Primes, partitions and power series

Mathematical truths and proofs from Euclid to Ramanujan

Mark Wildon

Royal Holloway, University of London

Heilbronn Institute for Mathematical Research, Bristol University

Primes, partitions and power series

Mathematical truths and proofs from Euclid to Ramanujan

Mark Wildon

Spot the prime. Spot the Grothendieck prime.

Spot the prime. Spot the Grothendieck prime.

- 31 is prime

Spot the prime. Spot the Grothendieck prime.

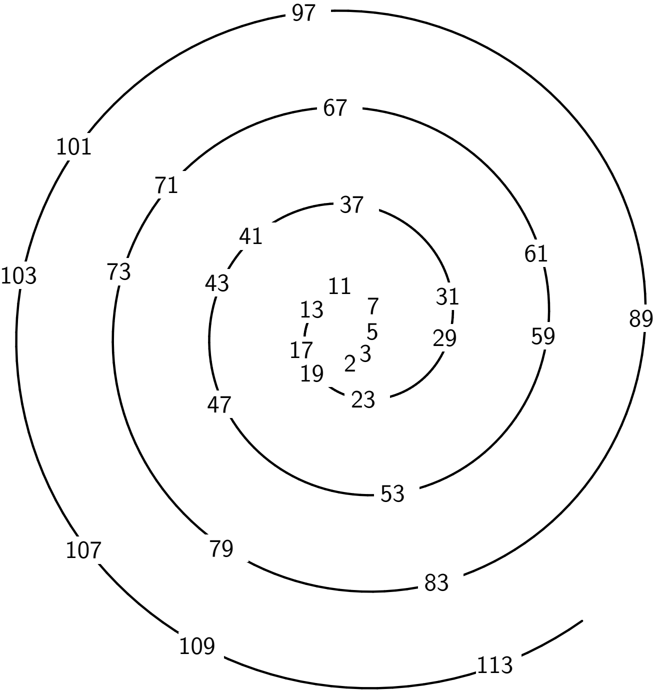
- 31 is prime
- 57 was, allegedly, given as an example of a prime by the great mathematician Alexander Grothendieck.

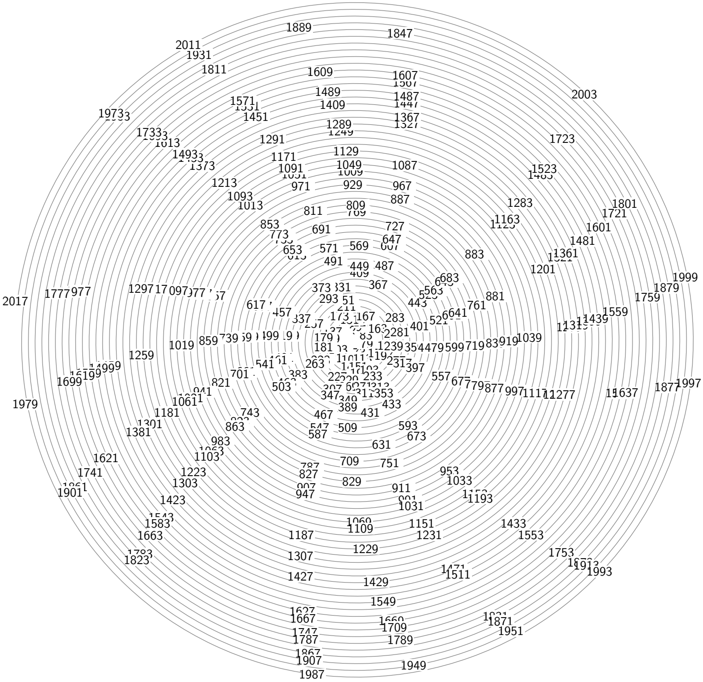
1 is not a prime

1 is not a prime — says who?

1 is not a prime — says who?

Since we want unique factorization, and not $57 = 3 \times 19 = 1 \times 3 \times 19 = \cdots$.


97
67
101
71
37
41
61
103
73
43
11
31
7
13
89
5
59
29
17
3
2
19
47
23
53
107
79
83
109
113



2, 3, 5, 7, 11, 13, …, 2003, 2011, 2017, 2027, 2029, …

2, 3, 5, 7, 11, 13, …, 2003, 2011, 2017, 2027, 2029, …, 1000000007, …

2, 3, 5, 7, 11, 13, …, 2003, 2011, 2017, 2027, 2029, …, 1000000007, …

- Does the sequence of primes ever stop?
- Or maybe there are infinitely many primes?

