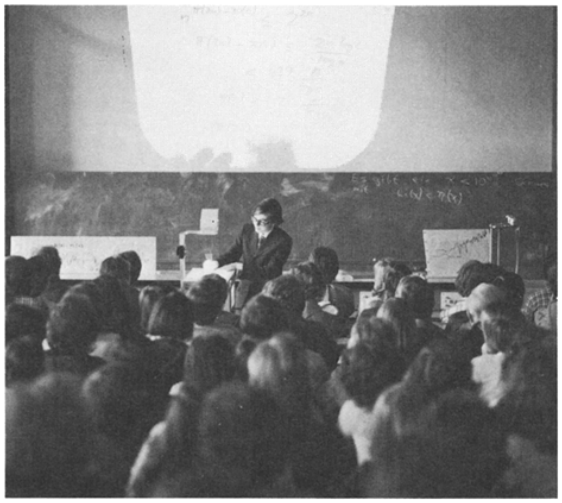
The First 50 Million Prime Numbers*

Don Zagier

To my parents



I would like to tell you today about a subject which, although I have not worked in it myself, has always extraordinarily captivated me, and which has fascinated mathematicians from the earliest times until the present - namely, the question of the distribution of prime numbers.

You certainly all know what a prime number is: it is a natural number bigger than 1 which is divisible by no other natural number except for 1. That at least is the number theorist's definition; other mathematicians sometimes have other definitions. For the function-theorist, for instance, a prime number is an integral root of the analytic function

$$1 - \frac{\sin \frac{\pi \Gamma(s)}{s}}{\sin \frac{\pi}{s}} ;$$

for the algebraist it is

"the characteristic of a finite field"

or

"a point in Spec $\mathbb{Z}$"

or

"a non-archimedean valuation";

the combinatorist defines the prime numbers inductively by the recursion (1)

$$p_{n+1} = [1 - \log_2 (\tfrac{1}{2} + \sum_{r=1}^{n} \sum_{1 \le i_1 < \ldots < i_r \le n} \frac{(-1)^r}{2^{p_{i_1} \cdots p_{i_r}} - 1})]$$

([x] = biggest integer ≤ x);

and, finally, the logicians have recently been defining the primes as the positive values of the polynomial (2)

$$\begin{aligned} &F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,\\ &\quad r,s,t,u,v,w,x,y,z)\\ &= [k+2]\,[1 - (wz+h+j-q)^2 -\\ &\quad (2n+p+q+z-e)^2 - (a^2y^2-y^2+1-x^2)^2 -\\ &\quad (\{e^4+2e^3\}\{a+1\}^2+1-o^2)^2 -\\ &\quad (16\{k+1\}^3\{k+2\}\{n+1\}^2+1-f^2)^2 -\\ &\quad (\{(a+u^4-u^2a)^2-1\}\{n+4dy\}^2+1-\{x+cu\}^2)^2\\ &\quad - (ai+k+1-l-i)^2 -\\ &\quad (\{gk+2g+k+1\}\{h+j\}+h-z)^2 -\\ &\quad (16r^2y^4\{a^2-1\}+1-u^2)^2 -\\ &\quad (p-m+l\{a-n-1\}+b\{2an+2a-n^2-2n-2\})^2 -\\ &\quad (z-pm+pla-p^2l+t\{2ap-p^2-1\})^2 -\\ &\quad (q-x+y\{a-p-1\}+s\{2ap+2a-p^2-2p-2\})^2 -\\ &\quad (a^2l^2-l^2+1-m^2)^2 - (n+l+v-y)^2]. \end{aligned}$$

But I hope that you are satisfied with the first definition that I gave.

There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definition and role as the building blocks of the natural numbers, the prime numbers belong to the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour, and that they obey these laws with almost military precision.

---

*The following article is a revised version of the author's inaugural lecture *(Antrittsvorlesung)* held on May 5, 1975 at Bonn University. Additional remarks and references to the literature may be found at the end.

Translated from the German by R. Perlis. The original German version will also be published in *Beihefte zu Elemente der Mathematik* No. 15, Birkhäuser Verlag, Basel.

To support the first of these claims, let me begin by showing you a list of the prime and composite numbers up to 100 (where apart from 2 I have listed only the odd numbers).

prime		composite	
2	43	9	63
3	47	15	65
5	53	21	69
7	59	25	75
11	61	27	77
13	67	33	81
17	71	35	85
19	73	39	87
23	79	45	91
29	83	49	93
31	89	51	95
37	97	55	99
41		57	

and lists of the primes among the 100 numbers immediately preceding and following 10 million:

The prime numbers between 9,999,900 and 10,000,000

9,999,901
9,999,907
9,999,929
9,999,931
9,999,937
9,999,943
9,999,971
9,999,973
9,999,991

The prime numbers between 10,000,000 and 10,000,100

10,000,019
10,000,079

I hope you will agree that there is no apparent reason why one number is prime and another not. To the contrary, upon looking at these numbers one has the feeling of being in the presence of one of the inexplicable secrets of creation. That even mathematicians have not penetrated this secret is perhaps most convincingly shown by the ardour with which they search for bigger and bigger primes - with numbers which grow regularly, like squares or powers of two, nobody would ever bother writing down examples larger than the previously known ones, but for prime numbers people have gone to a great deal of trouble to do just that. For example, in 1876 Lucas proved that the number $2^{127} - 1$ is prime, and for 75 years this remained unsurpassed - which is perhaps not surprising when one sees this number:

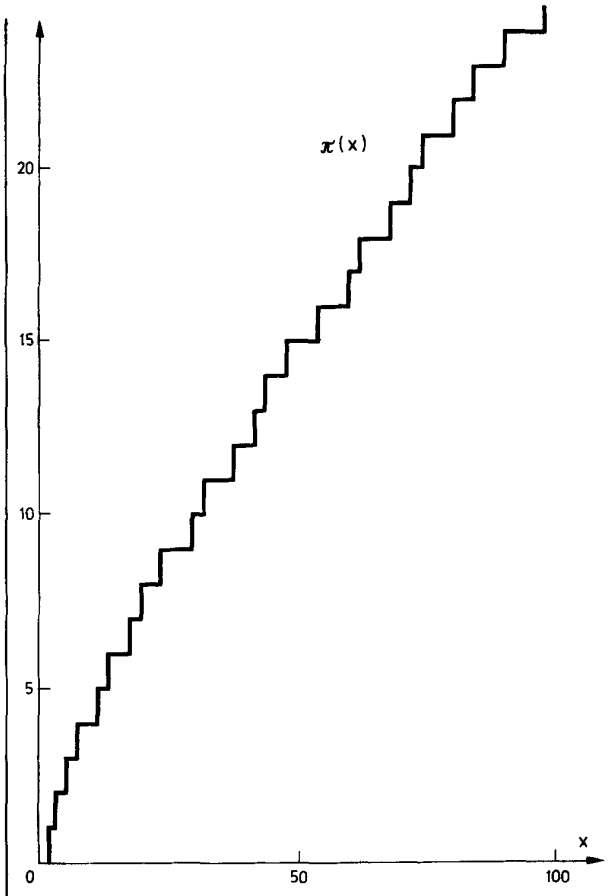
$2^{127} - 1 =$
170141183460469231731687303715884105727.

