PRIME NUMBERS

$n > 1$ is prime if n is divisible only by 1 and by itself.

(1 is not a prime)

sieve :

~~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~~

left with primes

2 3 5 7 11 13 17 19 23 29 31 37 41 43
47

. fundamental theorem of arithmetic :

every integer $n \geq 2$ factors uniquely into a product of primes

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_j \text{ distinct primes}$$

$e_j \geq 1$.

Immediate questions:

- How many primes are there?
- How many pairs of twin primes are there?
- Given a large number n can one tell quickly if it is prime?
- Is there a 'formula' for the next prime?

⋮

I. (Euclid) There infinitely many primes.

<u>PROOF</u>: If not list the primes

$$p_1 < p_2 < p_3 \quad \cdots \quad < p_k$$

p_k the largest.

Set $n = p_1 p_2 \cdots p_k + 1$, clearly n is not div. by p_j for any j.

(Euler): For $s > 1$

$$\prod_p \frac{1}{1-p^{-s}} := \frac{1}{(1-p_1^{-s})(1-p_2^{-s})\cdots\cdots}$$

$$= \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots\cdots)$$

$$= \sum_{j_1,\ldots,j_r\ldots} p_{j_1}^{-e_{j_1}s} p_{j_2}^{-e_{j_2}s} \cdots p_{j_r}^{-e_{j_r}s}$$

$$= \sum_{n=1}^{\infty} n^{-s}.$$ by the basic theorem of arith.

From calculus

$\sum_{n=1}^{\infty} n^{-s}$ converges if $s > 1$ (compare with $\int_1^{\infty} x^{-s}\, dx$.)

$\sum_{n=1}^{\infty} n^{-1} = \infty$ (harmonic series)

$$1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+(\qquad)+\dots$$

$$\geq 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}\cdots \longrightarrow$$

So in Euler's identity $s \to 1$.

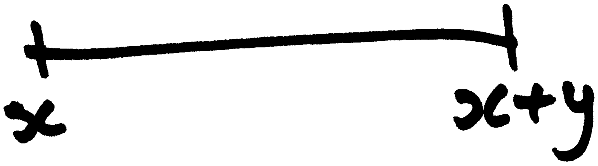
$$\Rightarrow \prod_p \left(1-\frac{1}{p}\right)^{-1} = \infty$$

$$\left(\text{so in fact } \sum_p \frac{1}{p} = \infty\right)$$

there are a lot of primes!

<u>GAUSS</u>: (experiments)

in an interval of length y



there are about $y/\log y$ primes.

5

2600000 . . . 2700000

	261	262	263	264	265	266	267	268	269	270	
0				1							1
1			2					2			4
2	1	2	1		2		1	2	1		10
3	3	6	2	2	4		3	3	3	2	28
4	9	6	6	12	3	7	7	8	6	7	71
5	11	15	14	11	13	17	22	16	18	21	158
6	26	17	24	18	13	19	20	24	19	15	195
7	23	12	27	20	22	21	21	24	22	21	201
8	14	23	16	13	15	16	12	8	12	13	142
9	9	10	13	16	10	10	5	10	5	8	96
10	3	6	5	4	2	8	2	5	8	10	53
11	1	2		2	3	1	4	4	5	2	22
12		3		2	4	1	1	4	1	1	17
13							1				1
14							1				1
	653	661	672	680	689	695	660	665	682	686	6762

$$\int\frac{dx}{\log x} = 6761{,}332$$

2800000 . . . 2900000

	281	282	283	284	285	286	287	288	289	290	
1					1		1				2
2		2	4		5	2		1	1		15
3	2	4	4	3	4	3	1	3	2	4	30
4	9	7	6	9	7	8	10	11	10	8	85
5	14	7	24	14	7	16	19	16	18	15	150
6	18	17	20	13	23	18	16	18	15	21	179
7	24	22	21	20	20	27	22	23	21	22	222
8	13	18	9	20	13	12	9	12	12	14	132
9	10	17	12	12	8	6	14	9	10	11	109
10	7	4	6	3	5	7	5	5	8	3	53
11		1	3	3	5		1	2	1	1	18
12	2	1				1	2		2		8
13			1	2	2						5
14	1			1							2
	690	693	667	704	671	654	672	653	676	662	[illegible]

