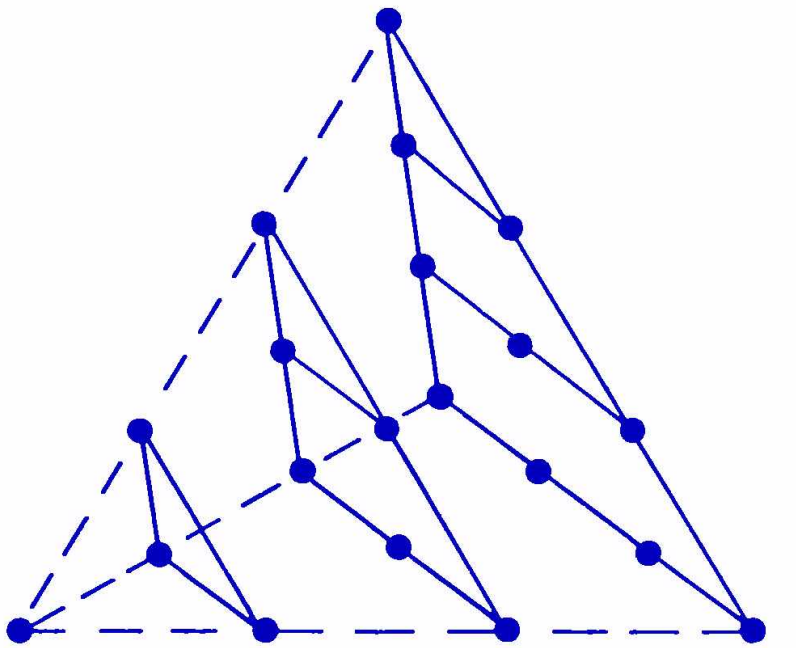
Facts and Speculations about Numbers

from Euclid to the latest Computers

A NUMBER FOR YOUR THOUGHTS



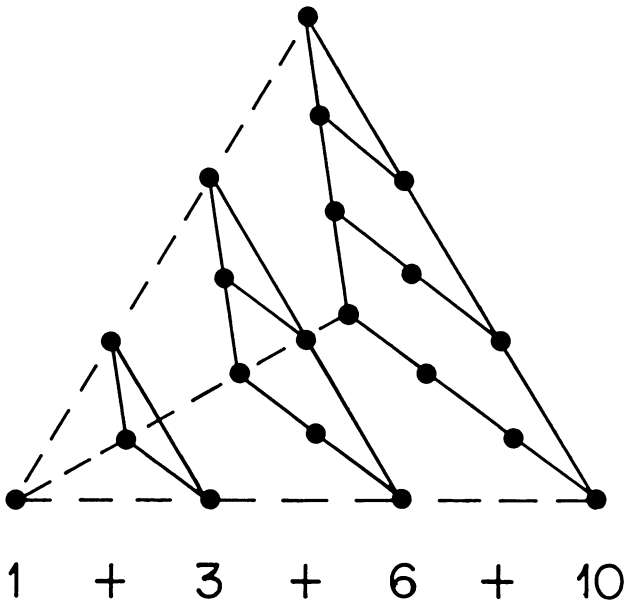
1 + 3 + 6 + 10

Stephen P. Richards

Facts and Speculations about Numbers

from Euclid to the latest Computers

A NUMBER FOR YOUR THOUGHTS



Stephen P. Richards

LIBRARY OF CONGRESS
CATALOG CARD NUMBER 82-90025

ISBN 0-9608224-0-2

—Published By—
S. P. RICHARDS
Box 501
New Providence, N. J. 07974

TABLE OF CONTENTS

1. COUNTING

From prehistoric times man has had the need to count. The stone-age hunter or hunting scout would doubtless have found it of great use to be able to give his hunting colleagues some indication of the number of animals he had located, in addition to their kind and approximate location. Although terms such as one, few, and many, may well have sufficed for a while, a more precise counting scheme would be needed eventually, perhaps for bartering, and some concept of number does seem to be possessed by even the most primitive tribes today. Counting, of course, can be performed without the *verbal* possession of number words. This can be achieved, for example, by placing the objects to be counted in a one-to-one correspondence with fingers, toes, or 'counting stones', but words for the most commonly occurring numbers (usually the smallest) are obviously convenient, and seem to have developed at quite an early stage in all forms of human society.