The first three primes are 2, 3, 5

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  $\dots$
- $30031 = 2310 \times 13 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  $\ldots$
- $30031 = 2310 \times 13 + 1$

But 30031 is either prime or divisible by a prime

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  $\dots$
- $30031 = 2310 \times 13 + 1$

But 30031 is either prime or divisible by a prime (in fact $30031 = 59 \times 209$)

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$

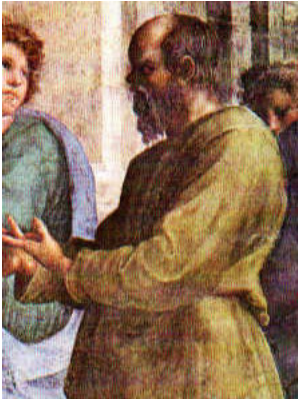
30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

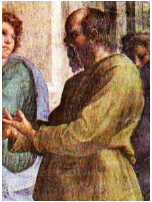
- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  ...
- $30031 = 2310 \times 13 + 1$

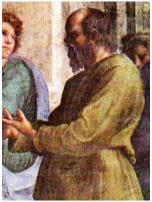
But 30031 is either prime or divisible by a prime (in fact $30031 = 59 \times 209$)

So 2, 3, 5, 7, 11, 13 are not all the primes

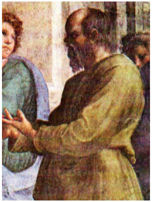




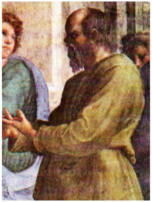
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes



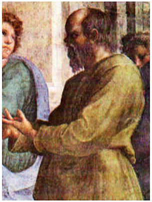
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$



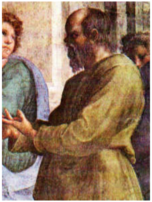
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must …



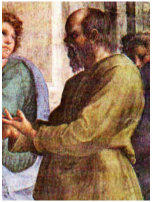
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must …
- Euclid: N leaves remainder 1 when divided by all your primes



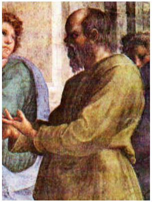
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must …
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct



- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must …
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime



- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime
- Socrates: Yes. So there is a prime not in my list



- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must …
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime
- Socrates: Yes. So there is a prime not in my list
- Euclid: Indeed. This shows there are more than any finite number of primes
- Socrates: You are correct

Consider the statement

$$P\text{: ‘there are finitely many primes’}$$

and its logical negation

$$\neg P\text{: ‘there are more than any finite number of primes’.}$$

Euclid proves $\neg P$ by showing Socrates that if he assumes P then he is led to a contraction. Therefore P is false, i.e. $\neg P$ is true.

Consider the statement

$$\mathrm{P}: \text{ 'there are finitely many primes'}$$

and its logical negation

$$\neg\mathrm{P}: \text{ 'there are more than any finite number of primes'.}$$

Euclid proves $\neg\mathrm{P}$ by showing Socrates that if he assumes P then he is led to a contraction. Therefore P is false, i.e. $\neg\mathrm{P}$ is true.

This differs subtly from 'proof by contradiction', where to prove a statement Q, we show that $\neg\mathrm{Q}$ leads to a contradiction, and so deduce $\neg\neg\mathrm{Q}$. In ordinary mathematics, $\neg\neg\mathrm{Q} \implies \mathrm{Q}$, but intuitionists do not accept this implication.

