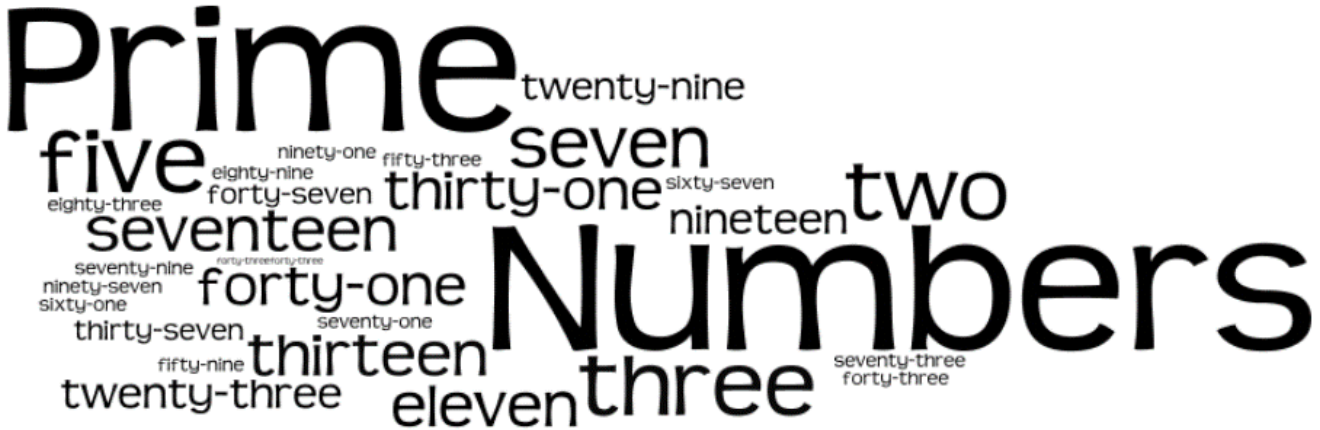
A Primer on Prime Numbers



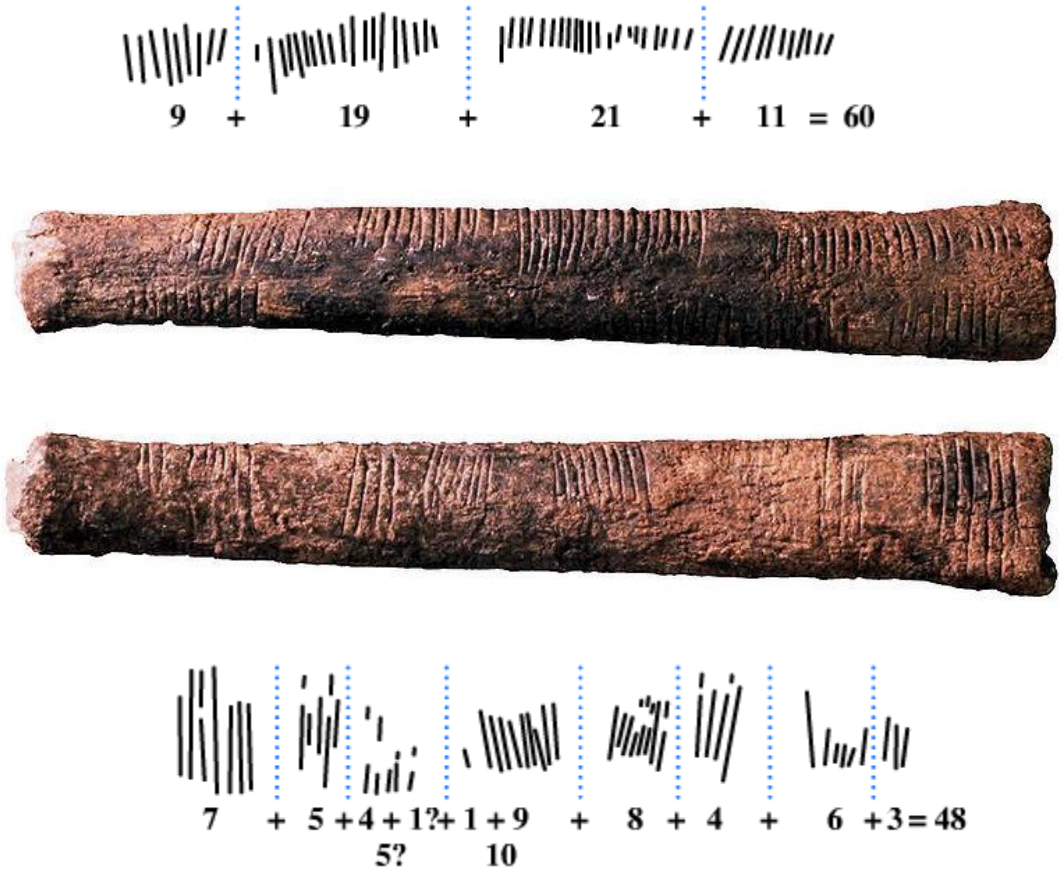
Prime Numbers

"Prime numbers are the very atoms of arithmetic. . . The primes are the jewels studded throughout the vast expanse of the infinite universe of numbers that mathematicians have studied down the centuries." Marcus du Sautoy, *The Music of the Primes*

- **Early Primes**
- Named Primes
- Hunting for Primes
- Visualizing Primes
- Harnessing Primes

Ishango bone

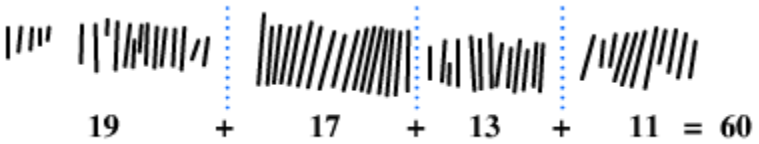
The Ishango bone is a bone tool, dated to the Upper Paleolithic era, about 18,000 to 20,000 BC. It is a dark brown length of bone, the fibula of a baboon, It has a series of tally marks carved in three columns running the length of the tool



Note: image is reversed

A History and Exploration of Prime Numbers

- In the book How Mathematics Happened: The First 50,000 Years, Peter Rudman argues that the development of the concept of prime numbers could have come about only after the concept of division, which he dates to after 10,000 BC, with prime numbers probably not being understood until about 500 BC. He also writes that "no attempt has been made to explain why a tally of something should exhibit multiples of two, prime numbers between 10 and 20,…



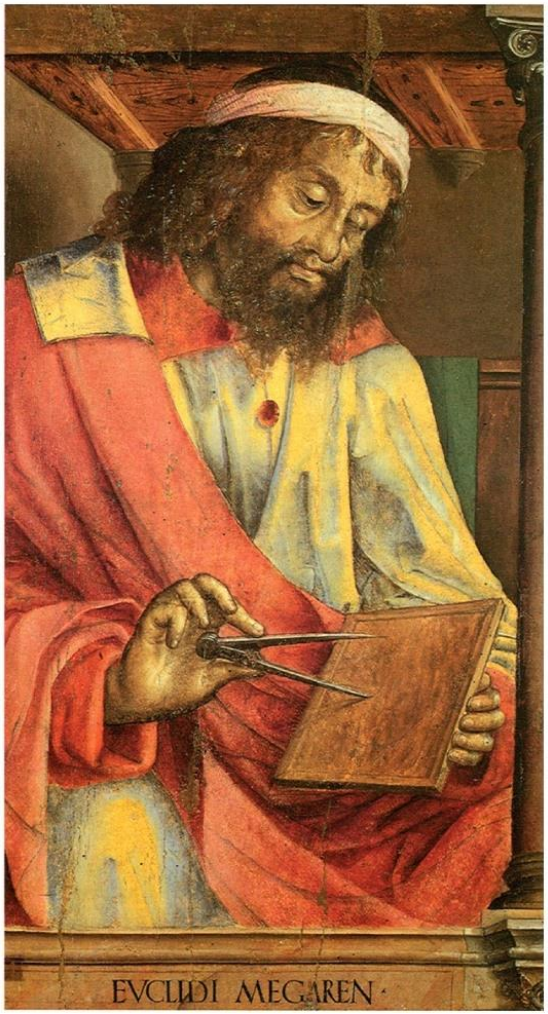
Left column

https://en.wikipedia.org/wiki/Ishango_bone

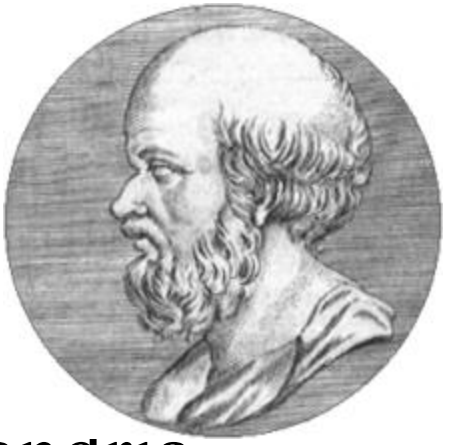
Euclid of Alexandria
325-265 B.C.

- The only man to summarize all the mathematical knowledge of his times.
- In Proposition 20 of Book IX of the Elements, Euclid proved that there are infinitely many prime numbers.

https://en.wikipedia.org/wiki/Euclid



Eratosthenes of Cyrene 276-194 B.C.



- Librarian of the University of Alexandria.
- Invented an instrument for duplicating the cube, measured the circumference of the Earth, calculated the distance from the Earth to the Sun and the Moon, and created an algorithm for finding all possible primes, the Eratosthenes Sieve.

https://en.wikipedia.org/wiki/Eratosthenes

Nicomachus of Gerasa
c. 100 A.D.

- Introduction to Arithmetic, Chapters XI, XII, and XIII divide odd numbers into three categories, “prime and incomposite”, “composite”, and “the number which is in itself secondary and composite, but relatively to another number is prime and incomposite.”
- In chapter XIII he describes Eratosthenes’ Sieve in excruciating detail.

https://en.wikipedia.org/wiki/Nicomachus

Pierre de Fermat
1601-1665

- Fermat's Little Theorem - If a is any whole number and p is a prime that is not a factor of a, then p must be a factor of the number (a^{p-1}-1). Using modular arithmetic $a^{p-1} \equiv 1 \pmod{p}$
- Mentioned in a letter in 1640 with no proof, proved by Euler in 1736

https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
https://en.wikipedia.org/wiki/Pierre_de_Fermat

Leonhard Euler
1707-1783

- Euler proved a stronger version of Fermat's Little Theorem to help test for Euler Probable Primes:

  "If p is prime and a is any whole number, then p divides evenly into a^p-a."

https://en.wikipedia.org/wiki/Leonhard_Euler

Carl Friedrich Gauss
1777-1855

- At 15, he received a table of logarithms and one of primes for Christmas
- He noticed that primes are distributed to approximately $\pi(N) \sim N/\log(N)$, now called The Prime Number Theorem
- First mentioned it in a letter 50 years later.

https://en.wikipedia.org/wiki/Carl_Friedrich_Gauss

Bernhard Riemann
1826-1866

- One of the million-dollar problems is the Riemann Hypothesis: "All non-trivial zeros of the zeta function have real part of one half."
- $\zeta(s) = \sum (n^{-s})$ $(n=1,2,3,\ldots)$
  or
- $\zeta(s) = \prod (p^s)/(p^s - 1)$ (p prime, Euler product Formula)

https://en.wikipedia.org/wiki/Bernhard_Riemann
https://en.wikipedia.org/wiki/Riemann_zeta_function

- Early Primes
- **Named Primes**
- Hunting for Primes
- Visualizing Primes
- Harnessing Primes

"...there is no apparent reason why one number is prime and another not. To the contrary, upon looking at these numbers one has the feeling of being in the presence of one of the inexplicable secrets of creation.“ D. Zagier


2357
PRIME SUSPECTS
oneDUhfool
CARTOONS
WWW.KOMEDIE.CO.ZA

19937
99371
93719
37199
71993
19937

Circular prime

- A circular prime is prime with the property that the number generated at each intermediate step when cyclically permuting its (base 10) digits will be prime.
- For example, 1193 is a circular prime, since 1931, 9311 and 3119 all are also prime. Other examples are: 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933.
- A type of prime related to the circular primes are the permutable primes, which are a subset of the circular primes (every permutable prime is also a circular prime, but not necessarily vice versa).

https://en.wikipedia.org/wiki/Circular_prime

Absolute Prime

- Also called permutable prime, an absolute prime is a prime with at least two distinct digits which remains prime on every rearrangement (permutation) of the digits.
- For example, 337 is a permutable because each of 337, 373 and 733 are prime.
- Most likely, in base ten the only permutable primes are 13, 17, 37, 79, 113, 199, 337, and their permutations.

https://en.wikipedia.org/wiki/Permutable_prime

410256793
41256793
4125673
415673
45673
4567
467
67
7

Deletable Prime

- A deletable prime is a prime number which has the property that deleting digits one at a time in some order gives a prime at each step.
- For example, 410256793 is a deletable prime since each member of the sequence 410256793, 41256793, 4125673, 415673, 45673, 4567, 467, 67, 7 is prime.
- The first few deletable primes are 13, 17, 23, 29, 31, 37, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97, 103, 107, ... (OEIS A080608). It is conjectured that there are infinitely many deletable primes.

http://mathworld.wolfram.com/DeletablePrime.html

Emirp

- An emirp (prime spelled backwards) is a prime number that results in a different prime when its decimal digits are reversed. This definition excludes the related palindromic primes. The term reversible prime may be used to mean the same as emirp, but may also, ambiguously, include the palindromic primes.
- The sequence of emirps begins 13, 17, 31, 37, 71, 73, 79, 97, 107, 113, 149, 157, 167, 179, 199, 311, 337, ... (A006567 OEIS).
- All non-palindromic permutable primes are emirps.

https://en.wikipedia.org/wiki/Emirp

Palindromic Prime

- A palindromic prime is a prime that is a palindrome.
- A pyramid of palindromic primes by G. L. Honaker, Jr.

