Is there a pattern in the prime numbers?

Paul Pollack

The stars of our show

Definition

A **prime number** is an integer > 1 whose only positive divisors are 1 and itself.

The stars of our show

Definition

A **prime number** is an integer > 1 whose only positive divisors are 1 and itself.

Examples

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, . . .

The stars of our show

Definition

A **prime number** is an integer > 1 whose only positive divisors are 1 and itself.

Examples

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, . . .

Theorem (Fundamental theorem of arithmetic)

Every natural number > 1 can be written as a product of primes in exactly one way.

For example,

$$2980398103281112391123 = 491 \cdot 967 \cdot 2767 \cdot 2268595952977.$$

Couldn't we just list all of the prime numbers?

Theorem (Euclid)

There are infinitely many primes.

What Euclid's argument actually shows is that no matter what finite list of primes you start with, there's always at least one prime that you're missing.

∞ly many primes, ctd.

Proof.

Suppose you start with a finite list of primes, say $p_1, \ldots, p_k$. Let

$$P = p_1 \cdots p_k + 1.$$

Certainly $P > 1$. So P can be factored into primes. Choose a prime that shows up in the factorization of P, call it p.

Claim: p isn't one of $p_1, \ldots, p_k$.

∞ly many primes, ctd.

Proof.

Suppose you start with a finite list of primes, say $p_1, \ldots, p_k$. Let

$$P = p_1 \cdots p_k + 1.$$

Certainly $P > 1$. So P can be factored into primes. Choose a prime that shows up in the factorization of P, call it p.

Claim: p isn't one of $p_1, \ldots, p_k$.

Why? Well, p goes evenly into P, but none of the p_i go evenly into P. In fact, we constructed P so that it was one more than a multiple of each p_i. So if you divide P by p_i, you'll get a remainder of 1 (not zero).

∞ly many primes, ctd.

For example, suppose you want to find a prime not on the list $2, 3, 5, 7$, and 11, and 13. We take

$$P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$$
$$= 30031.$$

Then any prime divisor of 30031 is a new prime not on our list. It turns out $30031 = 59 \cdot 509$. So we can replace our old list with the list $2, 3, 5, 7,\ 11,\ 13,\ 59,\ 509$.

We can repeat the argument as many times as desired to get a list of primes as long as desired.

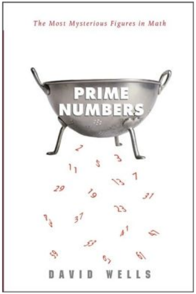
Moral: Since the sequence of primes continues forever, it makes sense to ask **how** it continues. In other words, how are the primes distributed?

Everyone loves a good mystery

Questions about the distribution of prime numbers are hard. It's safe to say that prime numbers are some of the most mysterious figures in all of mathematics.

Everyone loves a good mystery

Questions about the distribution of prime numbers are hard. It's safe to say that prime numbers are some of the most mysterious figures in all of mathematics.



In fact, one often hears that the prime numbers are **randomly distributed**, or seem to have **no pattern**.

Can we make sense of these claims?

Psychic math

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

Psychic math

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

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

Psychic math

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

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

Only two of the 6 columns contain primes.
$6n+2=2(3n+1)$, $6n+3=3(2n+1)$, $6n+4=2(3n+2)$, and $6n+6=6(n+1)$. Impressed yet?

What is a pattern?

Maybe “No pattern” means “no formula”?

What is a pattern?

Maybe "No pattern" means "no formula"?
But that's not true either!

Example (Sierpiński)

Consider the constant

$$A = 0.02030005000000070\ldots$$

defined by

$$\sum_{k=1}^{\infty} p_k \cdot 10^{-2^k},$$

where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... Then

$$p_k = \lfloor 10^{2^k} A \rfloor - 10^{2^{k-1}} \lfloor 10^{2^{k-1}} A \rfloor.$$

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.
$113 + 18 = 131$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.
$113 + 18 = 131$, which is **prime**.
$131 + 20 = 151$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.
$113 + 18 = 131$, which is **prime**.
$131 + 20 = 151$, which is **prime**.
$151 + 22 = 173$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.
$113 + 18 = 131$, which is **prime**.
$131 + 20 = 151$, which is **prime**.
$151 + 22 = 173$, which is **prime**.
$173 + 24 = 197$, which is **prime**.

