Patterns in Primes and Bunyakovsky's Conjecture

Bruno Eaves, Ivan Noden, Ioannis Pantelidakis

Bunyakovsky’s Conjecture

Bunyakovsky's Conjecture

- Prime numbers are largely elusive and functions to generate them are complex and computationally intensive.

Bunyakovsky's Conjecture

- Prime numbers are largely elusive and functions to generate them are complex and computationally intensive.
- However, there is a polynomial $f \in \mathbb{Z}[x]$ such that $f(n)$ is prime for infinitely many $n \in \mathbb{Z}$.

Bunyakovsky's Conjecture

- Prime numbers are largely elusive and functions to generate them are complex and computationally intensive.
- However, there is a polynomial $f \in \mathbb{Z}[x]$ such that $f(n)$ is prime for infinitely many $n \in \mathbb{Z}$.
- Of course, $f(x) = x$.

Bunyakovsky's Conjecture

- Prime numbers are largely elusive and functions to generate them are complex and computationally intensive.
- However, there is a polynomial $f \in \mathbb{Z}[x]$ such that $f(n)$ is prime for infinitely many $n \in \mathbb{Z}$.
- Of course, $f(x) = x$.
- Are there any more?

Bunyakovsky's Conjecture

- Consider the polynomial $p(x) = x^2 + x + 41$

Bunyakovsky's Conjecture

- Consider the polynomial $p(x) = x^2 + x + 41$
- If we calculate its first few values, see that
    - $p(0) = 41$
    - $p(1) = 43$
    - $p(2) = 47$
    - $p(3) = 53$

  are all prime.

Bunyakovsky's Conjecture

- Consider the polynomial $p(x) = x^2 + x + 41$
- If we calculate its first few values, see that
  - $p(0) = 41$
  - $p(1) = 43$
  - $p(2) = 47$
  - $p(3) = 53$

  are all prime.
- It turns out $p(n)$ is prime for all $n \in \{0, \ldots, 39\}$

Bunyakovsky's Conjecture

- Consider the polynomial $p(x) = x^2 + x + 41$
- If we calculate its first few values, see that
    - $p(0) = 41$
    - $p(1) = 43$
    - $p(2) = 47$
    - $p(3) = 53$

  are all prime.
- It turns out $p(n)$ is prime for all $n \in \{0, \ldots, 39\}$
- Even though $p(40)$ is composite, $p(42)$ is prime again.

Bunyakovsky's Conjecture

- Consider the polynomial $p(x) = x^2 + x + 41$
- If we calculate its first few values, see that
  - $p(0) = 41$
  - $p(1) = 43$
  - $p(2) = 47$
  - $p(3) = 53$

  are all prime.
- It turns out $p(n)$ is prime for all $n \in \{0, \ldots, 39\}$
- Even though $p(40)$ is composite, $p(42)$ is prime again.
- Is p prime infinitely often?

Bunyakovsky's Conjecture

- For all $f \in \mathbb{Z}[x]$, do there exist infinitely many $n \in \mathbb{N}$ such that $f(n)$ is prime?

Bunyakovsky's Conjecture

- For all $f \in \mathbb{Z}[x]$, do there exist infinitely many $n \in \mathbb{N}$ such that $f(n)$ is prime?
- No!

Bunyakovsky's Conjecture

- For all $f \in \mathbb{Z}[x]$, do there exist infinitely many $n \in \mathbb{N}$ such that $f(n)$ is prime?
- No!
- If we stick to the convention that prime numbers are positive then since polynomials like $-x^2 + 4$ are only positive for a finite number of natural numbers it can clearly only be prime finitely many times.

Bunyakovsky's Conjecture

- What if f has a positive leading coefficient?

Bunyakovsky's Conjecture

- What if f has a positive leading coefficient?
- No!

Bunyakovsky's Conjecture

- What if f has a positive leading coefficient?
- **No!**
- Consider a polynomial like $2x^2$.
- This will only be prime for $x = 1$ as every other value will be divisible by 2.