2

30203

133020331

1713302033171

12171330203317121

1512171330203317121 5121

181512171330203317121 5181

16181512171330203317121518161

3316181512171330203317121516133

- The first few decimal palindromic primes are: 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, … (A002385 OEIS)
- Note: Almost all palindrome numbers are composite

https://en.wikipedia.org/wiki/Palindromic_prime

Cuban prime

- A cuban prime (from the role cubes (third powers) play in the equations) is a prime number that is a solution to one of two different specific equations involving third powers of x and y. The first of these equations is:

$$p = \frac{x^3 - y^3}{x - y},\ x = y + 1,\ y > 0$$

and the first few cuban primes from this equation are: 7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919, 1657, ... (A002407 OEIS)

- The second of these equations is: $p = \frac{x^3 - y^3}{x - y},\ x = y + 2,\ y > 0.$

the first few cuban primes of this form are: 13, 109, 193, 433, 769, 1201, 1453, 2029, …(A002648 OEIS)

https://en.wikipedia.org/wiki/Cuban_prime

Cullen Primes

- Fr. James Cullen, SJ, was interested in the numbers $n \cdot 2^n + 1$ (denoted C_n). He noticed that the first, $C_1=3$, was prime, but with the possible exception of the 53rd, the next 99 were all composite.
- Later, Cunningham discovered that 5591 divides C_{53}, and noted these numbers are composite for all n in the range $2 < n < 200$, with the possible exception of 141.
- In a sense, almost all Cullen numbers are composite.

https://en.wikipedia.org/wiki/Cullen_number

Cullen Primes of the Second Kind

- Five decades later Raphael Robinson showed C_{141} was a prime. The only known Cullen primes C_n are those with n=1, 141, 4713, 5795, 6611, … (A005849 OEIS). Still, it is conjectured that there are infinitely many Cullen primes.
- These numbers are now called the Cullen numbers. Sometimes, the name "Cullen number" is extended to also include the Woodall numbers: $W_n = n \cdot 2^n - 1$. These are then the "Cullen primes of the second kind".

https://en.wikipedia.org/wiki/Woodall_number

Fermat Primes

- Fermat numbers are numbers of the form $2^{2^n}+1$
- Fermat believed every Fermat number is prime.
- The only known Fermat primes are F_0=3, F_1=5, F_2=17, F_3=257, and F_4=65537
- F_n is composite for $4 < n < 31$, (for example F_5=4294967297=641*6700417) but no one knows if there are infinitely many Fermat Primes.

https://en.wikipedia.org/wiki/Fermat_number

Euler PRP

- A probable prime (PRP) is an integer that satisfies a specific condition that is satisfied by all prime numbers, but which is not satisfied by most composite numbers. Different types of probable primes have different specific conditions. While there may be probable primes that are composite (called pseudoprimes), the condition is generally chosen in order to make such exceptions rare.
- Euler was able to prove a stronger statement of Fermat's Little Theorem which he then used as to test for Euler probable primes.
- If an Euler PRP n is composite, then we say n is an Euler pseudoprime.

https://en.wikipedia.org/wiki/Probable_prime

Fibonacci Prime

- A Fibonacci prime is a Fibonacci number that is prime.
- 1,1,2,3,5,8,13,21,34,55,89,144… 233, 1597, 28657, 514229, 433494437, 2971215073,… (A005478 OEIS)
- It is not known whether there are infinitely many Fibonacci primes.

https://en.wikipedia.org/wiki/Fibonacci_prime

Sophie Germain Prime

- A Sophie Germain prime is a prime p such that q=2p+1 is also prime: 2, 3, 5, 11, 23, … (OEIS A005384)
- Around 1825, Sophie Germain proved that the first case of Fermat's last theorem is true for such primes, i.e., if p is a Sophie Germain prime, then there do not exist integers x, y, and z different from 0 and none a multiple of p such that $x^p+y^p=z^p$.

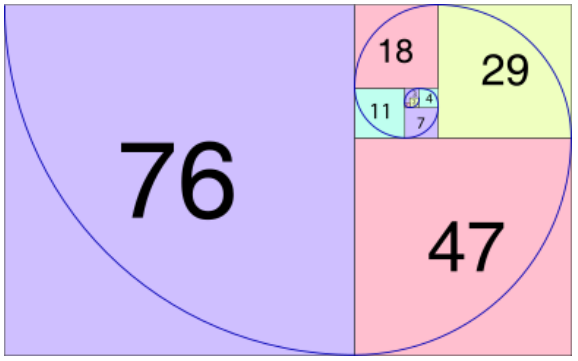
https://en.wikipedia.org/wiki/Sophie_Germain_prime

Illegal Primes

- Phil Carmody published the first known illegal prime. When converted to hexadecimal, the number is a compressed form of the computer code to crack Content Scramble System (CSS) scrambling. A digital rights management (DRM) and encryption system employed on many commercially produced DVD-Video discs.
- It is "illegal" because publishing this number could be considered trafficking in a circumvention device, in violation of the Digital Millenium Copyright Act.

https://en.wikipedia.org/wiki/Illegal_prime

Lucas Prime



- A Lucas prime is a Lucas number that is prime. The Lucas numbers can be defined as follows:

$$L_1 = 1, \quad L_2 = 3 \text{ and } L_n = L_{n-1} + L_{n-2} \ (n > 2)$$

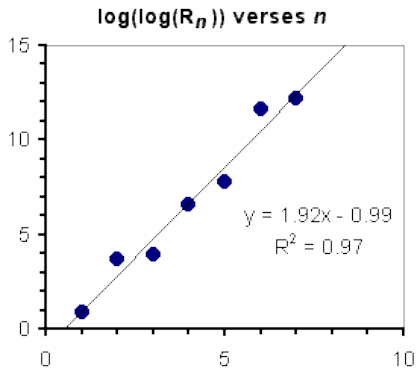
- Lucas numbers are like Fibonacci numbers, except that they start with 1 and 3 instead of 1 and 1.
- The first few Lucas primes are: 2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, (A005479 OEIS).

https://en.wikipedia.org/wiki/Lucas_number

Royal Prime

- Royal Primes are primes where the digits are all prime and a prime can be constructed through addition or subtraction using all the digits (23, 53, 223, 227,…).
- These are named after Royal Penewell, treasurer of the Puget Sound Council of Teachers of Mathematics (PSCTM) from 1973 to 2005 and who was born in `23, the first Royal Prime of the century.

Repunit Primes



- Repunits are positive integers in which all the digits are 1, denoted as $R_1 = 1$, $R_2=11$, etc. Of these, the following are known to be prime:11, 1111111111111111111, and 1111111111111111111111 (2, 19, and 23 digits), R_{317} $(10^{317}-1)/9$, and $R_{1,031}$ $(10^{1031}-1)/9$.
- In 1999 Dubner discovered that $R_{49081} = (10^{49081}-1)/9$ was a probable prime, in 2000 Baxter discovered the next repunit probable prime is R_{86453}, and in 2007 Dubner identified R_{109297} as a probable prime.
- Even though only a few are known, it has been conjectured that there are infinitely many repunit primes. As illustrated by a graph of repunit primes in a grid of log(log(Rn)) versus n. The points appear to lie very close to a line of constant slope.

https://en.wikipedia.org/wiki/Repunit

Ferrier's Prime

- Ferrier's Prime is the largest prime found before electronic calculators. Ferrier's Prime = $(2^{148}+1)/17$ =

209889366574405864861512642566102225938639 21

http://mathworld.wolfram.com/FerriersPrime.html

Mersenne Numbers

For $n = 1, 2, 3, \ldots$, the **Mersenne numbers** are those generated by the formula

$$M_n = 2^n - 1.$$

1. If n is composite, then M_n is composite.
2. If n is prime, then M_n may be prime or composite.

The prime values of M_n are called **Mersenne primes**.

Marin Mersenne (1588–1648), was a seventeenth-century monk.

https://en.wikipedia.org/wiki/Marin_Mersenne

Mersenne Prime

- Mersenne claimed that for n= 2,3,5,7,13,19,31,67,127,257 would yield primes (note M_{11}=2047=23*89)
- A Gaussian Mersenne prime is a prime using Gaussian integers (1, -1, *i*, -*i*).

https://en.wikipedia.org/wiki/Mersenne_prime

Gaussian Mersenne

- There are no primes of the form b^n-1 for any other positive integer b because these numbers are all divisible by b-1. This is a problem because b-1 is not a unit (that is, it is not +1 or -1).
- If we switch to the Gaussian integers, the corresponding primes in the form $(1 \pm i)^n-1$ for the following values of n:
- 2, 3, 5, 7, 11, 19, 29, 47, 73, 79, 113, 151, 157, 163,… (A057429 OEIS)

http://primes.utm.edu/glossary/xpage/GaussianMersenne.html

Landry and Aurifeuille

- The mathematician Landry devoted a good part of his life to factoring 2^n+1 and finally found the factorization of $2^{58}+1$ in 1869 (so he was essentially the first to find the Gaussian Mersenne with n=29).
- Just ten years later, Aurifeuille found the Gaussian factorization, which would have made Landry's massive effort trivial.

Double Mersenne Prime

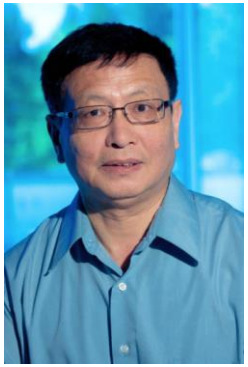
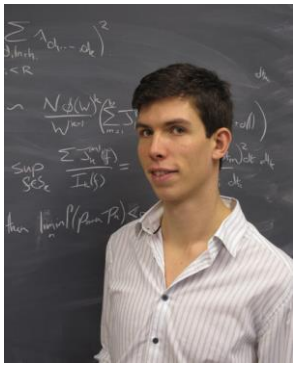
- A double Mersenne number is a Mersenne number of the form $M_{M_p} = 2^{2^p-1} - 1$ where p is a prime exponent.
- A double Mersenne number that is prime is called a double Mersenne prime. Since a Mersenne number Mp can be prime only if p is prime a double Mersenne M_{M_p} can be prime only if Mp is itself a Mersenne prime.
- For the first values of p for which Mp is prime, M_{M_p} is known to be prime for p = 2, 3, 5, 7 while explicit factors of M_{M_p} have been found for p = 13, 17, 19, and 31. OEIS A077586

https://en.wikipedia.org/wiki/Double_Mersenne_number

Twin Primes

- Twin primes are primes of the form p and $p + 2$
- The first few twin prime pairs are:
- (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), … OEIS A077800.
- The largest known twin primes are of the form $2996863034895 \cdot 2^{1,290,000} \pm 1$.
- The were found by the efforts of two research groups: Twin Prime Search and PrimeGrid in 2016.

http://en.wikipedia.org/wiki/Twin_prime


Twin Primes

- Conjectured but not proven that there are an infinite number of twin primes.
- All twin primes except (3, 5) are of the form $6n \pm 1$.
- $2486!!!! \pm 1$ are twin primes with 2151 digits
- The work of Yitang Zhang in 2013, as well as work by James Maynard, Terence Tao and others, has made substantial progress towards proving that there are infinitely many twin primes, but at present it remains unsolved.

https://www.quantamagazine.org/mathematicians-team-up-on-twin-primes-conjecture-20131119/

Cousin and Sexy Primes

- **Cousin** primes are primes of the form p and $p + 4$
- The first few Cousin prime pairs are:
- (3, 7), (7, 11), (13, 17), (19, 23), (37, 41), (43, 47), (67, 71), (79, 83), (97, 101) OEIS A023200
- **Sexy** primes are primes of the form p and $p + 6$
- The first few Sexy primes are:
- (5,11), (7,13), (11,17), (13,19), (17,23), (23,29), (31,37), (37,43), (41,47), (47,53), (53,59), (61,67), (67,73), (73,79), (83,89), (97,103)… OEIS A023201

http://en.wikipedia.org/wiki/Sexy_prime
http://en.wikipedia.org/wiki/Cousin_prime

Polignac's conjecture

- For any positive even number n, there are infinitely many prime gaps of size n. In other words: There are infinitely many cases of two consecutive prime numbers with difference n.

https://en.wikipedia.org/wiki/Polignac%27s_conjecture

Naughty Prime

- Naughty primes: primes in which the number of zeros is greater than the number of all other digits.
- That is composed of mostly naughts (i.e., zeros). Here are a few: 10007, 10009, 40009, 70001, 70003, 70009, 90001, 90007,… (A164968 OEIS)

http://primes.utm.edu/glossary/xpage/NaughtyPrime.html

Wieferich Prime

- By Fermat's Little Theorem any prime p divides $2^{p-1}-1$. A prime p is a Wieferich prime if p^2 divides $2^{p-1}-1$. In 1909 Wieferich proved that if the first case of Fermat's last theorem is false for the exponent p, then p satisfies this criterion. Since 1093 and 3511 are the only known such primes (and they have been checked to at least 32,000,000,000,000), this is a strong statement!
- In 1910 Mirimanoff proved the analogous theorem for 3 but there is little glory in being second. Such numbers are not called Mirimanoff primes.
- Over time, connections discovered have extended to cover more general subjects such as number fields and the abc conjecture.

https://en.wikipedia.org/wiki/Wieferich_prime

Colbert Prime

- A Colbert number is any megaprime whose discovery contributes to the long sought-after proof that k = 78557 is the smallest Sierpinski number. These are whimsically named after Stephen T. Colbert, the American comedian, satirist, actor and writer. There are currently only six known Colbert Numbers:

- $10223 \cdot 2^{31172165}+1$ 9,383,761 digits
- $19249 \cdot 2^{13018586}+1$ 3,918,990 digits
- $27653 \cdot 2^{9167433}+1$ 2,759,677 digits
- $28433 \cdot 2^{7830457}+1$ 2,357,207 digits
- $33661 \cdot 2^{7031232}+1$ 2,116,617 digits
- $5359 \cdot 2^{5054502}+1$ 1,521,561 digits

http://primes.utm.edu/glossary/xpage/ColbertNumber.html
https://en.wikipedia.org/wiki/Sierpinski_number

Factorial prime

- A factorial prime is a prime number that is one less or one more than a factorial (all factorials > 1 are even).

