An Experiment In Mathematics

PAUL RAYMOND PATTEN, Purcell High, Purcell

All too often, mathematics seems to be a mass of rigorous proofs that do not show the methods of induction and guessing that other sciences make manifest in their observations and experiments. It is the purpose of the following to show how mathematics may be explored by means of the same processes used in the other sciences. Of course, in the end the observations and experiments will lead to rigorous proofs of theorems; these observations only supplying the ideas upon which proofs are to be built.

The eighth proposition of the second book of Diophantus states the problem of finding integral solutions to the equation $x^2+y^2=z^2$. In the margin of a copy, the French mathematician, Pierre de Fermat, wrote that he had found a proof for the more general case, $x^n+y^n=z^n$, for integral solutions for $n>2$ but that it was too lengthy to describe in the margin remaining. An approach to this problem is described below in two phases, an experimental or exploratory phase, which relates the formulation of a hypothesis in research in mathematics, and a formal statement phase, which relates the proof of a theorem.

EXPLORING AND OBSERVING

If a positive integer is divided by another positive integer, the remainder is called the modulus of the first number with the second number as the base. This can be written $a=c \ (mod\ b)$, where c is the remainder in the division of a by b. A complete set of such moduli can be called a modular system.

The following modular systems will use only the moduli greater than zero and less than the base for x, y, and z in the equation, $x^n + y^n=z^n$. Since *1* is a factor of every number and since only solutions where $x \neq y$ are to be explored, the experiment will begin in modulo three (in modulo two, $x = y$ if x and $y \neq 0$).

From the summarized power table (See Table I) it can be seen that in modulo three $x^m + y^m = 2^m$ has no solutions such that $x \neq y$, x, y, and $2>0$; since, if $m = 2n -1$, the only possible value of $x^m + y^m$ is $1+2$. In modulo three, $1+2 = 0$, which is not greater than zero. If $m = 2n$, $x^m + y^m = 2$ which is no number to the 2n power (the 2n now does not contain *2*, and $0^{2n} = 0$, not *2*).

TABLE I

		1	2		multiplication table for modulo three
	1	1	2		
	2	2	1		
Power		1	2	number	Power table for modulo three since $K^{n+1}=K^n \cdot K$. It can be seen that when $K^n=1$ the preceding pattern is repeated which leads to the following summarization.
	1	1	2		
	2	1	1		
	3	1	2		
	4	1	1		
Power		1	2	number	
$2n - 1$		1	2		Summarized power table for modulo three
$2n$		1	1		

n is an integer > 0

TABLE II

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Multiplication table for modulo four

Power	1	2	3
1	1	2	3
2	1	0	1
3	1	0	3
4	1	0	1
5	1	0	3
6	1	0	1

Power table for modulo four

Power	1	2	3	number
1	1	2	3	
2n	1	0	1	
2n+1	1	0	3	

Summarized power table for modulo four $n>0$

From the modulo four summary (See Table II) it is evident that $x^m + y^m = z^m$ has solutions for any value of $m>0$ (m is an integer, $x \neq y$, and x, y, and $z>0$). Since if $m = 1$, (1,2,3) is such a solution; and if $m = 2n$, (1,2,3) is again such a solution, and if $m = 2n + 1$, (1,3,2) is a solution.

Doing the same for modulo five, the equation $x^m + y^m = z^m$ has the desired solutions only if *m* is odd. In modulo six, the equation has the desired type of solutions for all integral values of *m* greater than zero. In modulo seven, the equation has the desired solutions only if *m* cannot be put in the form *3(2n + 1)* or *3(2n + 2)* where *n* is an integer greater than or equal to zero. In modulo eight, the equation has the desired type of solutions for all integral values of *m>0*. In modulo nine, the equation has the desired type of solutions for all integral values of *m>0*, showing that the property of not having the desired solutions for certain values of *m* is not connected with the odd numbers. In modulo ten, the desired solutions may be found for any value of *m*>0, but in modulo eleven, if *m* can be an integer of the form *10n + 5* or *10n + 10* the equation does not have the desired solutions (*n* is an integer >0).

The preceding leads to the hypothesis that: if the base of the modular system is prime, there will be certain values of *m* for which the equation does not have the desired solutions since 3, 5, 7, and 11 are all prime.

Now the experiment has been completed and the results collected and formed into a hypothesis, but this is only a hypothesis, and it needs to be proven generally true. In the natural sciences, this is usually done by more tests and observations, but in mathematics it is better to demonstrate the veracity of a statement by the rules of logic. This is the finishing touch and makes mathematics the most exact science.

PROVING THE THEOREM

Lemma one: In a modular system with a prime base, a number to the power with the base as an exponent is itself.

The lemma states that if *k* is a number (in a modular system it will be a positive integer) $k^n = k$ if *n* is prime. Now $0^n = 0$, and $1^n = 1$. If $1^n = 1$ and if, on the basis of assuming that $k^n = k$, then $(k+1)^n = k + 1$ can be proved, the lemma will be true. $(k + 1)^n = k^n + n\,k^{n-1} + \frac{n\,(n-1)\,k^{n-2}}{2} + \ldots + \frac{n(n-1)\ldots(n-(n-2))\,k^{n-(n-1)}}{(n-1)!} + 1.$

Since *n* is prime, *n* and the denominators of terms which are not equal to one of k^n do not contain common factors greater than 1 with n, so that n will divide into the terms between k^n and 1 leaving zero remainders; such terms will be zero in the modular system base n. Thus $(k + 1)^n = k^n + 1$ in mod_n but $k^n = k$ by assumption; therefore, $(k + 1)^n = k + 1$, and thus follows the lemma.

Lemma two: In a modular system with a prime base, a number (not 0) to the power with the base minus one as an exponent is one.

By the first lemma, $k^n = k$ when n is prime. Now $k^{n-1}\,k = k^n = k$, but $1 \cdot k = k$; thus, $k^{n-1}{=}1$, which is the lemma.

Theorem: In a modular system with a prime base and using those members greater than zero and less than the base, there is at least one value of m for which the equation $x^m + y^m = z^m$ will have no solutions and that value of m will be the base minus one.

Let b be the base which is prime. Then, by lemma two, $k^{b-1} = 1$ for any value of k greater than zero, so that $x^{b-1} + y^{b-1} = 1 + 1 = 2$, $2 \neq 1$ or z^{b-1} thus follows the theorem which is the hypothesis derived from the experiment.

Note: $x^m + y^m = z^m$ is referred to as an equation instead of a congruence, since only the members less than the base are used and since congruence usually refers to different numbers having the same remainders (ie, 2 is congruent to 7 in mod 5). Here, since the x, y, and z are remainders left over after the division by the base, a situation such as the preceding does not exist—if a and b are less than the base, $a = a$, $b = b$, and $a \neq b$, and if a and b are not equal in the system of positive integers.

DISCUSSION

The preceding shows in some little way the fact that mathematics like the other sciences must start with observations. Even the proof for the theorem is not entirely separate from the experiment. In the next to the last row on all the summarized power tables of modular systems with prime bases, the only entry is one which leads one to the proof of the lemmas of the theorem.

It also must be realized that this is not the end—what about modular systems with composite bases? This is true in the other sciences, which shows that perhaps mathematics is as changing as the other sciences—one may always generalize and search for more questions.

BIBLIOGRAPHY

Smith, David E. 1959. Note on the equation $x^n + y^n = z^n$ *in A Source Book in Mathematics.* Dover Publ., Garden City.