Twin primes and their kin

Lola Thompson

Oberlin College

March 31, 2017

The “building blocks” of integers

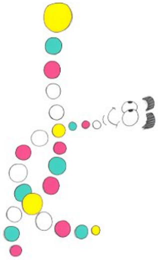


Figure: “D.N.A., the building blocks of life.” - Jurassic Park

Definition

A positive integer is *prime* if it is only divisible by 1 and itself.

Why do we care about primes?

Primes are the “building blocks” of integers: every positive integer (except 1) can be written uniquely as a product of primes.

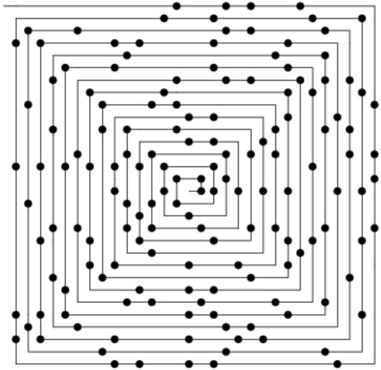
A pattern in the primes?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Table: primes $p \leq 100$

A pattern in the primes?

One often hears that the primes are **randomly distributed**, or seem to have no pattern.



Cautionary tale #1

In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n} + 1$ (where $n = 0, 1, 2, 3, 4, \ldots$) are prime.

Cautionary tale #1

In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n}+1$ (where $n = 0, 1, 2, 3, 4,\ldots$) are prime.

In 1732, Euler showed that Fermat's conjecture fails when $n = 5$.

Cautionary tale #1

In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n} + 1$ (where $n = 0, 1, 2, 3, 4, \ldots$) are prime.

In 1732, Euler showed that Fermat's conjecture fails when $n = 5$.

As of 2010, it is known that $2^{2^n} + 1$ is composite for $5 \leq n \leq 32$.

Cautionary tale #1

In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n}+1$ (where $n = 0, 1, 2, 3, 4, \ldots$) are prime.

In 1732, Euler showed that Fermat's conjecture fails when $n = 5$.

As of 2010, it is known that $2^{2^n}+1$ is composite for $5 \leq n \leq 32$.

Some mathematicians have even conjectured that $2^{2^n}+1$ is composite for all $n \geq 5$!

Cautionary tale #2

From Wikipedia (now deleted): Sollog is "an American numerologist, mystic, and self-proclaimed psychic. He is also a self-published author and a self-described artist, musician, poet, and filmmaker."

Cautionary tale #2

(This is his mugshot from a Florida police station.)

Why it is important to ask the right questions...

One of Sollog's mathematical "discoveries":

1	**2**
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18

Why it is important to ask the right questions...

Another mathematical "discovery" of Sollog:

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54

Sollog does not take criticism well...

My co-author, Paul Pollack, tried to help Sollog. Here was Sollog's response:

> *Hey MORON, This chart is a visual aid to show WHERE ALL PRIMES... MUST FALL, which means they follow a [expletive deleted] PREDICTABLE PATTERN*
> *Since youre a MORON, you cant comprehend what I posted...*
> *If you think that is no big deal, reread your math book, it will state either Primes are random or there is no known pattern.*

What is wrong with Sollog's "pattern"?

1	**2**
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18

Table: Pattern: (almost) all primes are odd!

What is wrong with Sollog's "pattern"?

1	**2**
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18

Table: Pattern: (almost) all primes are odd!

(This is not a deep fact...)

What is wrong with Sollog's "pattern"?

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54

Table: Pattern: Only two of the six columns contain primes

What is wrong with Sollog's "pattern"?

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54

Table: Pattern: Only two of the six columns contain primes

Notice:
$6n+2 = 2(3n+1), 6n+3 = 3(2n+1), 6n+4 = 2(3n+2)$ and $6n+6 = 6(n+1)$.

Sollog's "theorem"

Theorem (Sollog's theorem restated)

If $n \geq 5$ is prime, then n is not a multiple of 2 or 3.

Sollog's "theorem"

Theorem (Sollog's theorem restated)

If $n \geq 5$ is prime, then n is not a multiple of 2 or 3.

Conclusion: It's important to be a bit skeptical when looking for patterns in the primes.

Distribution of primes

How many primes are there?

Theorem

There are infinitely many primes.

Proof Sketch: It suffices to show that

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots = \infty.$$

The proof uses the Taylor series expansion for $\ln(x)$ as well as the sum of a geometric series!