Not until 1951, with the appearance of electronic computers, were larger prime numbers discovered. In the accompanying table, you can see the data on the successive title-holders [3]. At the moment, the lucky fellow is the 6002-digit number $2^{19937} - 1$ (which I would *not* care to write down); if you don't believe me, you can look it up in the Guinness book of records.

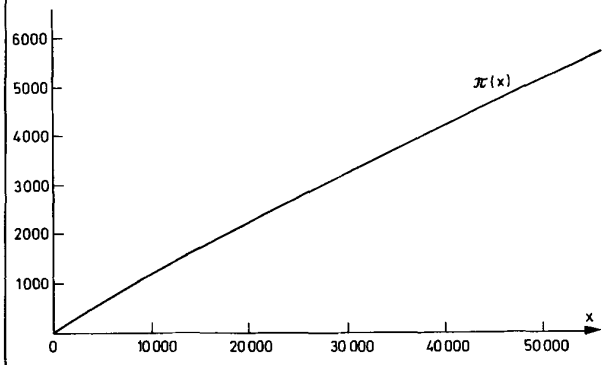
The largest known prime number

p	Number of digits	Year discovered	Discoverer
$2^{127} - 1$	39	1876	Lucas
$\frac{1}{17}(2^{148} + 1)$	44	1951	Ferrier
$114(2^{127} - 1) + 1$	41	1951	Miller + Wheeler + EDSAC 1
$180(2^{127} - 1)^2 + 1$	79		
$2^{521} - 1$	157	1952	Lehmer + Robinson + SWAC
$2^{607} - 1$	183		
$2^{1279} - 1$	386		
$2^{2203} - 1$	664		
$2^{2281} - 1$	687		
$2^{3217} - 1$	969	1957	Riesel + BESK
$2^{4253} - 1$	1281	1961	Hurwitz + Selfridge + IBM 7090
$2^{4423} - 1$	1332		
$2^{9689} - 1$	2917	1963	Gillies + ILIAC 2
$2^{9941} - 1$	2993		
$2^{11213} - 1$	3376		
$2^{19937} - 1$	6002	1971	Tuckerman + IBM 360

More interesting, however, is the question about the laws governing prime numbers. I have already shown you a list of the prime numbers up to 100. Here is the same information presented graphically. The function designated $\pi(x)$ (about which I will be continually speaking from now on) is the number of prime numbers not exceeding x; thus $\pi(x)$ begins with 0 and jumps by 1 at every prime number 2, 3, 5 etc. Already in this picture we can see that, despite small oscillations, $\pi(x)$ by and large grows quite regularly.



But when I extend the domain of x-values from a hundred to fifty thousand, then this regularity becomes breath-takingly clear, for the graph now looks like this:



For me, the smoothness with which this curve climbs is one of the most astonishing facts in mathematics.

Now, wherever nature reveals a pattern, there are sure to crop up scientists looking for the explanation. The regularity observed in the primes forms no exception to this rule. It is not difficult to find an empirical formula which gives a good description of the growth of the prime numbers. Below 100 there are 25 primes, that is, one-fourth of the numbers; below 1000 there are 168, or about one-sixth; up to 10,000 there are 1229 prime numbers, i.e. about one-eighth. If we extend this list, computing the proportion of prime numbers to natural numbers up to one hundred thousand, one million, etc., then we find the following table (in which the values of $\pi(x)$, listed so nonchalantly here, represent thousands of hours of dreary calculation).

x	$\pi(x)$	$x/\pi(x)$
10	4	2.5
100	25	4.0
1000	168	6.0
10,000	1,229	8.1
100,000	9,592	10.4
1,000,000	78,498	12.7
10,000,000	664,579	15.0
100,000,000	5,761,455	17.4
1,000,000,000	50,847,534	19.7
10,000,000,000	455,052,512	22.0

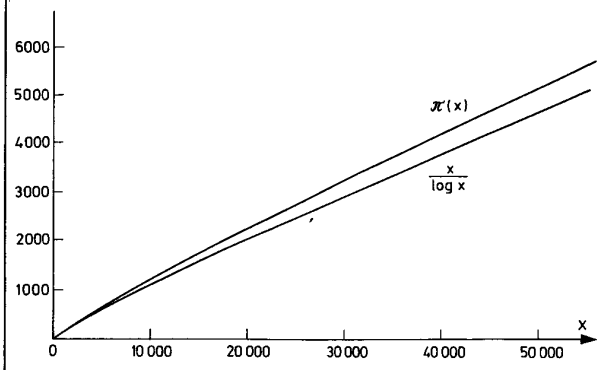
Here we see that the ratio of x to $\pi(x)$ always jumps by approximately 2.3 when we go from a power of 10 to the next. Mathematicians immediately recognize 2.3 as the logarithm of 10 (to the base e, of course). Thus we are led to conjecture that

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

where the sign $\sim$ means that the ratio $\pi(x)/(x/\log x)$ tends to 1 as x goes to infinity. This relationship (which was not proved until 1896) is known as the *prime number theorem*. Gauss, the greatest mathematician of them all, discovered it at the age of fifteen by studying prime number tables contained in a book of logarithms that had been given to him as a present the previous year. Throughout his life Gauss was keenly interested in the distribution of the prime numbers and he made extensive calculations. In a letter to Enke [4] he describes how he "very often used an idle quarter of an hour to count through another chiliad [i.e., an interval of 1,000 numbers] here and there" until finally he had listed all the prime numbers up to 3 million (!) and compared their distribution with the formula which he had conjectured.