OK, how about a **useful** formula?

Let's start with some observations of Leonhard Euler.

$41 + 2 = 43$, which is **prime**.
$43 + 4 = 47$, which is **prime**.
$47 + 6 = 53$, which is **prime**.
$53 + 8 = 61$, which is **prime**.
$61 + 10 = 71$, which is **prime**.
$71 + 12 = 83$, which is **prime**.
$83 + 14 = 97$, which is **prime**.
$97 + 16 = 113$, which is **prime**.
$113 + 18 = 131$, which is **prime**.
$131 + 20 = 151$, which is **prime**.
$151 + 22 = 173$, which is **prime**.
$173 + 24 = 197$, which is **prime**.
$197 + 26 = 223$, which is **prime**.

Things fall apart

The nth number output by this process is

$$41 + 2 + 4 + 6 + \cdots + 2n$$
$$= 41 + 2(1 + 2 + 3 + \cdots + n) = 41 + n^2 + n.$$

Things fall apart

The nth number output by this process is

$$41 + 2 + 4 + 6 + \cdots + 2n$$
$$= 41 + 2(1 + 2 + 3 + \cdots + n) = 41 + n^2 + n.$$

If we plug in $n = 40$, we get

$$41 + 40^2 + 40 = 41 + 40(40 + 1) = 41 + 40 \cdot 41 = 41^2,$$

which is composite.

Theorem

For almost all (asymptotically 100%) natural numbers n, the number $n^2 + n + 41$ is composite.

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

15,

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

15, 825,

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

15, 825, 725,

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

15, 825, 725, 1925,

Primes through fractions

The following is due to the contemporary mathematician John Conway. Consider the following list of fourteen fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}$$

We start by setting $n = 2$. To continue ...

* Find the first fraction in the list which you can multiply n by to get an integer; replace n with that new integer. Whenever you reach a power of 2, say 2^k, output the exponent k. Now repeat.

Going through this process, we run through the integers

15, 825, 725, 1925, 2275, 425, 390, 330, 290, 770, 910, 170, 156, 132, 116, 308, 364, 68, **4**, ...

A recent photograph of John Conway

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281
7	710

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281
7	710
11	2375

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281
7	710
11	2375
13	3893

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281
7	710
11	2375
13	3893
17	8102

Primes through fractions, ctd.

Remember that every time we see 2^k, we output the value of k.

Output	Number of steps required
2	19
3	69
5	281
7	710
11	2375
13	3893
17	8102

Theorem (Conway)

The set of outputs is exactly the set of primes, in increasing order.

Another way of generating the primes in increasing order

It's easy to write a computer program to generate the primes.

A (not so great) algorithm for generating the primes:

- Run through the integers $n = 1, 2, 3, \dots$ in order, outputting the number if only if it's prime.
- To test if n is prime, divide n by $n-1, n-2, \dots, 1$ successively until something goes in evenly. If we find a divisor before we get down to 1, then n is composite. Otherwise, n is prime.

Another way of generating the primes in increasing order

Actually this is exactly what we were doing before. Instead of programming in C or Pascal or Java, we were programming in a language based on fractions, called `FRACTRAN`.

Theorem (Conway)

For any sequence of positive integers that can be output by a computer program, there is a finite list of fractions which will generate this sequence.

This is an amazingly general theorem.

Unfortunately, precisely because it's so general, it's not reasonable to hope that it tell us anything interesting about the primes in particular.

Cutting our losses

At this point, maybe you (like me) are of the opinion that a **useful** formula for primes isn't likely to crop up.

Saying that no such formula exists is one way to make sense of the idea that "primes are patternless".

