Prime number theorem

From Wikipedia, the free encyclopedia

In number theory, the prime number theorem (PNT) describes the asymptotic distribution of the prime numbers among the positive integers. It formalizes the intuitive idea that primes become less common as they become larger by precisely quantifying the rate at which this occurs. The theorem was proved independently by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896 using ideas introduced by Bernhard Riemann (in particular, the Riemann zeta function).

The first such distribution found is $\pi(N) \sim N / \log(N)$, where $\pi(N)$ is the prime-counting function and $\log(N)$ is the natural logarithm of N. This means that for large enough N, the probability that a random integer not greater than N is prime is very close to $1 / \log(N)$. Consequently, a random integer with at most 2n digits (for large enough n) is about half as likely to be prime as a random integer with at most n digits. For example, among the positive integers of at most 1000 digits, about one in 2300 is prime ($\log(10^{1000}) \approx 2302.6$), whereas among positive integers of at most 2000 digits, about one in 4600 is prime ($\log(10^{2000}) \approx 4605.2$). In other words, the average gap between consecutive prime numbers among the first N integers is roughly $\log(N)$.[1]

Contents

Statement

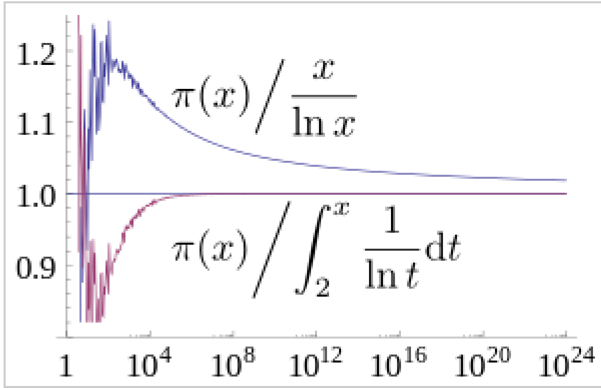
Let $\pi(x)$ be the prime-counting function that gives the number of primes less than or equal to x, for any real number x. For example, $\pi(10) = 4$ because there are four prime numbers (2, 3, 5 and 7) less than or equal to 10. The prime number theorem then states that $x / \log(x)$ is a good approximation to $\pi(x)$, in the sense that the limit of the quotient of the two functions $\pi(x)$ and $x / \log(x)$ as x increases without bound is 1:

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

known as the asymptotic law of distribution of prime numbers. Using asymptotic notation this result can be restated as

$$\pi(x) \sim \frac{x}{\log x}.$$

This notation (and the theorem) does not say anything about the limit of the difference of the two functions as x increases without bound. Instead, the theorem states that x/log(x) approximates π(x) in the sense that the relative error of this approximation approaches 0 as x increases without bound.



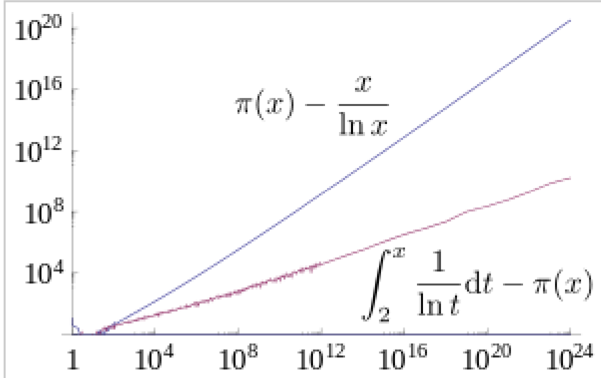
Graph showing ratio of the prime-counting function π(x) to two of its approximations, x/log x and Li(x). As x increases (note x axis is logarithmic), both ratios tend towards 1. The ratio for x/log x converges from above very slowly, while the ratio for Li(x) converges more quickly from below.

The prime number theorem is equivalent to the statement that the nth prime number p_n satisfies

$$p_n \sim n \log(n),$$

the asymptotic notation meaning, again, that the relative error of this approximation approaches 0 as n increases without bound. For example, the $200 \cdot 10^{15}$th prime number is 8512677386048191063,[2] and $(200 \cdot 10^{15})\log(200 \cdot 10^{15})$ rounds to 7967418752291744388, a relative error of about 6.4%.

The prime number theorem is also equivalent to $\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$, and $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$, where ϑ and ψ are the first and the second Chebyshev functions respectively.



