

The Prime Number Theorem

number theory. The main goal of finite group theory is to give a complete classification of all the "simple groups."

A major breakthrough occurred in 1963 when Walter Feit and John Thompson proved that every simple group is either cyclic or has an even number of elements. This had been conjectured by Burnside many years earlier. Following the inspiration of the Feit-Thompson success, a tremendous surge of new activity erupted in finite group theory. Today specialists in this area believe they are within a stone's throw of a complete classification of the simple groups.

Further Readings. See Bibliography

D. Gorenstein.

The Prime Number Theorem

THE THEORY of numbers is simultaneously one of the most elementary branches of mathematics in that it deals, essentially, with the arithmetic properties of the integers $1, 2, 3, \dots$ and one of the most difficult branches insofar as it is laden with difficult problems and difficult techniques.

Among the advanced topics in theory of numbers, three may be selected as particularly noteworthy: the theory of partitions, Fermat's "Last Theorem," and the prime number theorem. The theory of partitions concerns itself with the number of ways in which a number may be broken up into smaller numbers. Thus, including the "null" partition, two may be broken up as 2 or $1 + 1$. Three may be broken up as 3, $2 + 1$, $1 + 1 + 1$, four may be broken up as 4, $3 + 1$, $2 + 2$, $2 + 1 + 1$, $1 + 1 + 1 + 1$. The number of ways that a given number may be broken up is far from a simple matter, and has been the object of study since the mid-seventeen hundreds. The reader might like to experi-

Selected Topics in Mathematics



Pierre de Fermat
1601–1665

ment and see whether he can systematize the process and verify that the number 10 can be broken up in 42 different ways.

Fermat's "Last Theorem" asserts that if $n > 2$, the equation $x^n + y^n = z^n$ cannot be solved in integers x, y, z , with $xyz \neq 0$. This theorem has been proved (1979) for all $n < 30,000$, but the general theorem is remarkably elusive. Due to the peculiar history of this problem, it has attracted more than its share of mathematical crackpottery and most mathematicians ardently wish that the problem would be settled.

The prime number theorem, which is the subject of this section, has great attractions and mystery and is related to some of the central objects of mathematical analysis. It is also related to what is probably the most famous of the unsolved mathematical problems—the so-called Riemann Hypothesis. It is one of the finest examples of the extraction of order from chaos in the whole of mathematics.

Soon after a child learns to multiply and divide, he notices that some numbers are special. When a number is factored, it is decomposed into its basic constituents—its prime factors. Thus, $6 = 2 \times 3$, $28 = 2 \times 2 \times 7$, $270 = 2 \times 3 \times 3 \times 3 \times 5$ and these decompositions cannot be carried further. The numbers 2, 3, 5, 7, . . . are the prime numbers, numbers that cannot themselves be split into further multiplications. Among the integers, the prime numbers play a role that is analogous to the elements of chemistry.

Let us make a list of the first few 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	101	103	107	109	113 . . .

This list never ends. Euclid already had proved that there are an infinite number of primes. Euclid's proof is easy and elegant and we will give it.

Suppose we have a complete list of all the prime numbers up to a certain prime p_m . Consider the integer $N = (2 \cdot 3 \cdot 5 \cdot \cdot \cdot p_m) + 1$, formed by adding 1 to the product

