MAA Film Manual No. 1

MATHEMATICAL INDUCTION

by

LEON HENKIN
University of California, Berkeley

THE MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York

LITHOPRINTED IN THE UNITED STATES OF AMERICA BY
CUSHING - MALLOY, INC., ANN ARBOR, MICHIGAN, 1961

PREFACE

The Mathematical Association of America has for many years been interested in the use of films and television in the teaching of mathematics. For example, a session on instruction by television or films was a feature of the 1956 annual meeting, a demonstration lecture on closed circuit television was given at the 1957 summer meeting, and the June-July 1958 issue of the AMERICAN MATHEMATICAL MONTHLY (the official journal of the MAA) was devoted to the use of films and television in mathematics education.

Finally in 1958, a grant from the National Science Foundation enabled the Association's Committee on Production of Films to produce certain experimental films with accompanying manuals. Among the films produced by this Committee is "Mathematical Induction" (2 reels) by Professor Leon Henkin of the University of California, Berkeley. This booklet is written as a supplement to the film. It contains an approximation to the words spoken in the film, an appendix to amplify the treatment of the subject, and a number of problems.

TABLE OF CONTENTS

Part I

A. In mathematics we deal with many kinds of numbers. As schoolchildren we first learn about the whole numbers, then about fractions, later about negative numbers, and still later about the so-called "irrational" numbers, such as π and $\sqrt{2}$, and even "imaginary" numbers like $3i$, whose square is negative. As a matter of fact there are still *other* number systems which you may study if you pursue your work in mathematics. But the topic of mathematical induction, which we shall discuss today, concerns the simplest kind of numbers, the whole numbers (or positive integers), 1, 2, 3, etc.

If we look at the set of *all* positive integers there is one striking fact which distinguishes it sharply from the sets which we ordinarily encounter in the daily work of experience — namely, there are *infinitely many* elements in this set! The set of people in a room, the set of eggs in a market, even the set of leaves in a forest, are all finite sets. But the set of positive integers is infinite.

The way in which we can most readily see this difference is by imagining that we arrange the elements of each set in a line. If we deal with the people in a room, for example, we obtain a first, a second, ..., and finally a last person in the line. Similarly with the eggs in a market, say. But when we line up the positive integers — arranging them, for instance, in order of increasing size — we see that there is *no last number*! No matter how far down the line we go, we can always add 1 to the number we find there and obtain a new number which comes next in line.

Now the fact that there are infinitely many positive integers causes a special kind of problem for us mathematicians because of the fact that we are often interested in discovering things which are true of *all* positive integers. To understand the nature of this difficulty, let us contrast such a problem with that of showing that something is true of all people in this room.

Suppose, for example, that we are interested in some property of people, such as the property of *being more than 5 feet tall.* And suppose we wish to determine whether every person in this room has this property. One way in which we could proceed would be to line up all of the people in the room and then to go down the line measuring each one. If we come to a person measuring 5 feet or less, then we would know that *not* every person in the room has the specified property. On the other hand, if we come to the end of the line *without* having found a person measuring 5 feet or less, then we would know that indeed every person in the room *does* have this property. Notice how important it is for this procedure that we *finally come to the end of the line.*

By contrast, suppose we are interested in some property of the positive integers — say the property of *being equal to a sum of 4 or fewer squares of positive integers.* And suppose we wish to determine whether *every* positive integer has this property. Again, we could proceed by lining up all of the positive integers — in fact, these numbers come to us already lined up in a "natural" order, 1,2,3,4, ... — and then we could go down the line testing each one to see whether it has the property of being equal to a sum of 4 or fewer squares. Let us actually begin this test:

$$\begin{aligned}
1 &= 1^2 & 9 &= 3^2 \\
2 &= 1^2 + 1^2 & 10 &= 3^2 + 1^2 \\
3 &= 1^2 + 1^2 + 1^2 & 11 &= 3^2 + 1^2 + 1^2 \\
4 &= 2^2 & 12 &= 2^2 + 2^2 + 2^2 \\
5 &= 2^2 + 1^2 & 13 &= 3^2 + 2^2 \\
6 &= 2^2 + 1^2 + 1^2 & 14 &= 3^2 + 2^2 + 1^2 \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 & 15 &= 3^2 + 2^2 + 1^2 + 1^2 \\
8 &= 2^2 + 2^2 & 16 &= 4^2
\end{aligned}$$

So far, we see that each number tested has the desired property. *If* we should come, presently, to a number which is *not* equal to a sum of 4 or fewer squares of whole numbers, then we would say that *not* every positive integer has the specified property. This is entirely comparable to our procedure in measuring the people in the room. But suppose that each time we test a number we find that it *is* a sum of 4 or fewer squares of whole numbers. What then?

In our previous example, where we measured people, we were able to reach a conclusion about *every* person in the room *when we got to the end of the line*. But in the present case of positive integers, we know that *the line has no end*. That is, *there is no last number*. Thus it could happen that we test numbers one after another for 40 days and 40 nights — or for 40 centuries, for that matter, if we enlist the cooperation of our descendants — and it could turn out that each number tested is equal to a sum of 4 or fewer squares of whole numbers; and yet we could not conclude that *every* number has this property.

Because the line-them-up-and-test-each-one method will not work when we are seeking to establish some general proposition about all positive integers, the mathematician has had to develop other methods to handle such problems. And of these, perhaps the most fundamental is based upon mathematical induction. Before we explain this, however, we ought perhaps to settle in your mind the question we have raised above about sums of squares.

As a matter of fact, every positive integer *does* have the property of being equal to a sum of 4 or fewer squares of whole numbers. The question was considered by the early Greek mathematicians, and challenged many other well known mathematicians down through the centuries. A proof was finally given by the French mathematician Lagrange, in 1772. The proof is too long and complicated for us to give it here, but those of you who go on to study that branch of mathematics called the *theory of numbers* will see the proof, and you will find that mathematical induction plays an important role in it.

* * * * *

B. Well, we have mentioned mathematical induction quite a few times by now — we had better say exactly what it is. The modern mathematician prefers to formulate it as a proposition about *sets* of positive integers. We have already encountered one such set, namely, the set (let us call it N) of *all* the positive integers, $\{1,2,3,\ldots\}$. It is easy to make up other such sets. For example, we could consider the set N′ of all *even* positive integers, $\{2,4,6,8,\ldots\}$, or the set N″ of all positive integers *greater than 5*, $\{6,7,8,9,\ldots\}$, both of which are *infinite* sets (having no last elements); or we could consider the set M of all positive integers *less than 16*, $\{1,2,3,\ldots,14,15\}$, or the set M′ consisting of *just the numbers 3, 22, and 185*, $\{3,22,185\}$, both of which are finite sets.

Among all possible sets of numbers we shall be especially concerned with those which have the following property: *if we pick any number from the set, and add 1 to it, the resulting number is also in the set.* In other words: *Whenever a number n is in the set, then n + 1 is in the set.* The mathematician says that such a set is *closed under the addition of 1*. In order to have a shorter term, we shall call such a set *inductive*.

Let us examine the sets N, N′, N″, M, and M′ considered above, to see which ones are inductive. Certainly N is, because if we pick any positive integer and add 1 to it the result is again a positive integer. Equally certainly N′ is *not* inductive, because if we pick one of its elements (an even number) and add 1 to it we get an odd number — which is *not* one of the elements in N′. The set N″ is inductive, because if we pick a positive integer greater than 5 and add 1 to it, the resulting number, being even greater than the first one, must surely be greater than 5 (and hence will be in N″).

