Prime numbers

•••

Expert Analytics formiddag Tuesday 18th 2020

Prime numbers

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …, $2^{82\,589\,933} - 1$, …

Euclid's theorem from 300 BC:

There are infinetly many prime numbers

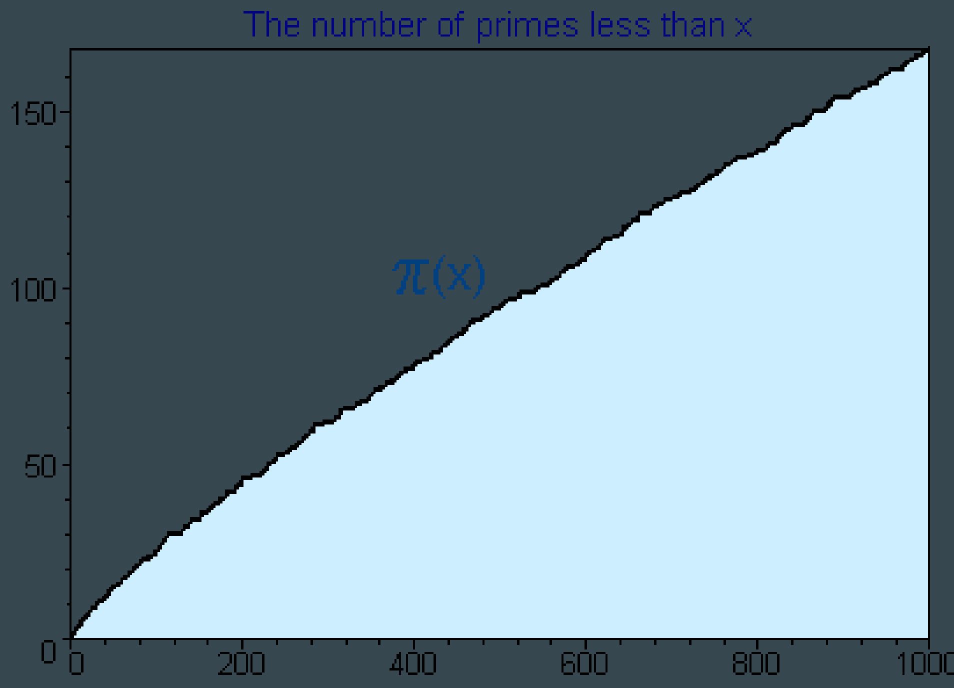
Number of primes smaller than n:

$\Pi(n) \sim n / \ln(n)$

$\Pi(100\,000) = 9\,592$

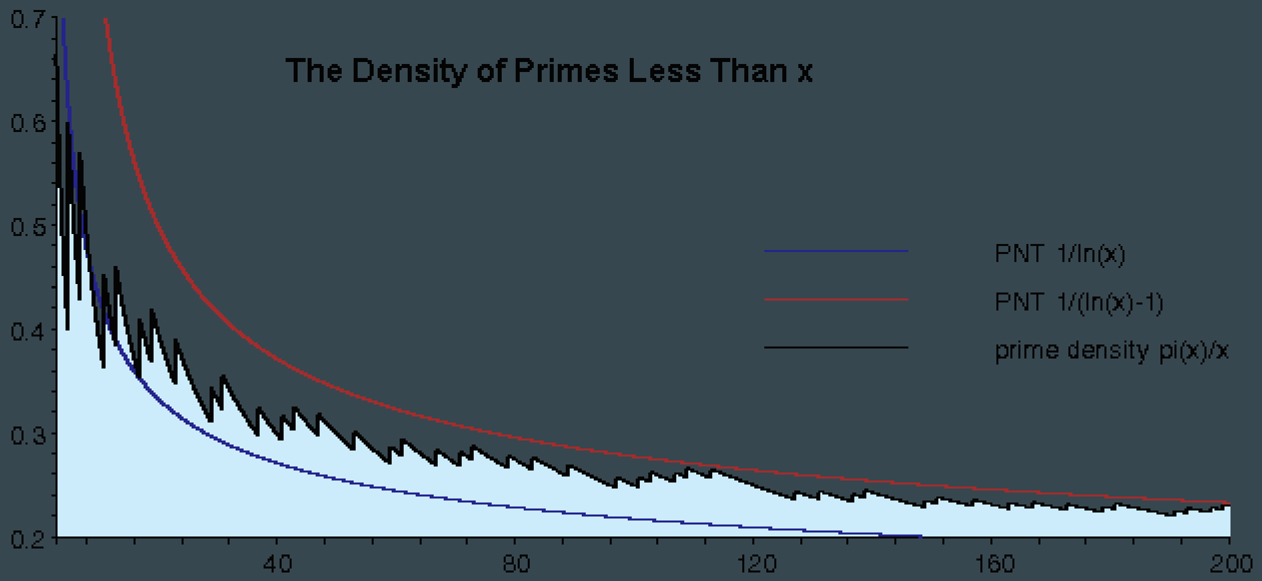
$\Pi(1\,000\,000) = 78\,498$

$\Pi(10\,000\,000) = 664\,579$



Prime numbers

The chance of a random integer n being prime is about 1/ln(n)



Prime numbers

- Palindromic primes: 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, ...
  - The largest known as of March 2019 is (474,501 digits): 10 474 500 + 999 × 10 237 249 + 1
- Binary palindromic primes: 11, 101, 111, 10001, 11111, 1001001, 1101011, ...
- Beastly palindromic primes: 700666007, 10000000000000666000000000000001
- Triply palindromic primes:
  - 10000500001 is prime with 11 digits. 11 is a palindromic prime with 2 digits. 2 is a palindromic prime.
  - p = 1011310 + 4661664×105652 + 1, which has q = 11311 digits, and 11311 has r = 5 digits.
- Emirp: 13, 17, 31, 37, 71, 73, 79, 97, 107, 113, ..., 311, ..., 701, ...

Patterns in primes

Twin primes:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), ...

Common form: (6n -1, 6n +1)

Unresolved: infinetly many, or is there a highest pair?

Patterns in primes

Prime triplet (p, p+2, p+6): (5, 7, 11), (7, 11, 13), ... (347, 349, 353), ...

Prime quadruplet (p, p+2, p+6, p+8): (5, 7, 11, 13), ... (2081, 2083, 2087, 2089), ...

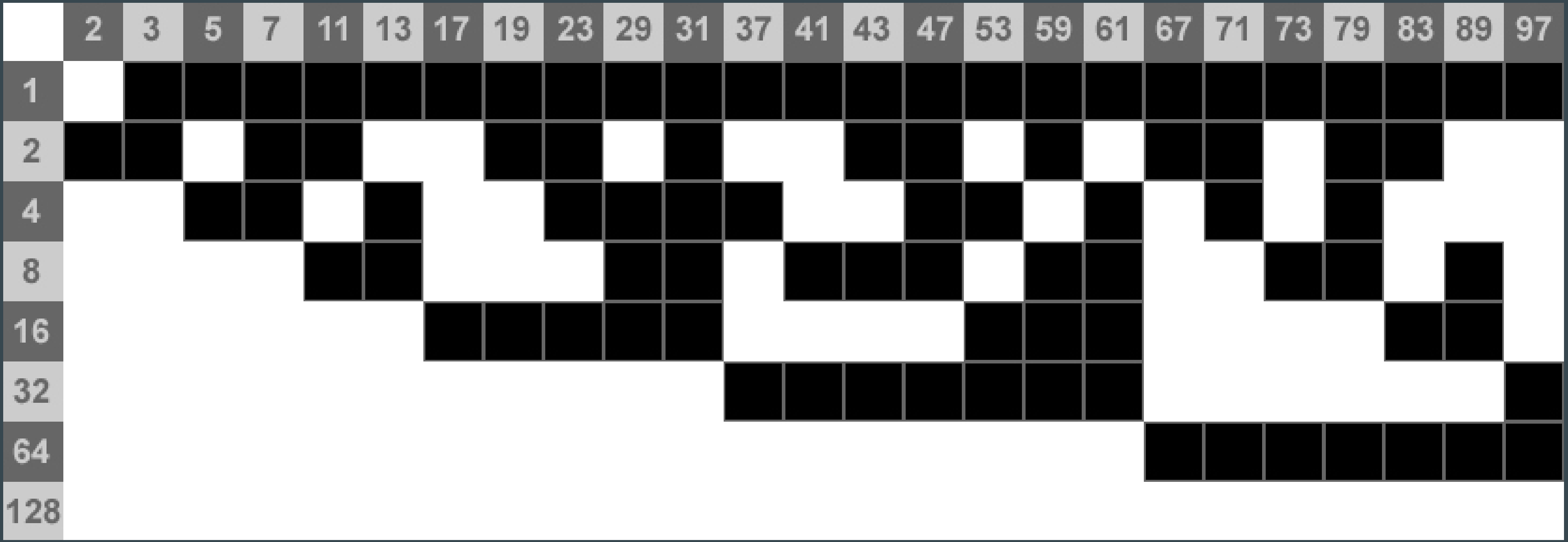
Sexy prime (p, p+6): (5, 11), (7, 13), ...