In order to proceed to large numbers in the counting process it soon becomes clear that some grouping arrangement is highly desirable. Thus, the number twenty three is much more conveniently recorded by two 'marking-stones' designating tens, and three perhaps smaller ones designating units, than by twenty three separate 'unit' stones. The grouping number is, in modern usage, referred to as the *base* of the counting system. It need not be equal to ten, of course, and systems based on five, twenty, and even sixty, have occurred in other cultures. Indeed, remnants of such systems are still with us today in the measurement of time (hours, minutes, and seconds - with base sixty) and in the words dozen (base twelve) and score (base twenty). It is even possible to evolve multi-base counting systems - the Mayans used one - and such systems abound among the English units of measurement which answer the question of 'how much?' rather than 'how many?'. Some readers may still recall the tribulations of working out the old English money system of twelve pence in one shilling and twenty shillings in one pound before it was mercifully decimalized in the early 1970's. Others may be more familiar with at least most of the units of weight such as tons, hundred-weights, stones, pounds, and ounces, but possibly without having a precise recollection of how many of these happen to be in one of those.

Doing arithmetic in these multi-base counting systems can be quite tricky, although familiarity helps to a surprising degree, and when the English currency was finally decimalized, many of the older generation found the new simplified system quite confusing and continued to

convert everything back to the old multi-base pounds, shillings, and pence before deciding on the advisability of a particular purchase. Fundamentally, however, the single- base system is the simplest, and such a system with base ten is used almost universally for counting today. For this reason the present book can very largely be restricted to this system alone. It is referred to as the *decimal* system of counting, and the choice of the number ten presumably arose from counting on the fingers, with the word 'digit' for any numeral between 0 and 9 seemingly attesting to this fact.

Numbers are an abstract concept and have no physical form. I cannot therefore write down the number 5. But you just did, I hear you say. Well, not really - I wrote down a particular mark (called a numeral) to represent it. Had I been a Roman I should have written V. There is fortunately nothing absolute about any one representation, and the fundamental properties of numbers are not at all dependent on the notation used. The fact that 5 is not exactly divisible by 2 is still true if I think of it as V divided by II. It is also just as true if I use a different base or grouping terminology. This means that if these properties can be demonstrated in our own familiar base-ten system, then we do not have to worry further about verifying them in other counting systems.

Counting in groups of ten, with the symbols 0,1,2,3,4,5,6,7,8,9, is so ingrained in us that the fact that it is quite an arbitrary choice comes almost as a surprise. That one can count quite happily in systems with other bases, right down to 'base-two', which uses only the two symbols 0 and 1, is something of an alien concept to most of us. After all, counting in groups of ten (or to the base ten as we should more formally say) has been a common procedure in many civilizations since the early Egyptians at least. On the other hand, the precise system which we use today, and so take for granted, is of much more recent origin. It contains within it one of the most important inventions ever made, a property which all earlier counting systems, even those using the base ten, did not have. Once again familiarity breeds contempt, and you may well be wondering what attribute of our simple counting system, which somehow seems so natural, could possibly deserve such an accolade. Wouldn't anyone, you may feel, who chose to count in tens, proceed roughly as we do with possibly different symbols for the numerals? The answer is almost certainly not.

The most natural way to count in groups of ten is first to choose symbols for the first nine digits, and then to choose other symbols to represent ten, twenty, etc., up to ninety, and still others for one

hundred, two hundred, and so on. Roman numerals, with which we are all acquainted tc some degree, are just such an example. They are based in groups of ten as follows:

Units: I, II, III, IV, V, VI, VII, VIII, IX
Tens: X, XX, XXX, XL, L, LX, LXX, LXXX, XC
Hundreds: C, CC, CCC, CD, D, DC, DCC, DCCC, CM
Thousands: M, MM, MMM, MMMM, MMMMM, and so on.