Coming to our two examples of finite sets, we might say that the set M is *almost* inductive. For if we happen to pick the number 4 from M, say, — or if we pick 7, or 12, or any of the elements of M *except 15* — and add 1 to it, the resulting number is also in M. But M is *not inductive*, because if we pick 15 from it and add 1, the resulting number, 16, is not in M. And for a set to be inductive, it must be true that *no matter which* number we pick from it, when we add 1 the resulting number is in the set... The set M′, of course, is obviously not inductive. Actually, it can be shown that *no* finite set can be inductive.

In terms of the concept of an inductive set we can give a concise formulation of the principle of

Mathematical Induction. If G is any set of positive integers, and if we find that

(i) The number 1 is in G, and
(ii) G is inductive,

then: Every positive integer must be in G.

Well, there you have a statement of mathematical induction. But in order to appreciate its meaning it is necessary to discuss two questions which naturally occur in connection with this assertion. First, how do we know it is true? How do we know that *every* set of positive integers which satisfies the hypotheses (i) and (ii) will contain every positive integer? And second, even if it is true, why are we concerned with such a remote-sounding proposition? What can we do with it?

* * * * *

C. Let us begin by tackling the first of these questions. Suppose, then, that some one hands us a set G of positive integers and we find somehow that

(i) The number 1 is in G, and
(ii) G is inductive.

How can we convince ourselves that *every* positive integer must be in G?

We may begin reasoning as follows. We know, of course, that the number 1 is in G, because this is our hypothesis (i). But we can also show that 2 must be in G. For let us pick the number 1, which we already know to be in G, and add 1 to it. Since, by (ii), G is inductive, we see that the resulting number, 2, must also be in G — for this is what the word "inductive" means!

Now that 2 is known to be in G we may pick it, add 1 to it, and thus (by another application of hypothesis (ii)) we can conclude that 3 is in G. And then, by repeating this procedure, we can establish that 4 is in G. Clearly, continuing in this way, we can show in turn that each positive integer is in G.

I think this is quite a convincing argument, and most people will be persuaded by it that the statement of mathematical induction is indeed correct. And yet, by the standards of logical rigor which prevail in modern mathematics, we cannot accept this argument as constituting a really satisfactory proof of mathematical induction. Can you see what the difficulty is?

The trouble, of course, is in the last line of the stated argument. We have certainly showed in full detail that, under the assumption that G is a set satisfying (i) and (ii), the numbers 1, 2, and 3 must be in G. But then we end up by appealing to the good nature of the reader: "You see, don't you," we say to him, "how I can then proceed to show that *every* positive integer is in G?" If he hesitates we might add "*Surely* you see *that*?" with the intention of suggesting that he would be rather stupid if he did not! And yet, he has a perfect right to doubt. For when we state that "we can show in turn that each positive integer is in G" he can justifiably reply: "You say you can show this — all right, do so!" This response, I think, makes clear the shortcomings of the alleged demonstration.

I want to return to the question of a precise proof of mathematical induction at a later point. But for the moment, let me suppose that our intuitive argument has at least convinced you that this proposition is likely to be true, and let us pass to the second of the questions raised above, inquiring how, if we assume the correctness of mathematical induction, we can use this proposition to establish general statements about all positive integers.

* * * * *

D. The first example I should like to consider concerns the notion of divisibility. We say that a positive integer a is *divisible* by another such number, b if the result of dividing b into a leaves no remainder; that is, if $\frac{a}{b}$ is itself some positive integer, say q. An equivalent way of expressing this is to state that a is divisible by b just in case $a = b \cdot q$ for some positive integer q. Thus, for example, 12 is divisible by 2, or by 3, or by 12, but not by 5 or by 9.

Now the fact which I wish to demonstrate for you is this: If I raise 5 to the power $2k$—where k is any positive integer—and subtract 1, the result will be divisible by 24. In other words, I assert the following general statement about positive integers:

For every positive integer k,

(*) $$5^{2k} - 1$$

is divisible by 24.

Certainly this is not obvious, so let us begin by checking the assertion for a few values of k.

For $k = 1$, $5^{2k} - 1 = 5^2 - 1 = 25 - 1 = 24$, and certainly there is no doubt that *that* is divisible by 24.

For $k = 2$ we find $5^{2k} - 1 = 5^4 - 1 = 625 - 1 = 624$. Since it happens that $624 = 26 \times 24$, we see that $5^{2k} - 1$ is indeed divisible by 24 when $k = 2$. But already the arithmetic involved in testing special values of k is beginning to get difficult. In any case, because of the infinitude of positive integers, we know that a general statement about them can never be established by testing the integers one at a time. So let us see how we can employ mathematical induction to demonstrate our assertion.

Since mathematical induction is a proposition about *sets* of positive integers, we begin any application of this proposition by selecting a particular set of positive integers which is appropriate to our problem. In the case of our assertion (*), it is natural to consider *the set G of those positive integers k for which $5^{2k} - 1$ is, in fact, divisible by 24.*

Once the set G has been chosen in this way, we see that our previous observations, to the effect that $5^{2 \times 1} - 1$ and $5^{2 \times 2} - 1$ are divisible by 24, can be expressed by saying that *the numbers 1 and 2 are in the set G.*

The next thing we shall show about the set G is that *it is inductive*. What will this accomplish? Well, knowing that (i) the number 1 is in this set G, and (ii) this set G is inductive, we see by reference to the statement of mathematical induction, that we can apply that proposition to conclude that *every positive integer is in this set G.* But according to the way in which we defined G, we put into G *only those numbers k* for which $5^{2k} - 1$ is divisible by 24. Hence we will have established that $5^{2k} - 1$ is divisible by 24 *for every positive integer k,* and this is precisely our assertion (*).

Thus a complete demonstration of (*) will be at hand if we can show that our set G is inductive. To do this, we begin by picking any number from G —let us call it j — and then we wish to demonstrate that if we add 1 to it the resulting number, $j + 1$, must also be in the set G.

Now since j was picked from G, we know that $5^{2j} - 1$ must be divisible by 24. That is, there is a positive integer q such that

$$5^{2j} - 1 = 24q \,,$$

so that

(1) $$5^{2j} = 24q + 1 \,.$$

Let us use this equation to obtain a value for $5^{2(j+1)}$. We find that

$$\begin{aligned} 5^{2(j+1)} &= 5^{2j+2} \\ &= 5^{2j} \cdot 5^2 \\ &= (24q + 1)(25) \text{ by equation (1)} \\ &= (24q \cdot 25) + 25 \,. \end{aligned}$$

Subtracting 1 from both sides of the resulting equation we see that

$$\begin{aligned} 5^{2(j+1)} - 1 &= (24q \cdot 25) + 24 \\ &= 24 \cdot (q \cdot 25 + 1) \,, \end{aligned}$$

and this shows that

$$5^{2(j+1)} - \textit{1 is divisible by 24.}$$

Since the set G contains *those* numbers k for which $5^{2k} - 1$ is divisible by 24, we see that we have established that *the number* $j + 1$ *is in the set* G.