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

History of the asymptotic law of distribution of prime numbers and its proof

Based on the tables by Anton Felkel and Jurij Vega, Adrien-Marie Legendre conjectured in 1797 or 1798 that π(a) is approximated by the function a/(A log(a) + B), where A and B are unspecified constants. In the second edition of his book on number theory (1808) he then made a more precise conjecture, with A = 1 and B = −1.08366. Carl Friedrich Gauss considered the same question at age 15 or 16 "ins Jahr 1792 oder 1793", according to his own recollection in 1849.[3] In 1838 Peter Gustav Lejeune Dirichlet came up with his own approximating function, the logarithmic integral li(x) (under the slightly different form of a series, which he communicated to Gauss). Both Legendre's and Dirichlet's formulas imply the same conjectured asymptotic equivalence of π(x) and x / log(x) stated above, although it turned out that Dirichlet's approximation is considerably better if one considers the differences instead of quotients.

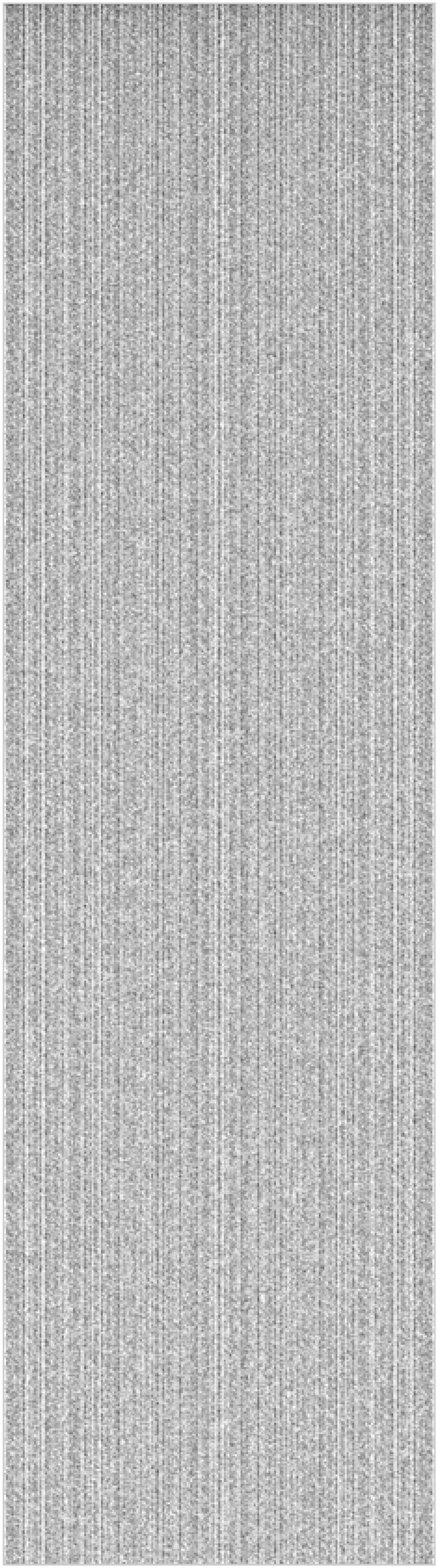
In two papers from 1848 and 1850, the Russian mathematician Pafnuty L'vovich Chebyshev attempted to prove the asymptotic law of distribution of prime numbers. His work is notable for the use of the zeta function ζ(s) (for real values of the argument "s", as are works of Leonhard Euler, as early as 1737) predating Riemann's celebrated memoir of 1859, and he succeeded in proving a slightly weaker form of the asymptotic law, namely, that if the limit of π(x)/(x/log(x)) as x goes to infinity exists at all, then it is necessarily equal to one.[4] He was able to prove unconditionally that this ratio is bounded above and below by two explicitly given constants near

1, for all sufficiently large x.[5] Although Chebyshev's paper did not prove the Prime Number Theorem, his estimates for $\pi(x)$ were strong enough for him to prove Bertrand's postulate that there exists a prime number between n and 2n for any integer $n \geqslant 2$.

An important paper concerning the distribution of prime numbers was Riemann's 1859 memoir On the Number of Primes Less Than a Given Magnitude, the only paper he ever wrote on the subject. Riemann introduced new ideas into the subject, the chief of them being that the distribution of prime numbers is intimately connected with the zeros of the analytically extended Riemann zeta function of a complex variable. In particular, it is in this paper of Riemann that the idea to apply methods of complex analysis to the study of the real function $\pi(x)$ originates. Extending the ideas of Riemann, two proofs of the asymptotic law of the distribution of prime numbers were obtained independently by Jacques Hadamard and Charles Jean de la Vallée-Poussin and appeared in the same year (1896). Both proofs used methods from complex analysis, establishing as a main step of the proof that the Riemann zeta function $\zeta(s)$ is non-zero for all complex values of the variable s that have the form $s = 1 + it$ with $t > 0$.[6]

During the 20th century, the theorem of Hadamard and de la Vallée-Poussin also became known as the Prime Number Theorem. Several different proofs of it were found, including the "elementary" proofs of Atle Selberg and Paul Erdős (1949). While the original proofs of Hadamard and de la Vallée-Poussin are long and elaborate, later proofs introduced various simplifications through the use of Tauberian theorems but remained difficult to digest. A short proof was discovered in 1980 by American mathematician Donald J. Newman.[7][8] Newman's proof is arguably the simplest known proof of the theorem, although it is non-elementary in the sense that it uses Cauchy's integral theorem from complex analysis.