Thus the number 8888 becomes MMMMMMMMDCCCLXXXVIII in Roman numerals, and a routine shopping list for our everyday Roman Centurian might look something like this:

III pairs sandals	III x VII	equals	XXI	den.
IV tunics	IV x IX	equals	XXXVI	den.
I ceremonial toga	I x XL	equals	XL	den.
II plumed helmets	II x XVIII	equals	XXXVI	den.
I sword (regular)	I x XXVIII	equals	XXVIII	den.
I shield	I x XXXIX	equals	XXXIX	den.
	TOTAL	equals	CC	den.

where den. stands for denarius, which was a Roman unit of currency.

Now I do not known whether the cost of living during any period of the Roman empire was such as to make these values realistic, but it is quite possible since rampant inflation was as much a part of Roman lives as it is of our own. The point which we are trying to make does not depend on this of course; it is that checking this shopping list does seem to be a bit tricky without converting it tc more familiar numbers. Similarly, multiplying that Roman equivalent of 8888 set out above by say IX or XI seems to be even more difficult. Are these difficulties due only to our lack of familiarity with the system, or is it more than that? Well, our lack of familiarity is certainly no help, but there is indeed a fundamental difficulty with the Roman system over and above this. We should probably sense it first in this way; there are no units columns and no tens columns. Now it is true that methods can be devised for putting the Roman addition and multiplication into some kind of column format (although there is no evidence that the Romans actually did this) which, when combined with special rules for transfering from some columns to others, enable these tasks to be carried out for relatively small numbers. For large numbers, however, the situation is so bad that to represent a million, let alone multiply it

by anything, a Roman would have to fill several pages of this book entirely with M's. It is true that more and more letters could be introduced to represent larger and larger groups of ten, but then the system itself rapidly gets out of hand in any case.

The arithmetic associated with these kinds of problems is eased a little bit if we have just one symbol for each numeral between 1 and 9, and then use a separate set of symbols to designate whether we are dealing with tens, hundreds, thousands, etc. For example, if we designate thousands by M, hundreds by C, and tens by X, to follow the Roman precedent, then the number 8888 referred to above would now appear as 8M8C8X8, or its equivalent with the numeral 8 replaced by whatever symbol might have been chosen to represent eight units. In fact, just such grouping systems as these were used at one time by the Chinese and the Japanese (with suitably oriental characters for the numerals and the group symbols of course). But with this system there are still significant problems remaining concerning the writing of large numbers. For each larger group of ten a new symbol is required. Millions are not too bad (requiring five group symbols) but astronomical calculations would certainly tax this system.

One important step remains to take us over to our familiar modern system. It is the all-important invention of a symbol for zero. With this symbol, 0, we are able to recognize the group to which a particular numeral belongs (that is hundreds, tens, or units, etc.) solely by its *position* in the number representation. Without the all-important zero we should not know whether 451 meant 4M5C1X, 4M5X1, or several other possibilities, but with it we can specify our meaning exactly. For example, when we write 4510 we know immediately that the meaning is 4M5C1X, so that the symbols for the groups are now entirely superfluous and can be removed. The importance of this is that now any number, *no matter how large,* can be written in its entirety with ten or fewer symbols. This is an enormous advance and , with a little effort, we can write numbers larger even than the number of grains of sand in the world, and only have to remember the ten numerals 0,1,2,3,4,5,6,7,8,9.

The development of the concept of zero, and its use in positional number systems, is attributed to the Hindus some twelve or thirteen centuries ago. The actual numerals which we use are commonly referred to as arabic numerals although their origin and development are not precisely known. The advantages of the positional system over the earlier counting methods are so great that it has become the closest

thing which the world has to a universal language. This being the case, it is perhaps worth our while to examine it a little more closely.