Bunyakovsky's Conjecture

- What if f has a positive leading coefficient?
- **No!**
- Consider a polynomial like $2x^2$.
- This will only be prime for $x = 1$ as every other value will be divisible by 2.
- To account for this, we can discount polynomials f where $\gcd(f(1), f(2), \ldots) \neq 1$.
- If this were the case, there must be some prime p such that p divides $f(n)$ for all natural numbers n.
- However, $f(n)$ can only equal p a finite number of times.
- So every other value of $f(n)$ will have p as a proper divisor.

Bunyakovsky's Conjecture

- What if f is also such that $\gcd(f(1), f(2), \dots) = 1$?

Bunyakovsky's Conjecture

- What if f is also such that $\gcd(f(1), f(2), \ldots) = 1$?
- No!

Bunyakovsky's Conjecture

- What if f is also such that $\gcd(f(1), f(2), \ldots) = 1$?
- **No!**
- Consider $f(x) = 2x^4 - 7x^2 + 3 = (x^2 - 3)(2x^2 - 1)$.
- Note then that $f(n)$ can be written as a product of two integers.
- One of these factors can be ± 1 only finitely many times.
- So $f(n)$ can be prime only finitely many times.
- Clearly this is true whenever f is reducible.

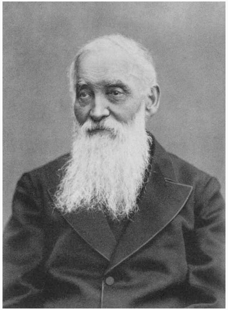
Bunyakovsky's Conjecture

Bunyakovsky's Conjecture

Let $f \in \mathbb{Z}[x]$ be such that

- f is irreducible over $\mathbb{Z}$
- The leading coefficient of f is positive
- $\gcd(f(1), f(2), f(3), \ldots) = 1$

then there are infinitely many $n \in \mathbb{N}$ such that $f(n)$ is prime.



Viktor Bunyakovksy

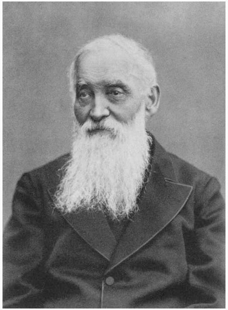
Bunyakovsky's Conjecture

Bunyakovsky's Conjecture

Let $f \in \mathbb{Z}[x]$ be such that

- f is irreducible over $\mathbb{Z}$
- The leading coefficient of f is positive
- $\gcd(f(1), f(2), f(3), \ldots) = 1$

then there are infinitely many $n \in \mathbb{N}$ such that $f(n)$ is prime.



Viktor Bunyakovksy

We believe this to be true but we have only been able to prove so when f is linear. This case is known as Dirichlet's theorem.

Dirichlet's Theorem

Dirichlet's Theorem

- We consider the case $f(x) = mx + a$ with a, m coprime

Dirichlet

Dirichlet's Theorem

- We consider the case $f(x) = mx + a$ with a, m coprime
- See that this case is equivalent to asking if there are infinitely many primes congruent to a mod m

Dirichlet

- We consider the case $f(x) = mx + a$ with a, m coprime
- See that this case is equivalent to asking if there are infinitely many primes congruent to a mod m
- We can prove some cases using a method similar to Euclid's.

Dirichlet

Dirichlet's Theorem

- We consider the case $f(x) = mx + a$ with a, m coprime
- See that this case is equivalent to asking if there are infinitely many primes congruent to a mod m
- We can prove some cases using a method similar to Euclid's.
- How can we do it in general?

Dirichlet

Dirichlet's Theorem

- Let's start simpler, can we prove such primes exist?