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	547	1229	1993	2749	3581	4421	5261	6143	7001	7927	8847	9739	10663	11677	12569	13513	14533	15413	16411	17393	18329	19427	20359	2139
2	3	567	1231	1995	2751	3593	4431	5271	6153	7011	7937	8857	9749	10673	11687	12579	13523	14543	15423	16421	17403	18339	19437	20369	2139
3	4	587	1233	2001	2753	3605	4443	5283	6165	7023	7949	8869	9761	10685	11699	12591	13535	14555	15435	16433	17415	18351	19449	20381	2141
4	5	569	1249	2003	2771	3607	4447	5287	6169	7027	7951	8871	9769	10689	11701	12593	13537	14557	15437	16435	17417	18353	19451	20383	2143
5	11	571	1259	2011	2789	3613	4453	5293	6173	7029	7959	8881	9779	10709	11711	12603	13547	14567	15447	16445	17427	18359	19457	20389	2145
6	13	577	1277	2017	2791	3617	4457	5303	6199	7034	7963	8887	9781	10711	11717	12611	13557	14567	15447	16445	17427	18379	19457	20401	2143
7	17	587	1287	2027	2797	3623	4463	5317	6203	7039	7969	8897	9787	10717	11723	12617	13563	14573	15453	16451	17433	18389	19469	20403	2149
8	19	593	1299	2039	2803	3633	4473	5327	6217	7049	7981	8903	9793	10733	11733	12633	13573	14573	15459	16459	17447	18391	19471	20411	2149
9	29	591	1291	2053	2819	3643	4493	5337	6221	7019	7981	8929	9811	10739	11777	12641	13619	14599	15497	16487	17477	18427	19477	20443	2149
10																									
11	31	607	1297	2063	2833	3659	4507	5393	6225	7039	7983	8933	9817	10753	11779	12647	13627	14617	15511	16487	17483	18433	19483	20477	2149
12	37	613	1301	2087	2837	3661	4513	5399	6247	7121	8039	8949	9829	10773	11783	12653	13633	14627	15527	16493	17489	18439	19489	20483	2159
13	41	619	1307	2091	2843	3667	4519	5405	6253	7127	8045	8955	9835	10789	11789	12659	13639	14633	15533	16499	17493	18443	19493	20489	2159
14	43	631	1307	2083	2851	3677	4519	5413	6263	7129	8059	8963	9839	10789	11801	12661	13649	14633	15533	16529	17497	18451	19507	20509	2151
15	47	631	1313	2087	2857	3683	4521	5431	6269	7131	8081	8969	9851	10799	11807	12689	13679	14639	15559	16567	17509	18457	19531	20589	2152
16	53	641	1321	2089	2861	3687	4547	5419	6271	7159	8087	8971	9857	10801	11813	12697	13681	14653	15569	16553	17519	18461	19541	20521	2152
17	59	643	1329	2099	2879	3701	4549	5431	6277	7159	8097	8979	9859	10807	11821	12703	13687	14659	15581	16561	17539	18461	19543	20533	2153
18	61	647	1361	2111	2887	3709	4561	5437	6287	7187	8093	9001	9861	10813	11827	12709	13693	14665	15587	16567	17539	18463	19545	20535	2153
19	63	651	1367	2117	2893	3715	4567	5443	6293	7193	8101	9007	9867	10819	11833	12715	13699	14671	15593	16573	17545	18465	19547	20537	2153
20	71	659	1373	2129	2903	3727	4583	5443	6301	7207	8111	9011	9887	10825	11839	12729	13699	14679	15599	16587	17553	18507	19571	20545	2155
21	73	661	1381	2131	2909	3733	4591	5449	6311	7211	8117	9013	9901	10861	11839	12743	13709	14713	15619	16607	17579	18523	19577	20563	2156
22	79	673	1393	2137	2917	3739	4597	5471	6317	7213	8123	9029	9907	10867	11863	12757	13711	14717	15629	16619	17581	18529	19583	20569	2157
23	83	677	1409	2141	2927	3743	4603	5477	6323	7219	8147	9041	9923	10883	11867	12763	13713	14723	15643	16631	17593	18539	19597	20591	2158
24	87	681	1417	2147	2933	3749	4609	5483	6329	7225	8149	9043	9925	10885	11869	12765	13715	14725	15645	16633	17595	18541	19601	20593	2158
25	77	691	1427	2153	2933	3763	4603	5483	6337	7237	8167	9049	9931	10889	11867	12791	13729	14737	15647	16649	17609	18553	19609	20627	2159
26	101	701	1429	2161	2957	3739	4639	5561	6343	7243	8131	9059	9941	10903	11891	12799	13739	14741	15649	16651	17623	18583	19661	20639	2161