The prime number theorem states that $\pi(x)$ is asymptotically - i.e., with a relative error of 0% - equal to x/log x. But if we compare the graph of the function x/log x with that of $\pi(x)$, then we

see that, although the function x/log x qualitatively mirrors the behaviour of $\pi(x)$, it certainly does not agree with $\pi(x)$ sufficiently well to explain the smoothness of the latter:



Therefore it is natural to ask for better approximations. If we take another look at our table of the ratios of x to $\pi(x)$, we find that this ratio is almost exactly log x - 1. With a more careful calculation and with more detailed data on $\pi(x)$, Legendre [5] found in 1808 that a particularly good approximation is obtained if in place of 1 we subtract 1.08366 from log x, i.e.

$$\pi(x) \approx \frac{x}{\log x - 1.08366}$$

Another good approximation to $\pi(x)$, which was first given by Gauss, is obtained by taking as starting point the empirical fact that the frequency of prime numbers near a very large number x is almost exactly 1/log x. From this, the number of prime numbers up to x should be approximately given by the

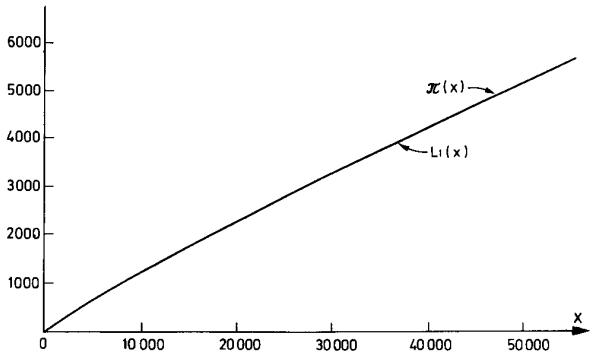
logarithmic sum

$$\mathrm{Ls}(x) = \frac{1}{\log 2} + \frac{1}{\log 3} + \ldots + \frac{1}{\log x}$$

or, what is essentially the same [6], by the *logarithmic integral*

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,dt.$$

If we now compare the graph of Li(x) with that of $\pi(x)$, then we see that within the accuracy of our picture the two coincide exactly.
There is no point in showing you the picture of Legendre's approximation as well, for in the range of the graph it is an even better approximation to $\pi(x)$.



There is one more approximation which I would like to mention. Riemann's research on prime numbers suggests that the probability for a large number x to be prime should be even closer to 1/log x if one counted not only the prime numbers but also the *powers* of primes, counting the square of a prime as half a prime, the cube of a prime as a third, etc. This leads to the approximation

$$\pi(x) + \tfrac{1}{2}\,\pi(\sqrt{x}) + \tfrac{1}{3}\,\pi(\sqrt[3]{x}) + \ldots \approx \mathrm{Li}(x)$$

or, equivalently,

$$\pi(x) \approx \mathrm{Li}(x) - \tfrac{1}{2}\,\mathrm{Li}(\sqrt{x}) - \tfrac{1}{3}\,\mathrm{Li}(\sqrt[3]{x}) - \ldots$$ [7].

The function on the right side of this formula is denoted by R(x), in honour of Riemann. It represents an amazingly good approximation to $\pi(x)$, as the following values show:

x	$\pi(x)$	R(x)
100,000,000	5,761,455	5,761,552
200,000,000	11,078,937	11,079,090
300,000,000	16,252,325	16,252,355
400,000,000	21,336,326	21,336,185
500,000,000	26,355,867	26,355,517
600,000,000	31,324,703	31,324,622
700,000,000	36,252,931	36,252,719
800,000,000	41,146,179	41,146,248
900,000,000	46,009,215	46,009,949
1,000,000,000	50,847,534	50,847,455

For those in the audience who know a little function theory, perhaps I might add that R(x) is an entire function of log x, given by the rapidly converging power series

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\log x)^n}{n!},$$

where $\zeta(n+1)$ is the Riemann zeta function [8].

At this point I should emphasize that Gauss's and Legendre's approximations to $\pi(x)$ were obtained only empirically, and that even Riemann, although he was led to his function R(x) by theoretical considerations, never proved the prime number theorem. That was first accomplished in 1896 by Hadamard and (independently) de la Vallée Poussin; their proofs were based on Riemann's work.

While still on the theme of the predictability of the prime numbers, I would like to give a few more numerical examples. As already mentioned, the probability for a number of the order of magnitude x to be prime is roughly equal to 1/log x; that is, the number of primes in an interval of length a about x should be approximately $a/\log x$, at least if the interval is long enough to make statistics meaningful, but small in comparison to x. For example, we would expect to find around 8142 primes in the interval between 100 million and 100 million plus 150,000 because

$$\frac{150{,}000}{\log\ (100{,}000{,}000)} = \frac{150{,}000}{18.427\ldots} \approx 8142$$

Correspondingly, the probability that two random numbers near x are both prime is approximately $1/(\log x)^2$. Thus if one asks how many prime twins (i.e. pairs of primes differing by 2, like 11 and 13 or 59 and 61) there are in the interval from x to x+a then we might expect approximately $a/(\log x)^2$. Actually, we should expect a bit more, since the fact that n is already prime slightly changes the chance that n+2 is prime (for example n+2 is then certainly odd). An easy heuristic argument [9] gives $C \cdot a/(\log x)^2$ as the expected number of twin primes in the interval [x, x+a] where C is a constant with value about 1.3 (more exactly: C = 1.3203236316...). Thus between 100 million and 100 million plus 150 thousand there should be about

$$(1.32\ldots)\frac{150{,}000}{(18.427)^2} \approx 584$$

pairs of prime twins. Here are data computed by Jones, Lal and Blundon [10] giving the exact number of primes and prime twins in this interval, as well as in several equally long intervals around larger powers of 10:

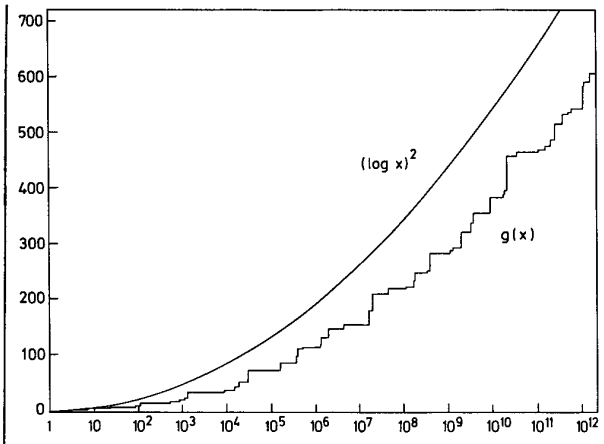
Interval	*Prime numbers*		*Prime twins*	
	expected	*found*	*expected*	*found*
100,000,000-100,150,000	8142	8154	584	601
1,000,000,000-1,000,150,000	7238	7242	461	466
10,000,000,000-10,000,150,000	6514	6511	374	389
100,000,000,000-100,000,150,000	5922	5974	309	276
1,000,000,000,000-1,000,000,150,000	5429	5433	259	276
10,000,000,000,000-10,000,000,150,000	5011	5065	221	208
100,000,000,000,000-100,000,000,150,000	4653	4643	191	186
1,000,000,000,000,000-1,000,000,000,150,000	4343	4251	166	161

As you can see, the agreement with the theory is extremely good. This is especially surprising in the case of the prime pairs, since it has not yet even been proved that there are infinitely many such pairs, let alone that they are distributed according to the conjectured law.