The groups which we use are units, tens, hundreds, thousands, and so on, and can be conveniently written in a kind of shorthand notation by putting ten equal to 10^1, one hundred equal to 10^2, one thousand equal to 10^3, etc., where the number above and to the right of the ten is called a *power* (or an *exponent*) and indicates the number of zeroes coming after the one when the number is written out in full. This power or exponent can also be thought of as the number of tens which multiply together to give the larger number in question. With this terminology it is apparent that we can now easily write down extremely large numbers without wasting much ink. Moreover it also becomes clear that what we really understand by the number 14,658, for example, is one lot of ten thousands, four lots of one thousand, six lots of one hundred, five tens, and eight units, all added together or, in symbols

$$1\times10^4 + 4\times10^3 + 6\times10^2 + 5\times10^1 + 8.$$

More generally, for a number which contains (n+1) digits, we write

$$a_n \ldots\ldots a_2 a_1 a_0,$$

where each subscripted digit a is a numeral and can take a value between 0 and 9, and we understand it to mean

$$a_n\times10^n + \cdots + a_2\times10^2 + a_1\times10 + a_0.$$

It is now a very simple step from here to be able to write numbers and to count in bases (or groups) other than ten. For instance, if instead of 10 we wish to count in groups of 5, then the number $a_n \cdots a_2 a_1 a_0$ now means

$$a_n\times5^n + \cdots + a_2\times5^2 + a_1\times5 + a_0,$$

but where each subscripted digit a can now take only one of the five values 0,1,2,3,4.

If the human race had evolved with only one five-fingered hand rather than two, then among the host of other inconveniences there might have appeared a counting system in groups of five such as that referred to above. To this race of one-handed people the number 14,658, for example, which seems so ordinary to us, would make no sense at all. To them it would look something like the number 3?7%2 appears to us. We should say that the symbols ? and % are not numerals and therefore don't mean anything in the context of

numbers; they would say that the symbols 6, 5, and 8 are just as meaningless. Nevertheless, they are able to count just as well with their base-5, or 'quinary', system as we can with our decimal one. For the number of marks

* * * * * * * *
* * * * * * * *

they would write 31, understanding it as three times the base (that is five) plus one. We, on the other hand, write this same number as 16, understanding it as one times the base (that is ten) plus six. Note that the system used by the 'quinary people' has no separate symbol for five. This is their base and they would write it as 10 and, let us suppose, call it ten as we do. Pointing to each of the stars above in turn they would count as follows:

1, 2, 3, 4,10,11,12,13,
14,20,21,22,23,24,30,31.

If you use the fingers of one hand to help, and count out loud, one, two, three, four, ten, eleven, twelve, thirteen, fourteen, twenty, and so on, the new system soon becomes familiar at least for smaller numbers.

Thus, having fewer numerals than ten with which to count is no great incovenience. In fact, at first sight it might appear to be an asset, since it requires us to remember fewer numerals. Let us take this procedure of reducing the number of numerals to its limit to investigate the ultimate in supposed counting efficiency. The smallest number of numerals which can be used to make up a counting system is two. This is the *binary* system, and for it we need only two different symbols, a zero 0 and one other, say 1. That certainly seems simple enough. How would the counting go? Since there is no separate symbol for two, this would be our 10 and counting would start from 1 as follows: 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100,1101, 1110, 1111, 10000,... in place of the decimal counting scheme: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, ..., and right away we can see a problem developing. The length of these base-two, or 'binary', numbers is increasing much faster than their decimal equivalents. Indeed, the binary equivalent of what we normally think of as one thousand is already quite formidable at 1,111,101,000, although it can be readily understood by interpreting it in the form

