The Riddle of the Primes[*]

Edwin Hewitt
Visiting Professor
Department of Mathematics
National University of Singapore

Let me first express my gratitude to President Louis H. Y. Chen of the Singapore Mathematical Society for his kind invitation to give this talk. My thanks are also due to the Department of Mathematics of the National University of Singapore for inviting me to serve for a term on their academic staff. It is a privilege and a pleasure to live in Singapore and participate in the vigorous mathematical life of the NUS. Next, let me offer my congratulations and good wishes to the twelve young men [I wish only that there were also some young women] who have received prizes here for their mathematical achievements. At least one of the mathematics academic staff at NUS won this same award a few years ago. Let us look forward to the not-distant day when some of you will be professional mathematicians and on the academic staff of the NUS.

The subject of our talk today is older than the Pyramids and younger than the newest supercomputer. It is concerned with the positive integers or natural numbers. These are the numbers we learn about as tiny children. They form an *infinite sequence.* In the all but universally used Arabic notation, we write

$$1, 2, 3, 4, 5, 6, \ldots, n, \ldots,$$

the symbol "n" standing for a general positive integer and the final three dots meaning that the sequence of positive integers never ends. It goes on, as we say, "forever". The positive integers are so important that we give them their own name: $\mathbb{N}$. The positive integers are the fundamental object of all of mathematics. Once God has given us $\mathbb{N}$, we can construct the rest.

[*] Lecture given at the prize presentation ceremony of the Singapore Mathematical Society on 30 August 1988 for the winners of the 1988 Interschool Mathematical Competition.

Scientists recongnized many thousands of years ago that $\mathbb{N}$ is infinite. The point has fascinated mankind ever since. We all recognize that we have short lives. We have small brains. We use computers as prosthetic devices for the brain, but computers too, and the largest computer that I can conceive of, are finite as well. And yet whoever or whatever put us here and gave us the gift of consciousness has allowed us to recognize, though not to understand, this enormous set $\mathbb{N}$.

The infinitude of $\mathbb{N}$ is what makes mathematics far greater than any game. Chess is a marvelous game. Its strategies and tactics, to say nothing of the gamesmanship that goes into it, make it a pursuit that men and women can devote their entire lives to. But chess is finite. There are only so many games of chess. The number on the human scale is very large, but after you have listed all of the possible games of chess, there are still an infinite number of positive integers to go. Computers today can play very good chess, and one fine day they may wipe out human chess geniuses. The same comments apply to the Japanese game of go. So far as I know, no one has programmed a computer to play go. Still the possibility exists, and if there were compelling reasons to teach a computer to play go, it could be done. For the number of games of go is also finite.

Mathematical minds love to play with the fact that $\mathbb{N}$ is infinite. The great German mathematician David Hilbert (1862-1943) had a little allegory about a hotel, which has gone into folklore as Hilbert's Hotel. The hotel could always accommodate one more guest, for it had an infinite number of rooms, labelled with the room numbers 1, 2, 3, ... If the hotel was full and a new guest arrived, the occupant of room 1 would move to room 2, and so on. This freed up room 1, which was occupied by the new guest, while the original guests were comfortably ensconced in their new quarters.

Another mathematical giant of recent times was the German Hermann Weyl (1885-1955). I once heard him on the radio, lecturing to the listening public on mathematics. In his sonorous voice with its German accent, he emphasized the vital importance of the infinitude of the positive integers.

Today we are going to consider, and I am going to talk about, prime numbers. A positive integer is *prime* if (a) it is greater than 1 and (b) its only positive integer divisors are itself and 1. We will give the set of all prime numbers a special name, $\mathbb{P}$ [this is common but not universal]. I am personally fond of primes [fonder of some than others]. I have memorized the first few primes, and I expect that you know them too:

$$(*)\begin{cases} 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \\ 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 113, \\ 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, \ldots . \end{cases}$$

Primes are the building blocks for $\mathbb{N}$. Every integer exceeding 1 is a product of positive integral powers of distinct primes. This factorization into a product of prime powers is unique, except obviously for the order in which we write the primes. For n in $\mathbb{N}$ and $n > 1$, we can write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s},$$

where the p's are distinct primes and the a's are positive integers. This great theorem goes back to Euclid, about 300 years before Christ, or about the time of Confucius [孔子].