But what was j to begin with? Looking back we see that j *was any number picked from* G. Thus we have shown that no matter what number we pick from G, when we add 1 to it the resulting number is also in G. That is, we have shown that G is inductive. And as we have seen before, this allows us to apply mathematical induction to obtain a proof of our general statement (*).

Well, that is about all we have time for in this first lecture. We have observed the infinitude of positive integers and the difficulty which this poses when we seek to establish a general statement about *all* positive integers; we have discussed a certain kind of set of positive integers called inductive, and have seen how to formulate mathematical induction in terms of inductive sets; we have seen an intuitive argument sketched which purports to establish the truth of mathematical induction, but have observed the shortcomings of this argument; and finally, we have seen an application of mathematical induction to establish a general statement about divisibility of positive integers. In our next lecture I would like to illustrate the possibilities of applying mathematical induction by an illustration of another kind, and then I want to return to the problem of giving a rigorous demonstration of this proposition.

Part II

A. In the previous lecture we formulated the principle of mathematical induction as a statement about sets of positive integers. You recall that a set G of positive integers is called *inductive* if, whenever we pick an element from G and add 1 to it, the resulting number is also in G. And in terms of this notion our statement of *mathematical induction* is as follows.

If G is any set of positive integers concerning which we find that:

(i) The number 1 is in G, and
(ii) G is inductive,

then every positive integer must be in this set G.

I want to begin this lecture by indicating an application of mathematical induction to a problem of addition; and I should like to introduce this problem by relating a little story.

In the year 1787, about the time that our American constitution was being formed, a ten year old boy named Karl Friedrich Gauss was attending a small school in his native country, Germany. One day, to keep the pupils busy while doing some work of his own, the schoolmaster assigned to his class the problem of adding all of the positive integers from 1 through 100. In those days schoolboys did not have paper, but each one carried a small slate and some chalk with which to do his writing; so the problem of adding together many numbers involved a good deal of writing and erasing, and the teacher was fairly confident that his students would be kept busy for a good hour or so with this task.

Much to the teacher's surprise, young Gauss brought up his slate after only a minute or two, and as was the custom, he laid it on the teacher's desk. On his slate he had written his answer to the problem: 5050. When, at the end of an hour, the other students had brought up their slates, the teacher found that only Gauss had obtained the correct solution. This incident so impressed him that he began to take a special interest in his star pupil, buying mathematical books for the young boy with his own money. Before Gauss was out of his 'teens he had made some remarkable mathematical discoveries; within a few years he was generally recognized as Europe's leading mathematician; and today many mathematicians consider him to be among the three or four greatest mathematicians of all times.

Now let us see how it is possible to obtain the sum of all of the numbers from 1 to 100 without actually carrying out the laborious additions. Actually, there is a very simple method which works equally well to give the sum of all numbers from 1 through k, where k may be *any* positive integer.

Let us use the symbol A_k for this sum; that is, we let

(1) $$A_k = 1 + 2 + 3 + \ldots + (k-1) + k ,$$

Clearly if the same numbers are added in reverse order the result will be the same. That is, we also have

(2) $$A_k = k + (k-1) + (k-2) + \ldots + 2 + 1 ,$$

Now let us combine equation (1) and (2) by addition. On the left side of the resulting equation we get, of course, $A_k + A_k$. On the right side let us carry out the addition by first forming the sum of the first terms of equations (1) and (2), then adding in the sum of the second terms of equations (1) and (2), etc. The result is:

(3) $A_k + A_k = [1 + k] + [2 + (k-1)] + [3 + (k-2)] + \ldots + [(k-1) + 2] + [k + 1].$

Clearly each term in brackets has the value $k + 1$, and altogether there are k such terms. Hence we get

(4) $$2A_k = k \cdot (k+1),$$

so that

(5) $$A_k = \frac{k \cdot (k+1)}{2}.$$

If, now, we take the case $k = 100$, we see by equation (5) that A_{100} (which is $1 + 2 + 3 + \ldots + 99 + 100$) has the value $\frac{100 \cdot (101)}{2} = 50 \cdot (101) = 5050$ — which was exactly the answer given by Gauss.

It is also possible to establish that equation (5) holds for every positive integer k by mathematical induction, but instead of showing this we will illustrate its use in solving a closely related problem. Namely, instead of asking for the sum of the first k positive integers, suppose we see if we can find the sum of their cubes.

Let us introduce the symbol C_k for this sum. That is, we set

$$C_k = 1^3 + 2^3 + 3^3 + \ldots + (k-1)^3 + k^3,$$

where k may be *any* positive integer. And we seek a formula which will permit us to evaluate C_k without having to carry out all of the k additions which are indicated in its definition. How shall we begin to look for such a formula?

Let us begin by constructing a table showing, for each whole number k from 1 up to 6, what the value of the sum of the first k cubes is. Our table will look like this:

k	k^3	C_k = sum of first k cubes
1	1	1
2	8	9
3	27	36
4	64	100
5	125	225
6	216	441

Here the entry 36 in the last column, for example, is obtained by adding the entries 1, 8 and 27 from the second column.

Now — do you notice anything special about the numbers in the last column? I'm sure that everyone will recognize that the first four entries are *squares of whole numbers*. Probably most of you will recognize that the fifth entry, 225, is also a square. Some of you may even realize that the last entry, 441, is a square too — it is the square of 21.

Well, do you suppose that if we continued the construction of our table beyond six lines we would continue to get squares in the third column? If $k \leq 6$ we have seen that C_k is a square; in particular, $C_1 = 1^2$, $C_2 = 3^2$, $C_3 = 6^2$, $C_4 = 10^2$, $C_5 = 15^2$, $C_6 = 21^2$. In order to try to find a formula which would express $\sqrt{C_k}$ in terms of k let us provide a fourth column for our table in which we enter the square roots of the entries in the third column.

k	k^3	C_k = sum of first k cubes	$\sqrt{C_k}$
1	1	1	1
2	8	9	3
3	27	36	6
4	64	100	10
5	125	225	15
6	216	441	21

Do you notice any regularity among the numbers of the last column? Let us look at the differences between successive entries of that column:

$\sqrt{C_k}$	Difference
1	
	2
3	
	3
6	
	4
10	
	5
15	
	6
21	

Well, there certainly is a regularity! From these differences it appears that we can express each of the numbers in the column $\sqrt{C_k}$ as a sum:

$$
\begin{array}{rl}
\multicolumn{2}{c}{\sqrt{C_k}} \\
\hline
1 & \\
3 & = 1 + 2 \\
6 & = (1+2) + 3 \\
10 & = (1+2+3) + 4 \\
15 & = (1+2+3+4) + 5 \\
21 & = (1+2+3+4+5) + 6
\end{array}
$$

In other words, at least for the six lines of our table, we find that $\sqrt{C_k}$ is A_k, the sum of the first k positive integers! Since we already know that $A_k = \frac{k \cdot (k+1)}{2}$ for every positive integer , we can say that at least for $k \leq 6$, we have $C_k = [\frac{k \cdot (k+1)}{2}]^2$. And it is natural to wonder whether this formula holds for *every* whole number k. We shall use mathematical induction to show that the answer is affirmative.

