1. $x^p + y^p = z^p$ has no solutions for which $p \nmid xyz$.
2. $x^p + y^p = z^p$ has no solutions for which p divides exactly one of x, y or z.

Progress

Fermat's Last Theorem was eventually broken into two cases: Let p be and odd prime

1. $x^p + y^p = z^p$ has no solutions for which $p \nmid xyz$.
2. $x^p + y^p = z^p$ has no solutions for which p divides exactly one of x, y or z.

Theorem (Germain, 1800's)

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Sophie Germain

Theorem

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Sophie Germain

Theorem

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Found explicit auxiliary primes to show this holds for $p < 100$.

Sophie Germain

Theorem

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Found explicit auxiliary primes
to show this holds for $p < 100$.
Legendre used this idea
to extend it to all $p < 197$.

Sophie Germain Cont'd

Theorem

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Theorem

If p is an odd prime and $q = 2p + 1$ is also prime then p must divide one of x, y or z. Thus, Case 1 of FLT is true.

Sophie Germain Cont'd

Theorem

If p is an odd prime and there exists an auxiliary prime $q = 2pn + 1$ which satisfies

- *there are no consecutive p^{th} power residues modulo q*
- *p is not a p^{th} power reside modulo q,*

then in any solution to $x^p + y^p = z^p$ we have p^2 must divide one of x, y or z. Thus, Case 1 of FLT is true.

Theorem

If p is an odd prime and $q = 2p + 1$ is also prime then p must divide one of x, y or z. Thus, Case 1 of FLT is true.

Primes p satisfying that $2p + 1$ is also prime are called Sophie Germain primes.

FLT - a new attack

Theorem

The positive integers x, y, z satisfying $x^2 + y^2 = z^2$ are described exactly by the following form:

$$x = r(s^2 - t^2), y = 2rst \text{ and } z = r(s^2 + t^2)$$

where $r, s, t \in \mathbb{Z}$

FLT - a new attack

Theorem

The positive integers x, y, z satisfying $x^2 + y^2 = z^2$ are described exactly by the following form:

$$x = r(s^2 - t^2), y = 2rst \text{ and } z = r(s^2 + t^2)$$

where $r, s, t \in \mathbb{Z}$

Lemma

Suppose $gcd(u, v) = 1$ and uv is a perfect square. Then both u and v are perfect squares.

FLT - a new attack

Theorem

The positive integers x, y, z satisfying $x^2 + y^2 = z^2$ are described exactly by the following form:

$$x = r(s^2 - t^2), y = 2rst \text{ and } z = r(s^2 + t^2)$$

where $r, s, t \in \mathbb{Z}$

Lemma

Suppose $gcd(u, v) = 1$ and uv is a perfect square. Then both u and v are perfect squares.

$$y^2 = z^2 - x^2 = (z - x)(z + x)$$

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

$$y^n = z^n - x^n = (z - x)(z^{n-1} + z^{n-2}x + \cdots + zx^{n-2} + x^{n-1})$$

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

$$y^n = z^n - x^n = (z - x)(z^{n-1} + z^{n-2}x + \cdots + zx^{n-2} + x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n = (z - x)(z - \xi x)(z - \xi^2 x) \cdots (z - \xi^{n-1} x)$$

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

$$y^n = z^n - x^n = (z - x)(z^{n-1} + z^{n-2}x + \cdots + zx^{n-2} + x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n = (z - x)(z - \xi x)(z - \xi^2 x) \cdots (z - \xi^{n-1} x)$$

⚠

FLT - a new attack

Why not try the approach used for $x^2+y^2=z^2$ for $x^n+y^n=z^n$ for $n\geq 3$?

$$y^n = z^n - x^n = (z-x)(z^{n-1}+z^{n-2}x+\cdots+zx^{n-2}+x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n = (z-x)(z-\xi x)(z-\xi^2 x)\cdots(z-\xi^{n-1}x)$$

⚠ We are not in $\mathbb{Z}$ anymore!