A *composition* of a number n is a way to write n as a sum of natural numbers. The compositions of 4 are

$$
\begin{gathered}
4 \\
3+1 \\
1+3 \\
2+2 \\
2+1+1 \\
1+2+1 \\
1+1+2 \\
1+1+1+1
\end{gathered}
$$

A *composition* of a number n is a way to write n as a sum of natural numbers. The compositions of 4 are

$$\begin{array}{ccc}
4 & & \{4\} \\
3+1 & & \{3,4\} \\
1+3 & & \{1,4\} \\
2+2 & & \{2,4\} \\
2+1+1 & \longleftrightarrow & \{2,3,4\} \\
1+2+1 & & \{1,3,4\} \\
1+1+2 & & \{1,2,4\} \\
1+1+1+1 & & \{1,2,3,4\}
\end{array}$$

A *composition* of a number n is a way to write n as a sum of natural numbers. The compositions of 4 are

$$\begin{array}{c} 4 \\ 3+1 \\ 1+3 \\ 2+2 \\ 2+1+1 \\ 1+2+1 \\ 1+1+2 \\ 1+1+1+1 \end{array} \quad \longleftrightarrow \quad \begin{array}{c} \{4\} \\ \{3,4\} \\ \{1,4\} \\ \{2,4\} \\ \{2,3,4\} \\ \{1,3,4\} \\ \{1,2,4\} \\ \{1,2,3,4\} \end{array} \quad \longleftrightarrow \quad \begin{array}{c} \varnothing \\ \{3\} \\ \{1\} \\ \{2\} \\ \{2,3\} \\ \{1,3\} \\ \{1,2\} \\ \{1,2,3\} \end{array}$$

In general, compositions of n are in bijection (one-to-one correspondence) with subsets of $\{1, 2, \ldots, n-1\}$.

A *composition* of a number n is a way to write n as a sum of natural numbers. The compositions of 4 are

$$\begin{array}{ccccc} 4 & & \{4\} & & \varnothing \\ 3+1 & & \{3,4\} & & \{3\} \\ 1+3 & & \{1,4\} & & \{1\} \\ 2+2 & & \{2,4\} & & \{2\} \\ 2+1+1 & \longleftrightarrow & \{2,3,4\} & \longleftrightarrow & \{2,3\} \\ 1+2+1 & & \{1,3,4\} & & \{1,3\} \\ 1+1+2 & & \{1,2,4\} & & \{1,2\} \\ 1+1+1+1 & & \{1,2,3,4\} & & \{1,2,3\} \end{array}$$

In general, compositions of n are in bijection (one-to-one correspondence) with subsets of $\{1, 2, \ldots, n-1\}$.

So to count the number of compositions, we can instead count the number of subsets.

A *composition* of a number n is a way to write n as a sum of natural numbers. The compositions of 4 are

$$\begin{array}{ccccc}
4 & & \{4\} & & \varnothing \\
3+1 & & \{3,4\} & & \{3\} \\
1+3 & & \{1,4\} & & \{1\} \\
2+2 & & \{2,4\} & & \{2\} \\
2+1+1 & \longleftrightarrow & \{2,3,4\} & \longleftrightarrow & \{2,3\} \\
1+2+1 & & \{1,3,4\} & & \{1,3\} \\
1+1+2 & & \{1,2,4\} & & \{1,2\} \\
1+1+1+1 & & \{1,2,3,4\} & & \{1,2,3\}
\end{array}$$

In general, compositions of n are in bijection (one-to-one correspondence) with subsets of $\{1, 2, \ldots, n-1\}$.

So to count the number of compositions, we can instead count the number of subsets.

There are 2^{n-1} subsets of $\{1, 2, \ldots, n-1\}$.

A *partition* of a number n is a way to write n as a sum of non-increasing natural numbers.

The partitions of 4 are 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$.

Let $p(n)$ be the number of partitions of n. So $p(4) = 5$.

n	0	1	2	3	4	5	6	7	8	9	10	...	14	15
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	...	135	176

There is no simple formula for $p(n)$. Instead we estimate how fast it grows.

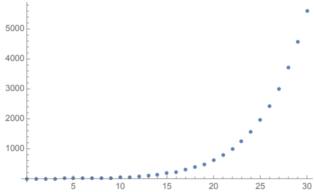
A *partition* of a number n is a way to write n as a sum of non-increasing natural numbers.

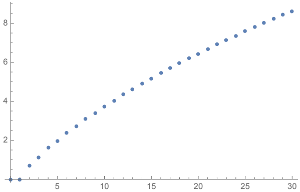
The partitions of 4 are 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$.