- The first 10 factorial primes (for n = 1, 2, 3, 4, 6, 7, 11, 12, 14) are (A088054 OEIS): 2 (0! + 1 or 1! + 1), 3 (2! + 1), 5 (3! − 1), 7 (3! + 1), 23 (4! − 1), 719 (6! − 1), 5039 (7! − 1), 39916801 (11! + 1), 479001599 (12! − 1), 87178291199 (14! − 1), ...

https://en.wikipedia.org/wiki/Factorial_prime

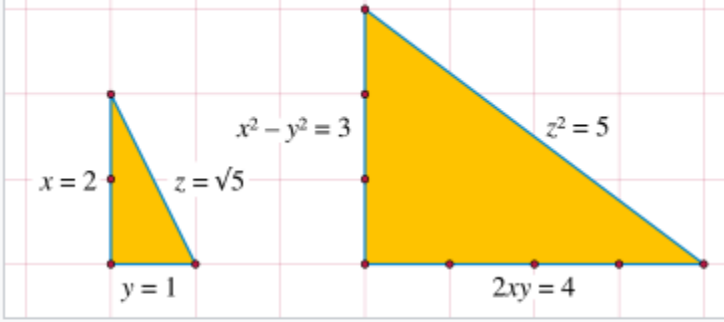
Primorial prime

- Prime numbers of the form $p_n\# \pm 1$, where $p_n\#$ is the primorial of p_n (the product of the first n primes).
- $p_n\# - 1$ is prime for n = 2, 3, 5, 6, 13, 24, ... (A057704 OEIS)
- $p_n\# + 1$ is prime for n = 0, 1, 2, 3, 4, 5, 11, ... (A014545 OEIS)

https://en.wikipedia.org/wiki/Primorial_prime

Pythagorean prime

https://en.wikipedia.org/wiki/Pythagorean_prime



The Pythagorean prime 5 and its square root are both hypotenuses of right triangles with integer legs. The formulas show how to transform any right triangle with integer legs into another right triangle with integer legs whose hypotenuse is the square of the first triangle's hypotenuse.

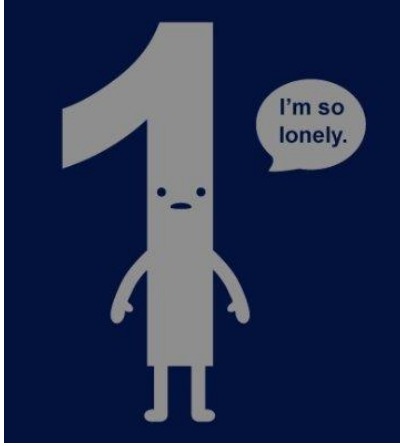
- A **Pythagorean prime** is a prime number of the form $4n + 1$. Pythagorean primes are exactly the odd prime numbers that are the sum of two squares; this characterization is Fermat's theorem on sums of two squares.
- Equivalently, by the Pythagorean theorem, they are the odd prime numbers p for which $\sqrt{p}$ is the length of the hypotenuse of a right triangle with integer legs, and they are also the prime numbers p for which p itself is the hypotenuse of a Pythagorean triangle.
- The first few Pythagorean primes are 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, ... OEIS A002144

More lists of notable types

- Still MORE!!!
- Ordinary primes; Pierpont primes; plateau primes, which have the same interior numbers and smaller numbers on the ends, such as 1777771; snowball primes, which are prime even if you haven't finished writing all the digits, like 73939133; Titanic primes; Wagstaff primes; Wall-Sun-Sun primes; Wolstenholme primes; Woodall primes; and Yarborough primes, which have neither a 0 nor a 1. A beastly prime has 666 in the center, etc.

https://en.wikipedia.org/wiki/List_of_prime_numbers

Why is the number one not prime?



- The number one is far more special than a prime! It is the unit (the building block) of the positive integers, hence the only integer which merits its own existence axiom in Peano's axioms. It is the only multiplicative identity ($1 \cdot a = a \cdot 1 = a$ for all numbers a). It is the only perfect nth power for all positive integers n. It is the only positive integer with exactly one positive divisor. But it is not a prime. So why not?
- Answer One: By definition of prime!
- Answer Two: Because of the purpose of primes.
- Answer Three: Because one is a unit.
- Answer Four: By the Generalized Definition of Prime.

https://primes.utm.edu/notes/faq/one.html

Oh, what a year makes: 2017

- We all know that 2017 is a prime number, but it is more than just another prime number.
- 2017π (rounds to nearest integer) is a prime.
- 2017e (rounds to nearest integer) is a prime.
- The sum of all odd primes up to 2017 is a prime number, i.e. 3+5+7+11+...+2017 is a prime number.
- The sum of the cube of gap of primes up to 2017 is a prime number. That is $(3-2)^3 + (5-3)^3 + (7-5)^3 + (11-7)^3 + \ldots + (2017-2011)^3$ is a prime number.
- The prime number before 2017 is 2017+(2-0-1-7), which makes it a sexy prime, and the prime after 2017 is 2017+(2+0+1+7).

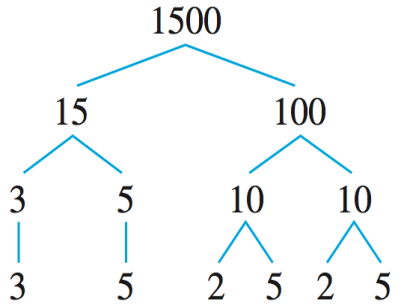
Number Facts about 2017 in 2:17
https://www.iafrikan.com/2017/01/01/hello-2017-more-than-prime-number/

Oh, what a year makes: 2017

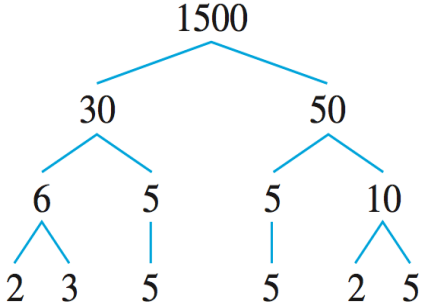
- Insert 7 into any two digits of 2017, it is still a prime number, i.e. 27017, 20717, 20177 are all primes. Plus, 20177 is also a prime number.
- Since all digits of 2017 is less than 8, it can be viewed as an octal. 2017 is still a prime number as an octal.
- 2017 can be written as a sum of three cubes of primes, i,e, $p^3 + q^3 + r^3$ for some primes p, q, r. 2017 can be written as a sum of cubes of five distinct integers.
- 2017 can be written as x^2+y^2, x^2+2y^2, x^2+3y^2, x^2+4y^2 x^2+6y^2, x^2+7y^2, x^2+8y^2, x^2+9y^2 (for positive integers x, y).
- 20170123456789 is also a prime.
- The 2017th prime number is 17539 and 201717539 is also a prime. Let p=2017, then both (p+1)/2 and (p+2)/3 are prime numbers.
- The first ten digits of the decimal expansion of the cubic root of 2017 contains all different digits 0~9. 2017 is the least integer has this property.
- $2017 = 2^{11}$ - 11th prime

- Early Primes
- Named Primes
- **Hunting for Primes**
- Visualizing Primes
- Harnessing Primes

"God may not play dice with the universe, but something strange is going on with the prime numbers."
C. Pomerance, suggesting something that P. Erdös might have said.



The Fundamental Theorem of Arithmetic



Every natural number can be expressed in one and only one way as a product of primes (if the order of the factors is disregarded). This unique product of primes is called the **prime factorization** of the natural number.

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic

Can the Primes end?

- At first, the primes are plentiful.

- But as our sights climb higher, the primes start thinning out. Long gaps pass without one

- The largest known prime gap with identified proven primes as gap ends has length 1,113,106

http://primes.utm.edu/notes/GapsTable.html

How Many Primes?

There is no largest prime number. Euclid proved this around 300 B.C.

https://mathwithbaddrawings.com/2013/07/04/a-fight-with-euclid/

The Infinitude of Primes

EXAMPLE 1 Proving the Infinitude of Primes

Prove by contradiction that there are infinitely many primes.

SOLUTION

Suppose there is a largest prime number, called P. Form the number M such that

$$M = p_1 \cdot p_2 \cdot p_3 \cdots \cdot P + 1,$$

where $p_1, p_2, p_3, \ldots, P$ represent all the primes less than or equal to P. Now the number M must be either prime or composite.

1. Suppose that M is prime.
   M is obviously larger than P, so if M is prime, it is larger than the assumed largest prime P. We have reached a *contradiction*.
2. Suppose that M is composite.
   If M is composite, it must have a prime factor. But none of $p_1, p_2, p_3, \ldots, P$ are factors of M, because division by each will leave a remainder of 1. (Recall the above argument.) So if M has a prime factor, it must be greater than P. But this is a *contradiction*, because P is the assumed largest prime.

In either case 1 or 2, we reach a contradiction. The whole argument was based upon the assumption that a largest prime exists, but as this leads to contradictions, there must be no largest prime, or equivalently, ***there are infinitely many primes.*** ■■■

https://en.wikipedia.org/wiki/Euclid%27s_theorem

The Infinitude of Primes

- Another proof, by the Swiss mathematician Leonhard Euler, relies on the fundamental theorem of arithmetic: that every integer has a unique prime factorization. If P is the set of all prime numbers, Euler wrote that:

$$\prod_{p \in P} \frac{1}{1 - 1/p} = \prod_{p \in P} \sum_{k \geq 0} \frac{1}{p^k} = \sum_n \frac{1}{n}.$$

- The first equality is given by the formula for a geometric series in each term of the product. The second equality is a special case of the Euler product formula for the Riemann zeta function. To show this, distribute the product over the sum:

$$\prod_{p \in P} \sum_{k \geq 0} \frac{1}{p^k} = \sum_{k \geq 0} \frac{1}{2^k} \times \sum_{k \geq 0} \frac{1}{3^k} \times \sum_{k \geq 0} \frac{1}{5^k} \times \sum_{k \geq 0} \frac{1}{7^k} \times \cdots$$

$$= \sum_{k, \ell, m, n, \cdots \geq 0} \frac{1}{2^k 3^\ell 5^m 7^n \cdots} = \sum_n \frac{1}{n}$$

- in the result, every product of primes appears exactly once and so by the fundamental theorem of arithmetic the sum is equal to the sum over all integers. The sum on the right is the harmonic series, which diverges. Thus the product on the left must also diverge. Since each term of the product is finite, the number of terms must be infinite; therefore, there is an infinite number of primes.

The Infinitude of Primes

- Proof using the irrationality of π.
- Representing the Leibniz formula for π as an Euler product gives

$$\frac{\pi}{4} = \frac{3}{4} \times \frac{5}{4} \times \frac{7}{8} \times \frac{11}{12} \times \frac{13}{12} \times \frac{17}{16} \times \frac{19}{20} \times \frac{23}{24} \times \frac{29}{28} \times \frac{31}{32} \times \cdots$$

- The numerators of this product are the odd prime numbers, and each denominator is the multiple of four nearest to the numerator.