I want to give one last illustration of the predictability of primes, namely the problem of the gaps between primes. If one looks at tables of primes, one sometimes finds unusually large intervals, e.g. between 113 and 127, which don't contain any primes at all. Let g(x) be the length of the largest prime-free interval or "gap" up to x. For example, the largest gap below 200 is the interval from 113 to 127 just mentioned, so g(200) = 14. Naturally, the number g(x) grows very erratically, but a heuristic argument suggests the asymptotic formula [11]

$$g(x) \sim (\log x)^2$$

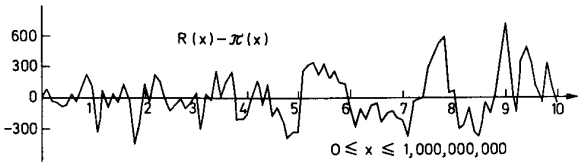
In the following picture, you can see how well even the wildly irregular function g(x) holds to the expected behaviour.



Up to now, I have substantiated my claim about the orderliness of the primes much more thoroughly than my claim about their disorderliness. Also, I have not yet fulfilled the promise of my title to show you the first 50 million primes, but have only shown you a few thousand. So here is a graph of $\pi(x)$ compared with the approximations of Legendre, Gauss, and Riemann up to 10 million [12]. Since these four functions lie so close together that their graphs are indistinguishable to the naked eye - as we already saw in the picture up to 50,000 - I have plotted only the differences between them:

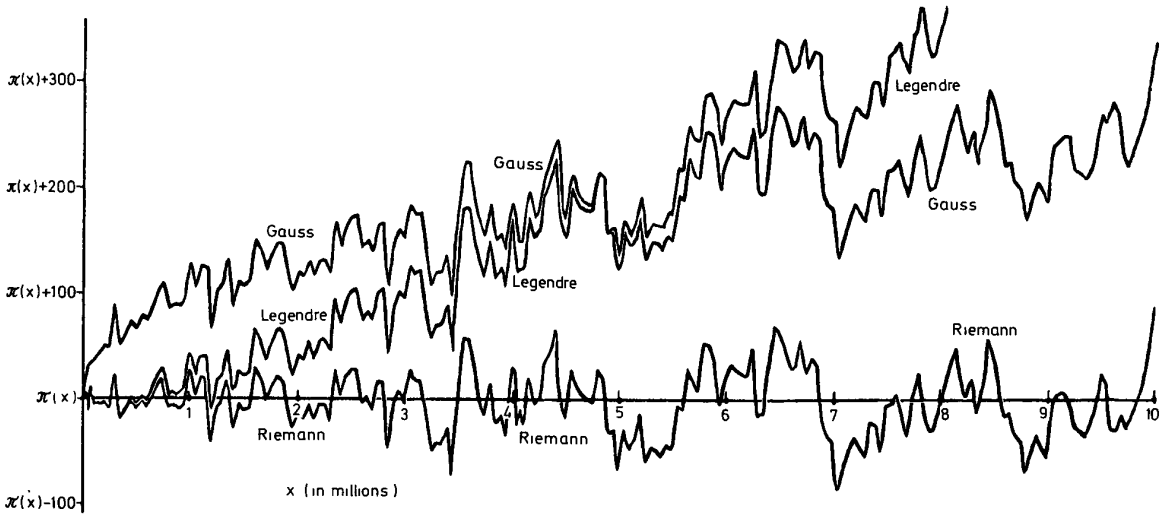
This picture, I think, shows what the person who decides to study number theory has let himself in for. As you can see, for small x (up to approximately 1 million) Legendre's approximation $x/(\log x - 1.08366)$ is considerably better than Gauss's $Li(x)$, but after 5 million $Li(x)$ is better, and it can be shown that $Li(x)$ stays better as x grows.

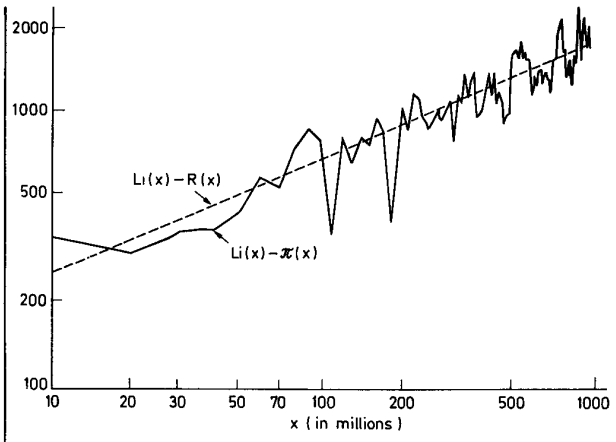
But up to 10 million there are only some 600 thousand prime numbers; to show you the promised 50 million primes, I have to go not to 10 million but all the way out to a billion (American style: 10^9). In this range, the graph of $R(x) - \pi(x)$ looks like this [13]:



The oscillation of the function $R(x) - \pi(x)$ become larger and larger, but even for these almost inconceivably large values of x they never go beyond a few hundred.

In connection with these data I can mention yet another fact about the number of prime numbers $\pi(x)$. In the picture up to 10 million, Gauss's approximation was always *bigger* than $\pi(x)$. That remains so until a billion, as you can see in the picture on the following page (in which the above data are plotted logarithmically).





Surely this graph gives us the impression that with increasing x the difference $\mathrm{Li}(x) - \pi(x)$ grows steadily to infinity, that is, that the logarithmic integral Li(x) consistently overestimates the number of primes up to x (this would agree with the observation that R(x) is a better approximation than Li(x), since R(x) is always smaller than Li(x)). But this is false: it can be shown that there are points where the oscillations of $R(x) - \pi(x)$ are so big that $\pi(x)$ actually becomes larger than Li(x). Up to now no such numbers have been found and perhaps none ever will be found, but Littlewood proved that they exist and Skewes[14] proved that there is one that is smaller than

$$10^{10^{10^{34}}}$$

(a number of which Hardy once said that it was surely the biggest that had ever served any definite purpose in mathematics). In any case, this example shows how unwise it can be to base conclusions about primes solely on numerical data.