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

$$y^n = z^n - x^n = (z - x)(z^{n-1} + z^{n-2}x + \cdots + zx^{n-2} + x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n = (z - x)(z - \xi x)(z - \xi^2 x) \cdots (z - \xi^{n-1} x)$$

⚠We are not in $\mathbb{Z}$ anymore! These factors now live in $\mathbb{Z}[\xi]$.

FLT - a new attack

Why not try the approach used for $x^2+y^2=z^2$ for $x^n+y^n=z^n$ for $n\geq 3$?

$$y^n=z^n-x^n=(z-x)(z^{n-1}+z^{n-2}x+\cdots+zx^{n-2}+x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n=(z-x)(z-\xi x)(z-\xi^2 x)\cdots(z-\xi^{n-1}x)$$

⚠ We are not in $\mathbb{Z}$ anymore! These factors now live in $\mathbb{Z}[\xi]$.
What is a prime? Can we factor uniquely? How do you define the notion of a common factor?

FLT - a new attack

Why not try the approach used for $x^2 + y^2 = z^2$ for $x^n + y^n = z^n$ for $n \geq 3$?

$$y^n = z^n - x^n = (z - x)(z^{n-1} + z^{n-2}x + \cdots + zx^{n-2} + x^{n-1})$$

Try over $\mathbb{C}$:

$$y^n = (z - x)(z - \xi x)(z - \xi^2 x) \cdots (z - \xi^{n-1} x)$$

⚠We are not in $\mathbb{Z}$ anymore! These factors now live in $\mathbb{Z}[\xi]$.
What is a prime? Can we factor uniquely? How do you define the notion of a common factor?
Unfortunately, if we consider $n = p > 19$, then for ξ a p^{th} root of unity we have $\mathbb{Z}[\xi]$ the *elements* **do not** have unique factorizations.

Emmy Noether

Next best thing: The ideals of $\mathbb{Z}[\xi]$ do have a unique decomposition

Emmy Noether

Next best thing: The ideals of $\mathbb{Z}[\xi]$ do have a unique decomposition

Studying these spaces and their properties is an active area of research

Emmy Noether

Next best thing: The ideals of $\mathbb{Z}[\xi]$ do have a unique decomposition

Studying these spaces and their properties is an active area of research

All of this was made possible by:

Emmy Noether

Next best thing: The ideals of $\mathbb{Z}[\xi]$ do have a unique decomposition

Studying these spaces and their properties is an active area of research

All of this was made possible by:

Diophantine Equations

The equation $x^n + y^n = z^n$ for any fixed n is an example of a Diophantine equation.

Diophantine Equations

The equation $x^n + y^n = z^n$ for any fixed n is an example of a Diophantine equation.
Ruled as having no positive integer solutions for $n > 2$.

Diophantine Equations

The equation $x^n + y^n = z^n$ for any fixed n is an example of a Diophantine equation.
Ruled as having no positive integer solutions for $n > 2$.
Another simpler example is, given $a, b, c \in \mathbb{Z}$ is it possible to find $x, y \in \mathbb{Z}$ such that

$$ax + by = c?$$

Diophantine Equations

The equation $x^n + y^n = z^n$ for any fixed n is an example of a Diophantine equation.
Ruled as having no positive integer solutions for $n > 2$.
Another simpler example is, given $a, b, c \in \mathbb{Z}$ is it possible to find $x, y \in \mathbb{Z}$ such that

$$ax + by = c?$$

We have a simple algorithm to check if a solution exists: check if $\gcd(a, b) | c$.

Hilbert's 10^{th} Problem

'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.' David Hilbert, 1900

Hilbert's 10$^{\text{th}}$ Problem

'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.' David Hilbert, 1900

The ultimate answer to this question is that it is 'unsolvable'.