Proof methodology



Distribution of primes up to 19# (9699690).

In a lecture on prime numbers for a general audience, Fields medalist Terence Tao described one approach to proving the prime number theorem in poetic terms: listening to the "music" of the primes. We start with a "sound wave" that is "noisy" at the prime numbers and silent at other numbers; this is the von Mangoldt function. Then we analyze its notes or frequencies by subjecting it to a process akin to Fourier transform; this is the Mellin transform. The next and most difficult step is to prove that certain "notes" cannot occur in this music. This exclusion of certain notes leads to the statement of the prime number theorem. According to Tao, this proof yields much deeper insights into the distribution of the primes than the "elementary" proofs.[9]

Proof sketch

Here is a sketch of the proof referred to in Tao's lecture mentioned above. Like most proofs of the PNT, it starts out by reformulating the problem in terms of a less intuitive, but better-behaved, prime-counting function. The idea is to count the primes (or a related set such as the set of prime powers) with weights to arrive at a function with smoother asymptotic behavior. The most common such generalized counting function is the Chebyshev function $\psi(x)$, defined by

$$\psi(x) = \sum_{\substack{p^k \le x, \\ p \text{ is prime}}} \log p.$$

This is sometimes written as $\psi(x) = \sum_{n \le x} \Lambda(n)$, where $\Lambda(n)$ is the von Mangoldt function, namely

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \ge 1, \\ 0 & \text{otherwise.} \end{cases}$$

It is now relatively easy to check that the PNT is equivalent to the claim that $\lim_{x \to \infty} \psi(x)/x = 1$. Indeed, this follows from the easy estimates

$$\psi(x) = \sum_{p \le x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor \le \sum_{p \le x} \log x = \pi(x) \log x$$

and (using big O notation) for any $\varepsilon > 0$,

$$\psi(x) \ge \sum_{x^{1-\varepsilon} \le p \le x} \log p \ge \sum_{x^{1-\varepsilon} \le p \le x} (1-\varepsilon) \log x = (1-\varepsilon)(\pi(x) + O(x^{1-\varepsilon})) \log x.$$

The next step is to find a useful representation for $\psi(x)$. Let $\zeta(s)$ be the Riemann zeta function. It can be shown that $\zeta(s)$ is related to the von Mangoldt function $\Lambda(n)$, and hence to $\psi(x)$, via the relation

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

A delicate analysis of this equation and related properties of the zeta function, using the Mellin transform and Perron's formula, shows that for non-integer x the equation

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log(2\pi)$$

holds, where the sum is over all zeros (trivial and non-trivial) of the zeta function. This striking formula is one of the so-called explicit formulas of number theory, and is already suggestive of the result we wish to prove, since the term x (claimed to be the correct asymptotic order of $\psi(x)$) appears on the right-hand side, followed by (presumably) lower-order asymptotic terms.

The next step in the proof involves a study of the zeros of the zeta function. The trivial zeros -2, -4, -6, -8, ... can be handled separately:

$$\sum_{n=1}^{\infty} \frac{1}{2n\, x^{2n}} = -\frac{1}{2} \log\left(1 - \frac{1}{x^2}\right),$$

which vanishes for a large x. The nontrivial zeros, namely those on the critical strip $0 \leq \Re(s) \leq 1$, can potentially be of an asymptotic order comparable to the main term x if $\Re(\rho) = 1$, so we need to show that all zeros have real part strictly less than 1.

To do this, we take for granted that $\zeta(s)$ is meromorphic in the half-plane $\Re(s) > 0$, and is analytic there except for a simple pole at $s = 1$, and that there is a product formula $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ for $\Re(s) > 1$. This product formula follows from the existence of unique prime factorization of integers, and shows that $\zeta(s)$ is never zero in this region, so that its logarithm is defined there and $\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_{p,n} p^{-ns}/n$. Write $s = x + iy$; then

$$|\zeta(x+iy)| = \exp(\sum_{n,p} \frac{\cos ny \log p}{np^{nx}}).$$

Now observe the identity $3 + 4\cos\phi + \cos 2\phi = 2(1 + \cos\phi)^2 \geq 0$, so that

$$|\zeta(x)^3 \zeta(x+iy)^4 \zeta(x+2iy)| = \exp \sum_{n,p} \frac{3 + 4\cos(ny\log p) + \cos(2ny\log p)}{np^{nx}} \geq 1$$

for all $x > 1$. Suppose now that $\zeta(1 + iy) = 0$. Certainly y is not zero, since $\zeta(s)$ has a simple pole at $s = 1$. Suppose that $x > 1$ and let x tend to 1 from above. Since $\zeta(s)$ has a simple pole at $s = 1$ and $\zeta(x + 2iy)$ stays analytic, the left hand side in the previous inequality tends to 0, a contradiction.