To this end we form a set G of whole numbers by putting into G just *those* number k for which it is true that $C_k = [\frac{k \cdot (k+1)}{2}]^2$. At the moment we know (from our table) that the numbers 1, 2, 3, 4, 5, and 6 are in this set G. And our question is equivalent to asking whether *every* positive integer is in G.

Now let us pick *any* number from G—call it j. Since j was picked from G, we know that $C_j = [\frac{j \cdot (j+1)}{2}]^2$. What can we say about C_{j+1}? Well, since C_j is the sum of the first j cubes, $C_j = 1^3 + 2^3 + \ldots + (j-1)^3 + j^3$, and since C_{j+1} is the sum of the first $j + 1$ cubes, $C_{j+1} = 1^3 + 2^3 + \ldots + (j-1)^3 + j^3 + (j+1)^3$. Clearly we have $C_{j+1} = C_j + (j+1)^3$, so that

$$C_{j+1} = [\frac{j \cdot (j+1)}{2}]^2 + (j+1)^3$$

$$= (j+1)^2 [\frac{j^2}{4} + (j+1)] = (j+1)^2 [\frac{j^2 + 4j + 4}{4}]$$

$$= (j+1)^2 [\frac{(j+2)^2}{4}] = [\frac{(j+1)(j+2)}{2}]^2 .$$

Recalling that we put into G those numbers k for which $C_k = [\frac{k \cdot (k+1)}{2}]^2$, we see that the formula $C_{j+1} = [\frac{(j+1)(j+2)}{2}]^2$, which has just been derived, guarantees that $j + 1$ is in G. But what was j to begin with? It was a number selected in an *arbitrary* way from G! That is, we have shown that whenever a positive integer j is in G, then also $j + 1$ will be in G. In other words, we have established that our set G is inductive.

Since we have previously observed that the number 1 is in G, this new observation allows us to apply the principle of mathematical induction immediately to conclude that *every positive integer is in G*. That is, for *every* positive integer k we have $C_k = [\frac{k \cdot (k+1)}{2}]^2$. Thus we have established a formula which enables us quickly to find the sum of the first k cubes — where k is *any* positive integer. In particular, we have found that this sum is equal to the square of the sum of the first k positive integers. Using the answer supplied by Gauss to his teacher's problem we can thus say that the sum of the first 100 cubes is $(5050)^2 = 25,502,500$.

* * * * *

B. I think we will not have time for further applications of mathematical induction, and I wish now to return to the question of the validity of this principle. You recall that in the previous lecture we gave an argument to indicate in an intuitive way that the statement of mathematical induction expresses a true fact about sets of positive integers; but we indicated that this argument could not be considered as a satisfactory proof because, after showing in detail that the numbers 1, 2, and 3 were in a set G, the argument ended with words like, "Well, you can see that in the same way we *could* show that every positive integer is in G."

Let us start again, now, with an arbitrary set G of positive integers concerning which we suppose that (i) the number 1 is in G, and (ii) G is inductive, and let us see if we can produce a really sound proof that *every* positive integer must be in G.

This time we will base our argument upon a logical device known as *proof by contradiction*. That is, we begin by *assuming* that in fact there *are* positive integers which are *not* in G, and we shall show that this assumption leads to a contradiction — and hence that it must be rejected.

Since we are assuming that there are positive integers which are not in G, let us choose the smallest of these and call it q. Of course $q \neq 1$, since q is not in G while 1 is in G (by hypothesis (i)). Because q is a positive integer different from 1, there must be another positive integer, say p, which comes just before q, so that $p + 1 = q$. Of course this means that p is smaller than q; and since q was the smallest of the numbers which are *not* in G, it follows that *p is* in G.

Now let us use our hypothesis (ii), to the effect that G is inductive. Let us pick the number p which we have just shown to be in G, and add 1 to it. Since G is inductive the resulting number, $p + 1$, must also be in G. But $p + 1 = q$. *So q is in G*.

On the other hand, *we picked q to be the smallest of the positive integers which are not in G*. So we have, indeed, arrived at a contradiction. Since this contradiction arose from our assumption that there are positive integers which are *not* in G, the assumption must be incorrect. After all, there are *no* positive integers which are not in G. In other words, ***every positive integer is in G.*** **And this concludes our proof of mathematical induction.**

Certainly this argument differs in character from the earlier one we gave, because it does not end by stating that we could do something which in fact we do not do. And yet, if we look carefully at the new argument, we may also begin to have doubts about certain of its points. For example, even if we assume that there are positive integers which are not in G, how do we know that there is a *smallest* one among them? After all, in the set of all odd positive integers, for example, we know there is no *largest* number; perhaps this other set, which enters into our proof, has no *smallest* number?

The question of what constitutes a fully satisfactory proof is a subtle one, and has itself been made the subject of extended mathematical investigation. But perhaps we can try to indicate in a few words here the principal form of solution which has been evolved by modern mathematicians.

In any proof whatever, we arrive at a conclusion by starting from certain statements which are taken for granted, and proceeding according to certain rules or laws of logic. Of course the statements taken for granted in a given proof may be called into question, and we may seek to give proofs for these. But these proofs in turn will start from other assumptions, and if we then obtain proofs of these, still other assumptions will be brought in. The frank recognition that any deductive theory must begin with *some* statements which we do *not* attempt to prove leads to the concept of an axiomatic theory.

I am sure you have all heard of the Greek mathematician Euclid, and of how he formulated an axiomatic theory of geometry. Not so well known is the fact that during the last eighty years or so, mathematicians have axiomatized many other parts of mathematics. In particular, an axiomatic theory of positive integers was first proposed by an Italian mathematician, Giuseppe Peano, in the last decade of the nineteenth century.

In Peano's theory the statement of mathematical induction was itself taken as an axiom, and so of course it makes no sense to ask for a proof of this statement in such a theory. On the other hand, later workers suggested a variety of other axiom systems for the theory of positive integers. Among the axioms which one often finds in these systems is the following statement (often referred to as a *well-ordering principle*): *If G is any set which contains one or more positive integers, then among all of the positive integers occurring in G there must be one which is smaller than each of the others.* In systems which include such an axiom, a proof of the principle of mathematical induction can be given along the lines of the proof sketched above. (On the other hand, in systems like that of Peano, where mathematical induction is taken as one of the axioms, the well-ordering principle can be proved as a theorem.)

* * * * *

C. This ends the mathematical content of my talk, but I should like to add a word concerning the significance of the principle of mathematical induction.

"Of what real good is this principle anyhow?" you may ask. Of course one answer is that it can be used to establish many general statements about positive integers, as you have seen in two detailed examples above. But perhaps you are not really interested in general statements about positive integers. You have heard that mathematics can be used to build bridges or guide rockets, and you may wonder if mathematical induction can be applied to problems in such domains.

As a matter of fact there are very few direct applications of mathematical induction to what we might call "engineering problems"; most of these arise in connection with computations in the elementary theory of probability. But in spite of this, mathematical induction is really of great importance to engineering, for it enters into the proofs of a great many of the most fundamental theorems in the branch of mathematics we call analysis — and these theorems are used over and over by engineers.

And yet, to me, the true significance of mathematical induction does not lie in its importance for practical applications. Rather I see it as a creation of man's intellect which symbolizes his ability to transcend the confines of his environment.