27	109	703	1433	2179	2963	3793	4643	5503	6353	7247	8139	9067	9949	10909	11909	12809	13757	14747	15659	16657	17627	18587	19681	20641	2161
28	119	719	1439	2203	2969	3749	4649	5507	6359	7253	8191	9067	9967	10917	11923	12821	13759	14753	15667	16661	17657	18593	19687	20663	2161
29	109	727	1447	2207	2971	3803	4651	5519	6361	7269	8209	9103	9973	10929	11929	12829	13769	14759	15673	16667	17667	18593	19687	20663	2161
30	113	735	1453	2213	2989	3803	4657	5521	6367	7271	8219	9107	10009	10949	11933	12829	13781	14767	15679	16671	17669	18593	19689	20667	2161
31	127	739	1453	2221	3001	3813	4663	5527	6373	7307	8219	9107	10009	10957	11939	12841	13789	14771	15683	16679	17681	18641	19707	20707	2164
32	137	743	1453	2221	3003	3813	4663	5527	6373	7307	8219	9107	10009	10957	11941	12853	13799	14779	15687	16679	17683	18641	19717	20717	2164
33	137	751	1471	2239	3019	3847	4679	5557	6389	7321	8233	9137	10039	10979	11953	12889	13807	14783	15731	16703	17679	18679	19727	20719	2167
34	139	751	1481	2243	3023	3851	4691	5563	6397	7331	8233	9137	10061	10987	11959	12893	13829	14783	15731	16703	17683	18679	19727	20719	2167
35	149	761	1483	2251	3037	3853	4703	5569	6401	7333	8243	9137	10067	10993	11961	12903	13831	14801	15731	16703	17683	18679	19727	20719	2167
36	151	769	1489	2267	3041	3863	4721	5573	6427	7349	8243	9161	10069	11003	11971	12907	13841	14821	15739	16747	17737	18731	19753	20747	2171
37	157	773	1493	2267	3041	3863	4721	5573	6427	7349	8243	9161	10069	11003	11971	12907	13841	14821	15739	16747	17737	18731	19759	20749	2172
38	163	783	1493	2273	3061	3881	4729	5591	6451	7369	8273	9181	10091	11047	11987	12917	13873	14831	15761	16763	17747	18731	19763	20753	2173
39	167	797	1499	2281	3067	3889	4733	5623	6469	7393	8287	9187	10093	11057	12007	12919	13877	14843	15767	16767	17761	18743	19773	20759	2173
40	173	809	1511	2287	3079	3907	4751	5639	6473	7411	8293	9199	10099	11059	12011	12923	13879	14851	15773	16781	17783	18749	19793	20767	2173
41	179	811	1523	2293	3083	3911	4759	5641	6481	7411	8293	9203	10103	11069	12037	12931	13883	14857	15787	16823	17789	18757	19801	20773	2175
42	181	821	1531	2297	3089	3917	4783	5647	6491	7433	8297	9209	10111	11073	12043	12937	13887	14863	15793	16829	17793	18763	19807	20779	2175
43	183	827	1541	2303	3093	3923	4789	5653	6497	7439	8303	9213	10119	11083	12049	12953	13903	14879	15793	16831	17801	18767	19813	20807	2175
44	185	827	1549	2311	3119	3923	4789	5653	6497	7439	8303	9213	10119	11083	12049	12953	13903	14879	15793	16831	17801	18767	19813	20807	2178
45	197	829	1553	2333	3123	3929	4793	5657	6547	7459	8329	9239	10141	11093	12071	12973	13913	14891	15809	16871	17837	19817	19843	20849	2179
46	199	839	1559	2339	3137	3931	4799	5659	6551	7477	8353	9241	10151	11113	12073	12979	13921	14897	15817	16879	17839	18803	19853	20857	2180
47	211	853	1567	2341	3163	3943	4801	5669	6553	7481	8363	9257	10159	11117	12097	12983	13931	14923	15823	16883	17853	18809	19861	20867	2181
48	223	857	1579	2351	3169	3949	4807	5673	6559	7487	8369	9263	10163	11127	12107	12993	13941	14933	15833	16893	17863	18813	19869	20873	2181
49	223	863	1583	2357	3181	3989	4831	5693	6571	7499	8387	9283	10177	11149	12109	13007	13957	14947	15881	16893	17869	18819	19869	20897	2184
50	233	877	1597	2371	3187	4013	4861	5701	6577	7507	8389	9293	10181	11159	12113	13007	13967	14957	15887	16923	17903	18911	19913	20899	2185
51	239	881	1603	2377	3193	4003	4871	5711	6581	7517	8413	9													