- If there were finitely many primes this formula would show that π is a rational number whose denominator is the product of all multiples of 4 that are one more or less than a prime number, contradicting the fact that π is irrational.

https://en.wikipedia.org/wiki/Euclid%27s_theorem

Primality test

- A primality test is an algorithm for determining whether an input number is prime.
- The simplest primality test is trial division: Given an input number n, check whether any prime integer p from 2 to $\sqrt{n}$ evenly divides n. If n is divisible by any p then n is composite, otherwise it is prime.

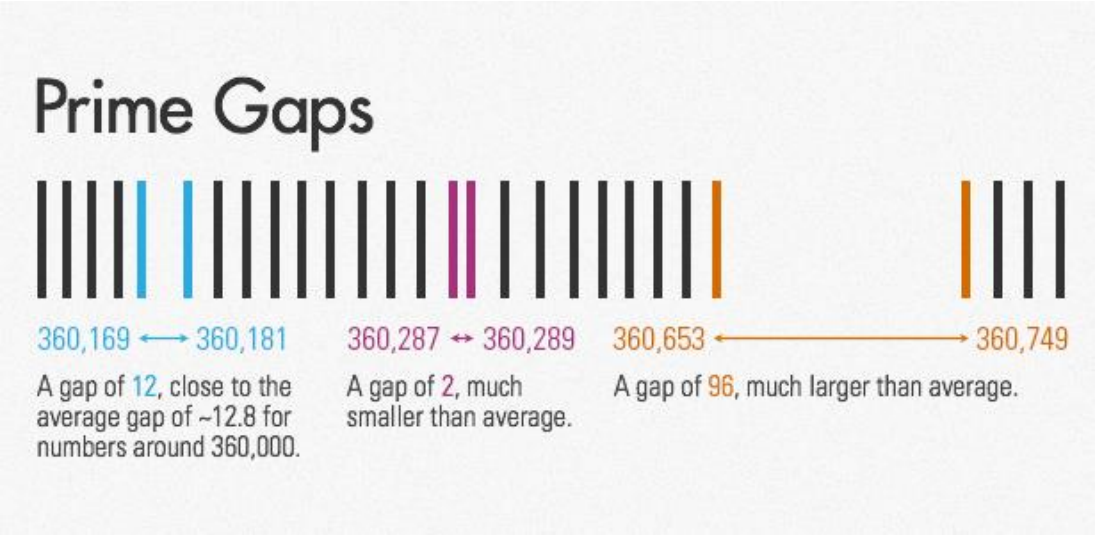
$$\text{If } a \cdot b = N \text{ where } 1 < a \leq b < N$$

$$N = ab \geq a^2 \iff a^2 \leq N \implies a \leq \sqrt{N}$$

https://en.wikipedia.org/wiki/Primality_test

Prime gap

- A prime gap is the difference between two successive prime numbers.



- The prime number theorem, says that the "average length" of the gap between a prime p and the next prime is ln(p). The actual length of the gap might be much more or less than this.

https://en.wikipedia.org/wiki/Prime_gap

Bertrand's postulate

- Is a theorem stating that for any integer n>1 there is always at least one prime p such that n<p<2n.
- The conjecture was first made by Bertrand in 1845
- It was proved in 1850 by Chebyshev
- The first elementary proof was by Ramanujan, and later improved by a 19-year-old Erdős in 1932.

https://en.wikipedia.org/wiki/Bertrand%27s_postulate

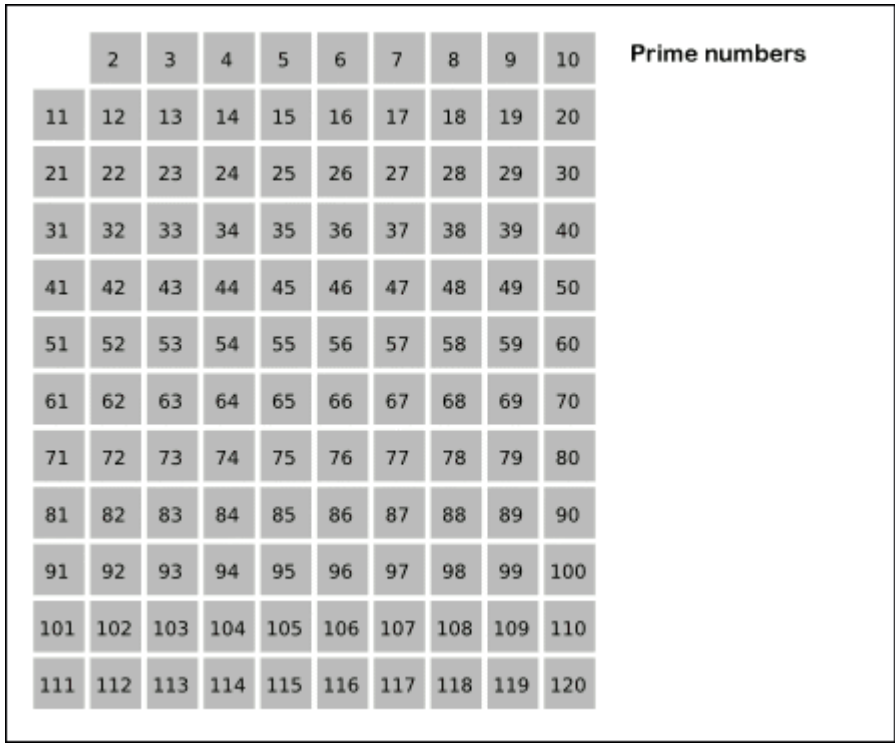
Sieve of Eratosthenes

A simple, ancient algorithm for finding all prime numbers up to any given limit. Attributed to Eratosthenes of Cyrene, a Greek mathematician.

It does so by iteratively marking as composite (i.e., not prime) the multiples of each prime, starting with the first prime number, 2. The multiples of a given prime are generated as a sequence of numbers starting from that prime, with constant difference between them that is equal to that prime. This is the sieve's key distinction from using trial division to sequentially test each candidate number for divisibility by each prime.

Sieve of Eratosthenes

- Create a list of consecutive integers from 2 through n: (2, 3, 4, ..., n).
- Initially, let p equal 2, the smallest prime number.
- Enumerate the multiples of p by counting to n from 2p in increments of p, and mark them in the list (these will be 2p, 3p, 4p, ...; the p itself should not be marked).
- Find the first number greater than p in the list that is not marked. If there was no such number, stop. Otherwise, let p now equal this new number (which is the next prime), and repeat from step 3.
- When the algorithm terminates, the numbers remaining not marked in the list are all the primes below n.
- The main idea here is that every value given to p will be prime, because if it were composite it would be marked as a multiple of some other, smaller prime. Note that some of the numbers may be marked more than once (e.g., 15 will be marked both for 3 and 5).



Competition for Eratosthenes

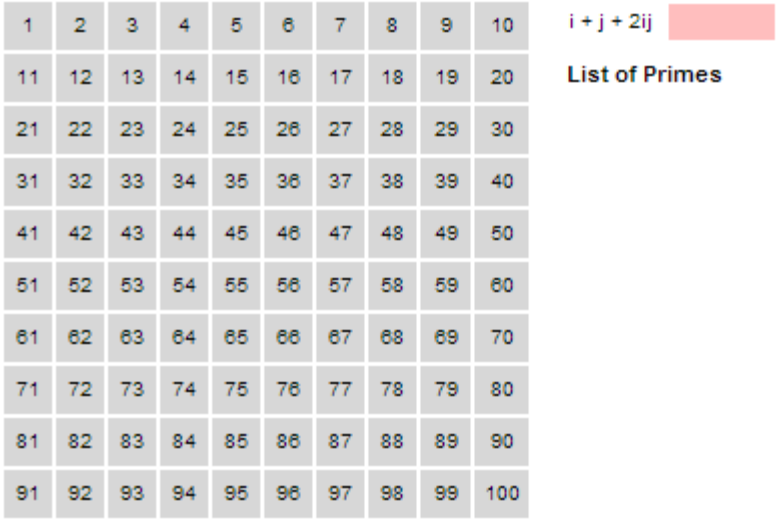
- A modern algorithm for finding all prime numbers up to a specified integer.
- Compared with the ancient sieve of Eratosthenes, which marks off multiples of primes, the sieve of Atkin does some preliminary work and then marks off multiples of squares of primes, thus achieving a better theoretical asymptotic complexity.
- It was created in 2003 by A. O. L. Atkin and Daniel J. Bernstein.

Sieve of Atkin

- The algorithm:
- All remainders are modulo-sixty remainders (divide the number by 60 and return the remainder).
- All numbers, including x and y, are positive integers.
- Flipping an entry in the sieve list means to change the marking (prime or nonprime) to the opposite marking.
- This results in numbers with an odd number of solutions to the corresponding equation being potentially prime (prime if they are also square free), and numbers with an even number of solutions being composite.

1. Create a results list, filled with 2, 3, and 5.
2. Create a sieve list with an entry for each positive integer; all entries of this list should initially be marked non prime (composite).
3. For each entry number n in the sieve list, with modulo-sixty remainder r :
    1. If r is 1, 13, 17, 29, 37, 41, 49, or 53, flip the entry for each possible solution to $4x^2 + y^2 = n$.
    2. If r is 7, 19, 31, or 43, flip the entry for each possible solution to $3x^2 + y^2 = n$.
    3. If r is 11, 23, 47, or 59, flip the entry for each possible solution to $3x^2 - y^2 = n$ when $x > y$.
    4. If r is something else, ignore it completely.
4. Start with the lowest number in the sieve list.
5. Take the next number in the sieve list still marked prime.
6. Include the number in the results list.
7. Square the number and mark all multiples of that square as non prime. Note that the multiples that can be factored by 2, 3, or 5 need not be marked, as these will be ignored in the final enumeration of primes.
8. Repeat steps four through seven.

Sieve of Sundaram



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

- A simple deterministic algorithm for finding all the prime numbers up to a specified integer. It was discovered by Indian mathematician S. P. Sundaram in 1934.
- Start with a list of the integers from 1 to n. From this list, remove all numbers of the form i + j + 2ij where: $i, j \in \mathbb{N}, 1 \leq i \leq j, and\ i + j + 2ij \leq n$
- The remaining numbers are doubled and incremented by one, giving a list of the odd prime numbers (i.e., all primes except 2) below 2n + 2.
- The sieve of Sundaram sieves out the composite numbers just as sieve of Eratosthenes does, but even numbers are not considered; the work of "crossing out" the multiples of 2 is done by the final double-and-increment step.

Quadratic Sieve

- Integer factorization algorithm
- Data collection phase computes a congruence of squares modulo the number to be factored
- Data processing phase uses Gaussian elimination to reduce a matrix of the exponents of prime factors of the remainders found in the data collection phase.
- It is a general-purpose factorization algorithm, meaning that its running time depends solely on the size of the integer to be factored, and not on special structure or properties.

https://en.wikipedia.org/wiki/Quadratic_sieve

Number Field Sieve

An extremely fast factorization method developed by Pollard which was used to factor the RSA-130 number. This method is the most powerful known for factoring general numbers.

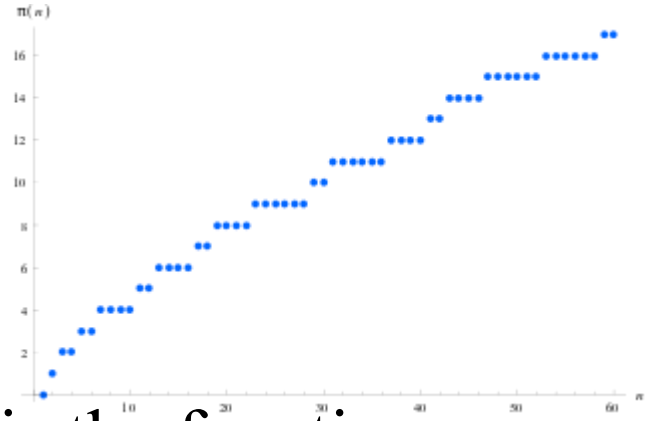
https://en.wikipedia.org/wiki/General_number_field_sieve

The First 300 Primes

For more information on primes see http://primes.utm.edu/

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107
109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223
227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337
347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457
461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593
599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719
727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857
859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997
1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093
1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213
1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303
1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439
1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543
1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627
1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753
1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877
1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987

Prime-counting function



- The prime-counting function is the function counting the number of prime numbers less than or equal to some real number n. It is denoted by π(n)

n	Number of Primes up to *n*	Proportion of Primes up to *n* (Number of Primes ≤ *n*)/*n*	1/Ln(*n*)	Proportion − 1/Ln(*n*)
10	4	0.4	0.43429. . .	–0.03429. . .
100	25	0.25	0.21714. . .	0.03285. . .
1000	168	0.168	0.14476. . .	0.02323. . .
10,000	1229	0.1229	0.10857. . .	0.01432. . .
100,000	9592	0.09592	0.08685. . .	0.00906. . .
1,000,000	78,498	0.078498	0.07238. . .	0.00611. . .
10,000,000	664,579	0.0664579	0.06204. . .	0.00441. . .
100,000,000	5,761,455	0.05761455	0.05428. . .	0.00332. . .
1,000,000,000	50,847,534	0.050847534	0.04825. . .	0.00259. . .