Sexy prime triplets (p, p+6, p+12): (7, 13, 19), (17, 23, 29), ...

Cousin prime (p, p+4): (3, 7), (7, 11), ...

Isolated prime: neither p-2 nor p+2 is prime: 2, 23, 37, 47, ...

Patterns in primes



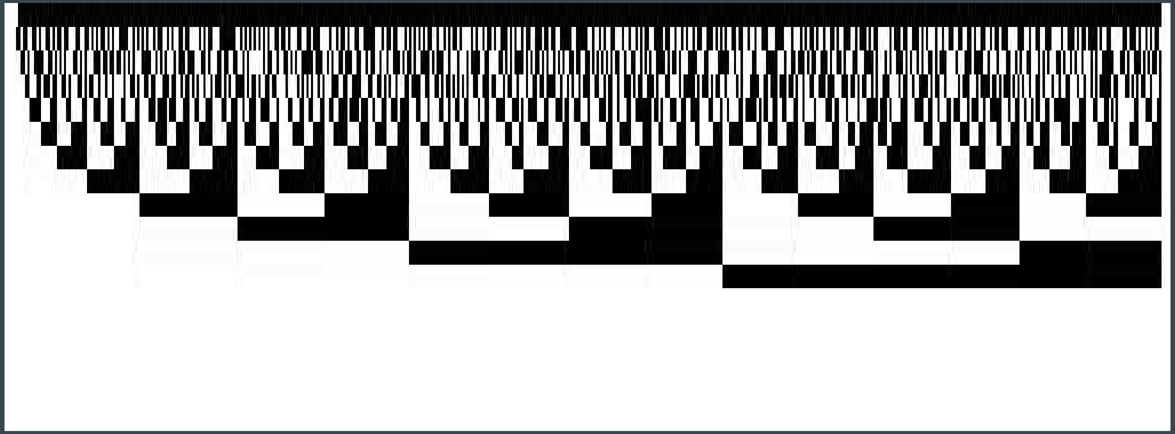
Patterns in primes

Concatenate binary primes:

3 = 11, 17 = 10001

3+17 = 1000111 = 71

17+3 = 1110001 = 113

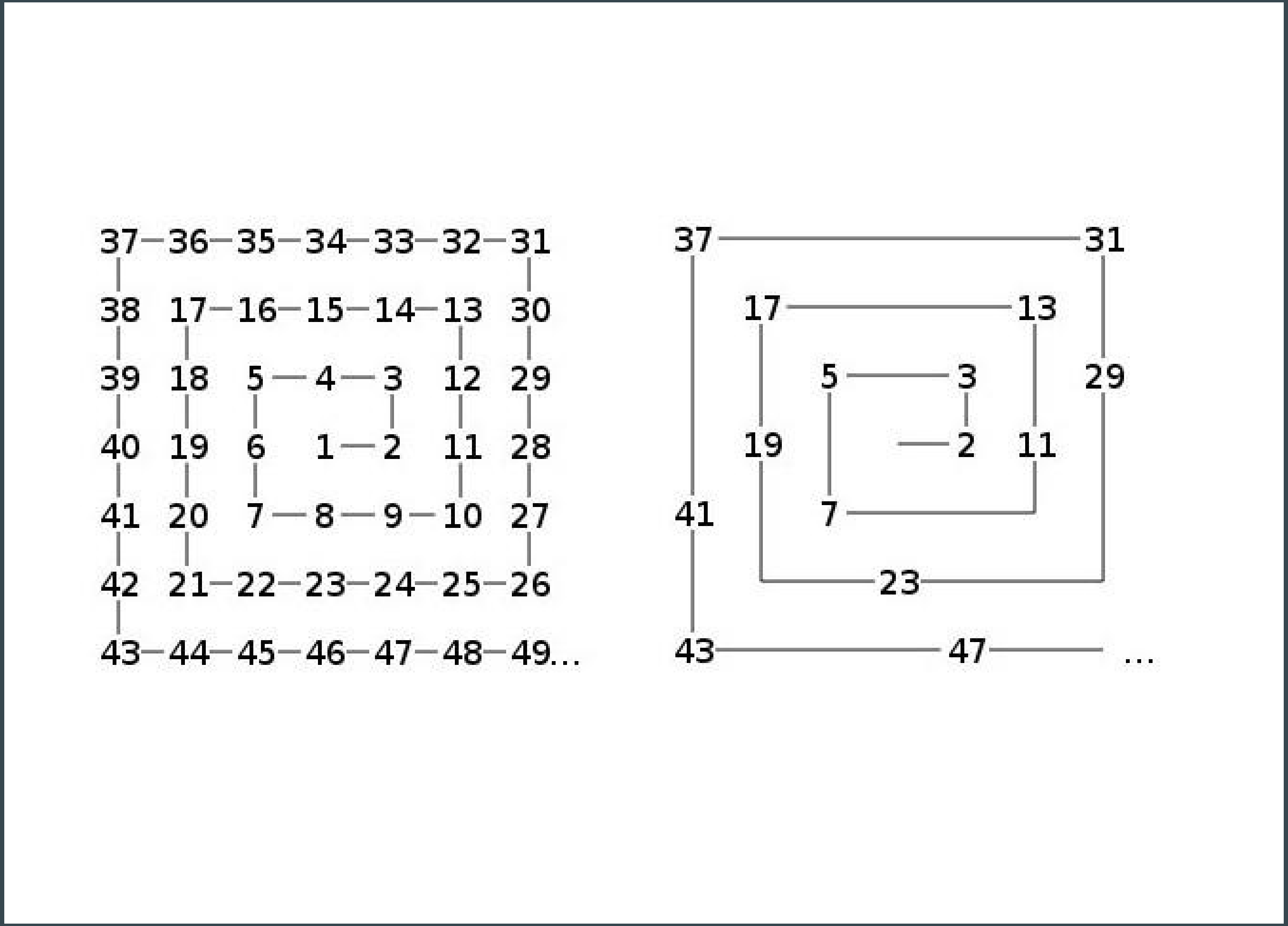


1049 = 10000011001

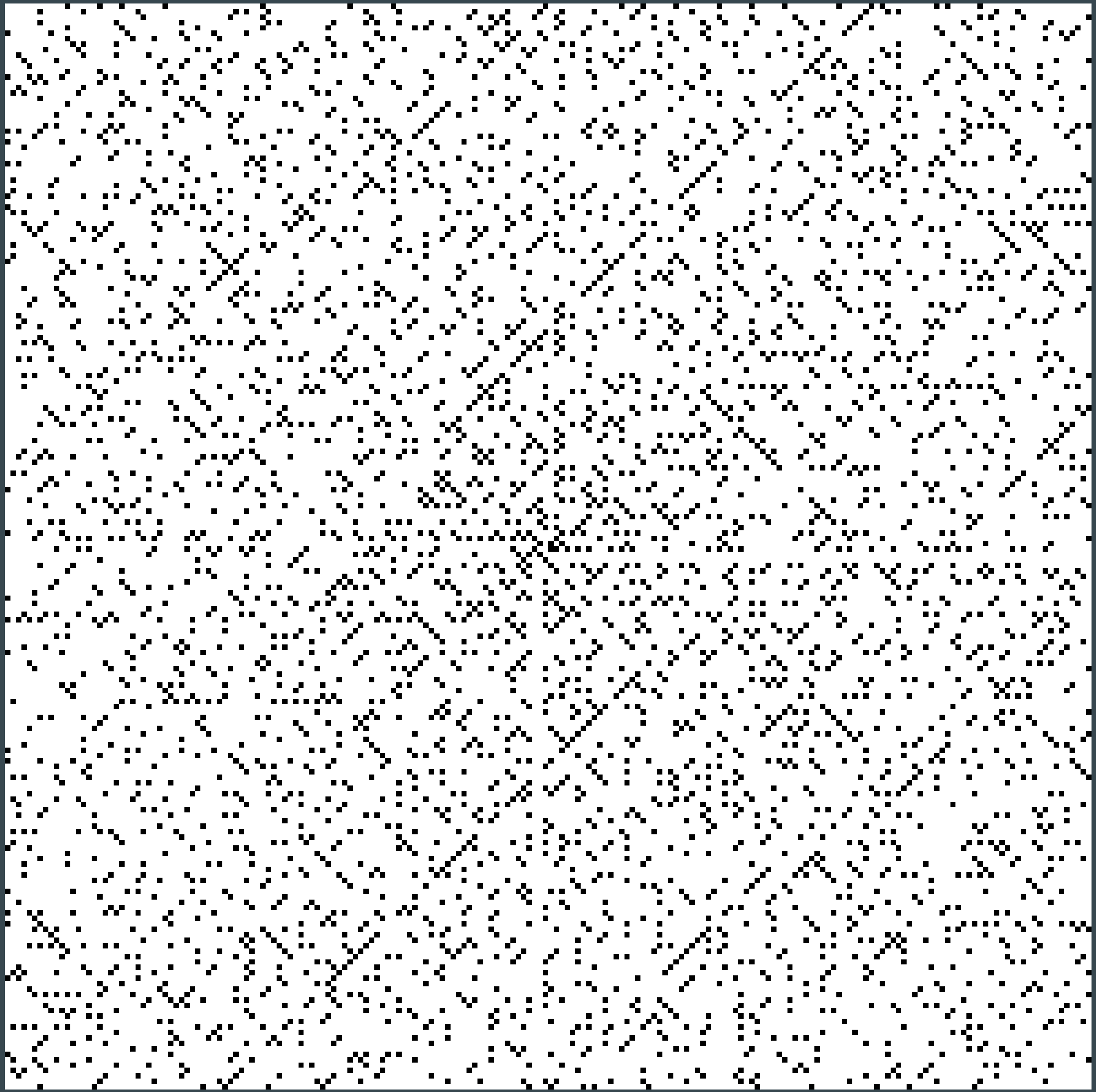
1051 = 10000011011

1051+1049 = 1000001100110000011011 = 2149403

Ulam’s Spiral



Ulam’s Spiral

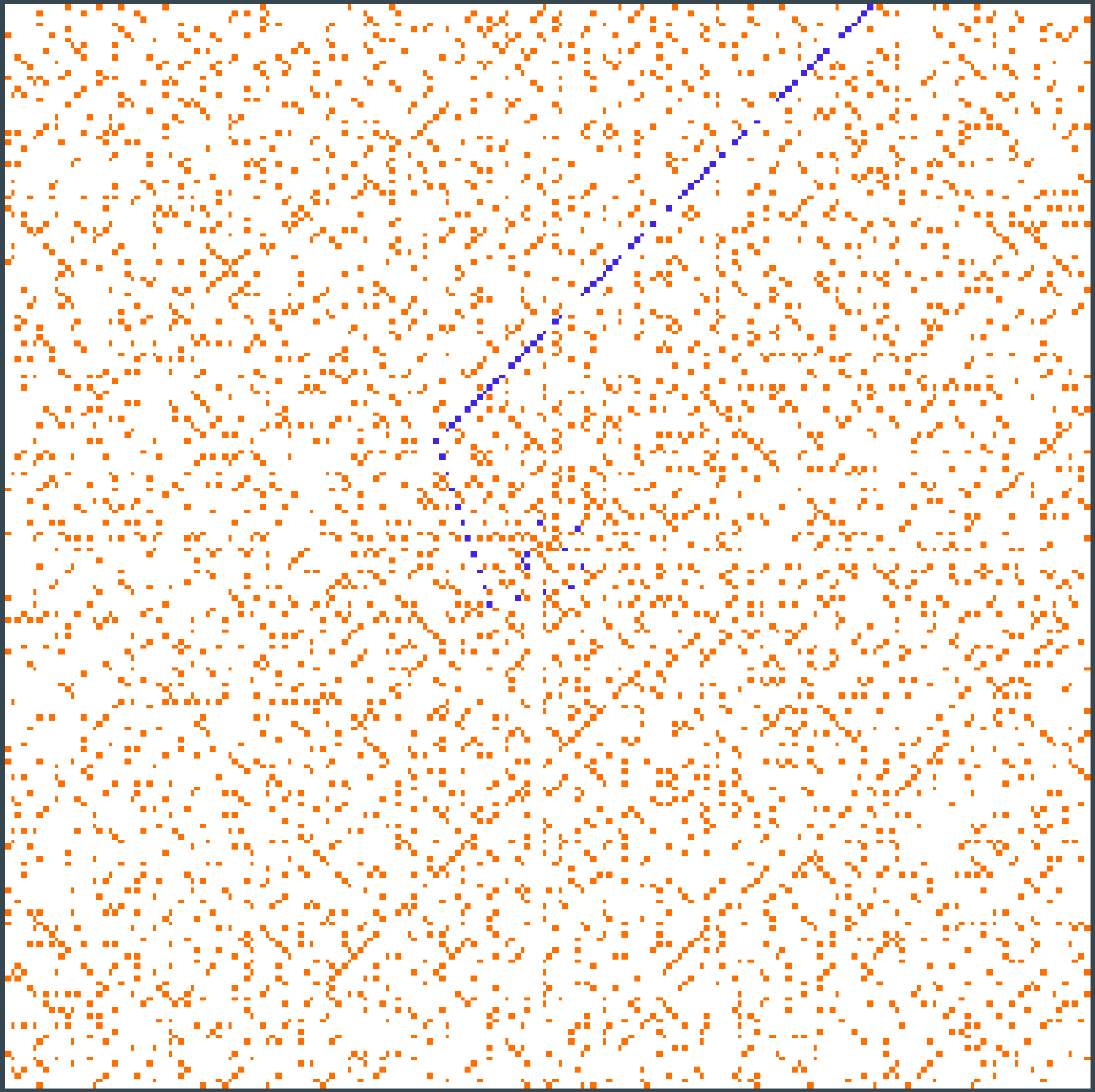


Ulam’s Spiral

Prime generating polynomials:

$P = n^2 + n + 1$

$P = 4x^2 – 2x + 41$



Prime formulas

Euclid: $E_n = p_n + 1$, where p_n is the product of the first n prime numbers.