In the last part of my lecture I would like to talk about some theoretical results about $\pi(x)$ so that you don't go away with the feeling of having seen only experimental math. A non-initiate would certainly think that the property of being prime is much too random for us to be able to prove anything about it. This was refuted already 2,200 years ago by Euclid, who proved the existence of infinitely many primes. His argument can be formulated in one sentence: If there were only finitely many primes, then by multiplying them together and adding 1, one would get a number which is not divisible by any prime at all, and that is impossible. In the 18th century, Euler proved more, namely that the sum of the reciprocals of the prime numbers diverges, i.e. eventually exceeds any previously given number. His proof, which is also very simple, used the function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots ,$$

whose importance for the study of $\pi(x)$ was fully recognized only later, with the work of Riemann. It is amusing to remark that, although the sum of the reciprocals of all primes is divergent, this sum over all the known primes (let's say the first 50 million) is smaller than four[15].

The first major result in the direction of the prime number theorem was proved by Chebyshev in 1850[16]. He showed that for sufficiently large x

$$0.89 \frac{x}{\log x} < \pi(x) < 1.11 \frac{x}{\log x}$$

i.e., the prime number theorem is correct with a relative error of at most 11%. His proof uses binomial coefficients and is so pretty that I cannot resist at least sketching a simplified version of it (with somewhat worse constants).

In the one direction, we will prove

$$\pi(x) < 1.7 \frac{x}{\log x} .$$

This inequality is valid for $x < 1200$. Assume inductively that it has been proved for $x < n$ and consider the middle binomial coefficient

$$\binom{2n}{n} .$$

Since

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \ldots + \binom{2n}{n} + \ldots + \binom{2n}{2n}$$

this coefficient is at most 2^{2n}. On the other hand

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(2n)\times(2n-1)\times\ldots\times 2\times 1}{(n\times(n-1)\times\ldots\times 2\times 1)} .$$

Every prime p smaller than 2n appears in the numerator, but certainly no p bigger than n can appear in the denominator. Thus

$$\binom{2n}{n}$$

is divisible by every prime between n and 2n:

$$\prod_{n<p\le 2n} p \;\Big|\; \binom{2n}{n} .$$

But the product has $\pi(2n) - \pi(n)$ factors, each bigger than n, so we get

$$n^{\pi(2n)-\pi(n)} \le \prod_{n<p\le 2n} p \le \binom{2n}{n} < 2^{2n}$$

or, taking logarithms

$$\pi(2n) - \pi(n) \le \frac{2n \log 2}{\log n} < 1.39 \frac{n}{\log n} .$$

By induction, the theorem is valid for n, so $\pi(n) < 1.7(n/\log n)$, and adding these relations gives

$$\pi(2n) < 3.09 \frac{n}{\log n} < 1.7 \frac{2n}{\log (2n)} \qquad (n > 1200).$$

Hence the theorem is valid also for 2n. Since

$$\pi(2n+1) \le \pi(2n) + 1 < 3.09 \frac{n}{\log n} + 1$$

$$\le 1.7 \frac{2n+1}{\log (2n+1)} \qquad (n > 1200),$$

it is also valid for 2n+1, completing the induction.

For the bound in the other direction, we need a simple lemma which can be proved easily using the well-known formula for the power of p which divides n! [17]:

Lemma: *Let p be a prime. If* p^{ν_p} *is the largest power of p dividing* $\binom{n}{k}$, *then*

$$p^{\nu_p} \le n.$$

Corollary: *Every binomial coefficient* $\binom{n}{k}$ *satisfies*

$$\binom{n}{k} = \prod_{p\le n} p^{\nu_p} \le n^{\pi(n)}$$

If we add the inequality of the corollary for all binomial coefficients $\binom{n}{k}$ with given n, then we find

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \le (n+1)\cdot n^{\pi(n)}$$

and taking logarithms gives

$$\pi(n) \ge \frac{n \log 2}{\log n} - \frac{\log (n+1)}{\log n}$$

$$> \frac{2}{3} \frac{n}{\log n} \qquad (n > 200).$$

In closing, I would like to say a few words about Riemann's work. Although Riemann never proved the prime number theorem, he did something which is in many ways much more astonishing - he discovered an *exact* formula for $\pi(x)$. This formula has the form

$$\pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \ldots = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}\,(x^{\rho})$$

where the sum runs over the roots of the zeta function $\zeta(s)$ [18]. These roots (apart from the so-called "trivial" roots $\rho = -2, -4, -6, \ldots$, which yield a negligible contribution to the formula) are complex numbers whose real parts lie between 0 and 1. The first ten of them are as follows [19]:

$$\rho_1 = \frac{1}{2} + 14.134725\, i,$$
$$\rho_2 = \frac{1}{2} + 21.022040\, i,$$
$$\rho_3 = \frac{1}{2} + 25.010856\, i,$$
$$\rho_4 = \frac{1}{2} + 30.424878\, i,$$
$$\rho_5 = \frac{1}{2} + 32.935057\, i,$$

$$\bar{\rho}_1 = \frac{1}{2} - 14.134725\, i,$$
$$\bar{\rho}_2 = \frac{1}{2} - 21.022040\, i,$$
$$\bar{\rho}_3 = \frac{1}{2} - 25.010856\, i,$$
$$\bar{\rho}_4 = \frac{1}{2} - 30.424878\, i,$$
$$\bar{\rho}_5 = \frac{1}{2} - 32.935057\, i.$$

It is easy to show that with each root its complex conjugate also appears. But that the real part of every root is exactly 1/2 is still unproved: this is the famous Riemann hypothesis, which would have far-reaching consequences for number theory [20]. It has been verified for 7 million roots.