$$\int\frac{dx}{\log x} = 6728{,}220$$

2700000 . . . 2800000

	271	272	273	274	275	276	277	278	279	280	
1						1			1		2
2	2		2			1			2		7
3	4	5	6	5	4	4	4	3	3	5	43
4	9	7	16	7	8	9	8	8	12	11	95
5	20	24	13	24	13	12	13	17	21	18	155
6	24	18	15	28	19	20	25	21	18	17	195
7	28	22	15	20	24	16	23	19	22	9	188
8	13	20	13	12	15	13	20	19	15	15	145
9	9	9	10	4	11	12	9	7	8	8	87
10	6	9	6	7	5	8	7	2	7	10	67
11	3	3	4	2		2		3	1	6	24
12	1	3		1	1	1			1	1	9
13							1	1			2
14											
15											
16											
17	1										1
	679	695	644	657	672	671	684	666	662	684	6714

$$\int\frac{dx}{\log x} = 6744{,}490$$

2900000 . . . 3000000

	291	292	293	294	295	296	297	298	299	300	
1		1							1		[illegible]
2		1	2	1	2	1		1	1	3	[illegible]
3	3	3	5	2	8	6	4	4	5	4	[illegible]
4	7	7	6	6	7	9	6	6	6	4	[illegible]
5	20	12	14	18	11	15	17	19	18	21	[illegible]
6	17	21	22	18	16	16	12	16	21	17	[illegible]
7	19	30	18	22	22	15	17	13	15	15	[illegible]
8	14	21	21	22	17	12	13	12	14	19	[illegible]
9	10	9	12	13	9	6	12	12	9	11	[illegible]
10	6	4	5	6	3	6	8	7	9	4	[illegible]
11	2	1	3	1		1	1		3	4	[illegible]
12	1	1		1	1	1		1	2		[illegible]
13			1								[illegible]
14											
15							1				[illegible]
	660	663	671	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

$$\int\frac{dx}{\log x} = \text{[illegible]}$$

A page of Gauss's Nachlass.

6

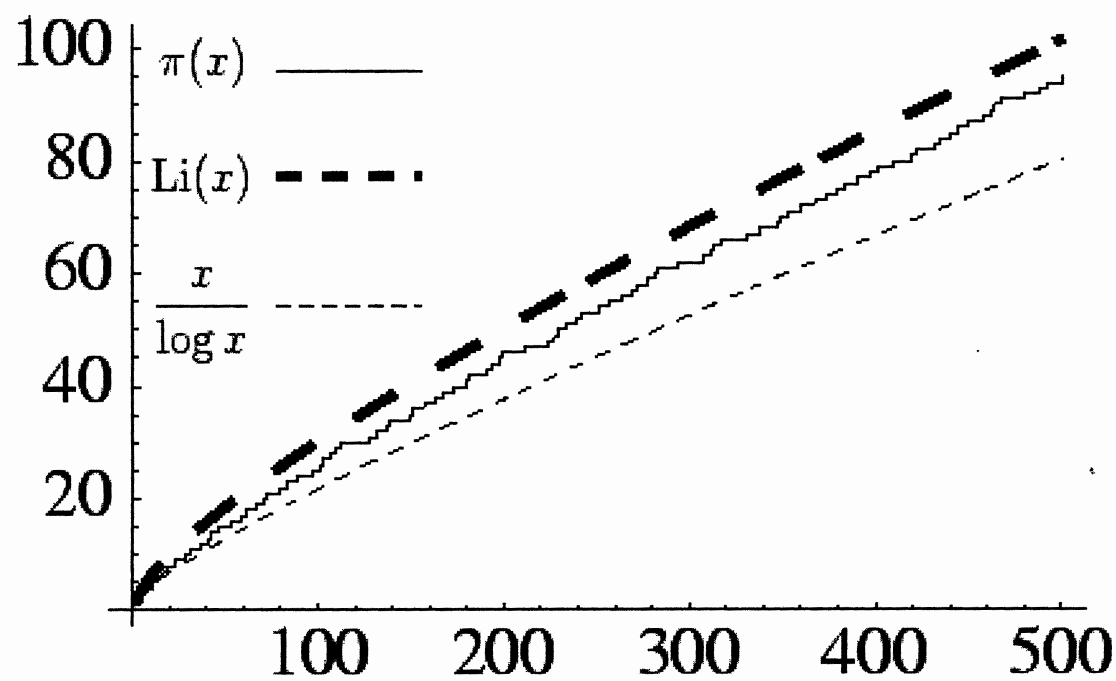
<u>Conjecture</u> (GAUSS). For $x \geq 2$ define

$\pi(x) :=$ number of primes $\leq x$

then

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} := \mathrm{Li}(x) \quad \left(\sim \frac{x}{\log x}\right)$$

when $x \to \infty$.



zeta(of s) =

RIEMANN (±1859)

- makes sense of $\sum_{n=1}^{\infty} n^{-s}$ for all complex numbers s.
- The values ρ of s for which

$$\sum_{n=1}^{\infty} n^{-s} = 0 \qquad \text{(zeros).}$$

are critical.