$E_1 = 3$, $E_2 = 7$, $E_3 = 31$, $E_4 = 211$, $E_5 = 2311$, $E_6 = 30031 = 59*509$, ...

Fermat: $F_n = 2^{2\hat{}n} + 1$, n = 0, 1, 2, 3, ...

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, $F_5 = 4294967297 = 641*6700417$, ...

Euler's prime generating formula: $P_n = n^2 + n + 41$

P_n is prime for all n = 0, 1, 2, 3, ..., 39

Wilson: n is prime iff (n-1)! mod(n) = n -1

n = 2, (2-1)!mod(2) = 2-1,   1 mod 2 = 1

n = 3, (3-1)!mod(3) = 3-1,   2 mod 3 = 2

n = 5, (5-1)!mod(5) = 5-1, 24 mod 5 = 4

Mersenne primes: $M_n = 2^n - 1$

$M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$,

$M_{11} = 2047 = 23*89$, ...

L. Euler proved $M_{31} = 2\,147\,483\,647$ in 1772

E. Lucas proved M_{127} in 1876

F. N. Cole proved $M_{67} = 193\,707\,721 * 761\,838\,257\,287$ in 1903

All n ≤ 257 has been tested by hand

The seven largest known primes are Mersenne primes.

As of June 2019, 51 Mersenne primes are known

Largest: $2^{82\,589\,933} - 1$ with 24 862 048 digits.