What proportion of numbers are prime?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Table: primes $p \leq 100$

What proportion of numbers are prime?

Prime number theorem
(illustrated by selected values n from 10^2 to 10^{14})

n	$\pi(n)$ = number of primes less than or equal to n	$\frac{\pi(n)}{n}$ = proportion of primes among the first n numbers	$\frac{1}{\log n}$ = predicted proportion of primes among the first n numbers
10^2	25	0.2500	0.2172
10^4	1,229	0.1229	0.1086
10^6	78,498	0.0785	0.0724
10^8	5,761,455	0.0570	0.0543
10^{10}	455,052,511	0.0455	0.0434
10^{12}	37,607,912,018	0.0377	0.0362
10^{14}	3,204,941,750,802	0.0320	0.0310

Distribution of primes

Theorem (Hadamard & de la Valée Poussin, 1896)

Let $\pi(X) = \#$ *of primes in* $[1, X]$. *Then, we have*

$$\lim_{X \to \infty} \frac{\pi(X)}{X/\log X} = 1.$$

Twin primes

A legitimate pattern?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Table: twin primes $p \leq 100$

Twin primes

Definition

A pair of primes $(p, p+2)$ is called a *twin prime pair.*

Examples:

$(3, 5)$
$(5, 7)$
$(11, 13)$
$(3756801695685 \cdot 2^{666,669} - 1,\ 3756801695685 \cdot 2^{666,669} + 1)$

This begs the question: How many twin prime pairs are there?

Gaps between primes: a brief history

Conjecture (de Polignac, 1849)

For even integers h, there are infinitely many pairs of (consecutive) primes $p, p + h$.

If $h = 2$ then this is the twin primes conjecture. We can study other values of h as well!

A close call

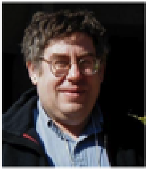
In 2003, Dan Goldston and Cem Yıldırım announced a proof that there are infinitely many pairs of primes that differ by at most 12.

A close call

In 2003, Dan Goldston and Cem Yıldırım announced a proof that there are infinitely many pairs of primes that differ by at most 12. Unfortunately, their work was quickly discredited by Granville and Soundararajan, who found a fatal flaw.

A conditional proof of the bounded gaps theorem

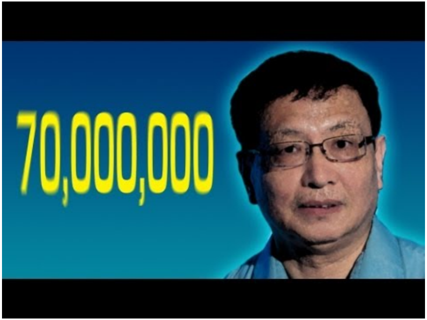
G P Y



Theorem (Goldston, Pintz and Yıldırım, 2005)

If [Big Unsolved Conjecture] is true, then there are infinitely many pairs of primes that differ by at most 16.

Bounded gaps between primes (at last!)



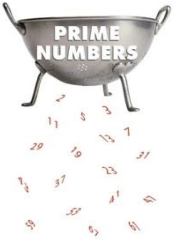
Theorem (Zhang, May 2013)

There are infinitely many pairs of primes that are at most $70,000,000$ *apart.*

An unlikely superhero

- Zhang was unable to secure an academic position after earning his Ph.D.
- Instead, he spent 5 years doing odd jobs ("sandwich artist" at Subway, motel employee in Kentucky, delivery worker in a New York City restaurant) before taking an adjunct position at the University of New Hampshire.
- Zhang had only written two other papers during his mathematical career.
- Zhang was in his late 50's when he made his groundbreaking discovery.

Key idea: sieve methods



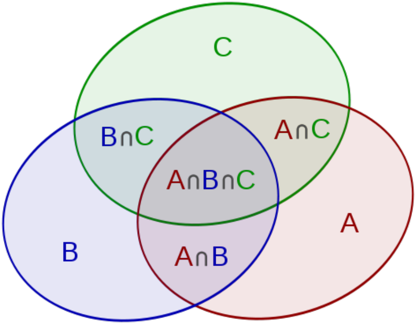
In number theory, a technique called "sieving" is used to filter numbers that possess certain properties out of a larger list of numbers.

The sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Another sieve: inclusion-exclusion



$$\begin{aligned}\#(A \cup B \cup C) = &\#A + \#B + \#C \\ &- \#(A \cap B) - \#(B \cap C) - \#(C \cap A) \\ &+ \#(A \cap B \cap C)\end{aligned}$$

An inclusion-exclusion example

Q: How many integers in $[1, 100]$ are not divisible by $2, 3$ or 5?

$A = \{n \in \mathbb{Z} : 2 \mid n\}, B = \{n \in \mathbb{Z} : 3 \mid n\}, C = \{n \in \mathbb{Z} : 5 \mid n\}.$

$$\#A = \lfloor 100/2 \rfloor = 50.$$

$$\#B = \lfloor 100/3 \rfloor = 33.$$

$$\#C = \lfloor 100/5 \rfloor = 20.$$

$$\#(A \cap B) = \lfloor 100/6 \rfloor = 16.$$

$$\#(B \cap C) = \lfloor 100/15 \rfloor = 6.$$

$$\#(C \cap A) = \lfloor 100/10 \rfloor = 10.$$

$$\#(A \cap B \cap C) = \lfloor 100/30 \rfloor = 3.$$

A: $100 - (50 + 33 + 20 - 16 - 6 - 10 + 3) = 26.$

An application of inclusion-exclusion

Theorem

The number of twin prime pairs $(p, p+2)$ *with* $p \leq X$ *is bounded above by*

$$100X/(\log X)^2$$

for large X.

An application of inclusion-exclusion

Theorem

The number of twin prime pairs $(p, p+2)$ with $p \leq X$ is bounded above by

$$100X/(\log X)^2$$

for large X.

Consequence:

$$B := \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots<\infty.$$

An application of inclusion-exclusion

Theorem

The number of twin prime pairs $(p, p+2)$ with $p \leq X$ is bounded above by

$$100X/(\log X)^2$$

for large X.

Consequence:

$$B := \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots < \infty.$$

Contrast this with our proof that there are infinitely many primes:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots=\infty.$$

The GPY sieve

Goldston, Pintz and Yildirim developed a new sieve that is now referred to as the "GPY sieve." It detects lists of numbers that are plausible candidates for having prime pairs in them.

It gets rid of most numbers, keeping only those that are:

1. Likely to be prime

The GPY sieve

Goldston, Pintz and Yildirim developed a new sieve that is now referred to as the "GPY sieve." It detects lists of numbers that are plausible candidates for having prime pairs in them.

It gets rid of most numbers, keeping only those that are:

1. Likely to be prime
2. Closer together than average.

The only hideous technical slide (I promise!)

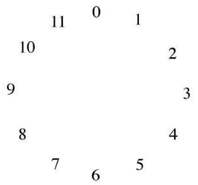
Here is how the GPY sieve actually works:

$$S(N) := \sum_{\substack{N \leq n < 2N \\ n \equiv \nu \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i) \right) w(n),$$

where $\chi_{\mathbb{P}}(n)$ is the characteristic function of the primes and the $w(n)$'s are nonnegative weights.

Prime k-tuples

"Clock" arithmetic



Definition

We say that $a \equiv b \pmod{m}$ if a and b have the same remainder when divided by m.

Example: Telling time on an analog clock:

$13 \equiv 1 \pmod{12}$, $14 \equiv 2 \pmod{12}$, $15 \equiv 3 \pmod{12}$, etc.

Admissible sets

Definition

We say that a k-tuple $(h_1, ..., h_k)$ of nonnegative integers is *admissible* if it doesn't cover all of the possible remainders (mod p) for any prime p.

Example: $(0, 2, 6, 8, 12)$ is an admissible 5-tuple.

Remainders not covered:

$1 \pmod 2$
$1 \pmod 3$
$4 \pmod 5$
$3 \pmod 7$
$3 \pmod{11}$

Prime k-tuples

Conjecture (Prime k-tuples)

Let $\mathcal{H} = (h_1, \ldots, h_k)$ be admissible. Then there are infinitely many integers n such that all of $n + h_1, \ldots, n + h_k$ are prime.

Q: Why do we need to specify that $\mathcal{H}$ is an admissible set?

Prime k-tuples

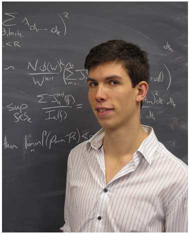
Conjecture (Prime k-tuples)

Let $\mathcal{H} = (h_1, ..., h_k)$ be admissible. Then there are infinitely many integers n such that all of $n + h_1$,...,$n + h_k$ are prime.