After all, wherever we go, wherever we look in our universe, we see only finite sets: The eggs in a market, the people in a room, the leaves in a forest, the stars in a galaxy — all of these are finite. But somehow man has been able to send his imagination soaring beyond anything he has ever seen, to create the concept of an infinite set. And mathematical induction is his most basic tool of discovery in this abstract and distant realm.

To me, this conception gives to mathematical study a sense of excitement. And I hope that some of you will carry your study of mathematics to the point where you too can experience the unique excitement which mathematics affords to its devoted students.

APPENDIX

I wish here to deal briefly with a few points closely related to the material of the talk, which could not be included in the talk itself for lack of time.

* * * * *

A. The fact that $5^{2k} - 1$ is divisible by 24 for every positive integer k is simply a special case of the fact that for *any* positive integers x, y, and k, if $x > y$ then $x^k - y^k$ is divisible by $x - y$; to see this, we have only to take $x = 5^2$ (i.e., $x = 25$), and $y = 1$. The more general law can be established by mathematical induction in quite the same way as we treated the special case; this is a very simple exercise which the reader should try.

It is natural to wonder whether there is a counterpart to the general law given above, stating that $x^k + y^k$ is divisible by $x + y$. However, it is easy to find examples of positive integers where this is not so. For example, if we take $x = 2$, $y = 1$, $k = 2$, it is evident that $2^2 + 1^2$, or 5, is not divisible by $2 + 1$, or 3. On the other hand, we can show that if x and y are any positive integers whatever, and if k is any *odd* positive integer, then indeed $x^k + y^k$ is divisible by $x + y$. And this, too, can be established by mathematical induction.

At first sight it may seem strange that mathematical induction, which is designed to prove general statements about *all* positive integers, is here used to prove a theorem which holds only for *some* positive integers, namely, the odd ones. However, it is a simple matter to formulate our result so that it has the form of a general statement: *For all positive integers x, y, and j, $x^{2j-1} + y^{2j-1}$ is divisible by* $x + y$. I think you will find the problem of proving this fact by mathematical induction a little more challenging than the previous exercise, but with a little work many of you should be able to carry it through.

* * * * *

B. Letting

$$A_k = 1 + 2 + 3 + \ldots + k,$$

and

$$C_k = 1^3 + 2^3 + 3^3 + \ldots + k^3$$

we have derived the formulas

$$A_k = \frac{k \cdot (k+1)}{2} \quad \text{and} \quad C_k = \left[\frac{k \cdot (k+1)}{2}\right]^2.$$

It is natural to wonder whether we can obtain a similar formula for

$$B_k = 1^2 + 2^2 + 3^2 + \ldots + k^2.$$

In particular, our expression for A_k can be written as a polynomial of degree 2, namely $\frac{1}{2}k^2 + \frac{1}{2}k$; and our expression for C_k is the polynomial $\frac{1}{4}k^4 + \frac{1}{2}k^3 + \frac{1}{4}k^2$ of degree 4.

Can we express B_k as a polynomial in k of degree 3? That is, can we find numbers $a_3, a_2, a_1\ a_0$ such that

$$(*) \qquad B_k = a_3 k^3 + a_2 k^2 + a_1 k + a_0$$

for all positive integers k? Of course, based upon our experience with A_k and C_k we have to expect the numbers a_3, a_2, a_1, a_0 to be rational numbers (fractions) rather than merely integers.

As we shall see, mathematical induction can be used not only to supply an affirmative reply to this question, but also to furnish specific values of a_3, a_2, a_1, and a_0.

To do this, let us seek to establish that the equation (*) holds for all positive integers k. How do we go about it? We begin by considering the set G of those positive integers k for which the equation (*) *does* hold. We then seek to show that (i) the number 1 is in this set G, and (ii) G is inductive. If we can do this, then we can apply mathematical induction to conclude that *every* positive integer k must be in the set G, and this will show that the equation (*) holds for every such k.

Now for the number 1 to be in the set G we must have $B_1 = a_3 1^3 + a_2 1^2 + a_1 1 + a_0$ according to our definition of G. On the other hand, B_1 is defined to be simply 1^2, or 1. Thus we see that condition

(i) The number 1 is in G

will be satisfied, *provided* the numbers a_3, a_2, a_1, and a_0 are selected so that

$$(\mathrm{I}) \qquad a_3 + a_2 + a_1 + a_0 = 1.$$

Now let us turn to condition (ii). We wish to show that G is inductive. For this purpose we begin by selecting an arbitrary number — call it j — from the set G, so that

$$(\mathrm{II}) \qquad B_j = a_3 j^3 + a_2 j^2 + a_1 j + a_0 .$$

And we would like to show that when we add 1 to this number the resulting number, $j + 1$, must also be in G. That is, we wish to show that

$$(\mathrm{III}) \qquad B_{j+1} = a_3 (j+1)^3 + a_2 (j+1)^2 + a_1 (j+1) + a_0 .$$

But since $B_j = 1^2 + 2^2 + \ldots + j^2$ and since $B_{j+1} = 1^2 + 2^2 + \ldots + (j+1)^2$ we see that

$$(\mathrm{IV}) \qquad B_{j+1} = B_j + (j+1)^2 .$$

By combining the equations (II), (III), and (IV), we see that the condition

(ii) G is inductive

will hold *providing* we can be sure that the numbers a_3, a_2, a_1, and a_0 are such that the equation

$$(\mathrm{V}) \qquad a_3(j+1)^3 + a_2(j+1)^2 + a_1(j+1) + a_0 = (a_3 j^3 + a_2 j^2 + a_1 j + a_0) + (j+1)^2$$

holds. By expanding each side of this equation and equating coefficients of like powers of j we reach the following conclusion: The condition

(ii) G is inductive

will hold, *providing* that the numbers a_3, a_2, a_1, and a_0 satisfy the system of equations

$$(\mathrm{VI}) \qquad \begin{cases} 3a_3 + a_2 = a_2 + 1 \\ 3a_3 + 2a_2 + a_1 = a_1 + 2 \\ a_3 + a_2 + a_1 + a_0 = a_0 + 1 . \end{cases}$$

Thus, to insure that *both* conditions (i) and (ii) holds, and hence (by mathematical induction) that equation (*) holds for all positive integers k, it is sufficient to choose the four numbers a_3, a_2, a_1, and a_0 so that the four equations (I) and (VI) are satisfied.

The rest is elementary algebra. Of course not every set of four equations in four unknowns has a solution; and in some cases there may be many solutions. But in the present case we quickly obtain a unique solution. Indeed the first equation of (VI) gives $a_3 = \frac{1}{3}$ immediately, and then using this in the next equation we get $a_2 = \frac{1}{2}$. Now combining the last equation of (VI) with equation (I) we get $a_0 = 0$; and finally, using these values of a_3, a_2, and a_0, we find from (I) that $a_1 = \frac{1}{6}$.

Thus we have found and established, by mathematical induction, that

$$1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{1}{3}k^3 + \frac{1}{2}k^2 + \frac{1}{6}k$$

for every positive integer k.

Of course no true mathematician will be willing to leave the subject at this point. We have found formulas for the sum of the first k positive integers, for the sum of the first k squares, and for the sum of the first k cubes . . . . What about higher powers?