Cutting our losses

At this point, maybe you (like me) are of the opinion that a **useful** formula for primes isn't likely to crop up.

Saying that no such formula exists is one way to make sense of the idea that "primes are patternless".

But there's another way in which primes behave randomly that I think is enlightening. Before doing that, I need to summarize some of what modern mathematicians have shown about the distribution of the prime numbers.

Recall our notation $\pi(x)$ for the number of primes not exceeding x.

The counts of primes up to x, for $x = 10^k$

x	$\pi(x)$
10	4

The counts of primes up to x, for $x = 10^k$

x	$\pi(x)$
10	4
10^2	25

The counts of primes up to x, for $x = 10^k$

x	$\pi(x)$
10	4
10^2	25
10^3	168

The counts of primes up to x, for $x = 10^k$

x	$\pi(x)$
10	4
10^2	25
10^3	168
10^4	1,229
10^5	9,592
10^6	78,498
10^7	664,579
10^8	5,761,455
10^9	50,847534
10^{10}	455,052,511
10^{11}	4,118,054,813
10^{12}	37,607,912,018
10^{13}	346,065,536,839
10^{14}	3,204,941,750,802

While a young teenager, Gauss became interested in understanding the rate at which the primes thinned out. He reports that he often

> *spent an idle quarter of an hour to count another chiliad here and there.*

Gauss's guess about $\pi(x)$

These investigations led to the following conjecture.

Conjecture

The number of primes $p \leq x$ is approximately

$$\frac{x}{\ln x},$$

where $\ln x$ is the natural logarithm of x. Here "approximately" means that the relative error you make if you approximate $\pi(x)$ by $x/\ln x$ tends to 0 as $x \to \infty$.

Note: If you haven't seen the function $\ln$ before, you can pretend that

$$\ln(x) = 1 + 1/2 + 1/3 + \cdots + 1/\lfloor x \rfloor.$$

Testing Gauss's guess

By the **relative error**, we mean the ratio $\frac{\pi(x) - x/\ln x}{\pi(x)}$.

x	$\pi(x)$	relative error
10^3	168	13.7%
10^4	1,229	11.6%
10^5	9,592	9.4%
10^6	78,498	7.8%
10^7	664,579	6.6%
10^8	5,761,455	5.8%
10^9	50,847534	5.1%
10^{10}	455,052,511	4.6%
10^{11}	4,118,054,813	4.1&
10^{12}	37,607,912,018	3.8%

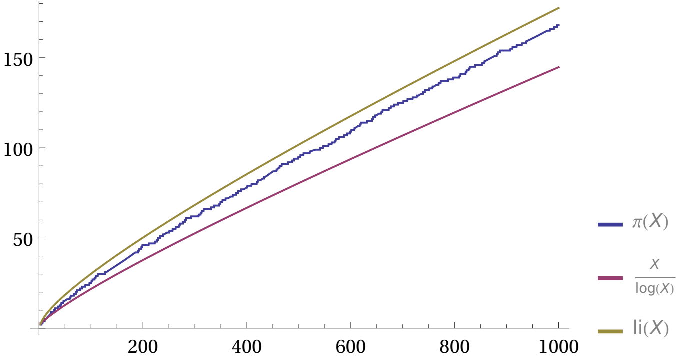
Testing Gauss's guess, ctd.

So Gauss's guess is looking pretty good. Gauss also suggested what he thought was an even better approximation to $\pi(x)$, the function

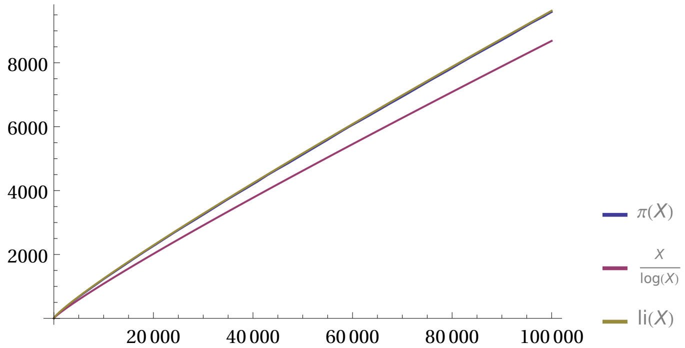
$$\mathrm{li}(x) := \int_2^x \frac{1}{\ln t}\,dt.$$

It turns out that $\mathrm{li}(x)$ and $x/\ln x$ are close enough for large x that if one of them is a good approximation to $\pi(x)$ — in the sense of Gauss's guess — then the other is too.

