PRIME NUMBERS

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

(1 is not a prime)

sieve:

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

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

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_i \text{ distinct primes, } e_i > 1.$$
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.

Proof: If not list the primes

\[ P_1 < P_2 < P_3 \ldots < P_n \]

\( P_n \) the largest.

Set \( N = P_1 P_2 \ldots P_n + 1 \), clearly \( N \) is not divisible by \( P_i \).
(Euler): For \( S > 1 \)

\[
\prod_p \frac{1}{1-p^{-S}} = \frac{1}{(1-p_1^{-S})(1-p_2^{-S}) \cdots}
\]

\[
= \prod_p \left( 1 + p^{-S} + p^{-2S} + p^{-3S} + \cdots \right)
\]

\[
= \sum_{j_1, j_2, \ldots} \frac{-e^{iS}}{p_{j_1}^{S} p_{j_2}^{S} \cdots}
\]

\[
= \sum_{n=1}^{\infty} \frac{-S}{n^S} \quad \text{by the basic theorem of arithmetic.}
\]

From calculus,

\[
\sum_{n=1}^{\infty} \frac{1}{n^S} \text{ converges if } S > 1
\]

(compare with \( \int_1^{\infty} x^{-S} \, dx \) )

\[
\sum_{n=1}^{\infty} \frac{1}{n} = \infty \quad \text{(harmonic series)}
\]
\[ 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} \cdots \]
\[ \Rightarrow 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} \cdots \]

So in Euler's identity, \( s \to 1 \).

\[ \prod_p \left( 1 - \frac{1}{p} \right)^{\frac{1}{2}} = \infty \]

(20 in fact \( \sum_{p} \frac{1}{p} = \infty \frac{1}{2} \))

There are a lot of primes!

\textbf{GAUSS: (experiments)}

in an interval of length \( y \)

\[ x \quad x+y \quad y/\log y \quad \text{primes.} \]
A page of Gauss's Nachlass.
Legendre's Conjecture (Gauss). For \( x \geq 2 \) define

\[ \pi(x) := \text{number of primes} \leq x \]

then

\[ \pi(x) \sim \int_{2}^{x} \frac{dt}{\log t} := \text{Li}(x) \]

when \( x \to \infty \).
RIEMANN (1859)

\[ zeta(s) \]

- Makes sense if \( \sum_{n=1}^{\infty} n^{-s} \) for all complex numbers \( s \).
- The values \( \rho \) of \( s \) for which \( \sum_{n=1}^{\infty} n^{-s} = 0 \) (zeros) are critical.

**Formula:** \( x \geq 2 \)

\[ \psi(x) = \sum_{p \leq x} \log p + \sum_{p^2 \leq x} \log p + \sum_{p^3 \leq x} \log p + \ldots \]

\[ \psi(x) = x - \sum_{\rho} \frac{xe^{\rho}}{\rho} \]

**Riemann Hypothesis:** All the zeros \( \rho \) have \( \text{Real}(\rho) = \frac{1}{2} \).
PRIME NUMBER THEOREM (HADAMARD - DE LA VALETTE - POUSIN) (1899)

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

(proof uses riemann's formula.)

It appears that \( \pi(x) < \text{Li}(x) \) for all \( x \), but in fact this becomes false at \( x \approx 10^{320} \)!
**Primes in Progressions:**

$\text{ p a prime, }$

$\text{ p } \equiv \text{ remainder when } p \text{ is divided by 3.}$

either $1, 2 \text{ (or 0 but then } p = 3).$

One might expect that $\frac{1}{2}$ of the primes

$\text{ p } \equiv 1 (3) \text{ remainder}$

and

$\text{ p } \equiv 2 (3).$

Similarly mod 4

$\text{ p } \equiv 2 \text{ or 0 (mod 4) } \Rightarrow \text{ p } = 2.$

How many

$\text{ p } \equiv 1 (4) \text{ ? infinitely}$

$\text{ p } \equiv 3 (4) \text{ ? may }$
In general fix $q \geq 1$ an integer and $(a, q) = gcd$ of $a$ and $q = 1$.

Are there infinitely many primes with $p \equiv a \pmod{q}$?

Theorem (Dirichlet)

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

$$\Pi(x; q, a) = \# \text{of primes } p \leq x$$

which give remainder $a$ when divided by $q$.

Then as $x \to \infty$

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

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

$\phi(4) = 2$, $\phi(3) = 2$, ...
There are biases (Chebyshev):

\[ q = 3, \text{"there are more primes } P \equiv 2(3) \text{ than } 1(3),\]

\[ \equiv 2(3) \quad 2 \quad 5 \quad 11 \quad 17 \quad 23 \quad 29 \]

\[ \equiv 1(3) \quad 7 \quad 13 \quad 19 \]

\[ \uparrow \]

is

\[ \pi(x; 3, 1) < \pi(x; 3, 2) \]

for all \( x? \)

No: first time not is \( x = 6089813029 \) (Bayes-)

If we choose \( x \) at random what would you bet \( \uparrow \) on the event remainder 1 beats remainder 2 mod 3?