Finally, we can conclude that the PNT is "morally" true. To rigorously complete the proof there are still serious technicalities to overcome, due to the fact that the summation over zeta zeros in the explicit formula for $\psi(x)$ does not converge absolutely but only conditionally and in a "principal value" sense. There are several ways around this problem but many of them require rather delicate complex-analytic estimates that are beyond the scope of this article. Edwards's book[10] provides the details. Another method is to use Ikehara's Tauberian theorem, though this theorem is itself quite hard to prove. D. J. Newman observed that the full strength of Ikehara's theorem is not needed for the prime number theorem, and one can get away with a special case that is much easier to prove.

Prime-counting function in terms of the logarithmic integral

In a handwritten note on a reprint of his 1838 paper "Sur l'usage des séries infinies dans la théorie des nombres", which he mailed to Carl Friedrich Gauss, Peter Gustav Lejeune Dirichlet conjectured (under a slightly different form appealing to a series rather than an integral) that an even better approximation to π(x) is given by the offset logarithmic integral function Li(x), defined by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,\mathrm{d}t = \mathrm{li}(x) - \mathrm{li}(2).$$

Indeed, this integral is strongly suggestive of the notion that the 'density' of primes around t should be 1/log t. This function is related to the logarithm by the asymptotic expansion

$$\mathrm{Li}(x) \sim \frac{x}{\log x} \sum_{k=0}^{\infty} \frac{k!}{(\log x)^k} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \cdots.$$

So, the prime number theorem can also be written as π(x) ~ Li(x). In fact, in another paper in 1899 La Vallée Poussin proved that

$$\pi(x) = \mathrm{Li}(x) + O\left(x \mathrm{e}^{-a\sqrt{\log x}}\right) \quad \text{as } x \to \infty$$

for some positive constant a, where O(...) is the big O notation. This has been improved to

$$\pi(x) = \mathrm{Li}(x) + O\left(x \,\exp\left(-\frac{A(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right).$$

Because of the connection between the Riemann zeta function and π(x), the Riemann hypothesis has considerable importance in number theory: if established, it would yield a far better estimate of the error involved in the prime number theorem than is available today. More specifically, Helge von Koch showed in 1901[11] that, if and only if the Riemann hypothesis is true, the error term in the above relation can be improved to

$$\pi(x) = \mathrm{Li}(x) + O\left(\sqrt{x}\log x\right).$$

The constant involved in the big O notation was estimated in 1976 by Lowell Schoenfeld:[12] assuming the Riemann hypothesis,

$$|\pi(x) - \mathrm{li}(x)| < \frac{\sqrt{x}\,\log x}{8\pi}$$

for all x ⩾ 2657. He also derived a similar bound for the Chebyshev prime-counting function ψ:

$$|\psi(x) - x| < \frac{\sqrt{x}\,\log^2 x}{8\pi}$$

for all x ⩾ 73.2. This latter bound has been shown to express a variance to mean power law (when regarded as a random function over the integers), 1/f noise and to also correspond to the Tweedie compound Poisson distribution.[13] Parenthetically, the Tweedie distributions represent a family of scale invariant distributions that serve as foci of convergence for a generalization of the central limit theorem.[14]

The logarithmic integral Li(x) is larger than π(x) for "small" values of x. This is because it is (in some sense) counting not primes, but prime powers, where a power p^n of a prime p is counted as 1/n of a prime. This suggests that Li(x) should usually be larger than π(x) by roughly $\mathrm{Li}(x^{1/2})/2$, and in particular should usually be larger than π(x). However, in 1914, J. E. Littlewood proved that this is not always the case. The first value of x where π(x) exceeds Li(x) is probably around $x = 10^{316}$; see the article on Skewes' number for more details.

