DISTRIBUTION OF PRIME NUMBERS

We shall study some functions
of a real or a complex variable
That are related to the
distribution of prime numbers.

DISTRIBUTION OF PRIME NUMBERS

OCCURRENCE OF PRIMES

From 1 to 100, there are 25 prime numbers:

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			

DISTRIBUTION OF PRIME NUMBERS

OCCURRENCE OF PRIMES

From 1 to 1000, each 100 contains
25-21-16-16-17-14-16-14-15-14

From 10^6 to 10^6+1000, each 100 contains
6-10-8-8-7-7-10-5-6-8

From 10^{12} to 10^{12}+1000, each 100 contains
4-6-2-4-2-4-3-5-1-6

The occurrence of primes is very irregular. However, when the large scale distribution of primes is considered, it appears in many way quite regular.

DISTRIBUTION OF PRIME NUMBERS

OCCURRENCE OF PRIMES

Except 2 and 3, any two consecutive primes must have a distance that is at least equal to 2. Pairs of primes with this shortest distance are called twin primes. Of the positive integers ≤ 100, there are eight twin primes, namely,

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

There are however arbitrarily long distances between two consecutive primes, that id, there are arbitrarily long sequences of consecutive composite numbers. For an arbitrary positive number $n > 1$, the following $n-1$ numbers

$$n!+2, n!+3, n!+4, \ldots, n!+n$$

are all composite numbers.

DISTRIBUTION OF PRIME NUMBERS

PRIME DISTRUBUTION FUNCTION

DEFINITION

Let x be a positive integer ≥ 1.

Then $\pi(x)$, prime distribution function,
prime counting function,
is defined as follows:

$$\pi(x) = \Sigma_{(p \leq x,\ p\ \text{prime})}\ 1.$$

That is $\pi(x)$ is the number of primes less than or equal to x.

The numerical values of the ratio of $\pi(x)/x$ is

$$\lim_{x\to\infty} \pi(x)/x = 0$$

DISTRIBUTION OF PRIME NUMBERS

PRIME DISTRUBUTION FUNCTION

EXAMPLE

x	$\pi(x)$	$\pi(x)/x$
10	4	0.4
10^2	25	0.25
10^3	168	0.168
10^4	1229	0.1229
10^5	9592	0.09592
10^6	78498	0.078498
10^7	664579	0.0664579
10^8	5761455	0.05761455
10^9	50847534	0.050847534
10^{10}	455052511	0.04550525110
…	…	…
10^{20}	2220819602560918840	0.02220819602560918840

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

RESULTS

1789 Legendre proposed
(using the sieve of Eratosthenes)

$$\pi(x) = \pi(\sqrt{x}) - 1 + \Sigma\, \mu(d) \lfloor n/d \rfloor$$

where
the sum is over all divisors d of the product of all primes $p \leq x$, and
$\mu(d)$ is the Mobius function.

1808 Legendre proposed

$$\pi(x) \approx x \,/\, (\ln x - A(x))$$

with
for large x, $A(x) = 1.08366\ldots$

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

RESULTS

1850 Chebyshev shown that

$$\lim_{(x\to\infty)} A(x) = 1.08366\ldots$$

and

$$0.92129\,(x / \ln x) < \pi(x) < 1.1056\,(x / \ln x)$$

for large x.

1892 Sylvester shown that

$$0.95695\,(x / \ln x) < \pi(x) < 1.04423\,(x / \ln x)$$

for every sufficiently large x.

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

THEOREM

PRIME NUMBER THEOREM (GAUSS)

$\pi(x)$ is asymptotic to $x/\ln x$.
That is

$\lim_{x\to\infty} \pi(x)/(x/\ln x) = 1.$

CHEBYSHEV's θ-FUNCTION
Let θ-function, $\theta(x) = \Sigma(p\le x) \ln p$.
We have that

$\lim_{x\to\infty} \theta(x)/x = 1.$

1896 THE COMPLETED PROOF BY
Jacques Hadamard & De la Vallée-Poussin

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

EXAMPLE

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10	4	4.3...	0.93...
10^2	25	21.7...	1.15...
10^3	168	144.8...	1.16...
10^4	1229	1085.7...	1.13...
10^5	9592	8685.8...	1.13...
10^6	78498	72382.5...	1.08...
10^7	664579	620420.5...	1.07...
10^8	5761455	5428680.9...	1.06...
10^9	50847534	48254942.5...	1.05...
10^{10}	455052511	434294481.9...	1.04...
...	...	...	...
10^{20}	2220819602560918840	2171472409516259138.2...	1.02

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

THEOREM

PRIME NUMBER THEOREM (GAUSS)