https://en.wikipedia.org/wiki/Prime-counting_function

Gauss and Legendre

- Gauss noticed the frequency of primes approached N/log(N) but didn't publish.
- Legendre noticed that the frequency of primes approaches N/(log(N)-1.80366) and published in 1808, finding that yet again, Gauss had been there first.

https://en.wikipedia.org/wiki/Adrien-Marie_Legendre

Prime Number Theorem

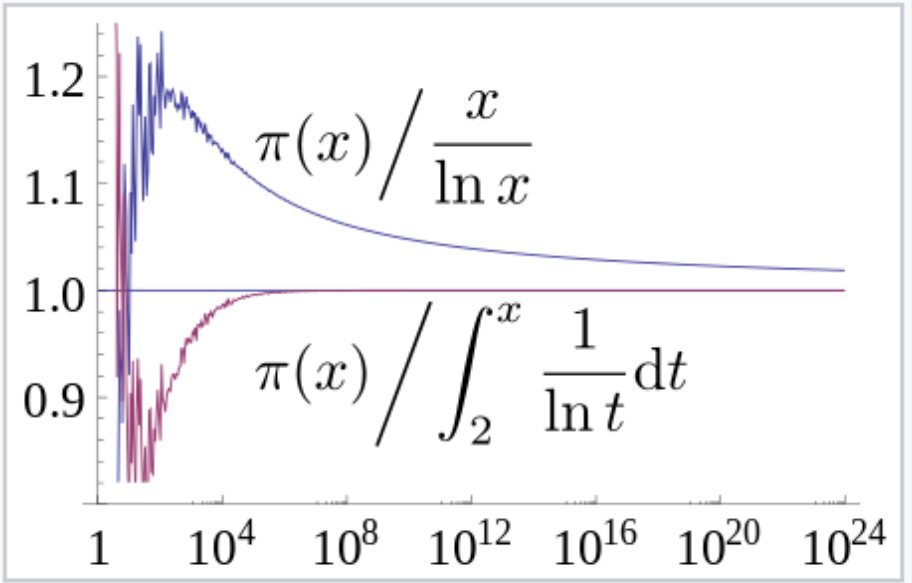
- Gauss mentioned in a letter, but did not prove, that the number of primes less than x can be approximated by:

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

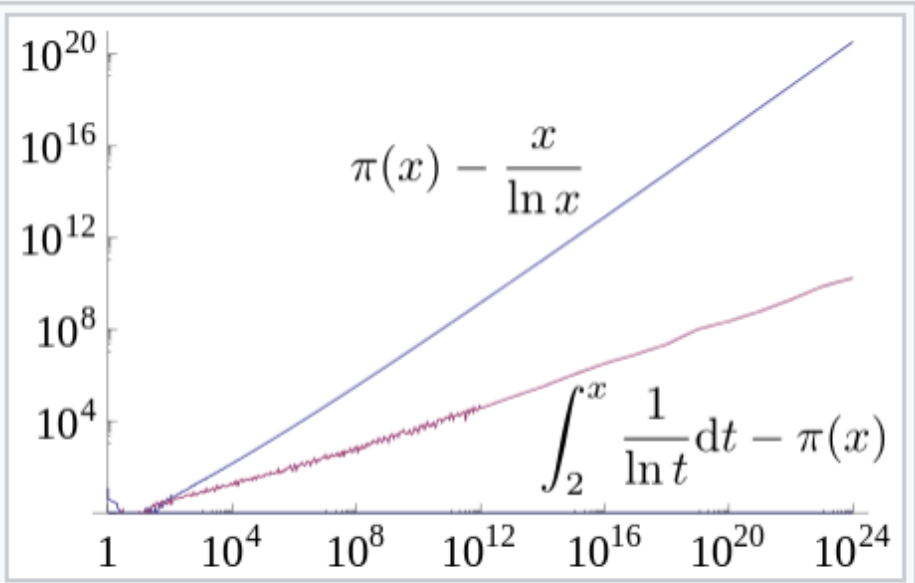
- Proved independently by Jacques Hadamard of France and Charles de la Vallee Poussin of Belgium in 1896

https://en.wikipedia.org/wiki/Prime_number_theorem

Prime Number Theorem



Graph showing ratio of the prime-counting function $\pi(x)$ to two of its approximations, $x / \log x$ and $\mathrm{Li}(x)$. As x increases (note x axis is logarithmic), both ratios tend towards 1. The ratio for $x / \log x$ converges from above very slowly, while the ratio for $\mathrm{Li}(x)$ converges more quickly from below.



Log-log plot showing absolute error of $x / \log x$ and $\mathrm{Li}(x)$, two approximations to the prime-counting function $\pi(x)$. Unlike the ratio, the difference between $\pi(x)$ and $x / \log x$ increases without bound as x increases. On the other hand, $\mathrm{Li}(x) - \pi(x)$ switches sign infinitely many times.

Peter Gustav Lejeune-Direchlet

- Direchlet used Euler's connection of primes to the zeta function to prove Fermat's conjecture about infinitely many primes modulo 1 to any base
- The Riemann Zeta function can be calculated as

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \quad \mathrm{Re}(s) > 1$$

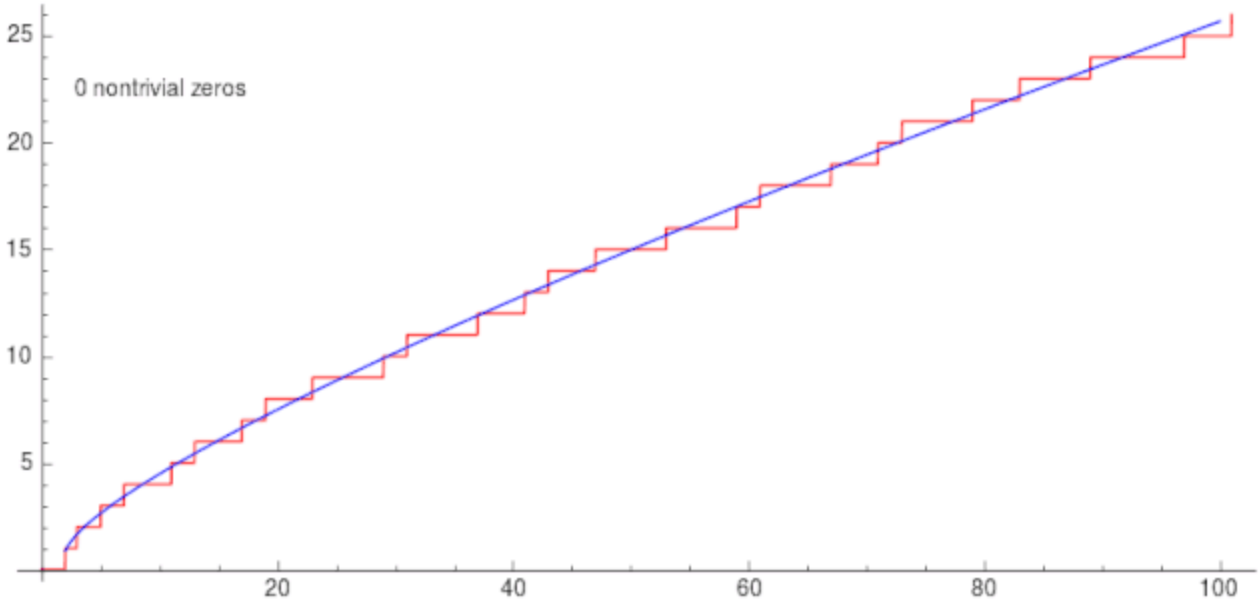
- Notable values: for s=1, we get the harmonic series

$$\zeta(1) = 1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots = \infty$$

- For s=2, the demonstration of this equality is known as the Basel problem. $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6} \approx 1.645$

https://en.wikipedia.org/wiki/Peter_Gustav_Lejeune_Dirichlet

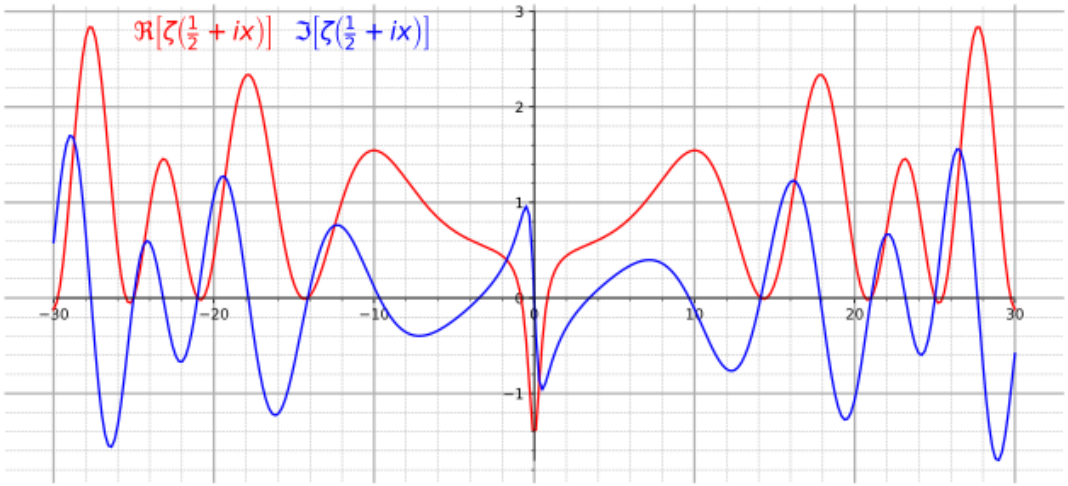
Density Function



- Gauss introduced π(x)= # of primes less than or equal to x
- Riemann showed that the zeta function can also be written as a product over its *zeroes* in the complex plane:

$$\zeta(s) = f(s)(1 - s/\rho_1)(1 - s/\rho_2)(1 - s/\rho_3)\cdots$$

Riemann's Hypothesis



- Fourier's technique of adding waveforms to model complex graphs, Cauchy's weird world of complex numbers, and Direchlet's fascination with Euler's zeta function are basic to Bernhard Riemann's conjecture:

"The real part of any non-trivial zero of the Riemann zeta function is 1/2."

https://en.wikipedia.org/wiki/Riemann_hypothesis

The Search for Large Primes

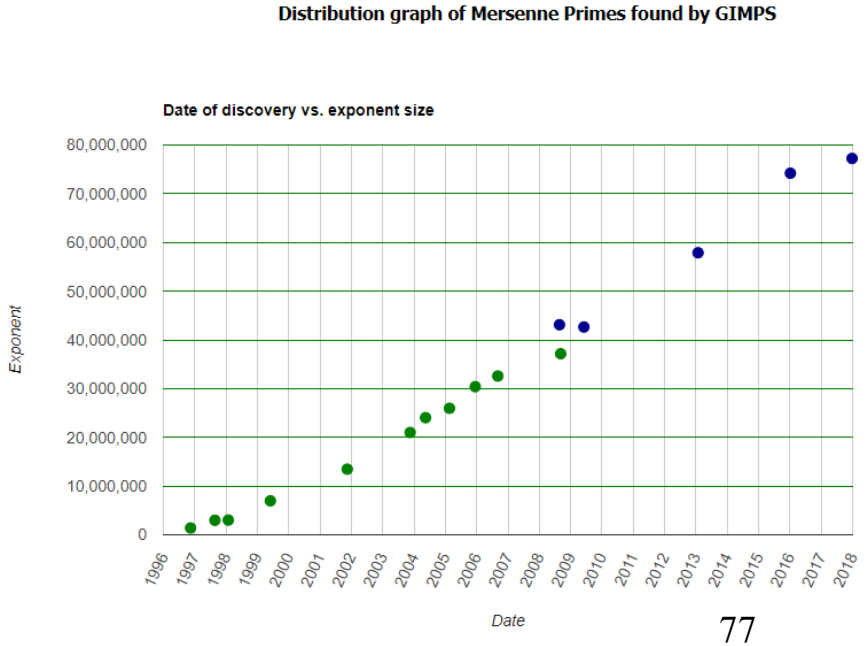
Primes are the basis for modern cryptography systems, or secret codes. Mathematicians continue to search for larger and larger primes.

The theory of prime numbers forms the basis of security systems for vast amounts of personal, industrial, and business data.

Great International Prime Search

Great International Mersenne Prime Search lets anyone with a computer be part of the search for the next record-setting prime.

https://www.mersenne.org/



Lucas-Lehmer Number

The Lucas-Lehmer test is an efficient deterministic primality test for determining if a Mersenne number M_n is prime. A Mersenne Number $2^n - 1$ is prime if it divides the Lucas-Lehmer number L_n where $L_n=(L_{n-1})^2-2$

https://en.wikipedia.org/wiki/Lucas%E2%80%93Lehmer_primality_test

Largest known prime number

- The longest record-holder known was M_{19} = 524,287, which was the largest known prime for 144 years. Almost no records are known before 1456.