All of us use this unique factorization theorem whenever we find the divisors of a positive integer. In a humble way, it is used today in the City of Rome, where only cars with even license numbers are admitted to the city on days with even dates and only cars with odd license numbers are admitted to the city on days with odd dates. [Have you heard about the young lady who went out with extremely weird men? She liked odd dates.]

Let's go back and look at the little list (*). It looks as if it might go on much further. And indeed it does. Another celebrated theorem of Euclid is :

The set $\mathbb{P}$ is infinite.

Euclid's proof, the same one we use today, is a marvel. We assume that the theorem is false, and get a contradiction. As the English mathematician G. H. Hardy (1877-1947) has pointed out, this manoeuvre shows the boldness of mathematicians. A chess player may put forth a pawn for sacrifice, hoping to lure her opponent into a parlous position. *Euclid offers the whole game.* Write down the first k primes :

$$(**) \qquad 2, 3, 5, 7, 11, \ldots, p_k .$$

Multiply these numbers together and add 1. We get a number that we call $E(p_k)$, in honor of Euclid:

$$(***) \qquad E(p_k) = (2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p_k) + 1.$$

Now assume that the sequence $(**)$ ends somewhere. That is, there is a largest prime p_l. Compute the number $E(p_l)$. By the unique factorization theorem, $E(p_l)$ has at least one prime divisor: $E(p_l)$ may or may not be prime, but it has a prime divisor, say q. The prime q cannot be any of the primes listed in $(**)$ for $k = l$, as $E(p_l) = A_j \cdot p_j + 1$ for each p_j appearing in $(**)$ and some positive integer A_j. Therefore q is not in the list $(**)$, and so there is no largest prime number.

We issue a caveat at his point. We do *not* claim that the numbers $E(p_k)$ are prime. The numbers $E(3)$, $E(5)$, $E(7)$, and $E(11)$ are in fact prime. The number $E(13)$ is the product of 59 and 509. Dr. Y. K. Leong of NUS has computed the prime factors of the E's from $E(17)$ out to $E(53)$. The only prime among them is $E(31)$, which is the imposing number 20056049013. Dr. Leong used a program devised by Professor T. A. Peng, also of NUS, using the language MUMATH.

At the end of this homily, I have appended a table of the primes less than 2000. A look at this table shows that these primes are distributed among the positive integers in a highly irregular way. Early on there is a gap of 14, between 113 and 127. A gap of 14 is reached for the second time between 317 and 331. A gap of 18 is reached between 523 and 541. A small table of first occurrences of gaps appears as Table II, also at the end of this essay.

For some 2300 years the only way known to compile tables of primes was to write a list of the positive integers to be examined and to strike out all proper multiples of 2, then of 3, then of 5, and so on. This method is called the *sieve of Eratosthenes,* after its discoverer, who flourished about 200 B.C.

The advent of the computer has rendered the search for primes far more sophisticated. It is now easy to find primes of the order of 10^{50}. Finding "large" primes is a flourishing industry, partly at least because primes are useful in cryptography. One devises a code based on the product of two distinct primes, and publishes the product for the world to see. To decode a message one must know the factors of this product. Up to now, it has been far more difficult to factor an integer than to locate primes. Thus the code is all but unbreakable, though with the highly ingenious people who work on factoring methods, one cannot tell what breakthroughs may appear. The difficulties encountered at present in factoring are well illustrated by a news story that appeared in the Singapore Straits Times in October 1988. A team of mathematicians got together and enlisted the use of 400 computers worldwide. With the joint operation they succeeded in finding the prime factors of

$$11^{104} + 1.$$

I have no idea what the factors are, apart from 2, which is obvious, and 17, which can be shown to be a factor in a few moments with a 10-place calculator.