$\pi(x)$ is asymptotic to x/ln x.
That is

$\lim_{x\to\infty} \pi(x)/Li(x) = 1.$

Li(x) = logarithmic integral

$$Li(x) = \int_0^x (1/\ln t)\ dt$$

DISTRIBUTION OF PRIME NUMBERS

APPROXIMATIONS OF $\pi(x)$

EXAMPLE

x	$\pi(x)$	Li(x)	$\pi(x)/Li(x)$
10^3	168	178	0.94382...
10^4	1229	1246	0.98635...
10^5	9592	9630	0.99605...
10^6	78498	78628	0.99834...
10^7	664579	664918	0.99949...
10^8	5761455	5762209	0.99986...
10^9	50847534	50849235	0.99996...
10^{10}	455052511	455055615	0.999993...
...	...	...	...
10^{19}	234257667276344607	234057667376222382	0.999999999573...

Approximation of the n^{th} prime number N.
$N \sim n \ln n.$

THEORY OF CONGRUENCES

PROPERTIES

DEFINITION

Let a be an integer.
Let n be a positive integer.

"a mod n" to be the remainder r
when a is divided by n.
That is
$r = a \bmod n = a - \lfloor a/n \rfloor n$.

"a congruent to b modulo n" ,
denoted $a \equiv b \pmod{n}$,
if n is a divisor of a-b, or equivalently,
if $n \mid (a-b)$.

THEORY OF CONGRUENCES

PROPERTIES

THEOREM

Let a be an integer.
then the congruence modulo n is

reflexive
symmetric
transitive.

THEORY OF CONGRUENCES
PROPERTIES

DEFINITION

If $x \equiv a \pmod{n}$, then
a is called a residue of x modulo n.

The residue class of a mod n,
denoted by $[a]_n$ is the set of all those integers
that are congruent to a modulo n.

That is

$$[a]_n = \{ x \mid x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n} \} = \{ a + kn \mid k \in \mathbb{Z} \}$$

THEORY OF CONGRUENCES
PROPERTIES

DEFINITION

If $x \equiv a \pmod{n}$ and
$0 \le a \le n-1$, then
a is called the least (nonnegative) residue of x modulo n.

The set of all residue classes modulo n,
often denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$, is

$$\mathbb{Z}/n\mathbb{Z} = \{ [a]_n \mid 0 \le a \le n-1 \} = \{ 0, 1, 2, \ldots, n-1 \}.$$

EXAMPLE

$-a < 0$ is in $[n-a]_n$, provided $n \ge a$, since $-a \equiv n-a \pmod{n}$.

THEORY OF CONGRUENCES

PROPERTIES

THEOREM

Let n be a positive integer.
Then we have

$[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$,

$[a]_n \neq [b]_n$ if and only if $a \cap b = \varnothing$.

Two residue classes modulo n are either disjoint or identical.

There are exactly n distinct residue classes modulo n,
namely, $[0]_n$, $[1]_n$, …, $[n-1]_n$,
and they contain all of the integers.

THEORY OF CONGRUENCES

PROPERTIES

DEFINITION

Let n be a positive integer.
A set A is called a complete system of residues modulo n,
if the set contains exactly
one element of each residue class modulo n.

Let $[a]_n$ be a residue class modulo n.
We say that $[a]_n$ is relatively prime to n
if each element in $[a]_n$ is relatively prime to n.

EXAMPLE

The ten residue classes modulo 10,
clearly, $[1]_{10}$, $[3]_{10}$, $[7]_{10}$, $[9]_{10}$ are residue classes
that are relatively prime to 10.

THEORY OF CONGRUENCES

PROPERTIES

PROPOSITIONS

If a residue class modulo n has one element
which is relatively prime to n,
then every element in that residue class
is relatively prime to n.

If n is prime, then every residue classes modulo n
(except $[0]_n$) are relatively prime to n.

DEFINITION

Let n be a positive integer.
$\phi(n)$ denotes the number of residue classes modulo n
which is relatively prime to n.
A set contains one element from each such residue class
is called a reduced system of residues.

THEORY OF CONGRUENCES

MODULAR ARITHMETIC

$[a]_n +_n [b]_n = [a+b]_n$

$[a]_n -_n [b]_n = [a-b]_n$

$[a]_n \times_n [b]_n = [ab]_n$

But

$[a]_n \div_n [b]_n$ = Problem

(a/b) mod n exists if and only if (1/b) mod n exists.

(1/b) mod n is called the multiplicative inverse
(modular inverse) of b mod n.

THEORY OF CONGRUENCES

MODULAR ARITHMETIC

THEOREM

The multiplicative inverse $(1/b) \bmod n$ exists
if and only if
$\gcd(b,n) = 1$.