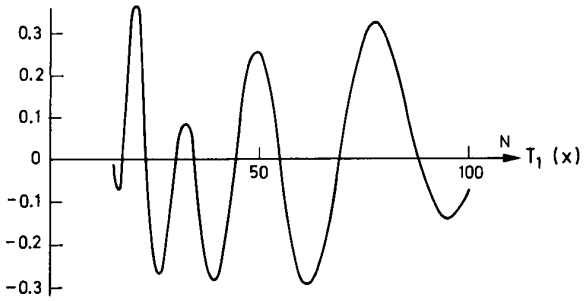
With the help of the Riemann function R(x) introduced above we can write Riemann's formula in the form

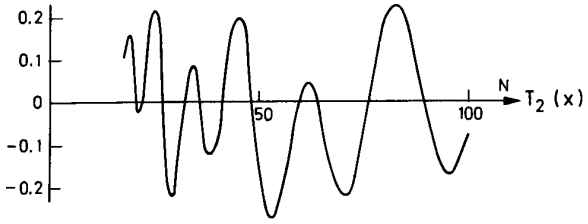
$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

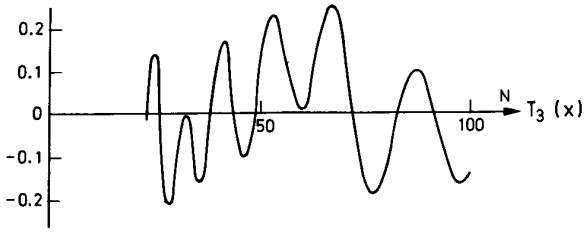
The k^{th} approximation to $\pi(x)$ which this formula yields is the function

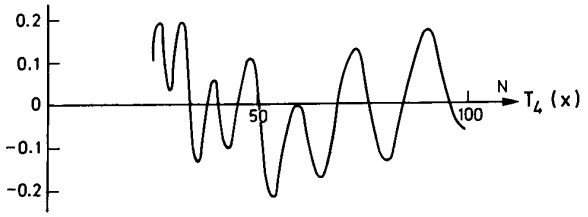
$$R_k(x) = R(x) + T_1(x) + T_2(x) + \ldots + T_k(x),$$

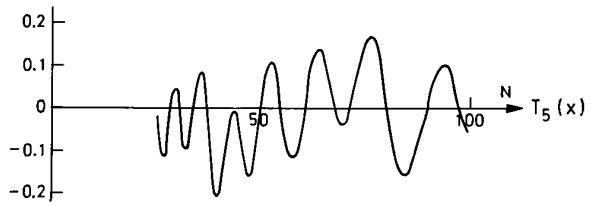
where $T_n(x) = -R(x^{\rho_n}) - R(x^{\rho_n})$ is the contribution of the n^{th} pair of roots of the zeta function. For each n the function $T_n(x)$ is a smooth, oscillating function of x. The first few look like this (21):