It does not take much imagination to *guess*, on the basis of our experience so far, that if n is *any* positive integer, the sum of the first k nth powers can be expressed as a polynomial in k of degree $n + 1$. That is, if

$$Z_k = 1^n + 2^n + 3^n + \dots + k^n$$

we wish to ascertain whether there exist rational numbers $b_{n+1}, b_n, b_{n-1}, \dots, b_1, b_0$ such that $Z_n = b_{n+1}k^{n+1} + b_n k^n + \dots + b_1 k + b_0$ for all positive integers k.

That this is indeed so can be shown by means of mathematical induction, treating the problem along the lines shown above for the case $n = 2$. If you carry through the details you will find that the problem is reduced to showing that a certain set of $n + 2$ equations in the $n + 2$ letters $b_{n+1}, b_n, \dots, b_1, b_0$ has a solution, and the form of these equations will then permit a simple argument showing the existence of a unique solution. In order to set up this system of equations you will need to know that any term of the form $(j+1)^p$ can be expressed as a polynomial in j of degree p, with first and last coefficients equal to 1:

$$(j+1)^p = j^p + c_{p-1}j^{p-1} + c_{p-2}j^{p-2} + \dots + c_1 j + 1 .$$

Probably this is well known to you; but in any case it can easily be established itself by mathematical induction.

While to prove that the numbers $b_{n+1}, b_n, \dots, b_0$ can be obtained as solutions of a system of simultaneous linear equations is not too difficult, it is a somewhat harder problem to find explicit formulas for $b_{n+1}, \dots, b_0$ which will enable us to compute their numerical values in any specific case. In order to do so, it is first necessary to find explicit formulas for the numbers $c_{p-1}, \dots, c_1$ which enter into the formula for $(j+1)^p$. As it happens, however, the latter numbers (under the name *binomial coefficients*) have been very thoroughly studied by mathematicians, and the desired explicit formulas are known. In fact we have

$$c_i = \frac{p!}{i!\,(p-i)!} \quad \text{for any} \quad i = p-1,\ p-2, \dots, 1,$$

where in general the notation $q!$ stands for the product $q \cdot (q-1) \cdot (q-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$. To establish these formulas for the binomial coefficients one can again use mathematical induction; the reader who tries this will find it convenient to place the subscript p on those binomial coefficients which appear in the expansion of $(j+1)^p$.

* * * * *

C. In our talk we have spoken of an axiom system for the theory of positive integers, such as Peano's, in which the principle of mathematical induction is taken as one of the axioms. It may be of interest to see what a complete set of axioms of this kind looks like. Here is one involving only four axioms.

Axiom 1. For every positive integer x, we have $x + 1 \neq 1$.

Axiom 2. If x and y are any positive integers which are *distinct* (i.e., $x \neq y$), then also the numbers $x + 1 \neq y + 1$.

Axiom 3. For any positive integers x and y we have $(x + y) + 1 = x + (y + 1)$.

Axiom 4. *Mathematical Induction.*

On the basis of these four axioms all of the fundamental theorems of arithmetic can be established. Consider, for example, the associative law of addition, which states that for any positive integers x, y, and z we have $(x+y) + z = x + (y+z)$. In order to obtain a proof of this by mathematical induction (Axiom 4), we begin by picking *any* pair of positive integers, x and y, and we then form the set G of all *those* positive integers z for which in fact we *do* have $(x+y) + z = x + (y+z)$. We then proceed to show that (i) the number 1 is in G, and (ii) G is inductive — in both cases making use of Axiom 3. With (i) and (ii) established we apply Axiom 4 to conclude that *every* positive integer is in G and this gives the desired result.

The reader should carry through the details of this proof. And he may then attempt in a similar way to establish the commutative law of addition, which states that for any positive integers x and y we have $x + y = y + x$.

The full development of the theory of positive integers on the basis of Axioms 1 - 4 requires us to bring into the theory, by definition, such concepts as the relation *less than*, or the operation *multiplication*, which do not appear in the axioms themselves. The interested reader may discover how this can be done by consulting a book such as *Foundations of Analysis* by Edmund Landau, (Chelsea Publishing Company, New York, 1951).

* * * * *

D. In each of the applications of mathematical induction which we have so far considered our aim has been to establish some proposition which could be expressed by means of an *equation*. However, there is no necessary connection between equations and mathematical induction, and the latter can equally well be applied to establish propositions expressed by means of *inequations* (or *inequalities*, as they are often called). Below we illustrate this possibility.

Consider the first few successive powers of 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$. Clearly we have $2^k > k$ for $k = 1, 2, 3, 4$, and it seems quite likely that this inequation will continue to hold for larger values of k. Using mathematical induction it is a simple matter to give a rigorous proof that $2^k > k$ for *every* positive integer k. We simply form the set G of *those* numbers k for which we *do* have $2^k > k$; we already know that 1 (as well as 2, 3, and 4) are in G; and it remains only to show that G is inductive. To do this, we pick *any* number from G — call it j — so that we know $2^j > j$. Since $2^{j+1} = 2^j \cdot 2^1 = 2^j + 2^j$, we get $2^{j+1} = 2^j + 2^j > j + 2^j$; and since $2^j > 1$ this gives $2^{j+1} > j+1$. Thus $j+1$ is in G (as we see by reference to our definition of the set G); and since j was *any* number picked from G, the fact that we have shown $j+1$ to be in G demonstrates that G is inductive. As noted above, this enables us to conclude, by mathematical induction, that $2^k > k$ for *every* positive integer k.

Now let us look briefly at certain closely related inequalities. We shall discover an interesting extension of mathematical induction, as well as learn a fundamental fact about the rapidity with which the exponential function grows.

Instead of comparing values of 2^k with k itself, let us compare 2^k with k^2. A table for the first four values of k looks as follows.

k	2^k	k^2
1	2	1
2	4	4
3	8	9
4	16	16

The relation between 2^k and k^2 appears very different from that between 2^k and k: Whereas $2^k > k$ for *all* values of k, we find in our table that we have $2^k > k^2$ for one value of k, $2^k = k^2$ for two values of k, and $2^k < k^2$ for one value of k. There does not seem to be any general law here.

But let us continue the table a little further.

k	2^k	k^2
5	32	25
6	64	36
7	128	49
8	256	64

Well — in *this* part of the table we have $2^k > k^2$ for all four values of k listed! Furthermore, as we proceed down the table the difference between 2^k and k^2 increases, and this may serve to give us the feeling that in fact we will find $2^k > k^2$ for *all* values of $k \geq 5$. This is, in fact, correct. But how do we prove it?

"By mathematical induction," you will probably say. For after all, this *is* a paper on mathematical induction. And yet there is an obvious difficulty in applying mathematical induction — at least if we try to apply it in the obvious way. For if we form the set G consisting of *those* numbers k for which we *do* have $2^k > k^2$, we find that G is *not* inductive. This can be seen from our little table above which shows that 1 is in G but that 1+1 (i.e., 2) is *not* in G. Since G is not inductive, we cannot apply mathematical induction to it.

The difficulty here is that as we have defined our set G it contains numbers less than 5, and so involves the early part of the table of values of 2^k — which we have come to believe is exceptional. We might, therefore, consider instead of G the set H of *those numbers k which are greater than or equal to 5 and* for which we *do* have $2^k > k^2$; and we might reasonably hope to show that this set H is inductive. But then a new difficulty arises. For *we do not have 1 in this set H* — and hence we cannot apply mathematical induction to it.

