(Mind the) gaps between primes

Lola Thompson

Utrecht University

January 9, 2021
The “building blocks” of integers

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.

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

A pattern in the primes?
Distribution of primes
Twin primes
Sieves in number theory
Prime k-tuples
A polynomial analogue
Other applications
A pattern in the primes?

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

Table: primes $p \leq 100$
One often hears that the primes are \textit{randomly distributed}, or seem to have no pattern.
In 1650, Fermat famously conjectured that all numbers of the form $2^{2n} + 1$ (where $n = 0, 1, 2, 3, 4,...$) are prime.
In 1650, Fermat famously conjectured that all numbers of the form $2^{2n} + 1$ (where $n = 0, 1, 2, 3, 4, \ldots$) are prime.

In 1732, Euler showed that Fermat’s conjecture fails when $n = 5$. 
In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n} + 1$ (where $n = 0, 1, 2, 3, 4, ...$) 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 $5 \leq n \leq 32$. 
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 $n \geq 5$!
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.”
One of Sollog’s mathematical “discoveries”:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>
Another mathematical “discovery” of Sollog:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>38</td>
<td>39</td>
<td>40</td>
<td>41</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>50</td>
<td>51</td>
<td>52</td>
<td>53</td>
<td>54</td>
<td></td>
</tr>
</tbody>
</table>
What is wrong with Sollog’s “pattern”?

Table: Pattern: (almost) all primes are odd!
What is wrong with Sollog’s “pattern”?

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>

(This is not a deep fact...)

(Mind the) gaps between primes

Lola Thompson

A pattern in the primes?

Distribution of primes

Twin primes

Sieves in number theory

Prime \(k\)-tuples

A polynomial analogue

Other applications
What is wrong with Sollog’s “pattern”? 

Table: Pattern: Only two of the six columns contain primes
What is wrong with Sollog’s “pattern”?  

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

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

Notice:

\[ 6n + 2 = 2(3n + 1), \quad 6n + 3 = 3(2n + 1), \quad 6n + 4 = 2(3n + 2) \]
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.
Gaps between primes

Lola Thompson

A pattern in the primes?

Distribution of primes

Twin primes

Sieves in number theory

Prime $k$-tuples

A polynomial analogue

Other applications
How many primes are there?

Theorem

There are infinitely many primes.

Proof.
Theorem

_There are infinitely many primes._

Proof.

Suppose that there are only finitely many primes. Then we can write down the complete list: \( p_1, \ldots, p_k \).
How many primes are there?

**Theorem**

There are infinitely many primes.

**Proof.**

Suppose that there are only finitely many primes. Then we can write down the complete list: \( p_1, \ldots, p_k \). Let

\[ n = p_1 \cdot p_2 \cdots p_k + 1. \]
How many primes are there?

**Theorem**

*There are infinitely many primes.*

**Proof.**

Suppose that there are only finitely many primes. Then we can write down the complete list: \( p_1, \ldots, p_k \). Let

\[
n = p_1 \cdot p_2 \cdots p_k + 1.
\]

Then \( n > 1 \), so \( n \) is either prime or a product of primes.
How many primes are there?

**Theorem**

*There are infinitely many primes.*

**Proof.**

Suppose that there are only finitely many primes. Then we can write down the complete list: \( p_1, \ldots, p_k \). Let

\[
  n = p_1 \cdot p_2 \cdots p_k + 1.
\]

Then \( n > 1 \), so \( n \) is either prime or a product of primes. If \( n \) is prime, then we’ve found a new prime that isn’t in our list.
How many primes are there?

**Theorem**

There are infinitely many primes.

**Proof.**

Suppose that there are only finitely many primes. Then we can write down the complete list: $p_1, \ldots, p_k$. Let

$$n = p_1 \cdot p_2 \cdot \cdots p_k + 1.$$ 

Then $n > 1$, so $n$ is either prime or a product of primes. If $n$ is prime, then we’ve found a new prime that isn’t in our list. If $n$ is a product of primes, it must be divisible by a prime that isn’t in our list.
How many primes are there?

**Theorem**

There are infinitely many primes.

**Proof.**

Suppose that there are only finitely many primes. Then we can write down the complete list: \( p_1, \ldots, p_k \). Let 

\[
    n = p_1 \cdot p_2 \cdots p_k + 1.
\]

Then \( n > 1 \), so \( n \) is either prime or a product of primes. If \( n \) is prime, then we’ve found a new prime that isn’t in our list. If \( n \) is a product of primes, it must be divisible by a prime that isn’t in our list. Either way, this contradicts the notion that \( p_1, \ldots, p_k \) is the complete list of primes.
There are MANY ways of proving that there are infinitely many primes! Here’s another approach:

Proof Sketch: It suffices to show that

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots = \infty.$$
What proportion of numbers are prime?