Table of the First 2500
Prime Numbers

From D. N. Lehmer, List of
prime numbers from 1 to
10,006,721, Carnegie Institution
of Washington. Publication No.
165, Washington, D.C., 1914.

Selected Topics in Mathematics

of all the primes up to p_m . Now N is larger than p_m (for it is certainly more than twice its size). When N is divided by 2 it goes $3 \cdot 5 \cdot \dots \cdot p_m$ times and leaves a remainder 1. When it is divided by 3, it goes $2 \cdot 5 \cdot \dots \cdot p_m$ times and leaves a remainder 1. Similarly, it leaves a remainder of 1 when divided by any of the primes 2, 3, 5, \dots , p_m .

Now N is either a prime number or it isn't. If it is a prime number, it is a prime number greater than p_m . If it isn't a prime number, it may be factored into prime numbers. But none of its prime factors can be 2, 3, 5, \dots , p_m as we just saw. Therefore there is a prime number greater than p_m .

The logical argument (actually, the dilemma, which forces one to the same conclusion whichever path one is compelled to take) tells us that the list of primes never ends.

The second feature of the list of primes that strikes one is the absence of any noticeable pattern or regularity. Of course all the prime numbers except 2 are odd, so the gap between any two successive primes has to be an even number. But there seems to be no rhyme or reason as to which even number it happens to be.

There are nine 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.			

But among the next hundred integers, from 10,000,000 to 10,000,100, there are only two:

10,000,019 and 10,000,079.

"Upon looking at these numbers, one has the feeling of being in the presence of one of the inexplicable secrets of creation," writes Don Zagier in an outburst of modern number mysticism.

What is known about primes and what is not known or conjectural would fill a large book. Here are some samples. The largest known prime in 1979 was $2^{21,701} - 1$. There is a prime between n and $2n$ for every integer $n > 1$. Is there a prime between n^2 and $(n + 1)^2$ for every $n > 0$? No one

The Prime Number Theorem

knows. Are there an infinity of primes of the form $n^2 + 1$ where n is an integer? No one knows. There are runs of integers of arbitrary length which are free of primes. No polynomial with integer coefficients can take on only prime values at the integers. There is an irrational number A such that $[A^{3^n}]$ takes on only prime values as $n = 0, 1, 2, \dots$. (Here the notation $[x]$ means the greatest integer $\leq x$.) Is every even number the sum of two odd primes? No one knows; this is the notorious Goldbach conjecture. Are there an infinite number of prime pairs, such as 11;13 or 17;19 or 10,006,427;10,006,429 which differ by 2? This is the problem of the twin primes, and no one knows the answer though most mathematicians are convinced that the statement is very likely to be true.

Some order begins to emerge from this chaos when the primes are considered not in their individuality but in the aggregate; one considers the social statistics of the primes and not the eccentricities of the individuals. One first makes a large tabulation of primes. This is difficult and tedious with pencil and paper, but with a modern computer it is easy. Then one counts them to see how many there are up to a given point. The function $\pi(n)$ is defined as the number of primes less than or equal to the number n . The function $\pi(n)$ measures the distribution of the prime numbers. Having obtained it, it is only natural to compute the ratio $n/\pi(n)$ which tells us what fraction of the numbers up to a given point are primes. (Actually, it is the reciprocal of this fraction.) Here is the result of a recent computation.

n	$\pi(n)$	$n/\pi(n)$
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

Notice that as one moves from one power of 10 to the next, the ratio $n/\pi(n)$ increases by roughly 2.3. (For example,