Dirichlet's Theorem

- Let's start simpler, can we prove such primes exist?
- Assume it is true, so that, for all coprime integers m and a, there exists a prime congruent to a mod m.
- Fix a pair of coprime integers m_0 and a_0
- There thus exists $x \in \mathbb{Z}$ such that $p = m_0x + a_0$ is prime.
- Note, p and m_0 are coprime so there exists a $y \in \mathbb{Z}$ such that $q = m_0y + p$ is prime.

Dirichlet's Theorem

- Let's start simpler, can we prove such primes exist?
- Assume it is true, so that, for all coprime integers m and a, there exists a prime congruent to a mod m.
- Fix a pair of coprime integers m_0 and a_0
- There thus exists $x \in \mathbb{Z}$ such that $p = m_0 x + a_0$ is prime.
- Note, p and m_0 are coprime so there exists a $y \in \mathbb{Z}$ such that $q = m_0 y + p$ is prime.
- But $q = m_0 y + p = m_0(x + y) + a_0$.
- So, q is another prime congruent to a_0 mod m_0 but different from p.
- It follows by induction that there must be infinitely many primes congruent to a_0 mod m_0.

Dirichlet's Theorem

- Let's start simpler, can we prove such primes exist?
- Assume it is true, so that, for all coprime integers m and a, there exists a prime congruent to a mod m.
- Fix a pair of coprime integers m_0 and a_0
- There thus exists $x \in \mathbb{Z}$ such that $p = m_0 x + a_0$ is prime.
- Note, p and m_0 are coprime so there exists a $y \in \mathbb{Z}$ such that $q = m_0 y + p$ is prime.
- But $q = m_0 y + p = m_0(x + y) + a_0$.
- So, q is another prime congruent to a_0 mod m_0 but different from p.
- It follows by induction that there must be infinitely many primes congruent to a_0 mod m_0.
- Thus, if $f(x) = mx + a$ is prime once then it is prime infinitely often.

Dirichlet’s Theorem

- To illustrate how the proof works, we will prove there are infinitely many primes.

Dirichlet's Theorem

- To illustrate how the proof works, we will prove there are infinitely many primes.
- We can write

$$\sum_{n \in \mathbb{N}} \frac{1}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

- Taking logarithms and manipulating we get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \sum_{n \in \mathbb{N}} \frac{1}{n^s} + g(s)$$

- RHS diverges as $s \to 1$ so LHS must as well, thus there are infinitely many primes

Dirichlet's Theorem

- To illustrate how the proof works, we will prove there are infinitely many primes.
- We can write

$$\sum_{n \in \mathbb{N}} \frac{1}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

- Taking logarithms and manipulating we get

$$\sum_{p \text{ prime}} \frac{1}{p^s} = \log \sum_{n \in \mathbb{N}} \frac{1}{n^s} + g(s)$$

- RHS diverges as $s \to 1$ so LHS must as well, thus there are infinitely many primes
- In a similar way, we can show that the series

$$\sum_{\substack{p \equiv a \bmod m \\ p \text{ prime}}} \frac{1}{p^s}$$

  diverges as $s \to 1$, proving Dirichlet's theorem.

Green-Tao Theorem

- Recall, we found $p(x) = x^2 + x + 41$ was prime for its first 40 values.
- Now we know linear polynomials are prime infinitely often, can we beat that?

Green-Tao Theorem

- Recall, we found $p(x) = x^2 + x + 41$ was prime for its first 40 values.
- Now we know linear polynomials are prime infinitely often, can we beat that?

Green-Tao Theorem

For all $k \in \mathbb{N}$ there exists $f \in \mathbb{Z}[x]$ linear such that $f(n)$ is prime for all $n \in \{0, \ldots, k-1\}$.