Let $p(n)$ be the number of partitions of n. So $p(4) = 5$.

n	0	1	2	3	4	5	6	7	8	9	10	…	14	15
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	…	135	176

There is no simple formula for $p(n)$. Instead we estimate how fast it grows. The graphs below show $p(n)$, $\log p(n)$





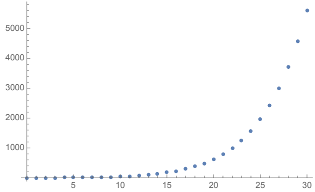
A *partition* of a number n is a way to write n as a sum of non-increasing natural numbers.

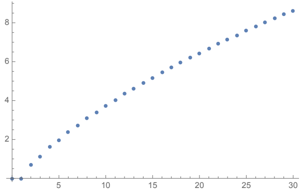
The partitions of 4 are 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$.

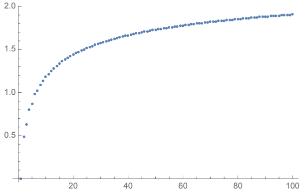
Let $p(n)$ be the number of partitions of n. So $p(4) = 5$.

n	0	1	2	3	4	5	6	7	8	9	10	$\ldots$	14	15
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	$\ldots$	135	176

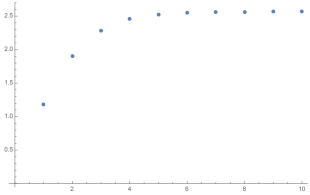
There is no simple formula for $p(n)$. Instead we estimate how fast it grows. The graphs below show $p(n)$, $\log p(n)$ and $\frac{\log p(n)}{\sqrt{n}}$.







The graph below again shows $\frac{\log p(n)}{\sqrt{n}}$, but now with a logarithmic x axis, so the points plotted are for $n = 1, 10, 100, \ldots, 10^{10}$.

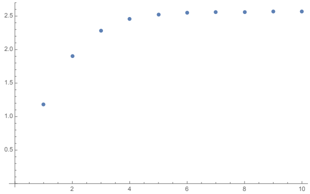


As this hints, $\log p(n) \sim 2\sqrt{\frac{\pi^2}{6}}\sqrt{n}$, where $\sim$ means that the ratio of the two sides tends to 1 as n tends to ∞. The constant $2\sqrt{\frac{\pi^2}{6}}$ is about 2.5651.

Theorem (Hardy–Ramanujan, 1918)

$$p(n) \sim \frac{\exp\left(2\sqrt{\frac{\pi^2}{6}}\sqrt{n}\right)}{4\sqrt{3}n}.$$

The graph below again shows $\frac{\log p(n)}{\sqrt{n}}$, but now with a logarithmic x axis, so the points plotted are for $n = 1, 10, 100, \ldots, 10^{10}$.



As this hints, $\log p(n) \sim 2\sqrt{\frac{\pi^2}{6}}\sqrt{n}$, where $\sim$ means that the ratio of the two sides tends to 1 as n tends to ∞. The constant $2\sqrt{\frac{\pi^2}{6}}$ is about 2.5651.

Theorem (Hardy–Ramanujan, 1918)

$$p(n) \sim \frac{\exp(2\sqrt{\frac{\pi^2}{6}}\sqrt{n})}{4\sqrt{3}n}.$$

In fact Hardy and Ramanujan proved something more precise: they gave a divergent series for $p(n)$. My paper *Counting partitions on the abacus*, Ramanujan Journal, 2008 gives an elementary proof of the theorem above.

The Hardy–Ramanujan proof takes as its starting point the *generating function* for the function $p(n)$:

$$P(x) = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + \cdots + p(n)x^n + \cdots .$$

Even though $p(n)$ has no simple closed formula, there is a beautifully simple formula for $P(x)$.

As a warm-up, let $q(n)$ be the number of partitions of n into distinct parts. So $q(4) = 2$, counting 4 and $3 + 1$.

- We do not count count $2 + 2$ because the part 2 appears twice.
- We do not count $2 + 1 + 1$ or $1 + 1 + 1 + 1$ because the part 1 appears (at least) twice.

Let

$$Q(x) = q(0) + q(1)x + q(2)x^2 + q(3)x^3 + q(4)x^4 + \cdots + q(n)x^n + \cdots$$

The Hardy–Ramanujan proof takes as its starting point the *generating function* for the function $p(n)$:

$$P(x) = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + \cdots + p(n)x^n + \cdots .$$

Even though $p(n)$ has no simple closed formula, there is a beautifully simple formula for $P(x)$.