$$1\times2^9 + 1\times2^8 + 1\times2^7 + 1\times2^6 + 1\times2^5 + 1\times2^3$$

$$= 512 + 256 + 128 + 64 + 32 + 8 = 1{,}000.$$

For everyday purposes this rapid increase in the number of digits obviously leads to complexities which greatly outweigh the convenience of only having to remember two symbols 0 and 1. What, for example, should we call this number 1,111,101,000 if we wished to speak about it? Presumably it would be one billion, one hundred and eleven million, one hundred and one thousand; hardly a simplification over its decimal equivalent of 'one thousand'. At the other extreme we might think of trying a very large base such as one hundred. In this system the decimal number 'one hundred' would be our new 'ten'. The drawback, of course, is the fact that we should need to know and recognize no less than one hundred different symbols, which would be required for the numerals. It seems clear that for greatest efficiency, at least in human society, some compromise is desirable between the two conflicting conveniences of having few numerals (or symbols) and having short numbers. Looked at from this point of view, the decimal system with its base of ten does not seem to be too bad a choice. There are those who think that a duodecimal system, with a base of twelve, would be better, since the 'duodecimal 10' (that is twelve) would be exactly divisible by one, two, three, four, and six, whereas the 'decimal 10' is only exactly divisible by one, two, and five. However, since society is hardly likely to make such drastic changes at this late date, we can feel fortunate that the counting system literally *hand*ed down to us is, for our daily needs at least, close to one with optimum efficiency.

Before we leave this little excursion which we have made into counting, it is fun to note that it is also possible to count in a system for which the base is a negative integer. Although no evidence exists that any civilization has ever done so, the scheme in fact does have some advantages. A counting system of this kind can include all the minus numbers $-1,-2,-3,-4,-5,\ldots$ in addition to all the plus ones without the need to distinguish between them by introducing a special sign $(-)$ to denote the numbers smaller than zero. There is nothing very special about how the new system works; it just follows the same rules that we set out for the positive based systems.

As an example we might consider counting to the base -10. What would we mean by the number 136 in this system? Well, following our earlier rules, which are general for any base, we must mean

$$1\times(-10)^2 + 3\times(-10) + 6$$

which, if we recall from our schooldays that a minus times a minus makes a plus, works out to be 100 − 30 + 6 or 76 in our regular decimal number language. What about the number 1360? Obviously this means

$$1\times(-10)^3 + 3\times(-10)^2 + 6\times(-10)$$

and works out to be −1000 + 300 −60, which is −760, in regular numbers. It follows that in the base −10 counting system the number written as 136 is a positive integer, while that written as 1360 is a negative one. How, you may ask, do the smallest counting numbers go in base −10? Well, counting up from one on our fingers, for example, would go like this:

1,2,3,4,5,6,7,8,9,190.

What is this one hundred an ninety which crops up so unexpectedly? It is simply ten in our new system as can easily be checked out:

$$190 = 1\times(-10)^2 + 9\times(-10) = 10.$$

Convinced of this it is now easy to check that, continuing to count on our toes, the next set of ten integers come out like

191,192,193,194,195,196,197,198,199,180.

But we could now count equally well starting from zero and going down the minus numbers. In our ordinary decimal system it is necessary to invent the new symbol '−' and proceed in the following manner:

−1,−2,−3,−4,−5,−6,−7,−8,−9,−10.

In the new system, however, the counting goes as follows;

19,18,17,16,15,14,13,12,11,10,29,28,27,....

as you may readily check out, and no new symbol is necessary at all.

The counting sequence in base −10 certainly looks a bit strange, but it is perfectly logical. It is true that there are some difficulties for the casual observer. How, for example, do you tell by looking at a base −10 number whether it is positive or negative? The answer is quite simple; it is positive if it contains an odd number of digits and negative

if it contains an even number of digits. There are also simple rules for telling which of two numbers is the larger - another point which looks a bit baffling to the beginner - so that the system suffers mainly from lack of familiarity rather than any other shortcoming. New rules have to be learned for adding, subtracting, multiplying, and dividing, but they exist and are quite simple, although I do not intend to confuse you further by going into more details.