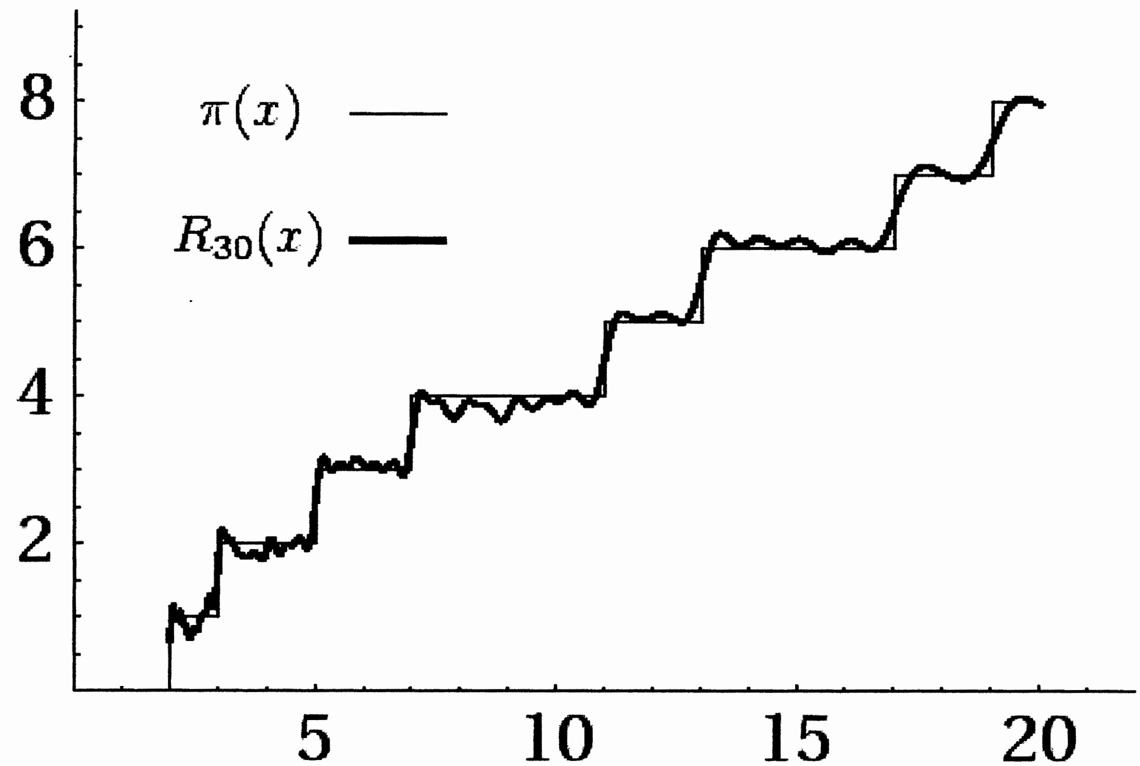
FORMULA: $x \geqslant 2$

if $\psi(x) := \sum_{p \leq x} \log p + \sum_{p^2 \leq x} \log p + \sum_{p^3 \leq x} \log p + \dots$

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho}$$

Riemann Hypothesis: all the zeroes ρ have $\text{Real}(\rho) \leq \frac{1}{2}$.

RIEMANN'S FORMULA IN ACTION



Approximating $\pi(x)$ using the first 30 zeros of the zeta function.

PRIME NUMBER THEOREM (HADAMARD - DE LA VALEE POUSSIN) (1899)

$$\lim_{x\to\infty} \frac{\log x}{x} \pi(x) = 1 .$$

(PROOF USES RIEMANN'S FORMULA.)

IT APPEARS THAT $\pi(x) < Li(x)$ for all x, but in fact this becomes false at $x \approx 10^{320}$!