For reasons that are far from clear to me, people expend lots of personal effort and computer time in locating larger and larger primes. Part of this is a game, of course, a sort of get-it-into-the-Guinness-book-of-records thing.

If an integer of the form $2^a - 1$ (a in $\mathbb{N}$) is a prime, then a has to be a prime. To prove this is a trifling exercise. Primes of the form $2^p - 1$ (p a prime) are called *Mersenne primes,* after the French mathematician-priest Father Marin Mersenne (1588-1648). We write $2^p - 1$ as $M(p)$. The French mathematician Edouard Lucas showed in 1914 that $M(127)$ is prime. This to my knowledge is the largest prime ever found by noncomputer methods. With computer searches, a number of Mersenne primes have been found: $M(p)$ is prime for $p = 11213$, 44497, 86243, 123049, and 216091. These numbers $M(p)$ are indeed large on the human scale, but beyond $2^{216091} - 1$, which written out to base 10 has some 72000 digits, there are still an infinite number of positive integers. Humankind will never be able to compute all Mersenne primes simply by checking individual cases.

It's a grim thought, and it raises doubts in my mind as to the utility of grinding out more and more Mersenne primes. Of course it beats watching television and drinking beer.

The great Frenchman Pierre de Fermat (1601-1665) looked at numbers of the form

$$2^{2^m} + 1 = F_m.$$

The numbers F_0, F_1, F_2, F_3 and F_4 are prime, while F_5 is equal to 641 times 6700417. You can check these assertions in a few moments with your calculator. No larger primes F_m are known. The number F_{3310} is known to be divisible by $5 \cdot 2^{3313} + 1$. The number F_{3310} is roughly equal to

$$10^{(10^{990})},$$

which looks pretty large to me. But once again, it doesn't even make a dent in the infinite set $\mathbb{N}$.

Enough of this arithmetical elephantiasis. Let us turn to a theorem about all primes that we can prove.

We ask: what primes are the sums of two squares (of integers of course)? Let's look at the first few primes. We find:

$$2 = 1^2 + 1^2;$$

$$5 = 2^2 + 1^2;$$

$$13 = 3^2 + 2^2;$$

$$17 = 4^2 + 1^2;$$

$$29 = 5^2 + 2^2.$$

This small sample hints that all primes of the form $4m + 1$ might be sums of two squares. This is in fact true. The prime 2 and all primes of the form $4m+1$ are sums of two squares. This wonderful fact was known to Fermat, but a proof had to wait for Leonhard Euler (1707-1783). Plainly any odd integer that is the sum of two squares has to be of the form $4m + 1$, so the theorem determines completely the primes that are sums of two squares.

We will finish this lecture by proving this theorem. We need a basic fact.

Fact 1. *If a prime p divides a product xy of integers x and y, then p divides x $(p \mid x)$ or p divides y $(p \mid y)$.*

We won't prove Fact 1.

We also use Gauss's notation [Carl Friedrich Gauss, (1777-1855)] for modular arithmetic. For a positive integer m (the modulus) and integers x and y, we write $x \equiv y \pmod m$ to mean that $m \mid (x - y)$ (m divides $(x - y)$).

Next, given a prime p, consider the set of numbers

$$\{1, 2, 3, \ldots, (p - 1)\} = A.$$

For an integer x in A, consider also the set of numbers

$$\{x, 2x, 3x, \ldots, (p - 1)x\} = Ax.$$

If there are j and k in A for which

$$jx \equiv kx \pmod p,$$

then $p \mid (j-k)x$. By Fact 1, $p \mid x$ or $p \mid (j-k)$. The first is impossible and so $p \mid (j-k)$. This means that $j-k=0$, or $j=k$. Thus, if we throw away multiples of p, the set of numbers Ax is the set A over again, and in particular, the number $1+up$ for some integer u appears in Ax. We thus have our second step.