Table: primes $p \leq 100$

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

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

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

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

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

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.
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.
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

![Sieve of Eratosthenes](image)

**Prime numbers**

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>22</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>32</td>
</tr>
<tr>
<td>41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>42</td>
</tr>
<tr>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>61</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>62</td>
</tr>
<tr>
<td>71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>72</td>
</tr>
<tr>
<td>81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>82</td>
</tr>
<tr>
<td>91</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>92</td>
</tr>
<tr>
<td>101</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>102</td>
</tr>
<tr>
<td>111</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>112</td>
</tr>
</tbody>
</table>

(Mind the) gaps between primes

Lola Thompson

A pattern in the primes?

Distribution of primes

Twin primes

Sieves in number theory

Prime \( \kappa \)-tuples

A polynomial analogue

Other applications

40 / 72
Another sieve: inclusion-exclusion

\[ (A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(B \cap C) - \#(C \cap A) + \#(A \cap B \cap C) \]
An inclusion-exclusion example

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

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

\[ \#A = \lfloor 100/2 \rfloor = 50. \]

\[ \#B = \lfloor 100/3 \rfloor = 33. \]

\[ \#C = \lfloor 100/5 \rfloor = 20. \]

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

\[ \#(B \cap C') = \lfloor 100/15 \rfloor = 6. \]

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

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

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

\[
\frac{100X}{(\log X)^2}
\]

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 the second 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
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.
Prime $\kappa$-tuples
It is natural to wonder whether there are infinitely many *tuples* of primes \((p + h_1, \ldots, p + h_k)\).

Some tuples clearly fail:

**Example:** The numbers \(p, p + 2, p + 4\) cannot simultaneously be prime infinitely often.
“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 $(h_1, \ldots, h_k)$ of nonnegative integers is \textit{admissible} if it doesn't cover all of the possible remainders $(\text{mod } p)$ for any prime $p$.

\textbf{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}
Conjecture (Hardy-Littlewood 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.
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.
Theorem (D. H. J. Polymath, February 2014)

There are infinitely many pairs of primes that are at most 246 apart.
A polynomial analogue
Recall: primes are the “building blocks” of integers.

What are the “building blocks” of polynomials?

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

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.

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:

$$4x^2 + 5x + 1 \equiv (\text{mod } 3).$$

$$\equiv (\text{mod } 3)$$

**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:

$$4x^2 + 5x + 1 \equiv x^2 + 2x + 1 \pmod{3}.\]

$$\equiv \quad \pmod{3}$$

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:

\[
4x^2 + 5x + 1 \equiv x^2 + 2x + 1 \pmod{3}.
\]

\[
\equiv (x + 1)^2 \pmod{3}
\]

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

(Mind the) gaps between primes

Lola Thompson

A pattern in the primes?

Distribution of primes

Twin primes

Sieves in number theory

Prime \( k \)-tuples

A polynomial analogue

Other applications

62 / 72

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.

\((p > 3 \text{ due to Hall}; \ p = 3 \text{ due to Pollack})\)
An improvement on Hall and Pollack’s work

(Mind the) gaps between primes

Lola Thompson

A pattern in the primes?

Distribution of primes

Twin primes

Sieves in number theory

Prime \( k \)-tuples

A polynomial analogue

Other applications

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

Let \( m \geq 2 \). For any admissible \( k \)-tuple \( (h_1, \ldots, h_k) \) 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 \( f + h_1, \ldots, f + h_k \) are irreducible.
Other applications of the Maynard-Tao method
A pattern in the primes? Distribution of primes
Twin primes
Sieves in number theory
Prime k-tuples
A polynomial analogue
Other applications

Application: digit sums

Definition: Let $s_g(n)$ denote the sum of the base-$g$ digits of $n$.

Example: $s_{10}(523) = 5 + 2 + 3 = 10$
$s_{10}(541) = 5 + 4 + 1 = 10$

Question (Sierpinski, 1961): Are there arbitrarily long runs of consecutive primes $p$ on which $s_g(p)$ is constant, increasing, decreasing?

(Mind the) gaps between primes
Lola Thompson
65 / 72
(Lola Thompson)
Digit sums of consecutive primes

A brief history:
Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.
Digit sums of consecutive primes

A brief history:

- **Sierpinski (1961):** $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.

- **Erdős (1962):** $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitely often.
A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.

- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitely often.

- Sierpinski (1968): Assuming Dickson’s prime $k$-tuples conjecture, $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$ infinitely often.
Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): \( s_{10}(p_n) < s_{10}(p_{n+1}) \) infinitely often.

- Erdős (1962): \( s_{10}(p_n) > s_{10}(p_{n+1}) \) infinitely often.

- Sierpinski (1968): Assuming Dickson’s prime \( k \)-tuples conjecture, \( s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2}) \) infinitely often.

- Schinzel (unpublished claim): Assuming Hypothesis H, there are arbitrarily long runs of consecutive \( p \) on which \( s_{10}(p) \) is increasing (decreasing).
Digit sums of consecutive primes

Theorem (Pollack, T., 2015)

*For any base* $g$, there are arbitrarily long runs of consecutive primes $p$ on which $s_g(p)$ is constant/increasing/decreasing.
Thank you!