Number	Decimal expansion (only for numbers < 10^{50})	Digits	Year found	Notes (for larger Mersenne primes, see Mersenne prime)
11	11	2	~1650 BCE	ancient Egyptians (disputed)[8]
7	7	1	~400 BCE	It was known to Philolaus that 7 is a prime[9]
M_7	127	3	~300 BCE	It was known to Euclid that 127 and 89 are primes[10][11]
M_{13}	8,191	4	1456	Anonymous discovery
M_{17}	131,071	6	1460	Anonymous discovery
M_{19}	524,287	6	1588	Found by Pietro Cataldi
$\frac{2^{32}+1}{641}$	6,700,417	7	1732	Found by Leonhard Euler
M_{31}	2,147,483,647	10	1772	Found by Leonhard Euler
$\frac{2^{64}+1}{274177}$	67,280,421,310,721	14	1855	Found by Thomas Clausen
M_{127}	170,141,183,460,469,231,731,687,303,715,884,105,727	39	1876	Found by Édouard Lucas
$\frac{2^{148}+1}{17}$	20,988,936,657,440,586,486,151,264,256,610,222,593,863,921	44	1951	Found by Aimé Ferrier with a mechanical calculator; the largest record not set by computer.
$180\times(M_{127})^2+1$		79	1951	Using Cambridge's EDSAC computer

Largest known prime number

- Curtis Niles Cooper is an American mathematician. He currently is a professor at the University of Central Missouri, in the Department of Mathematics and Computer Science.

40	20,996,011	125976895450...762855682047	6,320,430	2003 November 17	GIMPS / Michael Shafer[65]	LLT / Prime95 on 2 GHz Dell Dimension
41	24,036,583	299410429404...882733969407	7,235,733	2004 May 15	GIMPS / Josh Findley[66]	LLT / Prime95 on 2.4 GHz Pentium 4
42	25,964,951	122164630061...280577077247	7,816,230	2005 February 18	GIMPS / Martin Nowak[67]	LLT / Prime95 on 2.4 GHz Pentium 4
43	30,402,457	315416475618...411652943871	9,152,052	2005 December 15	GIMPS / Curtis Cooper & Steven Boone[68]	LLT / Prime95 on 2 GHz Pentium 4
44	32,582,657	124575026015...154053967871	9,808,358	2006 September 4	GIMPS / Curtis Cooper & Steven Boone[69]	LLT / Prime95 on 3 GHz Pentium 4
45	37,156,667	202254406890...022308220927	11,185,272	2008 September 6	GIMPS / Hans-Michael Elvenich[70]	LLT / Prime95 on 2.83 GHz Core 2 Duo
46[n 1]	42,643,801	169873516452...765562314751	12,837,064	2009 April 12[n 2]	GIMPS / Odd M. Strindmo[71][n 3]	LLT / Prime95 on 3 GHz Core 2
47[n 1]	43,112,609	316470269330...166697152511	12,978,189	2008 August 23	GIMPS / Edson Smith[70]	LLT / Prime95 on Dell Optiplex 745
48[n 1]	57,885,161	581887266232...071724285951	17,425,170	2013 January 25	GIMPS / Curtis Cooper[72]	LLT / Prime95 on 3 GHz Intel Core2 Duo E8400[73]
49[n 1]	74,207,281	300376418084...391086436351	22,338,618	2015 September 17[n 4]	GIMPS / Curtis Cooper[13]	LLT / Prime95 on Intel Core i7-4790

How a Church Deacon Found the Biggest Prime Number Yet

- Largest prime discovered Decemeber 26, 2017 by Jonathan Pace, A FedEx employee from Tennessee
- $2^{77,232,917} - 1$
- It is 23,249,425 digits long
- It's huge!! Big enough to fill an entire shelf of books totaling 9,000 pages!
- If every second you were to write five digits to an inch then 54 days later you'd have a number stretching over 73 miles (118 kilometers) -- almost 3 miles (5 kilometers) longer than the previous record prime.

http://en.wikipedia.org/wiki/Largest_known_prime_number
https://nyti.ms/2Fm5r5r https://www.mersenne.org/primes/?press=M77232917

ELECTRONIC FRONTIER FOUNDATION

Opportunity

EFF Cooperative Computing Awards

Thinking about claiming this award? You MUST read this entire page first!

The Electronic Frontier Foundation (EFF), the first civil liberties group dedicated to protecting the health and growth of the Internet, is sponsoring cooperative computing awards, with over half a million dollars in prize money, to encourage ordinary Internet users to contribute to solving huge scientific problems.

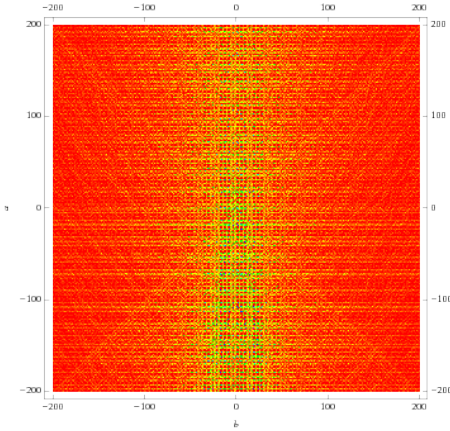
Through the EFF Cooperative Computing Awards, EFF will confer prizes of:

- **$50,000** to the first individual or group who discovers **a prime number with at least 1,000,000 decimal digits** (awarded Apr. 6, 2000)
- **$100,000** to the first individual or group who discovers **a prime number with at least 10,000,000 decimal digits** (awarded Oct. 22, 2009)
- **$150,000** to the first individual or group who discovers **a prime number with at least 100,000,000 decimal digits**
- **$250,000** to the first individual or group who discovers **a prime number with at least 1,000,000,000 decimal digits**

(Prize money comes from a special donation provided by an individual EFF supporter, earmarked specifically for this project. Prize money does NOT come from EFF membership dues, corporate or foundation grants, or other general EFF funds.)

Google's recruitment campaign

Prime Generators



- There are several polynomial functions that generate primes for a while before they start yielding composite numbers.
- The best-known polynomial that generates (possibly in absolute value) only primes is $x^2 + x + 41$ yields prime number for $0 \leq x \leq 39$ due to Euler in 1772 .
- By transforming the formula to $n^2-79n+1601=$

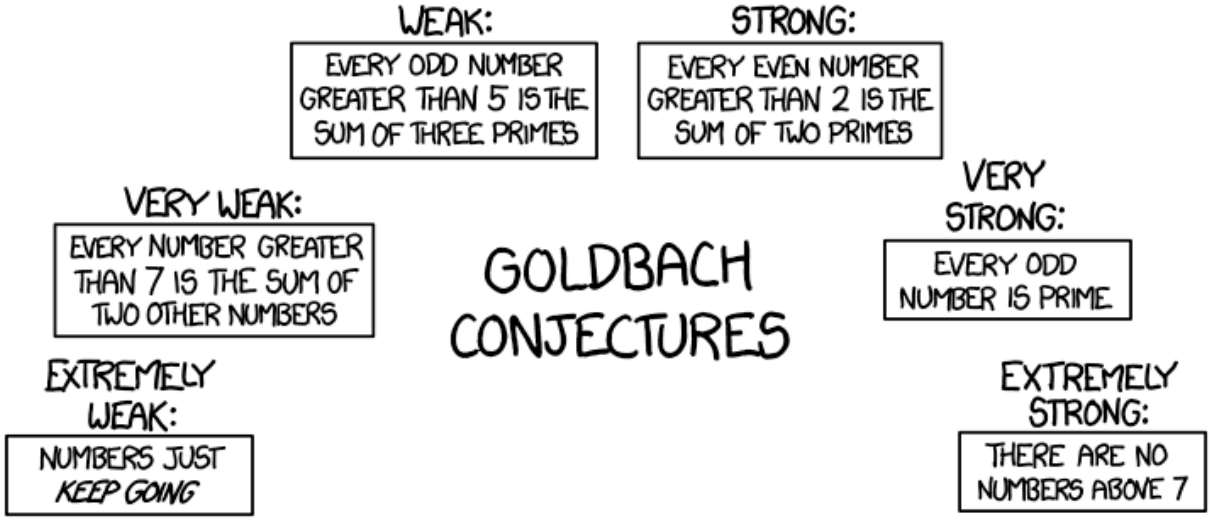
  $(n-40)^2+(n-40)+41$, primes are obtained for 80 consecutive integers, corresponding to the 40 primes given by the above formula taken twice each, due to E. B. Escott in 1879.

http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html
https://en.wikipedia.org/wiki/Bunyakovsky_conjecture

Generating all primes

- Legendre showed that there is no rational algebraic function which always gives primes.
- In 1752, Goldbach showed that no polynomial with integer coefficients can give a prime for all integer values.
- Jones, Sato, Wada, and Wiens found a polynomial of degree 25 in 26 variables whose positive values are exactly the prime numbers.
- $F(a,b,\ldots z) = (k + 2)(1 - (wz + h + j - q)^2 - ((gk + 2g + k + 1)(h + j) + h - z)^2 - (2n + p + q + z - e)^2 - (16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2)^2 - (e^3(e + 2)(a + 1)^2 + 1 - o^2)^2 - ((a^2 - 1)y^2 + 1 - x^2)^2 - (16r^2y^4(a^2 - 1) + 1 - u^2)^2 - (((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2)^2 - (n + l + v - y)^2 - ((a^2 - 1)l^2 + 1 - m^2)^2 - (ai + k + 1 - l - i)^2 - (p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m)^2 - (q + y(a - p - 1) + s(2ap + 2a + p^2 - 2p - 2) - x)^2 - (z + pl(a - p) + t(2ap - p^2 - 1) - pm)^2)$

http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html
https://en.wikipedia.org/wiki/Formula_for_primes



•In 1742, Christian Goldbach conjectured that every even number greater than or equal to 4 can be represented as the sum of two (not necessarily distinct) prime numbers.

•For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$.

http://en.wikipedia.org/wiki/Goldbach's_conjecture

Goldbach's Conjecture

- Is one of the oldest and best-known unsolved problems in number theory and all of mathematics.
- The conjecture has been shown to hold for all integers less than 4×10^{18}, but remains unproven despite considerable effort.
- In 2013, Harald Helfgott proved Goldbach's weak conjecture.

https://en.wikipedia.org/wiki/Mertens_conjecture
https://en.wikipedia.org/wiki/P%C3%B3lya_conjecture
https://en.wikipedia.org/wiki/Goldbach%27s_weak_conjecture

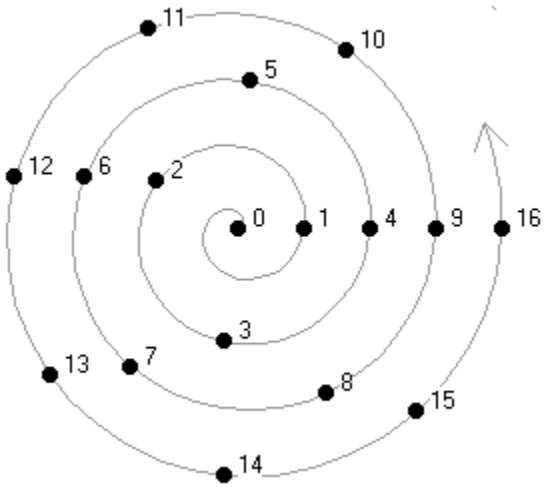
- Early Primes
- Named Primes
- Hunting for Primes
- **Visualizing Primes**
- Harnessing Primes

"To some extent the beauty of number theory seems to be related to the contradiction between the simplicity of the integers and the complicated structure of the primes, their building blocks. This has always attracted people.“ A. Knauf

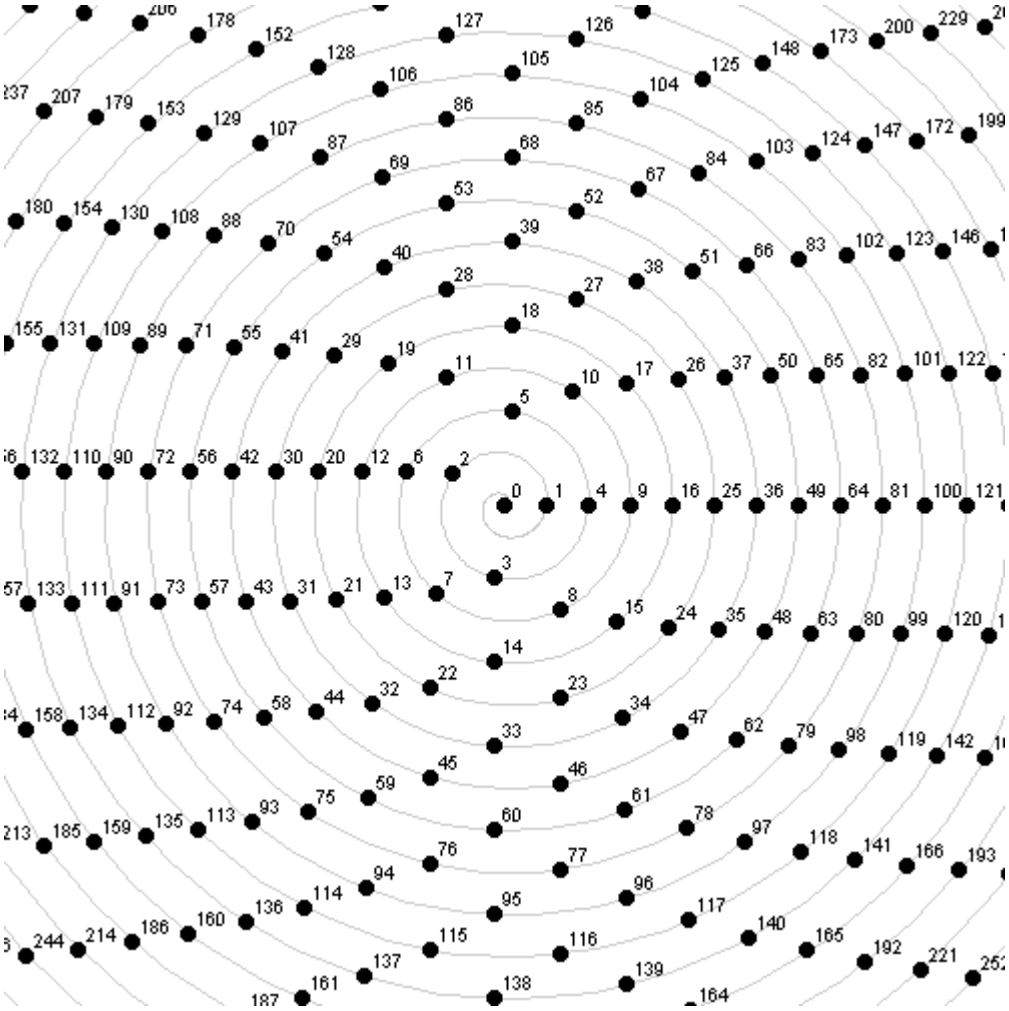
Number spirals

- To make one, we just write the non-negative integers on a ribbon and roll it up with zero at the center.