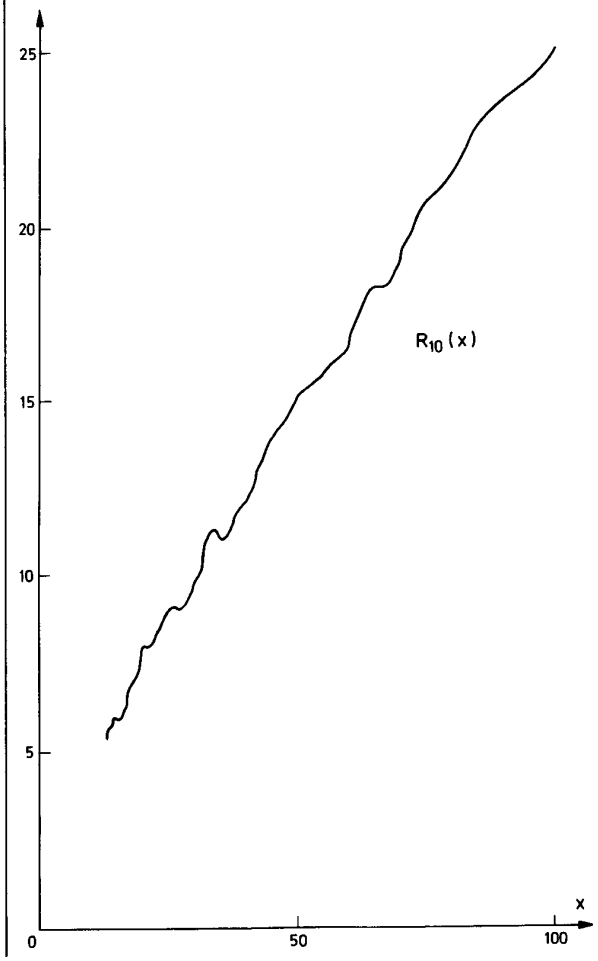


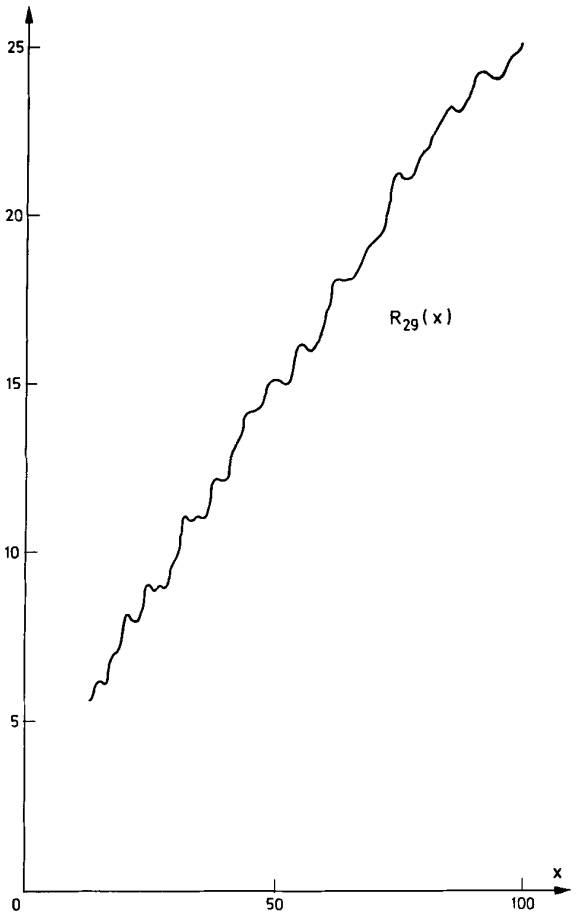




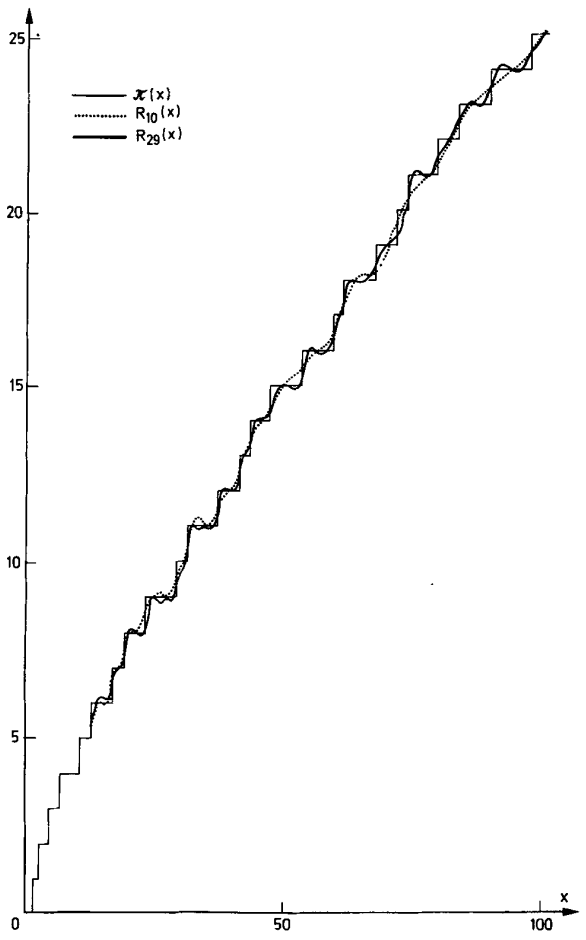


It follows that $R_k(x)$ is also a smooth function for each k. As k grows, these functions approach $\pi(x)$. Here, for example, are the graphs of the 10th and 29th approximations,





and if we compare these curves with the graph of $\pi(x)$ up to 100 (p. 9) we get the following picture:



I hope that with this and the other pictures I have shown, I have communicated a certain impression of the immense beauty of the prime numbers and of the endless surprises which they have in store for us.

Remarks

(1) J.M. Gandhi, Formulae for the nth prime, Proc. Washington State Univ. Conf. on Number Theory, Washington State Univ., Pullman, Wash., 1971 96 - 106

(2) J.P. Jones, Diophantine representation of the set of prime numbers, Notices of the AMS 22 (1975) A - 326.

(3) There is a good reason why so many of the numbers in this list have the form $M_k = 2^k - 1$: A theorem of Lucas states that M_k ($k>2$) is prime if and only if M_k divides L_{k-1}, where the numbers L_n are defined inductively by $L_1 = 4$ and $L_{n+1} = L_n^2 - 2$ (so $L_2 = 14$, $L_3 = 194$, $L_4 = 37634$, ...) and hence it is much easier to test whether M_k is prime than it is to test another number of the same order of magnitude.
The prime numbers of the form $2^k - 1$ (for which k itself must nec-

essarily be prime) are called Mersenne primes (after the French mathematician Mersenne who in 1644 gave a list of such primes up to 10^{79}, correct up to 10^{18}) and play a role in connection with a completely different problem of number theory. Euclid discovered that when $2^p - 1$ is prime then the number $2^{p-1}(2^p-1)$ is "perfect", i.e. it equals the sum of its proper divisors (e.g. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$) and Euler showed that *every* even perfect number has this form. It is unknown whether there are any odd perfect numbers at all; if they exist, they must be at least 10^{100}. There are exactly 24 values of $p < 20{,}000$ for which $2^p - 1$ is prime.

(4) C.F. Gauss, Werke II (1892) 444 - 447. For a discussion of the history of the various approximations to $\pi(x)$, in which an English translation of this letter also appears, see L.J. Goldstein: A history of the prime number theorem, Amer. Math. Monthly, 80 (1973) 599 - 615.

(5) A.M. Legendre, Essai sur la theorie de Nombres, 2nd edition, Paris, 1808, p. 394.

(6) More precisely

$$Ls(x) - 1.5 < Li(x) < Ls(x),$$

i.e. the difference between Li(x) and Ls(x) is bounded. We should also mention that the logarithmic integral is often defined as the Cauchy principal value

$$Li(x) = \not\int_0^x \frac{dt}{\log t} \underset{DEF}{=} \lim_{\varepsilon \to 0} \left(\int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1-\varepsilon}^{x} \frac{dt}{\log t} \right),$$

but this definition differs from that given in the text only by a constant.

(7) The coefficients are formed as follows: the coefficient of $Li(\sqrt[n]{x})$ is $+ 1/n$ if n is the product of an even number of distinct primes, $-1/n$ if n is the product of an odd number of distinct primes, and 0 if n contains multiple prime factors.

(8) Ramanujan has given the following alternative forms for this function:

$$R(x) = \int_0^\infty \frac{(\log x)^t \, dt}{t \, \Gamma(t+1) \zeta(t+1)}$$

($\zeta(s)$ = the Riemann zeta function and $\Gamma(s)$ = the gamma function) and

$$R(e^{2\pi x}) \doteq \frac{2}{\pi} \left(\frac{2}{B_2} x + \frac{4}{3B_4} x^3 + \frac{6}{5B_6} x^5 + \ldots \right)$$

$$= \frac{2}{\pi} \left(12x + 40x^3 + \frac{252}{5} x^5 + \ldots \right)$$

(B_k = k^{th} Bernoulli number; the symbol $\doteq$ means that the difference of the two sides tends to 0 as x grows to infinity). See G.H. Hardy, Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work, Cambridge University Press, 1940, Chapter 2.

(9) Namely: The probability that for a randomly chosen pair (m, n) of numbers both m and n are $\not\equiv 0 \pmod p$ is obviously $[(p-1)/p]^2$, while for a randomly chosen number n, the probability that n and n+2 are both $\not\equiv 0 \pmod p$ is $1/2$ for $p = 2$ and $(p-2)/p$ for $p \neq 2$. Thus the probability for n and n+2 modulo p to be prime twins differs by a factor

$$\frac{p-2}{p} \cdot \frac{p^2}{(p-1)^2}$$

for $p \neq 2$ and by 2 for $p = 2$ from the corresponding probability for two independent numbers m and n. Altogether, we have therefore improved our chances by a factor

$$C = 2 \cdot \prod_{\substack{p>2 \\ p \text{ prime}}} \frac{p^2 - 2p}{p^2 - 2p + 1}$$

$= 1.32032$. For a somewhat more careful presentation of this argument, see Hardy and Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1960, § 22.20 (p. 371 - 373)

(10) M.F. Jones, M. Lal, and W.J. Blundon, Statistics on certain large primes, Math. Comp. 21 (1967) 103 - 107.

(11) D. Shanks, On maximal gaps between successive primes, Math. Comp. 18 (1964) 646 - 651. The graph of g(x) was made from the tables found in

the following papers: L.J. Lander and T.R. Parkin, On first appearance of prime differences, Math. Comp. 21 (1967) 483 - 488, R.P. Brent, The first occurrence of large gaps between successive primes, Math. Comp. 27 (1973) 959 - 963.

(12) The data for this graph are taken from Lehmer's table of prime numbers (D.N. Lehmer, List of Prime Numbers from 1 to 10,006,721, Hafner Publishing Co., New York, 1956).