There is a way of surmounting this difficulty. But rather than carry it out for our particular problem it will be worth our while to show that the same sort of difficulty can be overcome in a large number of cases. We do this by extending our fundamental law of mathematical induction.

EXTENDED PRINCIPLE OF MATHEMATICAL INDUCTION. *Suppose that p is a positive integer, and that H is any set of numbers concerning which we know that*

(i) *the number p is in H, and*
(ii) *H is inductive.*

Then we must have k in H for every positive integer $k \geq p$.

We may notice that the extended principle appears to be stronger than our original formulation of mathematical induction since we can obtain the latter as a special case of the extended principle by taking p to be 1. In spite of this we can *prove* the extended principle by *using* the original law — in the following way.

Suppose that p is a positive integer, and that H is a set which satisfies the hypothesis (i) and (ii) of the extended principle. We wish to show that for any positive integer $k \geq p$ we must have k in H.

To do this we form a new set of numbers, G, by taking as its elements all the numbers in H *as well as* all positive integers $< p$ (some of which may happen to be in H). Concerning this new set G we can show two things.

(a) *The number 1 is in G.* For if p is 1, then by (i) we have 1 in H and so also 1 is in G by construction. On the other hand if p is a positive integer other than 1, then of course we have $1 < p$ and so again 1 qualifies as an element of G — this time as one of the second kind of elements to be put into G.

(b) *The set G is inductive.* We see this by choosing *any* element from G -- call it j — and showing that the number $j+1$ must also be in G. If j happens to be in H, then — by hypothesis (ii) — $j+1$ will also be in H, and so $j+1$ will be one of the first kind of elements put into G. On the other hand if j is *not* in H, then (since j was chosen from G) it must be one of the second kind of elements put into G — that is, j must be a positive integer which is $< p$. Now if j happens to be just one less than p, that is, if $j = p-1$, then $j+1 = p$ and so $j+1$ is in H (by hypothesis (i)) and so $j+1$ is in G. But if j is more than one less than p, that is, if $j < p-1$, then $j+1 < p$ and so again $j+1$ qualifies as an element of G (this time one of the second kind). Thus in every case $j+1$ is shown to be in G, and this completes the demonstration that G is inductive.

Now combining (a) and (b) we conclude, by the original law of mathematical induction, that *every positive integer is in the set G.* By referring to our definition of the set G we see that this means that *every positive integer is either an element of H or else is* $< p$. But then if k is any positive integer $\geqq p$ we must have k in H. This is the desired conclusion of the extended principle — whose proof is thus completed.

Having established the extended principle of mathematical induction, let us seek to apply it to the problem we were considering. We are seeking to show that $2^k > k^2$ for every positive integer $k \geqq 5$. We have formed the set H consisting of all *those* positive integers k *which are* $\geqq 5$ *and* for which we *do* have $2^k > k^2$. We already know, from our table, that the number 5 is in this set H. If, now, we could show that H were inductive, then the extended principle would apply to assure us that *every* positive integer $\geqq 5$ is in H, and this would establish our proposition.

So let us seek to show that H is inductive. We pick an arbitrary element from H — call it j — so that j is a positive integer $\geqq 5$, and $2^j > j^2$. Of course $j+1$ will also be a positive integer $\geqq 5$, and we would like to know that $2^{(j+1)} > (j+1)^2$ (for this would allow us to conclude that $j+1$ is in H, and hence that H is inductive).

Now how can we reason from the facts that $j \geqq 5$ and $2^j > j^2$ to the desired conclusion that $2^{(j+1)} > (j+1)^2$? We know, of course, that $2^{(j+1)} = 2^j \cdot 2^1 = 2^j + 2^j$ and $(j+1)^2 = j^2 + (2j+1)$. Thus we *would like to* establish that $2^j + 2^j > j^2 + (2j+1)$. Using our knowledge that $2^j > j^2$ we *can* establish that $2^j + 2^j > j^2 + j^2$. Thus our work would be completed *if we could show* that $j^2 > 2j+1$.

Of course it is not true that for *every* positive integer i we have $i^2 > 2i+1$, as we see by considering the case $i = 1$. But remember that we know that our integer j must be $\geqq 5$. Could it be that for every integer $j \geqq 5$ we have $j^2 > 2j+1$? By trying a few special values for j say $j = 5, 6, 7$, it seems rather likely that this is so. But how do we *prove* it? By the extended principle of mathematical induction, of course!

Thus it appears that in order to complete the proof that $2^k > k^2$ for every positive integer $k \geqq 5$ by the extended principle, we must first prove that $j^2 > 2j+1$ for every positive integer $j \geqq 5$ —*again* by using the extended principle. But this latter task is a straightforward matter, and we shall leave the details to the interested reader.

Well then, we know that $2^k > k$ for every positive integer k and that $2^k > k^2$ for every $k \geqq 5$. Do any generalizations suggest themselves to your mathematical intuition? What about the inequality $2^k > k^3$? On the basis of our earlier experience we might expect that it does not hold for *all* positive integers k, but that it may hold for *all sufficiently large* k, i.e., that we can find a certain number q such that $2^k > k^3$ for every positive integer k which is $\geqq q$. If we are more daring, we may even conjecture that something similar is true for each of the inequalities $2^k > k^4$, $2^k > k^5$, etc. Let us formulate this general proposition explicitly.

CONJECTURE. *Given any positive integer n, we can find a positive integer q such that $2^k > k^n$ for every positive integer $k \geq q$.*

It happens that this proposition is correct. In general, the larger the value of the given integer n, the larger we will have to take q. That is, if n is very large we have to go very far out in the sequence of positive integers before we get to values of k where 2^k becomes and remains $> k^n$.

By direct computation we can find a suitable value of q, and then employ the extended principle of mathematical induction to show that $2^k > k^3$ whenever k is equal to or exceeds this value of q. This task should be quite feasible for most readers — albeit a fair amount of effort will be required. However, to establish the conjecture in its full generality is a much more difficult task, and we therefore supply a few hints for the enterprising reader who wishes to tackle it.

It will be useful first for such a reader to establish two preliminary results, which we may call *lemmas*.

Lemma 1. For every positive integer n we have $2^{n+1} > n^2+n$.

Lemma 2. If $j \geq 2^n$ then $2j^n \geq (j+1)^n$.

With these results at hand one can employ the extended principle of mathematical induction to show that our conjecture will be true if we take $q = 2^{n+1}$, i.e., to show that $2^k > k^n$ for all integers $k \geq 2^{n+1}$. The pattern of the proof follows that which we gave for the case $n = 2$ above.

To prove Lemma 1 we may use mathematical induction (in its original form). To prove Lemma 2 it is best to proceed as follows.

We recall from Section B of this Appendix that there are numbers $c_1, \ldots, c_{n-1}$ (the so-called *binomial coefficients*) for which the equation

$$(j+1)^n = j^n + c_{n-1}j^{n-1} + \ldots + c_1 j + 1$$

holds identically (i.e., for all numbers j). By considering the case $j = 1$ we see that the sum of the coefficients on the right side of this equation, $1 + c_{n-1} + \ldots + c_1 + 1$, has the value 2^n so that when $j \geq 2^n$ certainly j must exceed each of these coefficients. Lemma 2 then follows directly from the observation that if we have *any* polynomial $a_n j^n + a_{n-1}j^{n-1} + \ldots + a_1 j + a_0$, then we must have

$$(**) \qquad (a_n+1)j^n \geq (a_n j^n + a_{n-1}j^{n-1} + \ldots + a_1 j + a_0)$$

for every value of j which exceeds each of the coefficients $a_0, \ldots, a_{n-1}$. This observation, in turn, is established by an inductive proof involving the set G of those numbers n for which the inequality (**) holds whenever j exceeds each of the coefficients $a_0, \ldots, a_{n-1}$.