There are $\phi(n)$ numbers b
for which $(1/b) \bmod n$ exists.

$\mathcal{Z}/n\mathcal{Z}$ is a field
if and only if
n is prime.

THEORY OF CONGRUENCES

LINEAR CONGRUENCES

Linear congruence $ax \equiv b \pmod{n}$
is equivalent to the
Diophantine equation $ax - ny = b$.

That is $ax \equiv b \pmod{n} \Leftrightarrow ax - ny = b$.

THEORY OF CONGRUENCES

LINEAR CONGRUENCES

THEOREMS

Let gcd(a,n) = 1.
Then the linear congruence $ax \equiv b \pmod{n}$
has exactly one solution.

Let gcd(a,n) = d.
Then the linear congruence $ax \equiv b \pmod{n}$
has solutions
if and only if
$d \mid b$.

THEORY OF CONGRUENCES

FERMAT's LITTLE THEOREM

THEOREM

Let a be a positive integer.
Let p be a prime number.
if gcd(a,p) = 1, then

$a^{p-1} \equiv 1 \pmod{p}$.

CONVERSE

Let n be an odd positive integer.
If gcd(a,n) = 1 and $a^{n-1} \not\equiv 1 \pmod{n}$.
Then n is composite.

THEORY OF CONGRUENCES

EULER's THEOREM

THEOREM

Let a and n be positive integers
with gcd(a,n) = 1.
Then

$a^{\phi(n)} \equiv 1 \pmod{n}$.

THEORY OF CONGRUENCES

CARMICHAEL'S THEOREM

THEOREM

Let a and n be positive integers
with gcd(a,n) = 1.
Then

$a^{\lambda(n)} \equiv 1 \pmod{n}$,

where $\lambda(n)$ is Carmichael's function.

THEORY OF CONGRUENCES

WILSON'S THEOREM

THEOREM

Let p be a prime number.
Then

$(p-1)! \equiv -1 \pmod{p}$.

CONVERSE

If n is an odd positive integer > 1
and $W(p) = ((p-1)!+1)/p \equiv 0 \pmod{p}$ is an integer,
or equivalently if
$(n-1)! \equiv -1 \pmod{p^2}$.

THEORY OF CONGRUENCES

MULTIPLICATIVE INVERSE

THEOREM

Let x be the multiplicative inverse 1/a modulo n.
if gcd(a,n) = 1, then

$x \equiv (1/a) \pmod{n}$ is given by $x \equiv a^{\phi(n)-1} \pmod{n}$.

COROLLARY

For b/a is assumed to be in lowest terms.
If gcd(a,n) = 1, then

$x \equiv (b/a) \pmod{n}$ is given by $x \equiv b \times a^{\phi(n)-1} \pmod{n}$.

THEORY OF CONGRUENCES

CHINESE REMAINDER THEOREM

THEOREM (CRT)

If $m_1,m_2,\ldots,m_k$ are pairwise relatively prime
and greater than 1,
$a_1,a_2,\ldots,a_k$ are any integers,

then there is a solution x
to the following simultaneous congruences:

$x \equiv a_1 \pmod{m_1}$,
$x \equiv a_2 \pmod{m_2}$,
…
$x \equiv a_k \pmod{m_k}$.

If x and x' are two solutions, $x \equiv x' \pmod{M}$
where $M = m_1m_2\ldots m_k$.

THEORY OF CONGRUENCES

CHINESE REMAINDER THEOREM

REMARK

If the system of linear congruences is soluble,
then its solution can be conveniently described
as follows:

$x = \Sigma_{(i=1 \text{ to } k)}\, a_iM_iM'_i \pmod{m}$,

where $m = m_1m_2\ldots m_k$,
$M_i = m/m_i$,
$M'_i = M_i^{-1} \pmod{m_i}$

for i = 1, 2, …, k.

THEORY OF CONGRUENCES

CHINESE REMAINDER THEOREM

EXAMPLE

Consider the problem,

$x \equiv 2 \pmod{3}$,
$x \equiv 3 \pmod{5}$,
$x \equiv 2 \pmod{7}$.

We have $m = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$,
$M_1 = m/m_1 = 105/3 = 35$,
$M'_1 = M_1^{-1} \pmod{m_1} = 35^{-1} \pmod{3} = 2$,
$M_2 = m/m_2 = 105/5 = 21$,
$M'_2 = M_2^{-1} \pmod{m_2} = 21^{-1} \pmod{5} = 1$,
$M_3 = m/m_3 = 105/7 = 15$,
$M'_3 = M_3^{-1} \pmod{m_3} = 15^{-1} \pmod{7} = 1$.
$x = 2\times35\times2 + 3\times21\times1 + 2\times15\times1 \pmod{105} = 23$.