Fact 2. *For every x in A, there is an x' in A such that $xx' \equiv 1 \pmod{p}$.*

We use Fact 2 to prove

Wilson's Theorem. *For a prime p, we have*

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

Proof. The theorem is obvious for $p=2$. For $p>2$, note that $(p-1)' = p-1$ (notation as in Fact 2). For s in the set $\{2,3,\ldots,p-2\}$ we must have $s' \neq s$. For, if $s^2 \equiv 1 \pmod{p}$, then

$$p \mid (s-1) \quad \text{or} \quad p \mid (s+1),$$

and so

$$s-1=0 \quad \text{or} \quad s+1=p.$$

Thus the product

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$$

is equal to

$$(p-1) \text{ times } \frac{1}{2}(p-3) \text{ products } ss',$$

so that $(p-1)!$ is -1 plus a multiple of p. □

Now suppose that p is a prime of the form $4m+1$. We use Wilson's theorem and a little algebra to write

$$\begin{aligned} -1 &\equiv (p-1)! && \pmod{p} \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \tfrac{1}{2}(p-1) \cdot \tfrac{1}{2}(p+1) \cdots (p-1) && \pmod{p} \\ &\equiv \left(\tfrac{1}{2}(p-1)\right)!(-1)^{\frac{1}{2}(p-1)} \left(\tfrac{1}{2}(p-1)\right)! && \pmod{p} \\ &\equiv ((2m)!)^2(-1)^{2m} && \pmod{p}. \end{aligned}$$

So we have

Fact 3. *For a prime p of the form $4m+1$, there is an integer a such that $a^2 \equiv -1 \pmod{p}$.*

We can now complete our proof. Let b be the unique integer such that $b < \sqrt{p} < b+1$. We look at all of the numbers

$$x + ay$$

where x and y run independently through the set $\{0, 1, \ldots, b\}$. There are $(b+1)^2$ of these expressions. Since $(b+1)^2 > p$, at least two of them must be congruent modulo p:

$$\begin{aligned} x_1 + ay_1 &\equiv x_2 + ay_2 && \pmod{p}, \\ x_1 - x_2 &\equiv a(y_2 - y_1) && \pmod{p}, \end{aligned}$$

or

$$x_0 \equiv ay_0 \qquad \pmod{p},$$

where not both x_0 and y_0 are zero. Squaring both sides, we get

$$\begin{aligned} x_0^2 &\equiv a^2 y_0^2 && \pmod{p}, \\ x_0^2 &\equiv -y_0^2 && \pmod{p}, \\ x_0^2 + y_0^2 &\equiv 0 && \pmod{p}, \end{aligned}$$

or

$$x_0^2 + y_0^2 = mp$$

for some m in $\mathbb{N}$. Since $0 \le x_j \le b$ and $0 \le y_j \le b$, we have $|x_0| = |x_1 - x_2| \le b$ and $|y_0| = |y_1 - y_2| \le b$. Squaring and adding, we get

$$x_0^2 + y_0^2 \le 2b^2 < 2p,$$

since we chose $b < \sqrt{p}$. The only way for $x_0^2 + y_0^2$ to be mp with $1 \le m < 2$ is for

$$x_0^2 + y_0^2 = p.$$

This completes our proof, which is the proof of Euler.

Number theory is a vast subject. Gauss called it the Queen of the Sciences. There are hundreds of excellent textbooks on number theory. A great classic is

Hardy, G. H. and E. M. Wright,
An introduction to the theory of numbers,
Oxford, Clarendon Press, first edition 1938,
now in its fifth edition (1984).