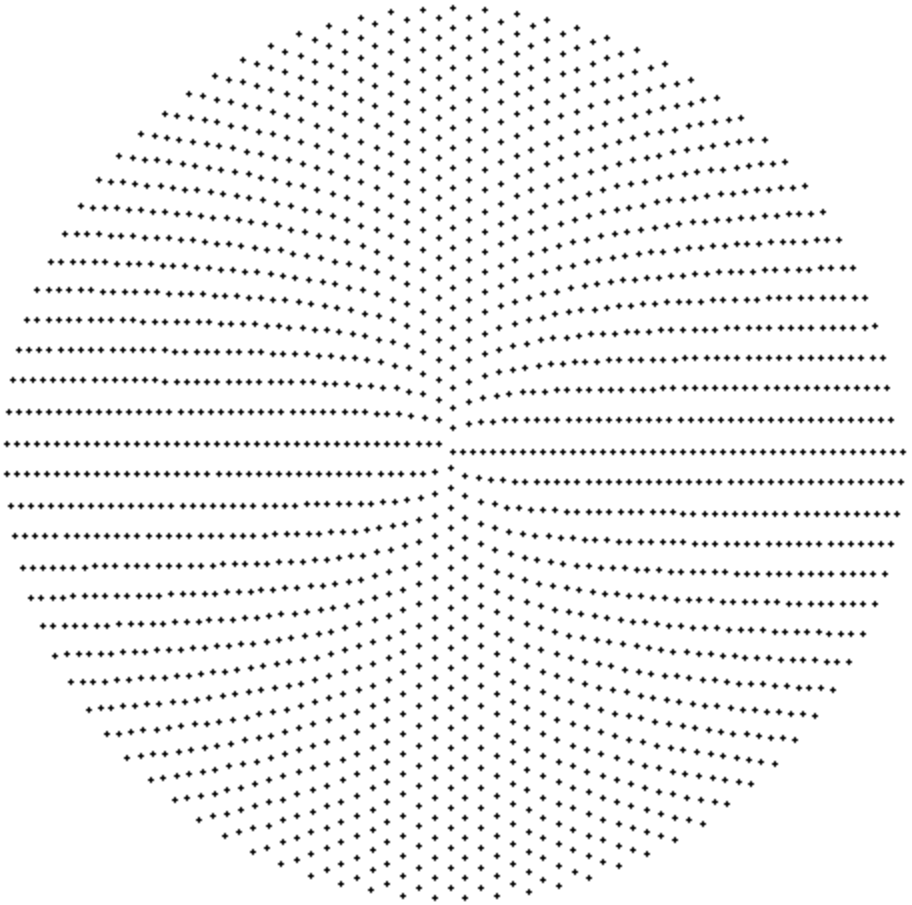
- The trick is to arrange the spiral so all the perfect squares (1, 4, 9, 16, etc.) line up in a row on the right side:



Continue winding for a while and zoom out a bit

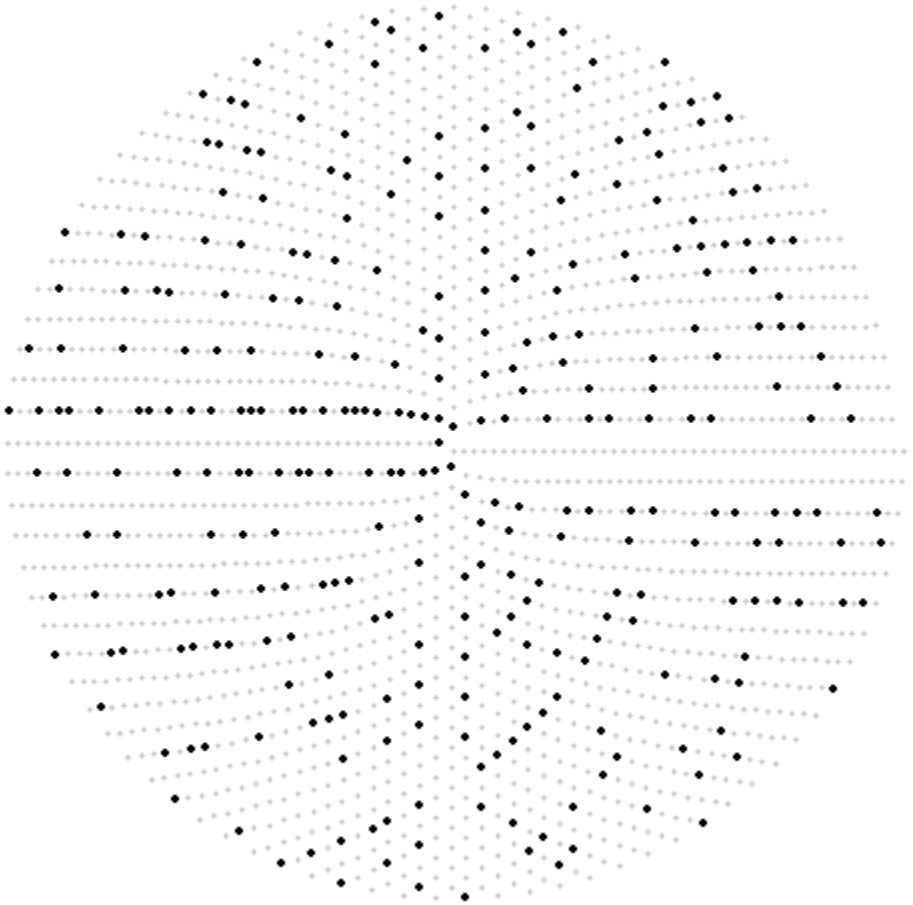


Number Spiral



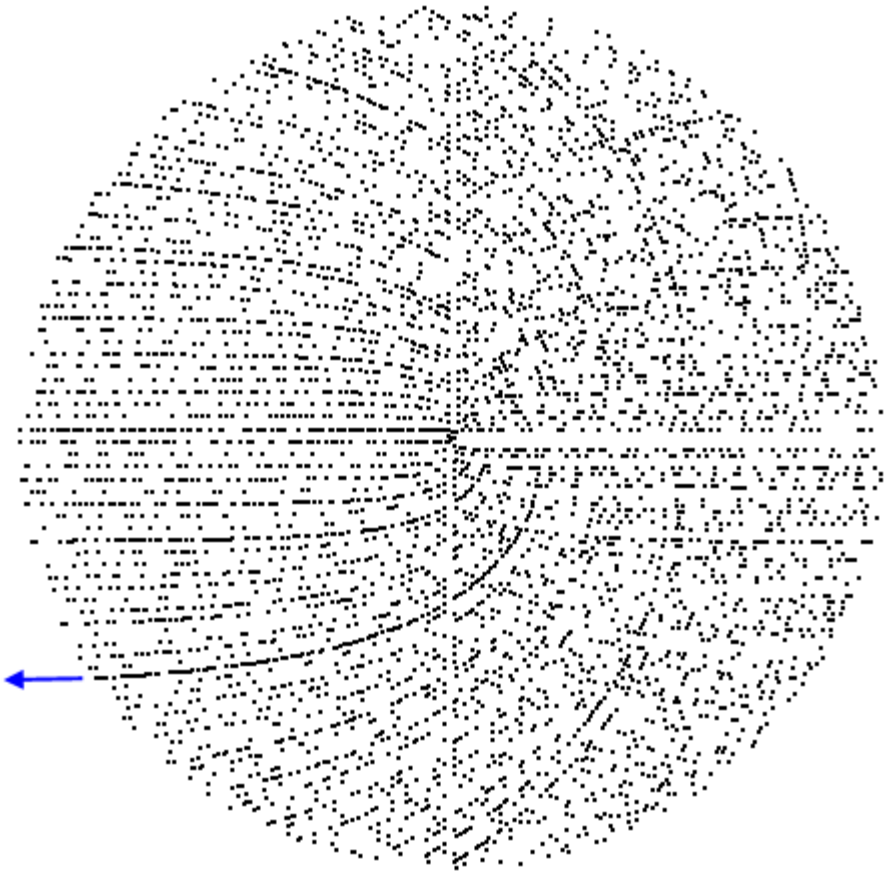
Prime Spirals

- Making the primes darker than the non-primes:



Prime Spirals

- The primes seem to cluster along certain curves.



Details

Numbers on the marked curve are of the form

$$x^2 + x + 41,$$

the famous prime-generating formula discovered by Euler in 1772.

https://www.numberspiral.com/index.html

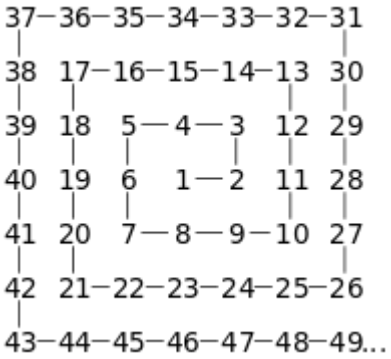
Ulam spiral

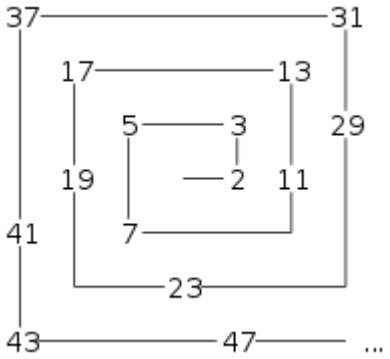
- Is a graphical depiction of the set of prime numbers, devised by mathematician Stanislaw Ulam in 1963 and popularized in Martin Gardner's Mathematical Games.
- It is constructed by writing the positive integers in a square spiral and specially marking the prime numbers.
- Ulam and Gardner emphasized the striking appearance in the spiral of prominent diagonal, horizontal, and vertical lines containing large numbers of primes. Both Ulam and Gardner noted that the existence of such prominent lines is not unexpected, as lines in the spiral correspond to quadratic polynomials, and certain such polynomials, such as Euler's prime-generating polynomial $x^2 + x + 41$, are believed to produce a high density of prime numbers.

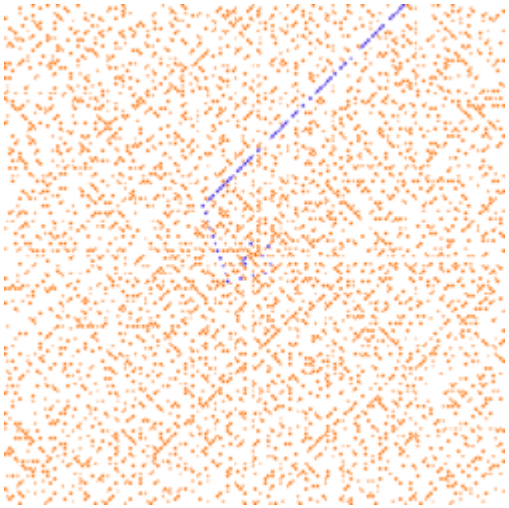
Prime Spirals – Numberphile
https://en.wikipedia.org/wiki/Ulam_spiral

Ulam spiral

- The number spiral is constructed by writing the positive integers in a spiral arrangement on a square lattice, as shown.