Those who are able to carry through all of these details successfully may wish to try their hand at proving the following strengthened form of the conjecture: Let r be any positive integer; then given any positive integer n, we can find a positive integer q such that $(1+\frac{1}{r})^k > k^n$ for every positive integer $k \geq q$. Clearly the original conjecture is a special case (as we see by taking $r = 1$).

PROBLEMS

Throughout the Appendix we have mentioned problems whose solution can be effected by the use of mathematical induction. Below we collect them in a list for ready reference, and then add a few others from various domains of mathematics. Letters before the problem numbers indicate the section of the Appendix from which the problems come; new problems are numbered but not lettered.

A1. Show that if x and y are positive integers such that $x > y$, then $x^k - y^k$ is divisible by $x - y$ for every positive integer k.

A2. Show that if x and y are any positive integers, and if k is any *odd* positive integer, then $x^k + y^k$ is divisible by $x + y$.

B1. Show that for each positive integer p, there are p numbers $c_1, \ldots, c_p$ such that the equation

$$(j + 1)^p = c_p j^p + \ldots + c_1 j + 1$$

holds identically (i.e., for all numbers j). In fact, show that if i is any of the numbers $1, \ldots, p$ then

$$c_i = \frac{p!}{i!(p - i)!}.$$

Here the notation $q!$ (read q-factorial) stands for the number $q \cdot (q - 1) \cdot (q - 2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ obtained by multiplying together all of the positive integers $\leq q$.

B2. Show that given any positive integer n we can find $n+2$ *rational* numbers $b_0, \ldots, b_{n+1}$ such that the equation

$$1^n + 2^n + \ldots + k^n = b_{n+1}k^{n+1} + b_n k^n + \ldots + b_1 k + b_0$$

holds for all positive integers k. In fact, using the formulas given in B1 one can show that $b_{n+1} = \frac{1}{n+1}$ and $b_n = \frac{1}{2}$. Try to find formulas for the other numbers $b_{n-1}, b_{n-2}, \ldots, b_0$.

C1. Using Axioms 1-4 for the theory of positive integers, as given in the Appendix, Part C, prove that $(x+y) + z = x + (y+z)$ for any positive integers x, y, z.

C2. Show that the same Axioms 1-4 imply that $x + y = y + x$ for any positive integers x, y.

D1. Find the smallest integer q such that, for every positive integer $k \geq q$, $2^k > k^3$.

D2. Show that if n is any positive integer then $2^k > k^n$ for all positive integers $k \geq 2^{n+1}$.

D3. Generalize the statement in D2 by showing that, given any positive integers n and r, one can find an integer q such that $(1 + \frac{1}{r})^k > k^n$ for all positive integers $k \geq q$.

1. Suppose that n is any positive integer, and that $\ell_1, \ldots, \ell_n$ are n distinct lines in a plane satisfying the following conditions:

(i) No two of the lines are parallel;
(ii) No more than two of the lines intersect in any one point.

Show that the n lines divide the plane into exactly $(\frac{1}{2} n^2 + \frac{1}{2} n + 1)$ different regions.

2. Suppose that n and k are positive integers, that $p_1, \ldots, p_n$ are distinct points on the surface of a sphere, and that $\ell_1, \ldots \ell_k$ are distinct curved line segments lying on the surface of this sphere, such that the following conditions are satisfied:

(i) Each of the given points is an end-point of one or more segments;
(ii) Each end-point of any of the given segments coincides with one of the given points;
(iii) No point of any of the given segments *other than an end-point* can coincide with one of the given points or can lie on one of the other segments.

Show that if r is the number of regions into which the surface of the sphere is cut by the network of given segments, then $n - k + r = 2$. (Two points on the surface of the sphere are said to be in the same region in case they can be joined by a curved segment, lying in the surface of the sphere, which does not pass through any of the given points or segments.)

3. Using the facts that for any positive integers n and k we have

$$n^1 = n \qquad \text{and} \qquad n^{k+1} = n^k \cdot n ,$$

and using no other facts about exponentiation, show by mathematical induction that for all positive integers n, k, and i we have

$$n^{k+i} = n^k \cdot n^i \qquad \text{and} \qquad n^{k \cdot i} = (n^k)^i .$$

4. Within the system of Axioms 1-4 given in the Appendix, Part C, show that if x and y are any distinct positive integers (i.e., if $x \neq y$), then for any positive integer z we have $x + z \neq y + z$. (Notice that from this result, by an elementary law of logic, there follows the well known cancellation law: whenever $x + z = y + z$ we have $x = y$.)

5. Within the theory of Axioms 1-4 given in the Appendix, Part C, we introduce the ordering relation $<$ by the rule of definition:

$x < y$ if and only if $x + z = y$ for some positive integer z.

Using this definition and the associative law for $+$ (Problem C1), it is easy to show the *transitive law* for $<$: whenever $x < y$ and $y < t$ we must also have $x < t$. Using mathematical induction, show in this theory that the *trichotomy law* holds for $<$: For any positive integers x and y, either $x < y$ or $x = y$ or $y < x$.

6. In Part D of the Appendix there is given a statement and proof of the *Extended Principle of Mathematical Induction*. Give *another* proof of this extended principle by considering the set I of all *those* positive integers k such that $k + p - 1$ is in H.

7. In addition to the *extended* principle discussed in Part D of the Appendix, there is *another* generalization of mathematical induction which is often very useful. In order to formulate this, we first specify that a set K of positive integers is to be called *weakly inductive* if, whenever we pick a number from K *such that every smaller positive integer is also in* K, then the number obtained by adding 1 to the chosen number will also be in K. Now we can state the

Principle of Strong Induction: If K is any set of positive integers such that

(a) the number 1 is in K, and
(b) K is weakly inductive,

then *every* positive integer must be in K.

Prove this Principle of Strong Induction using ordinary mathematical induction. Suggestion: Being given a set K which satisfies the hypotheses (a) and (b) above, consider the set G of all *those* numbers j such that j, *as well as every positive integer less than* j, is in K.

8. A positive integer is called *prime* if it is greater than 1 and is not divisible by any positive integer except 1 and itself. Using strong induction, as formulated in the preceding problem, show that every positive integer either is 1, or else is a product of one or more prime numbers.

9. Let s and k be positive integers. Show that given *any* positive integer n we can find another positive integer m such that $(s + \frac{1}{m})^k - s^k < \frac{1}{n}$. (This proposition is closely related to the fact that the operation of raising a number to the k-th power is a *continuous* operation.)

10. Let s and k be positive integers. Show that given *any* positive integer n we can find another positive integer m such that

$$\frac{(s + \frac{1}{m})^k - s^k}{\frac{1}{m}} - ks^{k-1} < \frac{1}{n}.$$

(This proposition is closely related to a fundamental result of differential calculus.)