The reader will perhaps now feel a sense of relief to learn that the rest of this book will concentrate on numbers written only in our familiar everyday decimal notation. Nevertheless, it is worthwhile to stress just one more time that the fundamental properties of numbers which make them so fascinating (such as their possible primeness, for example) are quite independent of the language in which we choose to express them. Indeed, whenever we have recourse to appeal to the all-powerful modern-day computer to help us in our efforts, we are using a system which works in a base-two notation. Since the computer utilizes electronic switches, which can be either on or off, it is ideally suited to counting in that 'binary' system which we found to be so cumbersome for humans. Translating an 'on' switch as 1 and an 'off' switch as 0 it can go searching for prime numbers, for example, with great speed and efficiency. Provided that it translates its findings back into our common decimal system before printing them out, its output is immediately understandable and the results are just as valid, although they have been entirely calculated in the binary world, as if some mathematical 'superman' had managed the task working throughout with ordinary numbers.

2. THE SEARCH FOR PRIME NUMBERS

Of all the numbers which the modern-day mathematician works with, the simplest to get a feel for are the 'counting numbers' 1,2,3,4,... . These are more formally referred to as the *natural* numbers, or the *integers*, and it is tempting to think that no scientific subject could possibly be simpler to study or to understand. Surprisingly, there is ample evidence to suggest that precisely the opposite is true. The 'theory of numbers' (meaning the natural numbers) is both one of the oldest and most challenging of sciences, abounding with tantalizing conjectures and unproven assertions to this day. It is perhaps the greatest of all challenges to the power of pure mathematical reasoning and the greatest treasury of mathematical truths.

Every integer can be broken down into constituent parts in a variety of ways such that, in a sense, each has a distinct personality. In this manner some groups of integers fall rather naturally into 'families' which have a particular characteristic in common. The best known family of all, and one which has maintained a fascination and mystery for mathematicians for well over 2,500 years, is the prime number family. Prime numbers are integers which can be divided exactly (that is without a remainder) only by themselves and by 1. Thus, the smallest ones are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

and they continue on to larger and larger values, becoming more and more tedious to calculate. It would be of enormous assistance in studying them if there were some sort of pattern in their appearance or if they had some outward sign to distinguish them from the rest. Unfortunately, if such a pattern exists or if such a sign be present, it has eluded discovery to this day. On the other hand this does not mean that a very great store of knowledge has not been accumulated over the centuries concerning what are colloquially referred to as 'the primes'.

One of the first questions which was asked by the early Greek mathematicians was 'do the prime numbers go on forever?' Since there are 15 primes between 1 and 50 (the number 1 itself is not normally counted as a prime) and only 10 primes between 50 and 100, it might appear that the primes become less densely distributed among the integers as we go to higher and higher values. A check of larger numbers seems to confirm this 'thinning out' (although the effect is

rather slow and irregular) so that it is then only natural to ask whether the prime numbers might eventually stop altogether. This question was asked and answered by the early Greeks themselves, and it was the great Euclid who first provided the answer in about 300 B.C. He argued in an impressively simple way as follows: suppose for the moment that they do stop. In this case there must then be some largest prime number of all. Let us call it N. Now consider the much larger number made up of all the prime numbers, up to and including N itself, multiplied together. This number looks like

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times \cdots \times N$$

and evidently is exactly divisible by every prime which exists - if the original conjecture is true. Now let us add 1 to this very large number to make a new number. This new number cannot be exactly divided by any of the original primes up to and including N since, from the way it is formed, division by any one of them will now always leave a remainder of 1. Therefore our new number, which is far larger that N, is either a new prime number itself or it is divisible by a new prime number larger than N. In either case we have established that there is a prime number larger than the one N which was assumed to be the largest . It follows that no such largest prime number can exist and that the primes therefore do go on, like the integers, for ever. Having understood this Euclidean proof, it is now of interest to ask whether numbers of the form

$$(2 \times 3 \times 5 \times 7 \times \cdots \times N) + 1$$

do usually turn out to be primes themselves, or whether they tend to be not prime but divisible by a prime number larger than N. For the smallest values of N, namely the first five primes $N = 2, 3, 5, 7, 11$, these numbers (which for the record are 3, 7, 31, 211, and 2311 respectively) are all prime. Surprisingly, thereafter these numbers are virtually all *composite* (which is the fancy word mathematicians use for those numbers which are not prime). In fact, the only other prime numbers of the above form for N less than 1000 occur when $N=31$ and $N=379$. Readers who are interested in recent computer investigations of these and related types of numbers can turn to Appendix 1 at the back of the book where further details are given.