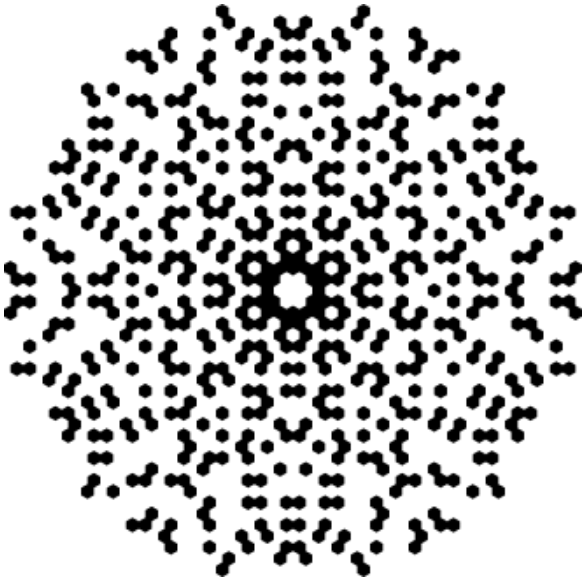






- The Ulam spiral is produced by specially marking the prime numbers

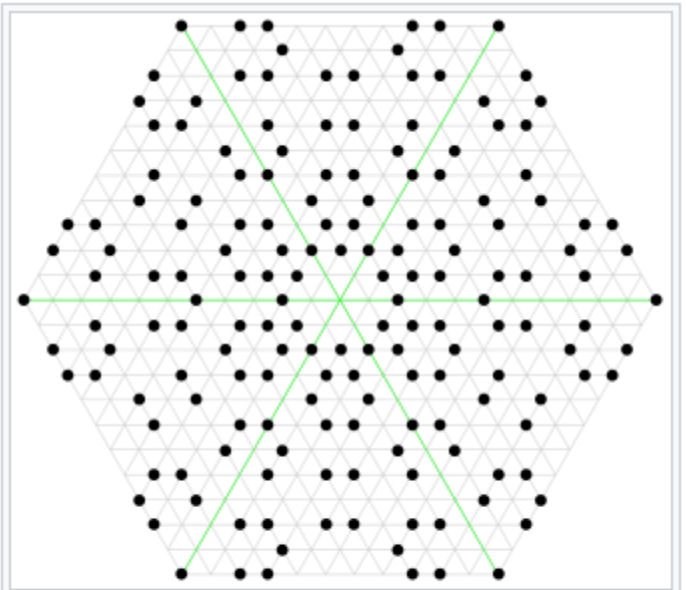
Eisenstein prime



- An Eisenstein prime is an Eisenstein integer

$$z = a + b\,\omega \qquad \text{where} \quad \omega = e^{\frac{2\pi i}{3}}$$

- that is irreducible (or equivalently prime) in the ring-theoretic sense: its only Eisenstein divisors are the units {±1, ±ω, ±ω2}, a + bω itself and its associates.
- The associates (unit multiples) and the complex conjugate of any Eisenstein prime are also prime.



Small Eisenstein primes. Those on the green axes are associate to a natural prime of the form $3n - 1$. All others have an absolute value squared equal to a natural prime.

https://en.wikipedia.org/wiki/Eisenstein_prime

- Early Primes
- Named Primes
- Hunting for Primes
- **Harnessing Primes**

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate."
Leonard Euler

Testing Processors

In 1995, Nicely discovered a flaw in the Intel® PentiumTM microprocessor by computing the reciprocals of 824633702441 and 824633702443, which should have been accurate to 19 decimal places but were incorrect from the tenth decimal place on.

Communication

In Carl Sagan's novel *Contact*, aliens send a series of prime numbers to show intelligence behind radio transmissions

Quantum Physics

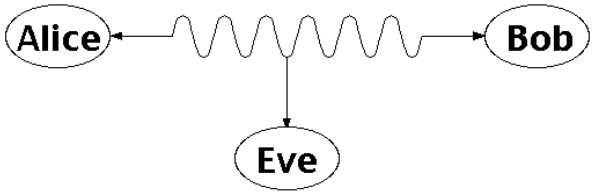
- The frequency of the zeroes of the Riemann zeta function appears to match the energy levels in the nucleus of a heavy atom when it is being bombarded with low-energy neutrons.
- Freeman Dyson noticed the similarity at a chance meeting with mathematician Hugh Montgomery.

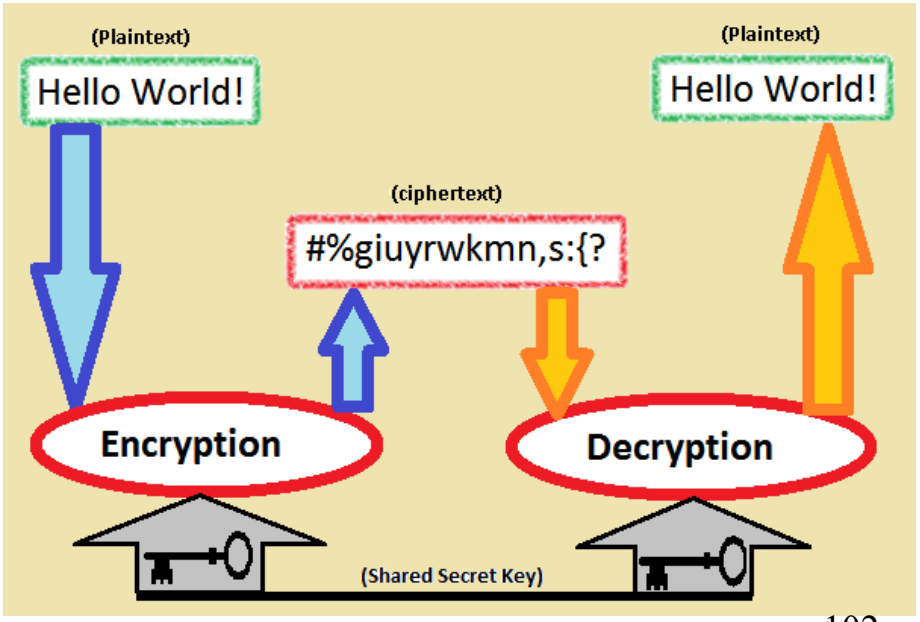
Quantum Physics, II

- German Sierra and Paul Townsend will publish a paper in Physical Review Letters that suggests that an electron constrained to move in two dimensions and constrained by electric and magnetic fields have energy levels that match the zeros of the zeta function.

Cryptography

Cryptography (or cryptology; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.





http://en.wikipedia.org/wiki/Cryptography

Cryptography

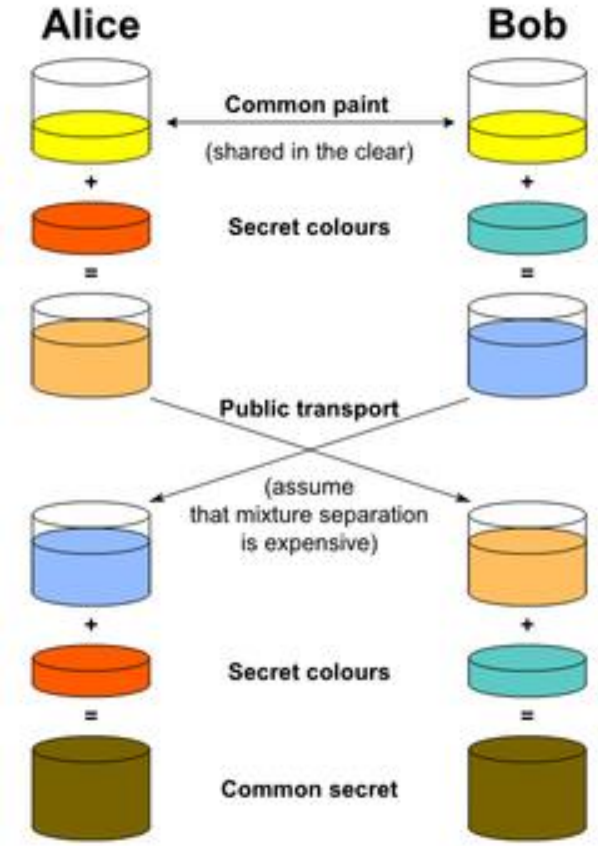
Basic Requirements of a Cryptography System

1. A *secret* algorithm (or function) for encrypting and decrypting data
2. A *secret* key that provides additional information necessary for a receiver to carry out the decrypting process

http://www.youtube.com/course?list=ECB4D701646DAF0817

http://en.wikipedia.org/wiki/Public-key_cryptography

Diffie-Hellman Key Exchange



http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.youtube.com/watch?v=3QnD2c4Xovk

Cryptography

The Diffie-Hellman-Merkle Key Exchange Scheme

Alice and Bob can establish a key (a number) that they both will know, but that Eve cannot find out, even if she observes the communications between Bob and Alice as they set up their key. Alice and Bob can agree to use the function $C = M^k \pmod{n}$ with specific values for M and n. (They can agree to all this by mail, telephone, e-mail, or even casual conversation. It won't matter if Eve finds out.) Then they carry out the following sequence of individual steps.

Alice's Actions

Step 1 Choose a value of a. (Keep this value secret.)

Step 2 Compute $\alpha = M^a \pmod{n}$.

Step 3 Send the value of α to Bob.

Step 4 Receive the value of β from Bob.

Step 5 Compute the key:

$$\boldsymbol{K = \beta^a \pmod{n}.}$$

Bob's Actions

Step 1 Choose a value of b. (Keep this value secret.)

Step 2 Compute $\beta = M^b \pmod{n}$.

Step 3 Send the value of β to Alice.

Step 4 Receive the value of α from Alice.

Step 5 Compute the key:

$$\boldsymbol{K = \alpha^b \pmod{n}.}$$

RSA Encryption

- Ron Rivest, Adi Shamir, and Len Adleman harnessed Fermat's Little Theorem to enable secure web communications
- Fermat's Little Theorem: if p is prime and a is an integer not divisible by p, then $(a^{p-1)}=1(\text{mod } p)$.
- Its security comes from the computational difficulty of factoring large numbers.

RSA algorithm (Basics)

- When the numbers are sufficiently large, no efficient, non-quantum integer factorization algorithm is known.
- An effort by several researchers, concluded in 2009, to factor a 232-digit number (RSA-768) utilizing hundreds of machines took two years and the researchers estimated that a 1024-bit RSA modulus would take about a thousand times as long.
- However, it has not been proven that no efficient algorithm exists

http://www.youtube.com/watch?v=vgTtHV04xRI&list
http://en.wikipedia.org/wiki/RSA_(algorithm)
https://www.youtube.com/watch?v=12Q3Mrh03Gk

Cryptography

RSA Basics: A Public Key Cryptography Scheme

Alice (the receiver) completes the following steps.

Step 1 Choose two prime numbers, p and q, which she keeps secret.

Step 2 Compute the *modulus* n (which is the product $p \cdot q$).

Step 3 Compute $\ell = (p - 1)(q - 1)$.

Step 4 Choose the *encryption exponent* e, which can be any integer between 1 and ℓ that is relatively prime to ℓ, that is, has no common factors with ℓ.

Step 5 Find her *decryption exponent* d, a number satisfying

$$e \cdot d = 1 \pmod{\ell}.$$

She keeps d secret.

Step 6 Provide Bob with her *public key*, which consists of the modulus n and the encryption exponent e.

(Bob's steps are on the next page.)

Cryptography

RSA Basics: A Public Key Cryptography Scheme (Cont.)

Now Bob (the sender) completes the following steps. (Recall that the purpose of all this is for Bob to be able to send Alice secure messages.)

Step 7 Convert the message to be sent to Alice into a number M (sometimes called the *plaintext*).

Step 8 Encrypt M, that is, use Alice's public key (n and e) to generate the encrypted message C (sometimes called the *ciphertext*) according to the formula

$$C = M^e \pmod{n}.$$

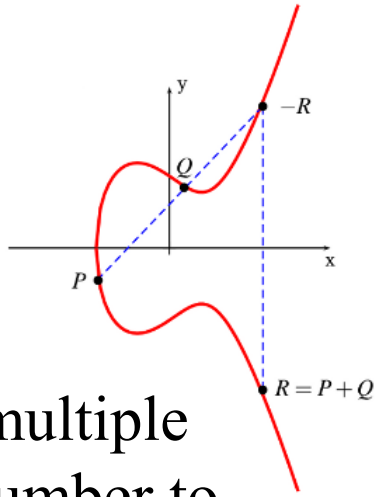
Step 9 Transmit C to Alice.

When Alice receives C, she completes the final step:

Step 10 Decrypt C, that is, use her private key, consisting of n (also part of her public key) and d, to reproduce the original plaintext message M according to the formula

$$M = C^d \pmod{n}.$$

Elliptic Curve Factorization



- Is a factorization algorithm that computes a large multiple of a point on a random elliptic curve modulo the number to be factored N.
- Faster than the Pollard rho factorization and Pollard p-1 factorization methods.
- Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security.

https://en.wikipedia.org/wiki/Lenstra_elliptic-curve_factorization
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Factorization algorithms

- Not enough time, but you can go deeper into the rabbit hole
- https://en.wikipedia.org/wiki/Trial_division
- https://en.wikipedia.org/wiki/Wheel_factorization
- https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm
- https://en.wikipedia.org/wiki/Fermat%27s_factorization_method
- https://en.wikipedia.org/wiki/Euler%27s_factorization_method
- https://en.wikipedia.org/wiki/Special_number_field_sieve

Thank you!