Comparing $\pi(x), x/\ln x$, and $\mathrm{li}(x)$ up to 1000



Comparing $\pi(x), x/\ln x$, and $\mathrm{li}(x)$ up to 100000



Vindication at last

About a hundred years after Gauss made his guess, two mathematicians — working independently but almost simultaneously — confirmed that Gauss was correct.

Prime number theorem (Hadamard and de la Vallee–Poussin)

Gauss's guess was correct. The relative error between $\pi(x)$ *and* $x/\ln x$ (or between $\pi(x)$ and $\mathrm{li}(x)$) tends to zero as $x \to \infty$.

Vindication at last

About a hundred years after Gauss made his guess, two mathematicians — working independently but almost simultaneously — confirmed that Gauss was correct.

Prime number theorem (Hadamard and de la Vallee–Poussin)

Gauss's guess was correct. The relative error between $\pi(x)$ and $x/\ln x$ (or between $\pi(x)$ and $\mathrm{li}(x)$) tends to zero as $x \to \infty$.

OK, great, but what does this have to do with randomness?

It turns out that Gauss's guess about the size of $\pi(x)$ is exactly what one would expect if primes behave randomly, in a sense we'll now make precise.

The sieve of Eratosthenes

The following method, discovered by the ancient Greek Eratosthenes, is a useful method for generating all of the primes up to a certain height N.

1. Start with a list of all of the natural numbers from 2 to N.
2. Look for the first natural number that hasn't been crossed out. This number is a prime; mark it as such. Now cross out all of its remaining multiples. Repeat this step.

The algorithm continues until all of the numbers are marked as prime or crossed out.

The sieve of Eratosthenes, ctd.

If you want the entire sequence of primes, you can run this process with the interval from 2 to N replaced by the entire set of integers at least 2. More formally:

- Let $A_1 = \{2, 3, 4, \dots\}$. Let p_1 be the first element of A_1 (so $p_1 = 2$). Remove from A_1 all of the elements are divisible by p_1, and call the resulting set A_2.
- Let p_2 be the first element of A_2 (so $p_2 = 3$). Remove from A_2 all of its remaining elements that are divisible by p_2. Call this A_3.
- Continue!

Then the sequence of primes is precisely $p_1, p_2, p_3, \dots$.

A random sieve

The sieve of Eratosthenes is completely deterministic. Let's introduce an element of chance into the picture. (This idea is due to David Hawkins.)

A random sieve

The sieve of Eratosthenes is completely deterministic. Let's introduce an element of chance into the picture. (This idea is due to David Hawkins.)

- Let $A_1 = \{2, 3, 4, \dots\}$. Let p_1 be the first element of A_1 (so $p_1 = 2$). Remove p_1 from A_1, and remove each remaining element with probability $1/p_1$. Call the resulting set A_2.
- Let p_2 be the first element of A_2. Remove p_2 from A_2, and then remove each remaining element with probability $1/p_2$. Call this A_3.
- Continue!

There are then **infinitely many** possibilities for the resulting sequence $p_1, p_2, p_3, \dots$.

A random sieve, ctd.

There are then **infinitely many** possibilities for the resulting sequence $p_1, p_2, p_3, \dots$. We'll call this an R-**primes sequence**.

Given a property of an infinite sequence, we can ask: What's the probability that a random R-primes sequence has the property.

Example

What's the probability that 3 is in our R-prime sequence?

A random sieve, ctd.