Elementary proofs

In the first half of the twentieth century, some mathematicians (notably G. H. Hardy) believed that there exists a hierarchy of proof methods in mathematics depending on what sorts of numbers (integers, reals, complex) a proof requires, and that the prime number theorem (PNT) is a "deep" theorem by virtue of requiring complex analysis.[15] This belief was somewhat shaken by a proof of the PNT based on Wiener's tauberian theorem, though this could be set aside if Wiener's theorem were deemed to have a "depth" equivalent to that of complex variable methods. There is no rigorous and widely accepted definition of the notion of elementary proof in number theory. One definition is "a proof that can be carried out in first order Peano arithmetic." There are number-theoretic statements (for example, the Paris–Harrington theorem) provable using second order but not first order methods, but such theorems are rare to date.

In March 1948, Atle Selberg established, by elementary means, the asymptotic formula

$$\vartheta(x)\log(x)+\sum_{p\le x}\log(p)\,\vartheta\left(\frac{x}{p}\right)=2x\log(x)+O(x)$$

where

$$\vartheta(x)=\sum_{p\le x}\log(p)$$

for primes p.[16] By July of that year, Selberg and Paul Erdős had each obtained elementary proofs of the PNT, both using Selberg's asymptotic formula as a starting point.[15][17] These proofs effectively laid to rest the notion that the PNT was "deep," and showed that technically "elementary" methods (in other words Peano arithmetic) were more powerful than had been believed to be the case. In 1994, Charalambos Cornaros and Costas Dimitracopoulos proved the PNT using only $I\Delta_0+\exp$,[18] a formal system far weaker than Peano arithmetic. On the history of the elementary proofs of the PNT, including the Erdős–Selberg priority dispute, see an article by Dorian Goldfeld.[15]

Computer verifications

In 2005, Avigad et al. employed the Isabelle theorem prover to devise a computer-verified variant of the Erdős–Selberg proof of the PNT.[19] This was the first machine-verified proof of the PNT. Avigad chose to formalize the Erdős–Selberg proof rather than an analytic one because while Isabelle's library at the time could implement the notions of limit, derivative, and transcendental function, it had almost no theory of integration to speak of (Avigad et al. p. 19).

In 2009, John Harrison employed HOL Light to formalize a proof employing complex analysis.[20] By developing the necessary analytic machinery, including the Cauchy integral formula, Harrison was able to formalize "a direct, modern and elegant proof instead of the more involved 'elementary' Erdős–Selberg argument".

Prime number theorem for arithmetic progressions

Let $\pi_{n,a}(x)$ denote the number of primes in the arithmetic progression a, a + n, a + 2n, a + 3n, ... less than x. Lejeune Dirichlet and Legendre conjectured, and Vallée-Poussin proved, that, if a and n are coprime, then

$$\pi_{n,a}(x)\sim\frac{1}{\varphi(n)}\,\mathrm{Li}(x),$$

where φ is the Euler's totient function. In other words, the primes are distributed evenly among the residue classes [a] modulo n with gcd(a, n) = 1. This is stronger than Dirichlet's theorem on arithmetic progressions (which only states that there is an infinity of primes in each class) and can be proved using similar methods used by Newman for his proof of the prime number theorem.[21]

The Siegel–Walfisz theorem gives a good estimate for the distribution of primes in residue classes.

Prime number race

Although we have in particular

$$\pi_{4,1}(x)\sim\pi_{4,3}(x),$$

empirically the primes congruent to 3 are more numerous and are nearly always ahead in this "prime number race"; the first reversal occurs at x = 26,861.[22]:1-2 However Littlewood showed in 1914[22]:2 that there are infinitely many sign changes for the function

$$\pi_{4,1}(x) - \pi_{4,3}(x),$$

so the lead in the race switches back and forth infinitely many times. The phenomenon that $\pi_{4,3}(x)$ is ahead most of the time is called Chebyshev's bias. The prime number race generalizes to other moduli and is the subject of much research; Pál Turán asked whether it is always the case that $\pi(x;a,c)$ and $\pi(x;b,c)$ change places when a and b are coprime to c.[23] Granville and Martin give a thorough exposition and survey.[22]

Bounds on the prime-counting function

The prime number theorem is an asymptotic result. It gives an ineffective bound on $\pi(x)$ as a direct consequence of the definition of the limit: for all $\varepsilon > 0$, there is an S such that for all $x > S$,

$$(1-\varepsilon)\frac{x}{\log x} < \pi(x) < (1+\varepsilon)\frac{x}{\log x}.$$

However, better bounds on $\pi(x)$ are known, for instance Pierre Dusart's

$$\frac{x}{\log x}\left(1+\frac{1}{\log x}\right) < \pi(x) < \frac{x}{\log x}\left(1+\frac{1}{\log x}+\frac{2.51}{(\log x)^2}\right).$$

The first inequality holds for all $x \geqslant 599$ and the second one for $x \geqslant 355991$.[24]