Q: Why do we need to specify that $\mathcal{H}$ is an admissible set?

A: If $\mathcal{H}$ "covers" all residues modulo p then one of $n + h_1$,...,$n + h_k$ **must** be divisible by p!

Maynard and Tao's independent work



Theorem (Maynard-Tao, November 2013)

Let $m \geq 2$. For any admissible k-tuple $(h_1, ..., h_k)$ with k "sufficiently large," there are infinitely many n such that at least m of $n + h_1, ..., n + h_k$ are prime.

The power of crowdsourcing...

Theorem (D. H. J. Polymath, February 2014)

There are infinitely many pairs of primes that are at most 246 *apart.*

A polynomial analogue

The "building blocks" of polynomials

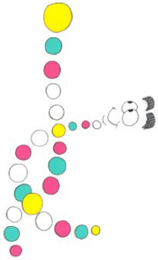


Figure: "D.N.A., the building blocks of life." - Jurassic Park

Recall: primes are the "building blocks" of integers.

What are the "building blocks" of polynomials?

The "building blocks" of polynomials

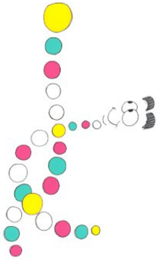


Figure: "D.N.A., the building blocks of life." - Jurassic Park

Recall: primes are the "building blocks" of integers.

What are the "building blocks" of polynomials?

Polynomials that cannot be factored any further. These are called *irreducible polynomials*.

The "building blocks" of polynomials

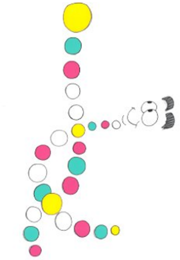


Figure: "D.N.A., the building blocks of life." - Jurassic Park

Recall: primes are the "building blocks" of integers.

What are the "building blocks" of polynomials?

Polynomials that cannot be factored any further. These are called *irreducible polynomials*.

Example

$x^3 - 1 = (x - 1)(x^2 + x + 1)$.

Polynomial arithmetic

Just like with integers, we can reduce polynomials (mod p).

Example:

$$4x^2 + 5x + 1 \equiv \qquad \pmod 3.$$
$$\equiv \qquad \pmod 3$$

Notation: $\mathbb{Z}_p$ is the set of integers (mod p).
$\mathbb{Z}_p[x]$ is the set of polynomials (mod p).

Polynomial arithmetic

Just like with integers, we can reduce polynomials (mod p).

Example:

$$\begin{aligned} 4x^2 + 5x + 1 &\equiv x^2 + 2x + 1 \pmod 3. \\ &\equiv \qquad\qquad\qquad \pmod 3 \end{aligned}$$

Notation: $\mathbb{Z}_p$ is the set of integers (mod p).
$\mathbb{Z}_p[x]$ is the set of polynomials (mod p).

Polynomial arithmetic

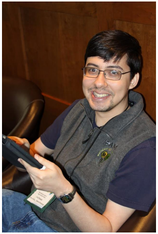
Just like with integers, we can reduce polynomials (mod p).

Example:

$$\begin{aligned} 4x^2 + 5x + 1 &\equiv x^2 + 2x + 1 \pmod 3. \\ &\equiv (x+1)^2 \pmod 3 \end{aligned}$$

Notation: $\mathbb{Z}_p$ is the set of integers (mod p).
$\mathbb{Z}_p[x]$ is the set of polynomials (mod p).

Twin prime polynomials: A tale of two dissertations

Theorem (Hall, Ph.D. 2006; Pollack, Ph.D. 2008)

If $p \geq 3$, then any $a \in \mathbb{Z}_p$ (excluding $a = 0$) occurs infinitely often as a gap between irreducible polynomials.

($p > 3$ due to Hall; $p = 3$ due to Pollack)

An improvement on Hall and Pollack's work

Theorem (Castillo, Hall, Lemke Oliver, Pollack, T., 2014)

Let $m \geq 2$. For any admissible k-tuple $(h_1, ..., h_k)$ of polynomials in $\mathbb{Z}_p[x]$ with k "sufficiently large," there are infinitely many $f \in \mathbb{Z}_p[x]$ such that at least m of $f + h_1, ..., f + h_k$ are irreducible.

Thank you!