Hilbert's 10^{th} Problem

'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.' David Hilbert, 1900

The ultimate answer to this question
is that it is 'unsolvable'.
Julia Robinson formulates a hypothesis
connecting the exponential function
to the problem

Hilbert's 10th Problem

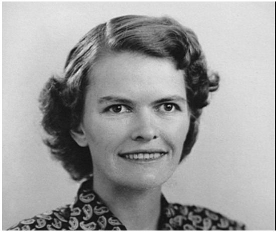
> *'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.'* David Hilbert, 1900

The ultimate answer to this question is that it is 'unsolvable'.
Julia Robinson formulates a hypothesis connecting the exponential function to the problem
Davis and Putnam adapt her ideas using (then open) Green-Tao theorem show that her hypothesis implies the tenth problem is undecidable.

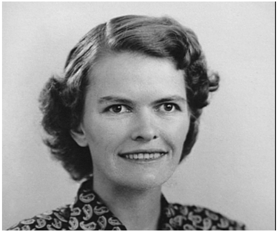
Hilbert's 10^{th} Problem

'Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.' David Hilbert, 1900

The ultimate answer to this question is that it is 'unsolvable'.
Julia Robinson formulates a hypothesis connecting the exponential function to the problem
Davis and Putnam adapt her ideas using (then open) Green-Tao theorem show that her hypothesis implies the tenth problem is undecidable.

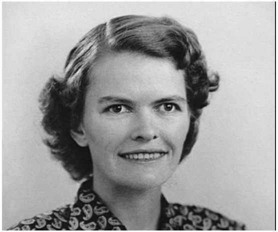


Julia Robinson cont'd



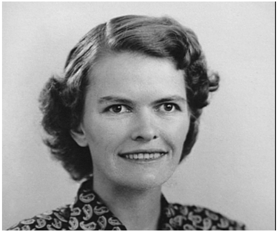
Robinson removes the conditional aspect of Davis and Putnam's work making her hypothesis sufficient

Julia Robinson cont'd



Robinson removes the conditional aspect of Davis and Putnam's work making her hypothesis sufficient
Davis and Putnam show her hypothesis is also necessary

Julia Robinson cont'd

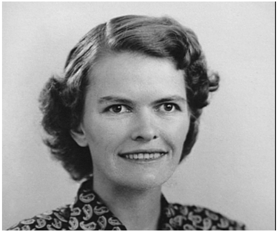


Robinson removes the conditional aspect of Davis and Putnam's work making her hypothesis sufficient

Davis and Putnam show her hypothesis is also necessary

1970 Matiyasevich proves Robinson's hypothesis which at this time was an open question for 20 years.

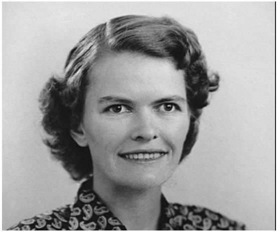
Julia Robinson cont'd



- Robinson removes the conditional aspect of Davis and Putnam's work making her hypothesis sufficient
- Davis and Putnam show her hypothesis is also necessary
- 1970 Matiyasevich proves Robinson's hypothesis which at this time was an open question for 20 years.

Robinson went on to solve many other problems about decidability.

Julia Robinson cont'd



Robinson removes the conditional aspect of Davis and Putnam's work making her hypothesis sufficient

Davis and Putnam show her hypothesis is also necessary

1970 Matiyasevich proves Robinson's hypothesis which at this time was an open question for 20 years.

Robinson went on to solve many other problems about decidability. Recent work of Alexandra Shlapentokh and co-authors generalize Hilbert's 10th problem to rings of integers in special algebraic number fields.