Mathematicians have been searching for centuries for a simple method which would enable them to determine, without great effort, whether or not a particular number is prime. It is true that methods do exist, but none materially shortens the work of testing from basic first

principles, which implies checking the possible divisibility by all primes less than the square root of the number. Nevertheless, a general method does exist for listing all primes from the smallest without missing any. The procedure is extremely simple in principle, but unfortunately becomes unwieldy when the numbers get too large. It was first proposed about 250 B.C. by the Greek philosopher Eratosthenes and is usually referred to as the 'sieve of Eratosthenes'.

The method is so simple as to be almost obvious. It consists of writing down all the integers up to a predetermined limit of interest, and of eliminating all the numbers which are composite (or not prime). The sieve is started by knocking out all the even numbers (which are all divisible by the first prime number 2). Having done this, the smallest remaining number is the second prime 3. We now eliminate all the numbers divisible by 3 (which are called *multiples* of 3) from those which survived the first sifting operation. Five is now the first number remaining, so its multiples drop out next, then the multiples of 7, then of 11, and so on. If at each stage we note the number we are sifting by, and record it as a prime, we gradually build up a list of all the prime numbers from the smallest with none omitted. This basic principle is still used today in formulating programs for modern electronic computers in order to generate primes. The computers, of course, can go to very much larger numbers than Eratosthenes could manage, but only by virtue of their quickness of operation and not by any significant improvement in understanding the fundamental code which imbeds the primes throughout the number system.

It would be so much nicer if a formula could be derived to generate prime numbers; even if it wasn't able to give them all. Many suggestions have been forthcoming over the centuries, but none has been successful although some have come enticingly close, only to fail on closer inspection. Consider for example the simple formula

$$n^2 - n + 41,$$

in which n is to be put equal to the positive integers starting from 1. Trying n equal to 1, 2, 3, 4, ... , in turn reveals that this formula generates prime numbers all the way up to $n=40$. Alas, it fails for $n=41$. At this value the formula gives $41^2 - 41 + 41$, which is equal to the perfect square 41×41. The equally simple formula

$$n^2 - 79n + 1601$$

does even better. Once again putting n equal to 1, 2, 3, 4, ..., and so on, we find that it generates prime numbers all the way up to $n=79$

only to fail us at $n=80$.

If we learn anything from this experience, it is that the apparent success of a formula for a finite number of tries does not guarantee anything. We should really be looking for a general property of some kind, rather than grasping for straws. Unfortunately prime numbers are frustrating objects which seemingly grow like weeds, without any discernable pattern, in the boundless garden of natural numbers. We have listed all the prime numbers less than 1000 in Table 1 for you to examine in case, by chance, you should care to check things out for yourself!

TABLE 1

THE PRIME NUMBERS UP TO 1000

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

101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,
181,191,193,197,199

211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293

307,311,313,317,331,337,347,349,353,359,367,373,379,383,389,397

401,409,419,421,431,433,439,443,449,457,461,463,467,479,487,491,
499

503,509,521,523,541,547,557,563,569,571,577,587,593,599

601,607,613,617,619,631,641,643,647,653,659,661,673,677,683,691

701,709,719,727,733,739,743,751,757,761,769,773,787,797

809,811,821,823,827,829,839,853,857,859,863,877,881,883,887

907,911,919,929,937,941,947,953,967,971,977,983,991,997

But even if we know very little about the precise pattern in which the prime numbers occur, we do know something about algebraic expressions like those in the formulas above. Expressions of this type, which are made up of terms in n, n^2, (and possibly higher powers of n) plus a number, are termed *polynomials* by the mathematicians. A bit of thought on our part can easily establish that these types of formulas