As a warm-up, let $q(n)$ be the number of partitions of n into distinct parts. So $q(4) = 2$, counting 4 and $3 + 1$.

- We do not count count $2 + 2$ because the part 2 appears twice.
- We do not count $2 + 1 + 1$ or $1 + 1 + 1 + 1$ because the part 1 appears (at least) twice.

Let

$$Q(x) = q(0) + q(1)x + q(2)x^2 + q(3)x^3 + q(4)x^4 + \cdots + q(n)x^n + \cdots$$

Proposition

$$Q(x) = (1 + x)(1 + x^2)(1 + x^3)(1 + x^4) \cdots .$$

The Hardy–Ramanujan proof takes as its starting point the *generating function* for the function $p(n)$:

$$P(x) = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + \cdots + p(n)x^n + \cdots .$$

Even though $p(n)$ has no simple closed formula, there is a beautifully simple formula for $P(x)$.

As a warm-up, let $q(n)$ be the number of partitions of n into distinct parts. So $q(4) = 2$, counting 4 and $3 + 1$.

- We do not count count $2 + 2$ because the part 2 appears twice.
- We do not count $2 + 1 + 1$ or $1 + 1 + 1 + 1$ because the part 1 appears (at least) twice.

Let

$$Q(x) = q(0) + q(1)x + q(2)x^2 + q(3)x^3 + q(4)x^4 + \cdots + q(n)x^n + \cdots$$

Proposition

$$Q(x) = (1 + x)(1 + x^2)(1 + x^3)(1 + x^4) \cdots .$$

Proof. When we multiply out the right-hand side, the coefficient of x^n is the number of ways to write x as a sum of distinct natural numbers. $\square$

The Hardy–Ramanujan proof takes as its starting point the *generating function* for the function $p(n)$:

$$P(x) = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + \cdots + p(n)x^n + \cdots .$$

Even though $p(n)$ has no simple closed formula, there is a beautifully simple formula for $P(x)$.

Proposition

$$P(x) = \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\dots$$

Proof. The right-hand side is

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)\dots$$

When we multiply out the right-hand side by taking x^{1m_1} from the first bracket, x^{2m_2} from the second bracket, x^{3m_3} from the third bracket, and so on, we get a contribution of 1 to the coefficient of $x^{1m_1+2m_2+3m_3+\cdots}$. This counts the partition with m_i parts of size i for each i. Hence the coefficient of x^n is $p(n)$. $\square$

The Hardy–Ramanujan proof takes as its starting point the *generating function* for the function $p(n)$:

$$P(x) = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + \cdots + p(n)x^n + \cdots .$$

Even though $p(n)$ has no simple closed formula, there is a beautifully simple formula for $P(x)$.

Proposition

$$P(x) = \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\cdots$$

Proof. The right-hand side is

$$(1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)(1+x^3+x^6+x^9+\cdots)\ldots$$

When we multiply out the right-hand side by taking x^{1m_1} from the first bracket, x^{2m_2} from the second bracket, x^{3m_3} from the third bracket, and so on, we get a contribution of 1 to the coefficient of $x^{1m_1+2m_2+3m_3+\cdots}$. This counts the partition with m_i parts of size i for each i. Hence the coefficient of x^n is $p(n)$. $\square$

For example $3+3+2+1+1+1$ has $m_1 = 3$, $m_2 = 1$, $m_3 = 2$.

Generating functions are very useful for counting combinatorial objects.

Proposition

The number of partitions of n into odd parts is equal to the number of partitions of n into distinct parts.

For example, when $n = 9$, there are 8 partitions of either type:

$$\left\{\begin{array}{c} 9 \\ 7+1+1 \\ 5+3+1 \\ 5+1+1+1+1 \\ 3+3+3 \\ 3+3+1+1+1 \\ 3+1+1+1+1+1+1 \\ 1+1+1+1+1+1+1+1+1 \end{array}\right\} \qquad \left\{\begin{array}{c} 9 \\ 8+1 \\ 7+2 \\ 6+3 \\ 6+2+1 \\ 5+4 \\ 5+3+1 \\ 4+3+2 \end{array}\right\}$$

Generating functions are very useful for counting combinatorial objects.