PRIMES IN PROGRESSIONS:

p a prime,

$p \pmod 3$ ie remainder when p is divided by 3.

either 1, 2 (or 0 but then $p=3$).

One might expect that ½ of the primes

$p \equiv 1 \ (3)$ ie give rem. 1

and

$p \equiv 2 \ (3)$.

Similarly mod 4

$p \equiv 2$ or $0 \pmod 4 \Rightarrow p = 2$

How many

$p \equiv 1 \ (4)$?

$p \equiv 3 \ (4)$?

infinitely many?

In general fix $q \geq 1$ an integer and $(a, q) = \gcd$ of a and q $= 1$.

are there infinitely many primes with $p \equiv a \pmod q$?

<u>Theorem (Dirichlet).</u>

Fix a and q, $(a, q) = 1$

let

$\pi(x; q, a) = $ # of primes $p \leq x$ which give remainder a when divided by q

Then as $x \to \infty$

$$\pi(x; q, a) \sim \frac{x}{(\log x)\, \phi(q)}$$

$$\phi(q) = \left| \{ 1 \leq a \leq q-1 ; (a, q) = 1 \} \right| .$$

$\phi(4) = 2$, $\phi(3) = 2, \ldots$

There are biases (Chebyshev):

$q=3$, "there are more primes $p \equiv 2\ (3)$ than $1\ (3)$",

$\equiv 2 (3)$	2	5		11		17		23	29
$\equiv 1 (3)$			7		13		19		

$\uparrow$
x

is $\pi(x;3,1) < \pi(x;3,2)$ for all x?

<u>No:</u> first time not is $x = 608981 3029$ (BAYES-HUDSON).

If we chose x at random what would you bet ~~for~~ on the event remainder 1 beats remainder 2 mod 3?

M. Rubinstein 95:

$$\text{Prob}\big(\pi(x;3,1) > \pi(x;3,2)\big) = 0.0001\ldots$$

a mod q is a (quadratic) residue

if $x^2 \equiv a \pmod{q}$ has a solution.

Eg: mod 3, 1 is a residue
2 is not.

"There are more primes in the classes a which are nonredidues".

There are more subtle biases
(with no apparent elementary explanation)

$q = 8$

$a = 3 \quad , \quad 5 \quad , \quad 7$

all are non-residues mod 8.

(x^2 mod 8 is
0, 4 or 1)

race - ie choose x at random large and see which residue classes have the most primes...

(Feuerverger + Martin 2002)

$$\text{Prob}(3 > 7 > 5) = \text{Prob}(5 > 7 > 3) = 0.16\ldots$$

$$\text{Prob}(5 > 3 > 7) = \text{Prob}(7 > 3 > 5) = 0.14\ldots$$

$$\text{Prob}(3 > 5 > 7) = \text{Prob}(7 > 5 > 3) = 0.19\ldots$$

So bet on 5 coming in second!

[all of these + Dirichlet use zeta functions $\perp$

TWIN PRIMES:

It is not known if there are infinitely many.

It is conjectured that (HARDY-LITTLEWOOD)

$$\pi_2(x) = \#\{p \leq x \mid p \text{ and } p+2 \text{ are prime}\}$$

$$\sim \frac{Bx}{(\log x)^2} \quad \text{as } x \to \infty$$

with

$$B = 2 . \prod_{p \neq 2} \left(1 - \frac{1}{(p-1)^2}\right)$$

Elementary Sieve methods (BRUNN - SELBERG) give <u>upper bounds</u> of the correct order of magnitude:

<u>THEOREM:</u> $\pi_2(x) \leq 8 \dfrac{Bx}{(\log x)^2}$ for x large.

SELBERG'S Λ^2 SIEVE

X large, $k \geq 2$ fixed, $a_1, \ldots a_k$ fixed

$R = X^{\delta}$, $\delta = \frac{1}{100}$ ie small power

$1 \leq d \leq R$, $\rho_d \in \mathbb{R}$, $\rho_1 = 1$.

$$\sum_{\substack{a_1+m=p_1 \\ a_2+m=p_2 \\ \vdots \\ a_k+m=p_k \\ R < m \leq X}} 1 \leq \sum_{m \leq X} \Bigg(\sum_{\substack{d \mid (m_1+a_1)(m_2+a_2)\cdots(m_k+a_k) \\ d \leq R}} \rho_d \Bigg)^2$$

$\shortparallel$

$\#$ of $(a_1+m, \ldots a_k+m)$ all prime "k-tuple's of primes"