A weaker but sometimes useful bound for $x \geqslant 55$ is

$$\frac{x}{\log x + 2} < \pi(x) < \frac{x}{\log x - 4}.$$ [25]

In Pierre Dusart's thesis there are stronger versions of this type of inequality that are valid for larger x. Later in 2010, Dusart proved:

$$\frac{x}{\log x - 1} < \pi(x) \quad \text{for } x \geq 5393, \text{ and}$$

$$\pi(x) < \frac{x}{\log x - 1.1} \quad \text{for } x \geq 60184.$$ [26]

The proof by de la Vallée-Poussin implies the following. For every $\varepsilon > 0$, there is an S such that for all $x > S$,

$$\frac{x}{\log x - (1-\varepsilon)} < \pi(x) < \frac{x}{\log x - (1+\varepsilon)}.$$

Approximations for the nth prime number

As a consequence of the prime number theorem, one gets an asymptotic expression for the nth prime number, denoted by p_n:

$$p_n \sim n \log n.$$

A better approximation is

$$\frac{p_n}{n} = \log n + \log\log n - 1 + \frac{\log\log n - 2}{\log n} - \frac{(\log\log n)^2 - 6\log\log n + 11}{2(\log n)^2} + o\left(\frac{1}{(\log n)^2}\right).$$ [27]

Again considering the $200 \cdot 10^{15}$ prime number 8512677386048191063, this gives an estimate of 8512681315554715386; the first 5 digits match and relative error is about 0.00005%.

Rosser's theorem states that p_n is larger than $n \log n$. This can be improved by the following pair of bounds:[28][29]

$$\log n + \log\log n - 1 < \frac{p_n}{n} < \log n + \log\log n \quad \text{for } n \geq 6.$$

Table of $\pi(x)$, $x / \log x$, and $\operatorname{li}(x)$

The table compares exact values of $\pi(x)$ to the two approximations $x / \log x$ and $\operatorname{li}(x)$. The last column, $x / \pi(x)$, is the average prime gap below x.

x	$\pi(x)$	$\pi(x) - x / \log x$	$\pi(x) / (x / \log x)$	$\mathrm{li}(x) - \pi(x)$	$x / \pi(x)$
10	4	−0.3	0.921	2.2	2.500
10^2	25	3.3	1.151	5.1	4.000
10^3	168	23	1.161	10	5.952
10^4	1,229	143	1.132	17	8.137
10^5	9,592	906	1.104	38	10.425
10^6	78,498	6,116	1.084	130	12.740
10^7	664,579	44,158	1.071	339	15.047
10^8	5,761,455	332,774	1.061	754	17.357
10^9	50,847,534	2,592,592	1.054	1,701	19.667
10^{10}	455,052,511	20,758,029	1.048	3,104	21.975
10^{11}	4,118,054,813	169,923,159	1.043	11,588	24.283
10^{12}	37,607,912,018	1,416,705,193	1.039	38,263	26.590
10^{13}	346,065,536,839	11,992,858,452	1.034	108,971	28.896
10^{14}	3,204,941,750,802	102,838,308,636	1.033	314,890	31.202
10^{15}	29,844,570,422,669	891,604,962,452	1.031	1,052,619	33.507
10^{16}	279,238,341,033,925	7,804,289,844,393	1.029	3,214,632	35.812
10^{17}	2,623,557,157,654,233	68,883,734,693,281	1.027	7,956,589	38.116
10^{18}	24,739,954,287,740,860	612,483,070,893,536	1.025	21,949,555	40.420
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	1.024	99,877,775	42.725
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	1.023	222,744,644	45.028
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	1.022	597,394,254	47.332
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1.021	1,932,355,208	49.636
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	1.020	7,250,186,216	51.939
10^{24}	18,435,599,767,349,200,867,866	339,996,354,713,708,049,069	1.019	17,146,907,278	54.243
10^{25}	176,846,309,399,143,769,411,680	3,128,516,637,843,038,351,228	1.018	55,160,980,939	56.546
OEIS	A006880	A057835		A057752	

The value for $\pi(10^{24})$ was originally computed assuming the Riemann hypothesis;[30] it has since been verified unconditionally.[31]

Analogue for irreducible polynomials over a finite field

There is an analogue of the prime number theorem that describes the "distribution" of irreducible polynomials over a finite field; the form it takes is strikingly similar to the case of the classical prime number theorem.