Proposition

The number of partitions of n into odd parts is equal to the number of partitions of n into distinct parts.

Proof. The generating function for the left-hand side is

$$\begin{aligned}
\prod_{i=1}^{\infty} \frac{1}{1-x^{2i-1}} &= \frac{1}{1-x}\frac{1}{1-x^3}\frac{1}{1-x^5}\cdots \\
&= \frac{1}{1-x}\frac{1-x^2}{1-x^2}\frac{1}{1-x^3}\frac{1-x^4}{1-x^4}\frac{1}{1-x^5}\frac{1-x^6}{1-x^6}\cdots \\
&= \frac{1-x^2}{1-x}\frac{1-x^4}{1-x^2}\frac{1-x^6}{1-x^3}\cdots \\
&= (1+x)(1+x^2)(1+x^3)\ldots \\
&= \prod_{i=1}^{\infty}(1+x^i)
\end{aligned}$$

which is the generating function for the right-hand side. Since the generating functions are equal so are the sequences they enumerate. $\square$

There are also bijective proofs of the proposition (like the bijective proof for the number of compositions) but all need more work than using generating functions.

$$\left\{\begin{array}{c} 9 \\ 7+1+1 \\ 5+3+1 \\ 5+1+1+1+1 \\ 3+3+3 \\ 3+3+1+1+1 \\ 3+1+1+1+1+1+1 \\ 1+1+1+1+1+1+1+1+1 \end{array}\right\} \overset{?}{\longleftrightarrow} \left\{\begin{array}{c} 9 \\ 8+1 \\ 7+2 \\ 6+3 \\ 6+2+1 \\ 5+4 \\ 5+3+1 \\ 4+3+2 \end{array}\right\}.$$

There are also bijective proofs of the proposition (like the bijective proof for the number of compositions) but all need more work than using generating functions.

$$\left\{\begin{array}{c} 9 \\ 7+1+1 \\ 5+3+1 \\ 5+1+1+1+1 \\ 3+3+3 \\ 3+3+1+1+1 \\ 3+1+1+1+1+1+1 \\ 1+1+1+1+1+1+1+1+1 \end{array}\right\} \stackrel{?}{\longleftrightarrow} \left\{\begin{array}{c} 9 \\ 8+1 \\ 7+2 \\ 6+3 \\ 6+2+1 \\ 5+4 \\ 5+3+1 \\ 4+3+2 \end{array}\right\}.$$

A one-line algebraic proof for experts: the Brauer character table of the symmetric group S_n in characteristic 2 is square.

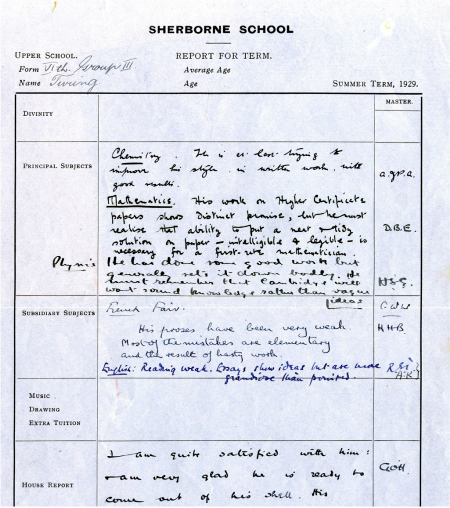
There are also bijective proofs of the proposition (like the bijective proof for the number of compositions) but all need more work than using generating functions.

$$\left\{\begin{array}{c} 9 \\ 7+1+1 \\ 5+3+1 \\ 5+1+1+1+1 \\ 3+3+3 \\ 3+3+1+1+1 \\ 3+1+1+1+1+1+1 \\ 1+1+1+1+1+1+1+1+1 \end{array}\right\} \stackrel{?}{\longleftrightarrow} \left\{\begin{array}{c} 9 \\ 8+1 \\ 7+2 \\ 6+3 \\ 6+2+1 \\ 5+4 \\ 5+3+1 \\ 4+3+2 \end{array}\right\}.$$

A one-line algebraic proof for experts: the Brauer character table of the symmetric group S_n in characteristic 2 is square.

What's the point of having proofs? What's the point of having multiple proofs?