(13) This and the following graph were made using the values of $\pi(x)$ found in D.C. Mapes, Fast method for computing the number of primes less than a given limit, Math. Comp. 17 (1963) 179 - 185. In contrast to Lehmer's data used in the previous graph, these values were calculated from a formula for $\pi(x)$ and not by counting the primes up to x.

(14) S. Skewes, On the difference $\pi(x) - li(x)$ (I), J. London Math. Soc, 8 (1933) 277 - 283. Skewes' proof of this bound assumes the validity of the Riemann hypothesis which we discuss later. Twenty-two years later (On the difference $\pi(x) - li(x)$ (II), Proc. Lond. Math. Soc. (3) 5 (1955) 48 - 70) he proved without using the Riemann hypothesis that there exists an x less than the (yet much larger) bound

$$10^{10^{10^{964}}}$$

for which $\pi(x) > Li(x)$. This bound has been lowered to

$$10^{10^{529.7}}$$

by Cohen and Mayhew and to 1.65×10^{1165} by Lehman (On the difference $\pi(x) - li(x)$, Acta Arithm. 11 (1966) 397 - 410). Lehman even showed that there is an interval of at least 10^{500} numbers between 1.53×10^{1165} and 1.65×10^{1165} where $\pi(x)$ is larger than Li(x). As a consequence of his investigation, it appears likely that there is a number near 6.663×10^{370} with $\pi(x) > Li(x)$ and that there is no number less than 10^{20} with this property.

(15) Namely (as conjectured by Gauss in 1796 and proved by Mertens in 1874)

$$\sum_{p<x} \frac{1}{p} = \log\log x + C + \varepsilon(x),$$

where $\varepsilon(x) \to 0$ as x tends to infinity and $C \approx 0.261497$ is a constant. This expression is smaller than 3.3 when $x = 10^9$, and even when $x = 10^{18}$ it still lies below 4.

(16) P.L. Chebyshev, Recherches nouvelles sur les nombres premiers, Paris, 1851, CR Paris 29 (1849) 397 - 401, 738 - 739. For a modern presentation (in German) of Chebyshev's proof, see W. Schwarz, Einführung in Methoden und Ergebnisse der Primzahltheorie BI-Hochschultaschenbuch 278/278a, Mannheim 1969, Chapt. II.4, P. 42 - 48.

(17) The largest power of p dividing p! is $p^{[n/p]+[n/p^2]+\ldots}$, where [x] is the largest integer $\le x$. Thus in the notation of the lemma we have

$$\nu_p = \sum_{r\ge1}\left(\left[\frac{n}{p^r}\right] - \left[\frac{k}{p^r}\right] - \left[\frac{n-k}{p^r}\right]\right) .$$

Every summand in this sum is either 0 or 1 and is certainly 0 for $r > (\log n/\log p)$ (since then $[n/p^r] = 0$). Therefore $\nu_p \le (\log n/\log p)$, from which the claim follows.

(18) The definition of $\zeta(s)$ as $1 + 1/2^s + 1/3^s + \ldots$ given above makes sense only when s is a complex number whose real part is larger than 1 (since the series converges for these values of s only) and in this domain $\zeta(s)$ has no zeroes. But the function $\zeta(s)$ can be extended to a function for all complex numbers s, so that it makes sense to speak of its roots in the whole complex plane. The simplest way to extend the domain of definition of $\zeta(s)$ at least to the half-plane $Re(s) > 0$ is to use the identity

$$(1-2^{1-s})\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \ldots\right) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} ,$$

which is valid for $Re(s) > 1$, and to observe that the series on the right converges for all s with positive real part. With this, the "interesting" roots of the zeta function, i.e. the roots $\rho = \beta + i\gamma$ with $0 < \beta < 1$, can be characterized in

an elementary way by the two equations

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^{\beta}} \cos(\gamma \log n) = 0,$$

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^{\beta}} \sin(\gamma \log n) = 0.$$

The sum over the roots ρ in Riemann's formula is not absolutely convergent and therefore must be summed in the proper order (i.e., according to increasing absolute value of $\mathrm{Im}(\rho)$).

Finally, I should mention that, although Riemann stated the exact formula for $\pi(x)$ already in 1859, it wasn't proved until 1895 (by von Mangoldt).

(19) These roots were calculated already in 1903 by Gram (J.-P. Gram, Sur les zeros de la fonction $\zeta(s)$ de Riemann, Acta Math. 27 (1903) 289 - 304). For a very nice presention of the theory of Riemann's zeta function, see H.M. Edwards, Riemann's Zeta Function, Academic Press, New York, 1974.

(20) Namely the Riemann hypothesis implies (and in fact is equivalent to the statement) that the error in Gauss's approximation $\mathrm{Li}(x)$ to $\pi(x)$ is at most a constant times $x^{1/2} \cdot \log x$. At the present it is even unknown whether this error is smaller than x^c for any constant $c < 1$.

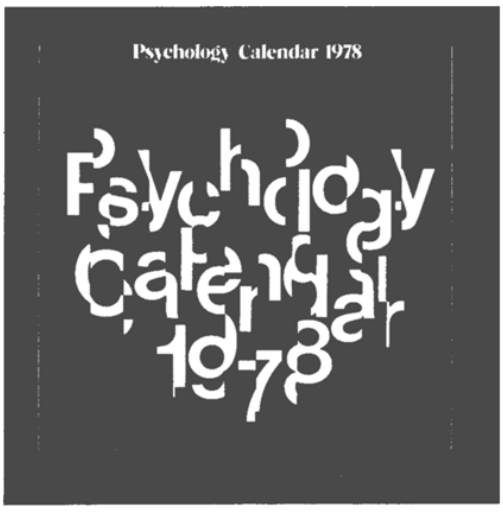
(21) This and the following graphs are taken from H. Riesel and G. Göhl, Some calculations related to Riemann's prime number formula, Math. Comp. 24 (1970) 969 - 983.

The 1977 *Mathematics Calendar* has found a worthy successor:

Psychology Calendar '78

containing a selection of twelve themes which portray something of the exciting spirit which pervades psychological inquiry:

- Dreaming
- Cognitive Contours
- Social Dominance in Monkeys
- McCollough Effect
- Dynamic Effects of Repetitive Patterns
- Harlow and Piaget
- Shadow and Light
- Memory Span Test
- Wilhelm Wundt Father of Psychology
- Recognition of Faces
- Split Brain
- Jerome Bruner's Theory of Cognitive Learning



P.S. No cause for concern. The next Mathematics Calendar will appear in 1979.