Selected Topics in Mathematics



Carl Friedrich Gauss
1777–1855



Jacques Hadamard
1865–1963

22.0 – 19.7 = 2.3.) At this point, any mathematician worth his salt thinks of $\log_e 10$ ($= 2.30258 \dots$) and on the basis of this evidence, it is easy to formulate the conjecture that $\pi(n)$ is approximately equal to $\frac{n}{\log n}$. The more formal statement that

$$\lim_{n \rightarrow \infty} \pi(n)/(n/\log n) = 1$$

is the famous prime number theorem. The discovery of the theorem can be traced as far back as Gauss, at age fifteen (around 1792), but the rigorous mathematical proof dates from 1896 and the independent work of C. de la Vallée Poussin and Jacques Hadamard. Here is order extracted from confusion, providing a moral lesson on how individual eccentricities can exist side by side with law and order.

While the expression $n/\log n$ is a fairly simple approximation for $\pi(n)$, it is not terribly close, and mathematicians have been interested in improving it. Of course, one does this at the price of complicating the approximant. One of the most satisfactory approximants to $\pi(n)$ is the function

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

where $\zeta(z)$ designates the celebrated Riemann zeta function: $\zeta(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \dots$. The accompanying table shows what a remarkably good approximation $R(n)$ is to $\pi(n)$:

	$\pi(n)$	$R(n)$
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

The Prime Number Theorem

Let us turn, finally, to the question of twin prime pairs. It is thought that there are an infinite number of such pairs, though this is still an open question.

Why do we believe it is true, even though there is no proof? First of all, there is numerical evidence; we find more prime pairs whenever we look for them; there does not seem to be a region of the natural number system so remote that it lies beyond the largest prime pair. But more than that, we have an idea *how many* prime pairs there are. We can get this idea by noticing that the occurrence of prime pairs in a table of prime numbers seem to be unpredictable or *random*. This suggests the conjecture that the chance of two numbers n and $n + 2$, both being prime, acts like the chance of getting a head on two successive tosses of a coin. If two successive random experiments are independent, the chance of success on both is the product of the chances of success on either; for example, if one coin has probability $\frac{1}{2}$ of coming up heads, two coins have probability $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ of coming up a pair of heads.

Now the prime number theorem, which *has* been proved, says that if n is a large number, and we choose a number x at random between 0 and n , the chance that x is prime will be "about" $\frac{1}{\log n}$. The bigger n is, the better is the approximation given by $\frac{1}{\log n}$ to the proportion of primes in the numbers up to n .

If we trust our feeling that the occurrence of twin primes is like two coins coming up heads, then the chance that both x and $x + 2$ are prime would be about $\frac{1}{(\log n)^2}$.

In other words, there would be about $\frac{n}{(\log n)^2}$ prime pairs to be found between 0 and n . This fraction approaches infinity as n goes to infinity, so this would provide a quantitative version of the prime pair conjecture.

For reasons involving the dependence of $x + 2$ being prime on the supposition that x is already prime, one should modify the estimate $\frac{n}{(\log n)^2}$ to $\frac{(1.32032...)n}{(\log n)^2}$.

Selected Topics in Mathematics

Appended is a comparison between what has been found and what is predicted by this simple formula. The agreement is remarkably good, but the final Q.E.D. is yet to be written.

Interval	Prime twins expec- ted	found
100,000,000– 100,150,000	584	601
1,000,000,000– 1,000,150,000	461	466
10,000,000,000– 10,000,150,000	374	389
100,000,000,000– 100,000,150,000	309	276
1,000,000,000,000– 1,000,000,150,000	259	276
10,000,000,000,000– 10,000,000,150,000	221	208
100,000,000,000,000– 100,000,000,150,000	191	186
1,000,000,000,000,000– 1,000,000,000,150,000	166	161

Further Readings. See Bibliography

E. Grosswald; D. N. Lehmer; D. Zagier.

The Mathematical Experience

Philip J. Davis
Reuben Hersh

With an Introduction by Gian-Carlo Rota

PENGUIN BOOKS