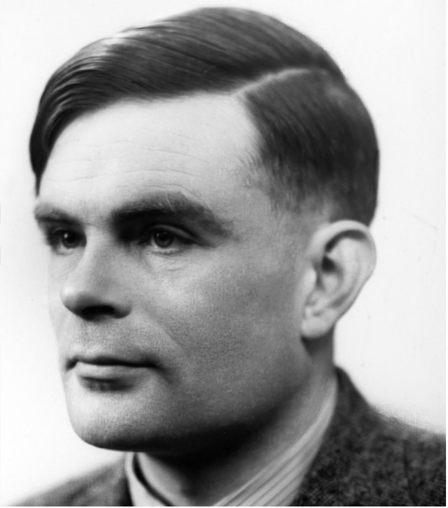
Alan Turing (1912 — 1952) was a polymathematic pioneer of early computing



SHERBORNE SCHOOL

UPPER SCHOOL. REPORT FOR TERM.
Form VIth. Group III *Average Age*
Name Turing *Age* SUMMER TERM, 1929.

		MASTER.
DIVINITY		
PRINCIPAL SUBJECTS	Chemistry. He is at last trying to improve his style in written work, with good results.	a.gp.a.
	Mathematics. His work on Higher Certificate papers shows distinct promise, but he must realise that ability to put a neat & tidy solution on paper – intelligible & legible – is necessary for a first-rate mathematician.	D.B.E.
Physics	He has done some good work but generally sets it down badly. He must remember that Cambridge will want sound knowledge rather than vague ideas	H.S.E.
SUBSIDIARY SUBJECTS	French Fair.	C.W.L.
	His proses have been very weak. Most of the mistakes are elementary and the result of hasty work.	H.H.B.
	English: Reading weak. Essays show ideas but are more grandiose than pointed.	R.S.I. / A.K.
MUSIC DRAWING EXTRA TUITION		
HOUSE REPORT	I am quite satisfied with him: & am very glad he is ready to come out of his shell. His	G.O.H.



Turing's maths teacher had a fair point: mathematics papers are mostly words.

A PROOF OF LIOUVILLE'S THEOREM

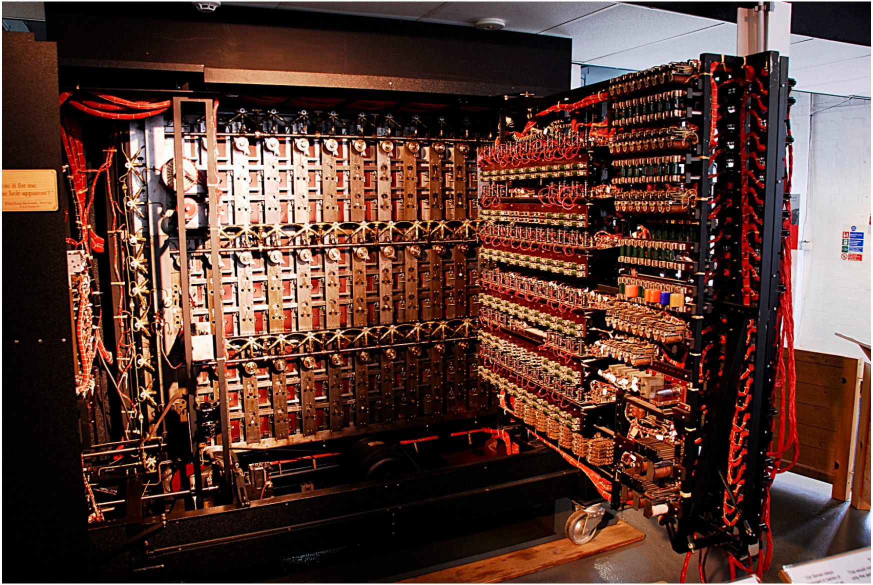
EDWARD NELSON

Consider a bounded harmonic function on Euclidean space. Since it is harmonic, its value at any point is its average over any sphere, and hence over any ball, with the point as center. Given two points, choose two balls with the given points as centers and of equal radius. If the radius is large enough, the two balls will coincide except for an arbitrarily small proportion of their volume. Since the function is bounded, the averages of it over the two balls are arbitrarily close, and so the function assumes the same value at any two points. Thus a bounded harmonic function on Euclidean space is a constant.