Green-Tao Theorem

- For example, if $k = 10$ we can consider $f(x) = 210x + 199$

Green-Tao Theorem

- For example, if $k = 10$ we can consider $f(x) = 210x + 199$
- The coefficients grow very quickly as k increases
- The 'smallest' they can be for $k = 20$ is $18846497670x + 214861583621$

Green-Tao Theorem

- For example, if $k = 10$ we can consider $f(x) = 210x + 199$
- The coefficients grow very quickly as k increases
- The 'smallest' they can be for $k = 20$ is $18846497670x + 214861583621$
- We expect the last prime in the sequence should be around

$$\left(\frac{k}{2}e^{-\gamma}\right)^{k/2}$$

where $\gamma = \lim_{n\to\infty}(-\log n + 1 + \frac{1}{2} + \cdots + \frac{1}{n})$

Green-Tao Theorem

- For example, if $k = 10$ we can consider $f(x) = 210x + 199$
- The coefficients grow very quickly as k increases
- The 'smallest' they can be for $k = 20$ is $18846497670x + 214861583621$
- We expect the last prime in the sequence should be around

$$\left(\frac{k}{2}e^{-\gamma}\right)^{k/2}$$

  where $\gamma = \lim_{n\to\infty}(-\log n + 1 + \frac{1}{2} + \cdots + \frac{1}{n})$
- So if f were to beat $x^2 + x + 41$ and $f(40)$ was prime then $f(40)$ would be around 4.9×10^{29}
- For comparison, there are roughly 7×10^{27} atoms in a human body

Green-Tao Theorem

One final remark:

- Suppose $mx + a$ is prime for the first k^d values
- Then $mx^d + a$ is prime for the first k values

Schinzel's Conjecture

Schinzel's Conjecture

Schinzel's Conjecture

Let $\{f_1, f_2, \ldots, f_k\}$ be a finite set of non-constant, irreducible polynomials over $\mathbb{Z}$ with positive leading coefficients such that there does not exist a prime p where p divides $f_1(n) \cdots f_k(n)$ for all $n \in \mathbb{N}$.

Then there are infinitely many $n \in \mathbb{Z}$ such that $f_1(n), \ldots, f_k(n)$ are all prime.

Andrzej Schinzel

This final condition prevents counter-examples such as $\{x, x+1\}$ where 2 always divides $x(x+1)$.

Schinzel's Conjecture

Schinzel's conjecture generalises many pre-existing conjectures related to patterns in primes. In particular that there exist infinitely many pairs of

- Sophie Germain primes: $\{x, 2x+1\}$

Sophie Germain

Schinzel's Conjecture

Schinzel's conjecture generalises many pre-existing conjectures related to patterns in primes. In particular that there exist infinitely many pairs of

- Sophie Germain primes: $\{x, 2x+1\}$
- Sexy prime: $\{x, x+6\}$

Sophie Germain

Schinzel's Conjecture

Schinzel's conjecture generalises many pre-existing conjectures related to patterns in primes. In particular that there exist infinitely many pairs of

- Sophie Germain primes: $\{x, 2x + 1\}$
- Sexy prime: $\{x, x + 6\}$
- Cousin primes: $\{x, x + 4\}$

Sophie Germain

Schinzel's Conjecture

Schinzel's conjecture generalises many pre-existing conjectures related to patterns in primes. In particular that there exist infinitely many pairs of

- Sophie Germain primes: $\{x, 2x + 1\}$
- Sexy prime: $\{x, x + 6\}$
- Cousin primes: $\{x, x + 4\}$
- Twin primes: $\{x, x + 2\}$

Sophie Germain

Twin Prime Conjecture

- The last few examples had the form $\{x, x + c\}$ for some $c \in \mathbb{N}$ even

Twin Prime Conjecture

- The last few examples had the form $\{x, x + c\}$ for some $c \in \mathbb{N}$ even
- The dream is to prove the twin prime conjecture, that is the case when $c = 2$.