To state it precisely, let F = GF(q) be the finite field with q elements, for some fixed q, and let N_n be the number of monic irreducible polynomials over F whose degree is equal to n. That is, we are looking at polynomials with coefficients chosen from F, which cannot be written as products of polynomials of smaller degree. In this setting, these polynomials play the role of the prime numbers, since all other monic polynomials are built up of products of them. One can then prove that

$$N_n \sim \frac{q^n}{n}.$$

If we make the substitution $x = q^n$, then the right hand side is just

$$\frac{x}{\log_q x},$$

which makes the analogy clearer. Since there are precisely q^n monic polynomials of degree n (including the reducible ones), this can be rephrased as follows: if a monic polynomial of degree n is selected randomly, then the probability of it being irreducible is about 1/n.

One can even prove an analogue of the Riemann hypothesis, namely that

$$N_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

The proofs of these statements are far simpler than in the classical case. It involves a short combinatorial argument,[32] summarised as follows. Every element of the degree n extension of F is a root of some irreducible polynomial whose degree d divides n; by counting these roots in two different ways one establishes that

$$q^n = \sum_{d|n} dN_d,$$

where the sum is over all divisors d of n. Möbius inversion then yields

$$N_n = \frac{1}{n}\sum_{d|n} \mu(n/d)q^d,$$

where μ(k) is the Möbius function. (This formula was known to Gauss.) The main term occurs for d = n, and it is not difficult to bound the remaining terms. The "Riemann hypothesis" statement depends on the fact that the largest proper divisor of n can be no larger than n/2.

See also

- Abstract analytic number theory for information about generalizations of the theorem.
- Landau prime ideal theorem for a generalization to prime ideals in algebraic number fields.
- Riemann hypothesis

Notes

1. Hoffman, Paul (1998). The Man Who Loved Only Numbers. New York: Hyperion Books. p. 227. ISBN 0-7868-8406-1. MR 1666054.
2. "Prime Curios!: 8512677386048191063". Prime Curios!. University of Tennessee at Martin. 2011-10-09.
3. C. F. Gauss. Werke, Bd 2, 1st ed, 444–447. Göttingen 1863.
4. N. Costa Pereira (August–September 1985). "A Short Proof of Chebyshev's Theorem". American Mathematical Monthly. 92 (7): 494–495. doi:10.2307/2322510. JSTOR 2322510.