PRINCETON UNIVERSITY

Received by the editors June 26, 1961.

Turing and his Hut 8 team used a mixture of cryptanalysis, statistical inference and computation — the 'Bombe' — to crack the Enigma code used by the German Navy in the Second World War.



Turing's finest mathematical achievement is the following theorem.

Theorem. There is no algorithm that will decide the truth or falsity of a mathematical statement

- There are infinitely many primes — True
- The number of partitions into odd parts is equal to the number of partitions into distinct parts — True
- There are infinitely many primes ending 1 — True
- There are infinitely many primes ending 2 — False
- A real function f is equal to its Taylor series $\sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n$ at any x for which the series converges

Turing's finest mathematical achievement is the following theorem.

Theorem. There is no algorithm that will decide the truth or falsity of a mathematical statement

- There are infinitely many primes — True
- The number of partitions into odd parts is equal to the number of partitions into distinct parts — True
- There are infinitely many primes ending 1 — True
- There are infinitely many primes ending 2 — False
- A real function f is equal to its Taylor series $\sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n$ at any x for which the series converges — False
- 2^3 and 3^2 are the only consecutive integer powers — ???
- There are infinitely many twin primes such as 3, 5 or 5, 7 or 11, 13 or 17, 19 or … or 2027, 2029 or … — ???
- $p(n)$ is equally likely to be even as odd — ???

Really what Turing proved is that there is no algorithm that will decide whether a Turing machine halts. ‘The Entscheidungsproblem is undecidable.’

Gödel proved his incompleteness theorem before Turing. Gödel’s theorem can now be understood as a corollary of Turing’s theorem on the Entscheidungsproblem.

Corollary (Gödel’s first incompleteness theorem)

Fix a formal proof system. There exists a true statement that has no formal proof.

For example, a formal proof from Russell–Whitehead *Principia Mathematica*.

$*54{\cdot}43$. $\vdash :. \alpha, \beta \in 1 \,.\supset : \alpha \cap \beta = \Lambda \,.\equiv .\, \alpha \cup \beta \in 2$

Dem.

$$\vdash . *54{\cdot}26 \,.\supset \vdash :. \alpha = \iota\text{‘}x \,.\, \beta = \iota\text{‘}y \,.\supset : \alpha \cup \beta \in 2 \,.\equiv .\, x \neq y \,.$$

$$[*51{\cdot}231] \qquad \equiv .\, \iota\text{‘}x \cap \iota\text{‘}y = \Lambda \,.$$

$$[*13{\cdot}12] \qquad \equiv .\, \alpha \cap \beta = \Lambda \qquad (1)$$

$$\vdash . (1) . *11{\cdot}11{\cdot}35 \,.\supset$$

$$\vdash :. (\exists x, y) \,.\, \alpha = \iota\text{‘}x \,.\, \beta = \iota\text{‘}y \,.\supset : \alpha \cup \beta \in 2 \,.\equiv .\, \alpha \cap \beta = \Lambda \qquad (2)$$

$$\vdash . (2) . *11{\cdot}54 \,.\, *52{\cdot}1 \,.\supset \vdash .\, \text{Prop}$$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Really what Turing proved is that there is no algorithm that will decide whether a Turing machine halts. 'The Entscheidungsproblem is undecidable.'

Gödel proved his incompleteness theorem before Turing. Gödel's theorem can now be understood as a corollary of Turing's theorem on the Entscheidungsproblem.

Corollary (Gödel's first incompleteness theorem)

Fix a formal proof system. There exists a true statement that has no formal proof.

Proof. Suppose, for a contradiction, that either P or $\neg P$ is provable for every statement P. Given a Turing machine M, let P_M be the statement 'M halts'.

- Spend week 1 looking for a formal proof of P_M,
- Spend week 2 looking for a formal proof of $\neg P_M$,
- Spend week 3 looking for a formal proof of P_M,

and so on. Since either P_M or $\neg P_M$ is provable, and formal proofs can be enumerated one-by-one, eventually we will succeed in finding a proof. Therefore we can detect when Turing machines halt. This contradicts Turing's result. Hence there are statements Q such that neither Q nor $\neg Q$ is provable. But either Q or $\neg Q$ is true. $\square$

Thank you. Any questions?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Heilbronn Institute for Mathematical Research