There are then **infinitely many** possibilities for the resulting sequence $p_1, p_2, p_3, \ldots$. We'll call this an R-**primes sequence**.

Given a property of an infinite sequence, we can ask: What's the probability that a random R-primes sequence has the property.

Example

What's the probability that 3 is in our R-prime sequence? It's $\frac{1}{2}$, since 3 has to not be killed by 2, and being killed by 2 happens with probability $\frac{1}{2}$.

Exercise: What's the probability 4 ends up in our R-prime sequence? Now there are two cases, depending on whether 3 is there too or not.

Primes are random, take 2

Remember the prime number theorem (Gauss's guess): The count of primes up to x is well-approximated by $x/\ln x$, in the sense that the relative error tends to 0.

Primes are random, take 2

Remember the prime number theorem (Gauss's guess): The count of primes up to x is well-approximated by $x/\ln x$, in the sense that the relative error tends to 0.

Theorem (Wunderlich)

The probability that Gauss's guess about $\pi(x)$ is true for a random R-prime sequence is 100%.

Primes are random, take 2

Remember the prime number theorem (Gauss's guess): The count of primes up to x is well-approximated by $x/\ln x$, in the sense that the relative error tends to 0.

Theorem (Wunderlich)

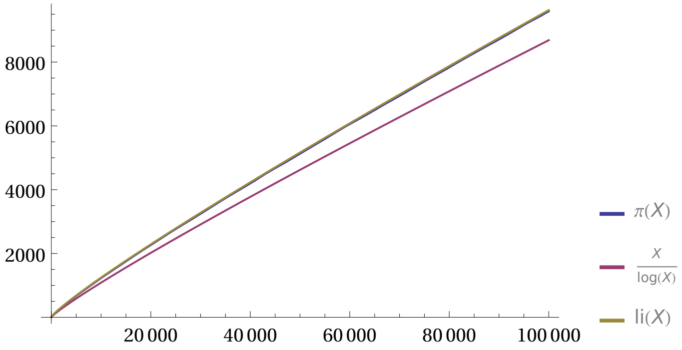
The probability that Gauss's guess about $\pi(x)$ is true for a random R-prime sequence is 100%.

If we didn't already know Gauss's guess was true, but thought primes were random, this would be a good reason to start believing Gauss.

Since we already know Gauss's guess is true, perhaps this is a good reason to think the primes are random!

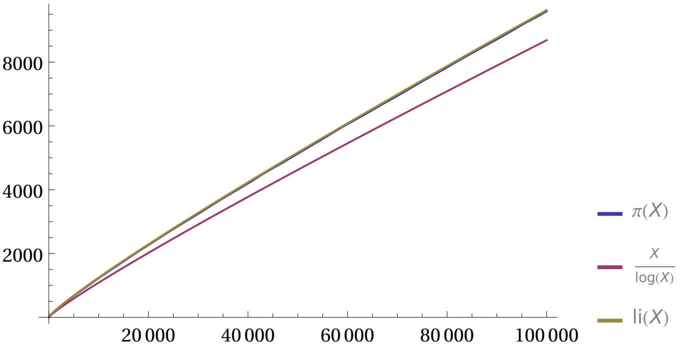
How to make a million bucks, the hard way

Let's put back up the graph comparing $\pi(x)$, $x/\ln x$, and $\mathrm{li}(x)$ for x up to 100000.



How to make a million bucks, the hard way

Let's put back up the graph comparing $\pi(x)$, $x/\ln x$, and $\mathrm{li}(x)$ for x up to 100000.



It's almost impossible to distinguish $\pi(x)$ and $\mathrm{li}(x)$ on this graph. How close are they?

How to make a million bucks, ctd.

The prime number theoem says that the relative error is small (heading to zero), but what about the absolute error?

Conjecture (Riemann Hypothesis)

For all $x > 3$, we have

$$|\pi(x) - \mathrm{li}(x)| < \sqrt{x}\ln x.$$

The Clay Mathematics Institute offers one million dollars if you can prove this.

What are you waiting for?

Thank you!