But of course, the primes

Consider

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \\ 0 & \text{otherwise.} \end{cases}$$

But of course, the primes

Consider

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \\ 0 & \text{otherwise.} \end{cases}$$

Trivially we have

$$\left| \sum_{n \leq x} \mu(n) \right| \leq x.$$

But of course, the primes

Consider

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \\ 0 & \text{otherwise.} \end{cases}$$

Trivially we have

$$\left| \sum_{n \le x} \mu(n) \right| \le x.$$

The 'small' improvement

$$\sum_{n \le x} \mu(n) = o(x)$$

But of course, the primes

Consider

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \\ 0 & \text{otherwise.} \end{cases}$$

Trivially we have

$$\left| \sum_{n \le x} \mu(n) \right| \le x.$$

The ‘small’ improvement

$$\sum_{n \le x} \mu(n) = o(x)$$

is equivalent to the prime number theorem:

$$\sum_{n \le x} \Lambda(n) = x + o(x),$$

where $\Lambda(n) = \log p$ if $n = p^k$ and 0 otherwise.

Chowla's conjecture and twin primes

A specialized version of Chowla's conjecture can be stated as:

$$\sum_{n \leq x} \mu(n)\mu(n+2) = o(x).$$

Chowla's conjecture and twin primes

A specialized version of Chowla's conjecture can be stated as:

$$\sum_{n \le x} \mu(n)\mu(n+2) = o(x).$$

This problem has connections to the twin primes conjecture.

Chowla's conjecture and twin primes

A specialized version of Chowla's conjecture can be stated as:

$$\sum_{n \le x} \mu(n)\mu(n+2) = o(x).$$

This problem has connections to the twin primes conjecture.

$$\sum_{n \le x} \Lambda(n)\Lambda(n+2) = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)x + o(x).$$

Chowla's conjecture and twin primes

A specialized version of Chowla's conjecture can be stated as:

$$\sum_{n \le x} \mu(n)\mu(n+2) = o(x).$$

This problem has connections to the twin primes conjecture.

$$\sum_{n \le x} \Lambda(n)\Lambda(n+2) = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)x + o(x).$$

where $\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = 0.66016\ldots$ implies twin primes

Chowla's conjecture and twin primes

A specialized version of Chowla's conjecture can be stated as:

$$\sum_{n \leq x} \mu(n)\mu(n+2) = o(x).$$

This problem has connections to the twin primes conjecture.

$$\sum_{n \leq x} \Lambda(n)\Lambda(n+2) = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) x + o(x).$$

where $\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) = 0.66016\ldots$ implies twin primes and if we have good control on the error term then we obtain the answer to the special case of Chowla's conjecture.

Rising stars

Recently a result of Kaisa Matomäki and Maxsym Radziwiłł has made some significant progress toward Chowla's conjecture.

Rising stars

Recently a result of Kaisa Matomäki and Maxsym Radziwiłł has made some significant progress toward Chowla's conjecture.

Rising stars

Recently a result of Kaisa Matomäki and Maxsym Radziwiłł has made some significant progress toward Chowla's conjecture.

The ideas in their paper are " expected to change the theory of multiplicative functions in a significant way".

Rising stars

Recently a result of Kaisa Matomäki and Maxsym Radziwiłł has made some significant progress toward Chowla's conjecture.

The ideas in their paper are " expected to change the theory of multiplicative functions in a significant way".

In a second paper Matomäki, Radziwiłł and Tao have also made significant progress to a different specialization of Chowla's conjecture.

Rising stars

Recently a result of Kaisa Matomäki and Maxsym Radziwiłł has made some significant progress toward Chowla's conjecture.

The ideas in their paper are " expected to change the theory of multiplicative functions in a significant way".

In a second paper Matomäki, Radziwiłł and Tao have also made significant progress to a different specialization of Chowla's conjecture. "[. . .] the prize notes, that Matomäki and Radziwiłł, through their impressive array of deep results and the powerful new techniques they have introduced, will strongly influence the development of analytic number theory in the future."

Women in Number Theory (WIN)

Women in Number Theory

Women in Number Theory (WIN)

Women in Number Theory

Women in Number Theory

Women in Number Theory (WIN)

Women in Number Theory



Women in Number Theory (WIN)

Women in Number Theory



Thanks for Listening !