A more recent text, also classic by now, is
Niven, I. M. and H. S. Zuckerman,
An introduction to the theory of numbers,
New York, John Wiley and Sons,
first published in 1960 and now in its fourth edition (1980).

A lively account of many special topics is found in
Schroeder, M. R.,
Number theory in science and communication,
Berlin-Heidelberg-New York-Tokyo, Springer-Verlag,
second edition, 1986.

I cut my eyeteeth on Hardy and Wright. Nowadays I find it slightly old-fashioned, but I treasure the myriad hours I spent over it. I had the privilege of watching Professors Niven and Zuckerman working on their book in the late 1950's in Helen and Herbert Zuckerman's cozy livingroom in Seattle, USA.

It remains only for me to thank all of you for your kind attention. Good evening to you all and godspeed to all of our young prizewinners.

Biographical note: Professor Edwin Hewitt is Professor Emeritus at the University of Washington, where he taught from 1948 to 1986. He obtained his A.B. in 1940 and his Ph.D. in 1942 from Harvard University. Professor Hewitt's field of specialization is mathematical analysis. He has published numerous papers and has written three research level books and five text books. Professor Hewitt is currently visiting the Department of Mathematics, National University of Singapore.

Table I

The primes from 2 to 1999

2	167	389	631	883	1153	1447	1709
3	173	397	641	887	1163	1451	1721
5	179	401	643	907	1171	1453	1723
7	181	409	647	911	1181	1459	1733
11	191	419	653	919	1187	1471	1741
13	193	421	659	929	1193	1481	1747
17	197	431	661	937	1201	1483	1753
19	199	433	673	941	1213	1487	1759
23	211	439	677	947	1217	1489	1777
29	223	443	683	953	1223	1493	1783
31	227	449	691	967	1229	1499	1787
37	229	457	701	971	1231	1511	1789
41	233	461	709	977	1237	1523	1801
43	239	463	719	983	1249	1531	1811
47	241	467	727	991	1259	1543	1823
53	251	479	733	997	1277	1549	1831
59	257	487	739	1009	1279	1553	1847
61	263	491	743	1013	1283	1559	1861
67	269	499	751	1019	1289	1567	1867
71	271	503	757	1021	1291	1571	1871
73	277	509	761	1031	1297	1579	1873
79	281	521	769	1033	1301	1583	1877
83	283	523	773	1039	1303	1597	1879
89	293	541	787	1049	1307	1601	1889
97	307	547	797	1051	1319	1607	1901
101	311	557	809	1061	1321	1609	1907
103	313	563	811	1063	1327	1613	1913
107	317	569	821	1069	1361	1619	1931
109	331	571	823	1087	1367	1621	1933
113	337	577	827	1091	1373	1627	1949
127	347	587	829	1093	1381	1637	1951
131	349	593	839	1097	1399	1657	1973
137	353	599	853	1103	1409	1663	1979
139	359	601	857	1109	1423	1667	1987
149	367	607	859	1117	1427	1669	1993
151	373	613	863	1123	1429	1693	1997
157	379	617	877	1129	1433	1697	1999
163	383	619	881	1151	1439	1699	

Table II

In this table we use Table I and some help from a larger table of primes to list the increasing gaps in the sequence of primes and the smallest primes before which these gaps occur. The column on the left gives the gap g, the corresponding entry in the column on the right is $p = p(g)$, which is the smallest prime such that for the greatest prime $p' < p$, the difference $p - p'$ is g.

g	$p(g)$
1	3
2	5
4	11
6	29
8	97
14	127
18	541
20	907
22	1151
34	1361
36	9587
44	15727
52	19661
72	31469
86	156007
96	360749
112	370373
114	492227
118	1349651
132	1357333
148	2010881
154	4652507
180	17051887

For more details, see Daniel Shanks's article in Mathematics of Computation 18 (1964), pp. 646-651 and R. P. Brent's article in the same journal 27 (1973), pp. 959-963.