Twin Prime Conjecture

- The last few examples had the form $\{x, x + c\}$ for some $c \in \mathbb{N}$ even
- The dream is to prove the twin prime conjecture, that is the case when $c = 2$.
- In 2013, Zhang proved there exists some $c < 70$ million for which the statement holds
- With some tweaking of Zhang's work, the bound was able to be reduced to 20 million
- Polymath8 reduced this further to 4680
- New methods by Tao and Maynard independently reduced this bound to 246

Twin Prime Conjecture

- It seems very intuitive that there should be infinitely many twin primes

Twin Prime Conjecture

- It seems very intuitive that there should be infinitely many twin primes
- Many primes we often encounter (3 and 5, 11 and 13) are twin primes
- The smallest pair greater than a billion is $1,000,000,007$ and $1,000,000,009$

Twin Prime Conjecture

- It seems very intuitive that there should be infinitely many twin primes
- Many primes we often encounter (3 and 5, 11 and 13) are twin primes
- The smallest pair greater than a billion is $1,000,000,007$ and $1,000,000,009$
- How often do they occur?

Hardy-Littlewood Conjecture

- By the prime number theorem, the number of primes less than n is asymptotic to

$$\frac{n}{\log n}$$

- So we may expect the number of primes p such that $p + 2$ is prime to be asymptotic to

$$\frac{n}{(\log n)^2}$$

Hardy-Littlewood Conjecture

- By the prime number theorem, the number of primes less than n is asymptotic to

$$\frac{n}{\log n}$$

- So we may expect the number of primes p such that $p+2$ is prime to be asymptotic to

$$\frac{n}{(\log n)^2}$$

- This clearly can't be true as the same argument would apply to p and $p+1$

Hardy-Littlewood Conjecture

- The issue is p being prime and $p + 2$ being prime are dependent events so we need to correct for this.

- The issue is p being prime and $p+2$ being prime are dependent events so we need to correct for this.
- We introduce the constant

$$C = 2 \prod_{\substack{q \text{ prime} \\ q \geq 3}} \frac{1 - 2/q}{(1 - 1/q)^2} = 1.3203236316\ldots$$

which takes into account the probability that p and $p+2$ have common divisors.

Hardy-Littlewood Conjecture

Hardy-Littlewood Conjecture

The number of pairs of primes p and $p+2$ less than or equal to $n \in \mathbb{N}$ is asymptotic to

$$C\frac{n}{(\log n)^2}$$

Hardy-Littlewood Conjecture

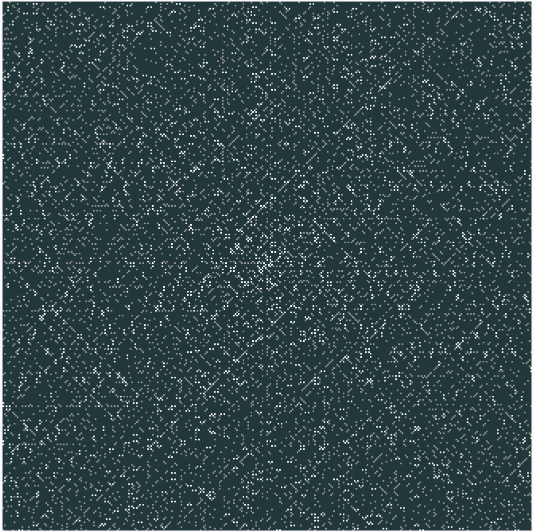
Hardy-Littlewood Conjecture

The number of pairs of primes p and $p + 2$ less than or equal to $n \in \mathbb{N}$ is asymptotic to

$$C \frac{n}{(\log n)^2}$$

- There are 8 twin primes less than 100, our estimate precicts there to be roughly 6.225, a 22% error.
- There are $3, 424, 506$ twin primes less than a billion, our estimate predicts there to be roughly $3, 074, 425$, a 10% error.

Ulam Spiral



Conclusion

- Like Schinzel's, Bunyakovsky's and the Twin Prime Conjecture, the Hardy-Littlewood Conjecture seems almost certainly true yet we seem far from proving it
- It seems easy for us to recognise patterns among the primes but the truth behind them is far more elusive

Questions?