5. M. Nair (February 1982). "On Chebyshev-Type Inequalities for Primes". American Mathematical Monthly. 89 (2): 126–129. doi:10.2307/2320934. JSTOR 2320934.
6. Ingham, A. E. (1990). The Distribution of Prime Numbers. Cambridge University Press. pp. 2–5. ISBN 0-521-39789-8.
7. Newman, Donald J. (1980). "Simple analytic proof of the prime number theorem". American Mathematical Monthly. 87 (9): 693–696. doi:10.2307/2321853. JSTOR 2321853. MR 0602825.
8. Zagier, Don (1997). "Newman's short proof of the prime number theorem". American Mathematical Monthly. 104 (8): 705–708. doi:10.2307/2975232. JSTOR 2975232. MR 1476753.
9. Video (http://www.youtube.com/watch?v=PtsrAw1LR3E) and slides (http://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf) of Tao's lecture on primes, UCLA January 2007.
10. Edwards, Harold M. (2001). Riemann's zeta function. Courier Dover Publications. ISBN 0-486-41740-9.
11. Von Koch, Helge (1901). "Sur la distribution des nombres premiers" [On the distribution of prime numbers]. Acta Mathematica (in French). 24 (1): 159–182. doi:10.1007/BF02403071. MR 1554926.
12. Schoenfeld, Lowell (1976). "Sharper Bounds for the Chebyshev Functions θ(x) and ψ(x). II". Mathematics of Computation. 30 (134): 337–360. doi:10.2307/2005976. JSTOR 2005976. MR 0457374..
13. Kendal, WS (2013). "Fluctuation scaling and 1/f noise: shared origins from the Tweedie family of statistical distributions". J Basic Appl Phys. 2: 40–49.
14. Jørgensen, Bent; Martínez, José Raúl; Tsao, Min (1994). "Asymptotic behaviour of the variance function". Scandinavian Journal of Statistics. 21: 223–243. JSTOR 4616314. MR 1292637.
15. Goldfeld, Dorian (2004). "The elementary proof of the prime number theorem: an historical perspective" (PDF). In Chudnovsky, David; Chudnovsky, Gregory; Nathanson, Melvyn. Number theory (New York, 2003). New York: Springer-Verlag. pp. 179–192. doi:10.1007/978-1-4419-9060-0_10. ISBN 0-387-40655-7. MR 2044518.
16. Selberg, Atle (1949). "An Elementary Proof of the Prime-Number Theorem". Annals of Mathematics. 50 (2): 305–313. doi:10.2307/1969455. MR 0029410.
17. Baas, Nils A.; Skau, Christian F. (2008). "The lord of the numbers, Atle Selberg. On his life and mathematics" (PDF). Bull. Amer. Math. Soc. 45 (4): 617–649. doi:10.1090/S0273-0979-08-01223-8. MR 2434348.
18. Cornaros, Charalambos; Dimitracopoulos, Costas (1994). "The prime number theorem and fragments of PA" (PDF). Archive for Mathematical Logic. 33 (4): 265–281. doi:10.1007/BF01270626. MR 1294272.
19. Avigad, Jeremy; Donnelly, Kevin; Gray, David; Raff, Paul (2008). "A formally verified proof of the prime number theorem". ACM Transactions on Computational Logic. 9 (1). arXiv:cs/0509025. doi:10.1145/1297658.1297660. MR 2371488.
20. Harrison, John (2009). "Formalizing an analytic proof of the Prime Number Theorem". Journal of Automated Reasoning. 43 (3): 243–261. doi:10.1007/s10817-009-9145-6. MR 2544285.
21. Souprounov, Ivan (1998). "A short proof of the Prime Number Theorem for arithmetic progressions" (PDF).
22. Granville, Andrew; Martin, Greg (2006). "Prime Number Races" (PDF). American Mathematical Monthly. 113 (1): 1–33. doi:10.2307/27641834. JSTOR 27641834. MR 2202918.
23. Guy, Richard K. (2004). Unsolved problems in number theory (3rd ed.). Springer-Verlag. A4. ISBN 978-0-387-20860-2. Zbl 1058.11001.
24. Dusart, Pierre (1998). Autour de la fonction qui compte le nombre de nombres premiers (PhD thesis) (in French).
25. Rosser, Barkley (1941). "Explicit Bounds for Some Functions of Prime Numbers". American Journal of Mathematics. 63 (1): 211–232. doi:10.2307/2371291. JSTOR 2371291. MR 0003018.
26. Dusart, Pierre. "Estimates of Some Functions Over Primes without R.H." (PDF). arxiv.org. Retrieved 22 April 2014.
27. Cesàro, Ernesto (1894). "Sur une formule empirique de M. Pervouchine". Comptes rendus hebdomadaires des séances de l'Académie des sciences (in French). 119: 848–849.
28. Bach, Eric; Shallit, Jeffrey (1996). Algorithmic Number Theory. Foundations of Computing Series. 1. Cambridge: MIT Press. p. 233. ISBN 0-262-02405-5. MR 1406794.
29. Dusart, Pierre (1999). "The kth prime is greater than k(log k + log log k−1) for k ⩾ 2". Mathematics of Computation. 68 (225): 411–415. doi:10.1090/S0025-5718-99-01037-6. MR 1620223.
30. "Conditional Calculation of pi(10^{24})". Chris K. Caldwell. Retrieved 2010-08-03.
31. Platt, David (2015). "Computing $\pi(x)$ analytically". Mathematics of Computation. 84 (293): 1521–1535. arXiv:1203.5712. doi:10.1090/S0025-5718-2014-02884-6. MR 3315519.
32. Chebolu, Sunil; Ján Mináč (December 2011). "Counting Irreducible Polynomials over Finite Fields Using the Inclusion π Exclusion Principle". Mathematics Magazine. 84 (5): 369–371. doi:10.4169/math.mag.84.5.369.

References

- Hardy, G. H. & Littlewood, J. E. (1916). "Contributions to the Theory of the Riemann Zeta-Function and the Theory of the Distribution of Primes". Acta Mathematica. 41: 119–196. doi:10.1007/BF02422942.

- Granville, Andrew (1995). "Harald Cramér and the distribution of prime numbers" (PDF). Scandinavian Actuarial Journal. 1: 12–28. doi:10.1080/03461238.1995.10413946.

External links

- Hazewinkel, Michiel, ed. (2001), "Distribution of prime numbers", Encyclopedia of Mathematics, Springer, ISBN 978-1-55608-010-4
- Table of Primes by Anton Felkel (http://www.scs.uiuc.edu/~mainzv/exhibitmath/exhibit/felkel.htm).
- Short video (http://www.youtube.com/watch?v=3RfYfMjZ5w0) visualizing the Prime Number Theorem.
- Prime formulas (http://mathworld.wolfram.com/PrimeFormulas.html) and Prime number theorem (http://mathworld.wolfram.com/PrimeNumberTheorem.html) at MathWorld.
- "Prime number theorem". PlanetMath.
- How Many Primes Are There? (http://primes.utm.edu/howmany.shtml) and The Gaps between Primes (http://primes.utm.edu/notes/gaps.html) by Chris Caldwell, University of Tennessee at Martin.
- Tables of prime-counting functions (http://www.ieeta.pt/~tos/primes.html) by Tomás Oliveira e Silva