M. Rubinstein 95:

\[ \text{Prob}(\pi(x; 3, 1) > \pi(x; 3, 2)) = 0.0001... \]
a \mod q \text{ is a quadratic residue if } \exists x \quad x^2 \equiv a \pmod{q} \quad \text{has a solution.}

E.g.: $\mod 3$, $1$ is a residue, $2$ is not.

"There are more prunes in the classes $a$ which are nonresidues."

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

$q = 8$

$a = 3, 5, 7$

all are nonresidues $\mod 8$.

$(x^2 \mod 8)$ is $0, 4 \text{ or } 1$.
race - ie choose $x$ at random large and see which residue classes have the most primes...

(Feuerberger + Martin 2002)

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

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

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

So bet on 5 coming in second!

[All of these + Dirichlet use Zeta functions]
TWIN PRIMES:

It is not known if there are infinitely many.

It is conjectured that (HARDY-LITTLEWOOD)

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

\[ \sim \frac{B x}{(\log x)^3} \quad \text{as } x \to \infty \]

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

Elementary sieve methods (BRUNN-SELBERG) give upper bounds of the correct order of magnitude:

**Theorem:**

\[ \pi_2(x) \leq 8 \frac{B x}{(\log x)^3} \quad \text{for } x \text{ large.} \]
\[ R = \frac{1}{S_{\alpha}} \quad \text{and} \quad S_{\alpha} = \frac{1}{100^{\epsilon}} \quad \text{is a small power} \]

\[ 1 \leq d \leq R, \quad p_d \in \mathbb{R}, \quad p_1 = 1. \]

\[ \sum_{a_i, m = \mathbb{P}, \ldots, a_k, m = \mathbb{P}} \frac{1}{m \leq x} \leq \sum_{m \leq x} \left( \sum_{d \mid (m+a_1), \ldots, (m+a_k) - (m+a_i)} p_d \right)^2 \]

\[ \text{# of } (a_1, \ldots, a_k, m) \text{ all prime "k-tuple primes"} \]

\[ \prod_{k} (a_1, p_d, x) \]

\[ = \sum_{m \leq x} \sum_{d_1 \mid (m+a_1), \ldots, (m+a_k)} \ldots \sum_{d_2 \mid (m+a_1), \ldots, (m+a_k)} p_{d_1} p_{d_2} \]

\[ (x) \]
For $d_1, d_2$ as above fixed

$m$ satisfy congruences mod $d_1$ and $d_2$.

hence is determined by a congruences mod

$$[d_1, d_2] = \gcd(d_1, d_2)$$

and for given $\alpha$

$$\sum_{m \leq x \atop m \equiv \alpha \pmod{[d_1, d_2]}} 1 = \frac{x}{[d_1, d_2]} + \text{small}$$

(bounded)

R.H.S. above is

$$x \sum_{d_1 \leq R \atop d_2 \leq R} \frac{g([d_1, d_2])}{[d_1, d_2]} \rho_1 \rho_2 + \text{"small"}$$

with $g([d_1, d_2])$ an

arithmetic function which counts

the no of solutions to the congruence

$$(m + \alpha_1) \cdots (m + \alpha_k) \equiv 0 \pmod{[d_1, d_2]}$$

"well understood"

Minimize the quadratic form

$$\sum_{d_1 \leq R \atop d_2 \leq R} \frac{g([d_1, d_2])}{[d_1, d_2]} \cdot p_{d_1} p_{d_2}, \quad \text{subject to the linear constraint}$$

$p_1 = 1$. 
One can do this explicitly (essentially) and finds basically

\[ P_d = \left( \frac{\log R/d}{\log R} \right)^k \mu(d) \]

where \( \mu(d) \) is the Möbius function

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

\[ \sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases} \]

\[ \frac{1}{B(s)} = \sum_{n=1}^{\infty} \mu(n) n^{-s} \]

With this one finds (using the prime number theorem to evaluate sums like)

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

as \( x \to \infty \)

\[ \prod_{k=1}^{\infty} (1 + \frac{a_k}{x}) \leq 2^{k-1} B x^{\log x - k} (1 + o(1)) \]

where \( B = \prod_{p} (1 - \frac{\nu(p)}{p})(1 - \frac{1}{p})^{-k} \), \( \nu(p) = \# \text{ of roots of } \nu \text{ mod } p \).
Recent developments: (21st century)

Progressions in primes (Erdos, 1959)

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

$$P_1 < P_2 < \ldots < P_k$$

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
  "Szemerédi'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 \[ \rightarrow \] 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. 

**Theorem:** (Agrawal-Saxena-Kayal) 2002

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

"The set of primes is in \(P\)"

**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

$$a^n \equiv a \pmod{n} \quad (\star)$$

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

Now if for some $a$ $(\star)$ fails

$\Rightarrow$ declare $n$ is not prime.

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