$\shortparallel$

$\pi_k(a_1, \ldots, a_k, X)$

$$= \sum_{m \leq X} \sum_{\substack{d_1 \mid (m+a_1)\cdots(m+a_k) \\ d_2 \mid (m+a_1)\cdots(m+a_k) \\ d_1 \leq R,\ d_2 \leq R}} \rho_{d_1} \rho_{d_2}. \qquad (*)$$

For d_1, d_2 as above fixed

m satisfies congruences mod d_1 and d_2.

hence is determined by congruences mod $[d_1, d_2]$

$= \operatorname{lcm}(d_1, d_2)$

and for given α

$$\sum_{\substack{m \le X \\ m \equiv \alpha (\mathrm{mod}\, [d_1,d_2])}} 1 = \frac{X}{[d_1,d_2]} + \text{small (bounded)}$$

R.H.S. above *

$$X \sum_{\substack{d_1 \le R \\ d_2 \le R}} \frac{g([d_1,d_2])}{[d_1,d_2]} \rho_{d_1}\rho_{d_2} + \text{“small”}$$

$[d_1, d_2] < R^2$

So with $g([d_1,d_2])$ an arithmetical function which counts the no' of solutions to the congruence

$$(m+a_1)\cdots(m+a_k) \equiv 0([d_1,d_2])$$

"well understood"

Minimize the quadratic form

$$\sum_{\substack{d_1 \le R \\ d_2 \le R}} \frac{g([d_1,d_2])}{[d_1,d_2]} \rho_{d_1}\rho_{d_2}$$ subject to the linear constraint $\rho_1 = 1$.

One can do this explicitly (essentially) and finds basically

$$\rho_d \approx \left(\frac{\log R/d}{\log R}\right)^k \mu(d)$$

where $\mu(d)$ is the Mobius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \quad r \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\longrightarrow \quad \frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \mu(n) n^{-s}$$

With this one finds (using the prime no' theorem to evaluate seems like

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d} = 0$$

as $x \to \infty$

$$\pi_k(x; a_1, \ldots a_k) \leq 2^k k!\, B\, x (\log x)^{-k} (1 + o(1))$$

where $B = \prod_p \left(1 - \frac{\nu(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k}$, $\nu(p) = \#$ of roots of $(m+a_1)\cdots(m+a_k)$ mod p.

Recent developments : (21 century)

Progressions in primes (Quest. ERDOS 1959)

given $k \geq 3$ can one find an arithmetic progression of length k in the primes? IE

$$p_1 < p_2 \ldots < p_k \quad \text{primes}$$

s.t. $$p_2 - p_1 = p_3 - p_2 \ldots = p_k - p_{k-1} \, ?$$

This is not the most "natural" question about primes but if we admit twin primes why not this?

THEOREM (2004) GREEN–TAO

Yes – for each $k \geq 3$ there is a k-term arithmetic progression in the primes.

- Their proof uses
  - sieve upper bounds as above
  - methods from combinatorics

  "Szemeredi's Theorem"

  [$\Rightarrow$ "any subset of the integers of positive density contains k-term arithmetic progressions"].

Testing primality:

Given a large n how quickly (ie no' of steps) can we tell if n is prime?

Elementary ~~sieve~~ division $\longrightarrow$ takes $\sqrt{n}$ steps.

Can one determine primality in a polynomial in the no of digits of n?

It has been known for some time (Miller) that assuming the Riemann Hypothesis (generalized) that one can test primality in at most $(\log n)^4$ steps.

<u>THEOREM</u>: (AGRAWAL - SAXENA - KAYAL) 2002

The primality of n can be checked in $(\log n)^{12}$ steps!

" The set of primes is in $\mathbb{P}$ "

Note: 1 Your computer will test quickly but it can in principle give a false positive.

2 The algorithm does not provide a factorization of n if it is not prime.

based on a result of Fermat

If p is prime then

$$a^p \equiv a \pmod{p}$$ for all a's.

So given n we test

$$a^n \equiv a \pmod{n} \quad \text{———} (*)$$

for many a's. Note $(*)$ can be computed quickly by repeated squaring.

Now if for some a $(*)$ fails
$\Rightarrow$ declare n is not prime.

The idea of the proof is to test a variant of $(*)$ for sufficiently many a's (but only poly$(\log n)$ many) and to show if all pass $\Rightarrow$ n is prime.