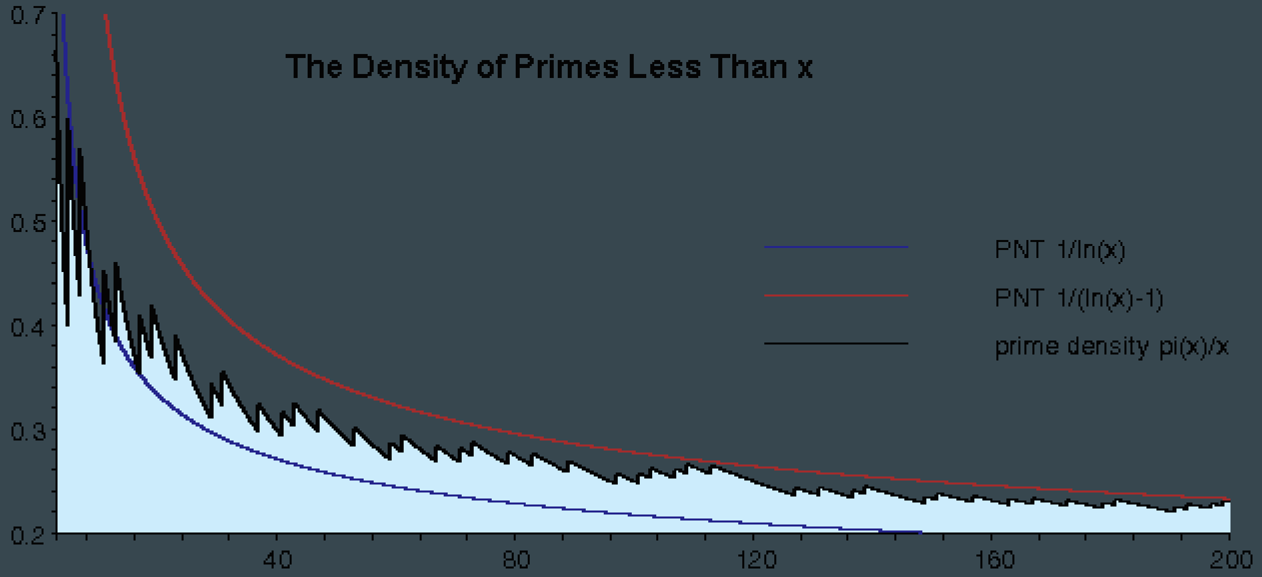
GIMPS – Great Internet Mersenne Prime Search-project

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

Computing primes

The chance of a random integer n being prime is about 1/ln(n).

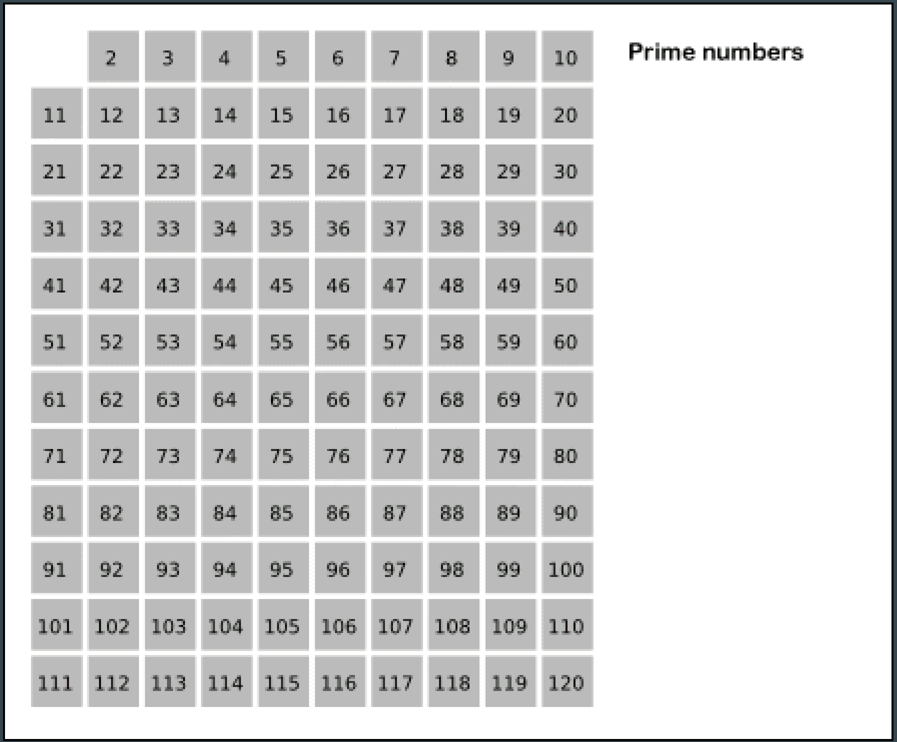
Computing a 1000 digit prime by choosing random numbers you expect to test about 2302 before finding a prime.



Computing primes

Sieve of Eratosthenes

1. Let $p = 2$
2. Remove all multiples of p
3. Let p = next integer
4. Iterate until $p^2 > n$



Computing primes – primality tests

For random integers:

- Probabilistic tests use $O(n^2)$
- Deterministic tests use $O(n^6)$

For Mersenne numbers:

Lucas–Lehmer primality test

```
var s = 4
var M = 2^p − 1
repeat p − 2 times:
    s = ((s × s) − 2) mod M
if s == 0 return PRIME else return COMPOSITE
```

This is deterministic and use $O(n^2)$