can never succeed in giving only primes. Thus, if we write a general polynomial in the form

$$a + b \times n + c \times n^2 + d \times n^3 + \ldots,$$

where a, b, c, and d, are integers, it is clear that when $n=a$, every term in the expression is exactly divisible by a so that the entire polynomial, which is the *sum* (that is addition) of these terms, must also be exactly divisible by a. This formula can therefore never generate a prime when n is equal to a no matter what we choose for b, c, d, etc., or how many terms we decide to put into it. We now see, without doing any calculation, that the first formula

$$n^2 - n + 41$$

used earlier was bound to fail when n reached 41, while the second formula

$$n^2 - 79n + 1601$$

was also bound to fail eventually when $n=1601$ (for a now well-understood reason) even if it had not succumbed at $n=80$ through sheer misfortune.

It follows that mathematics, although not providing us with the secret of the primes so far, does at least tell us where *not* to look for a suitable formula, and thereby does save us a lot of futile stumbling down useless pathways. All mathematical expressions are not polynomials, of course, so that there is still plenty of room for speculation. For example, one might notice a simple numeral pattern in the appearance of particular prime numbers themselves, and hope that this pattern will always generate prime numbers. Such an assertion may be extremely difficult to prove but, if it is not true, a little testing of some of the predicted numbers may soon spell out its demise. This, unfortunately, seems to be the common fate of such efforts to date. An example or two may shed light on this approach. One might notice from a table of prime numbers that 31 is prime, and that so also are 331, 3331, and 33331. This seems to be a promising beginning; is it perhaps a pattern which could give prime numbers indefinitely? There is certainly no known mathematical proof which says that this is impossible. The pattern has been pursued and does produce additional primes with 333,331, 3,333,331, and 33,333,331 but eventually, as always seems to be the case, it fails; this time at 333,333,331 which is exactly divisible by 17.

One further well documented effort in this search for a formula which always gives primes was made by the famous seventeenth century French mathematician Pierre de Fermat who proposed that the expression

$$2^{2^n} + 1$$

would only generate prime numbers when n was put equal to 1, 2, 3, 4, ... and so on. The first term in this formula means 2 raised to the power 2^n, and this number gets extremely large very quickly as we continue along the series n=5,6,7,8 etc. so that, until the dawn of the computer age, it was very tough to test any but the first few members of the series. Let us first consider the value of the exponent 2^n which is just n twos multiplied together. Starting from n=1 it goes like 2, 4, 8, 16, 32, etc. It follows that the predicted prime numbers, or Fermat 'primes' as they are commonly called, begin as

$$F_1 = 2^2 + 1 = 5$$

$$F_2 = 2^4 + 1 = 17$$

$$F_3 = 2^8 + 1 = 257$$

$$F_4 = 2^{16} + 1 = 65{,}537$$

$$F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297$$

and, as we can see, very rapidly become quite formidable. In Fermat's day it was known only that the first four were indeed primes, but whether that fifth one with ten digits (let alone the higher terms of the series) was also prime had not been determined. About a century after Fermat proposed this sequence of 'primes' (and we must remember that Fermat never claimed to have proved that they were so) the Swiss mathematician Leonhard Euler, about whom we shall be hearing much more, established that the fifth Fermat 'prime' F_5 was not a prime number at all but was equal to

$$6{,}700{,}417 \times 641.$$

In the normal course of events this would have ended all interest in these Fermat 'primes' but, surprisingly, they popped up again in an entirely different context in the early nineteenth century. In addition, with the arrival of the electronic computer in recent years, it has now become possible to check many of the larger Fermat numbers for primeness. Incredibly, not a single prime number in the Fermat series has yet been found larger than F_4 although scores have been tested. The present-day question has therefore been reversed from that