Diophantine Equations and Fermat's Last Theorem

There is little doubt that of all unsolved problems of mathematics the most widely known and most often attempted is that known as Fermat's Last Theorem. There are several reasons for its fame: the nature of the problem does not involve any difficult abstruse concepts, but on the contrary is quite simple to understand; a large prize of 100,000 marks offered by a Genman professor stimulated interest in the problem until inflation during the 1914-18 war rendered the amount offered insignificant; and then the mystery as to whether Fermat himself possessed a proof naturally arouses curiosity about the question.

Pierre Fermat (1601-1665) occupies an almost unique role amongst the really great mathematicians of history in that he did not make a living as an academic. He was in fact a lawyer, and mathematics was merely his hobby. His interests ranged over all the newly developing fields of mathematics of the age, analytic geometry, calculus, the theory of probability(important contributions) and the theory of numbers, in which he was especially gifted. In this last field his researches were inspired by a very ancient treatise, "The Arithmetica", by Diophantus, a Latin translation of which had been printed in 1621. In this masterpiece of Greek mathematics Diophantus did for "arithmetic" what Euclid had done earlier for geometry viz. collected all the important solved problems in the theory of numbers, and arranged them in a reasonable order, later propositions frequently making use of earlier material.

It is not too much to say that for the next century and more the major part of progress in the theory of numbers consisted in expanding, generalising and developing the ideas contained in this work. Indeed to this day the topic of Diophantine equations occupies an important place in the subject.

As an illustration of the simplest type of Diophantine equations consider the following question:

The cash register of the poultry counter shows a taking of £13/5/-. Only fowls and ducklings were sold, at prices of 25/- and 35/- per bird respectively. How many fowls and how many ducklings were sold?

If f is the number of fowls, and d the number of ducklings, we have the equation

$$25f + 35d = 265$$

or simplified:

$$5f + 7d = 53$$

This is one linear equation with <u>two</u> unknowns, and if we regard it on its own, and admit any values for f and d, we obtain an infinite number of solutions, hence the equation is indeterminate. However, it is obvious that f and d must be positive integers if we are to obtain a meaningful answer to the original question. We may solve the equation by trial and error, but it is more satisfactory to go about it in a systematic way, making sure that we find <u>all</u> the possible solutions.

We may proceed as follows: If

$$53 - 7d = 5f \quad (d, f \text{ positive integers}),$$

then 53-7d must be divisible by 5. We may simplify this by noticing that

$53 - 7d = 55 - 5d - (2 + 2d) = 5(11-d) - 2(1 + d)$, where

$5(11-d)$ is a multiple of 5. Hence $2(1 + d)$ must be divisible by 5; as 5 and 2 are relatively prime

(i. e. have no common factors apart from 1), it follows*) that 1+d is divisible by 5, that is, $1 + d = 5k$ for some integer k. Hence

$$d = 5k - 1 \text{ (k an integer)},$$

where k must be positive to make d positive. Substituting for d in the original equation,

$$53 - 7(5k - 1) = 5f,$$

that is,

$$f = 12 - 7k.$$

Since k, f are positive integers, the only possibility is $k = 1$. Putting $k = 1$, we obtain $d = 4$, $f = 5$ as the only solution.

The example discussed above represents a particularly simple case, that of a linear equation in two unknowns which has a single solution in positive integers. This is by no means the general result. If in the above problem the value of the cash takings were changed to £26/10/- we would have the equation

$$5f + 7d = 106,$$

which has three positive solutions

$f = 17$, $d = 3$; $f = 10$, $d = 8$; and $f = 3$, $d = 13$.

If the value were changed to £5 3/4, we would have

$$5f + 7d = 23$$

which has no positive integer solutions. (However it has an infinite number of integer solutions if negative numbers are allowed, as they might be in some other problem leading to the same equation.)

---

*) In this argument we use the fundamental theorem of arithmetic: Every positive integer except 1 can be expressed in one and only one way as a product of prime factors. This theorem is not "self-evident", as it appears to the beginner, but is readily proved.

Let us consider a second example of a Diophantine equation which is more relevant to the subject of this article. Find all sets of positive integers x, y and z such that

$$x^2 + y^2 = z^2 . \quad (1)$$

First note that if x and y have a common factor, h, so that $x = hX$ and $y = hY$ where X and Y are integers, then $z^2 = h^2 (X^2 + Y^2)$, whence h is also a factor of z, $z = hZ$, and $Z^2 = X^2 + Y^2$. (Similarly, if h is a factor of z and x it is a factor of y etc.). Thus, if the largest common factor is removed from any triple (x, y, z) satisfying (1) we obtain a triple (X, Y, Z) satisfying (1) such that no two elements have a common factor (i. e. X, Y and Z are relatively prime in pairs). It is clearly sufficient to find all triples satisfying (1) and subject to this extra condition.

Now it is a well known (and easily proved) fact that the squares of even numbers are divisible by 4, but the squares of odd numbers leave a remainder of 1 on division by 4. Hence if

$$X^2 + Y^2 = Z^2 \quad (2)$$

we must have either X or Y even, the other odd, and Z odd. (Or of course, all even, but we are assuming at this stage that X, Y and Z are relatively prime in pairs. Note that it is not possible for X and Y to be odd and Z even since the L. H. S. would leave a remainder of 2 on division by 4). For definiteness let us represent the even number by Y, so that X is odd. Rearranging (2) gives

$$X^2 = Z^2 - Y^2 = (Z-Y)(Z+Y)$$

Any common factor $k(>1)$ of the odd numbers $Z-Y$ and $Z+Y$ would also be a factor of both

$$Z = \frac{(Z+Y)+(Z-Y)}{2} \quad \text{and of} \quad Y = \frac{(Z+Y)-(Z-Y)}{2},$$

contradicting our assumption that Y and Z are relatively prime. Hence $(Z-Y)$ and $(Z+Y)$ are relatively prime. If p is any prime factor of $(Z-Y)$ then p/X^2, (read this as p divides $X2$) whence p/X and p^2/X^2. Since $p \nmid (Z+Y)$ we have $p^2/(Z-Y)$. It follows easily that $Z-Y$ is a perfect square $Z - Y = u^2$, say, and similarly

$Z + Y = v^2$. Note that u and v are both odd integers, $v > u$.

Solving we obtain $Z = \frac{u^2 + v^2}{2}$

$$Y = \frac{v^2 - u^2}{2}$$

and $X = Z^2 - Y^2 = uv$.

Finally, multiplying throughout by any common factor h we have obtained all solutions of $x^2 + y^2 = z^2$ in the form

$x = huv$, $y = h\frac{v^2 - u^2}{2}$, $z = h\frac{v^2 + u^2}{2}$ where u and v are any two odd integers.

(To test this solution try say, $h = 1$, $u = 1$, $v = 3$; $h = 1$, $u = 1$, $v = 5$; $h = 1$, $u = 3$, $v = 5$; obtaining for (x, y, z) the triples $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ respectively.)

It was in connection with the above problem that Fermat stated his famous theorem. He wrote the following note in the margin of his copy of Diophantus "On the other hand, it is impossible to separate a cube into two cubes, a biquadrate into two biquadrates or generally any power except a square into two powers with the same exponent. I have discovered a truly marvellous proof of this, which however the margin is not large enough to contain."

In other words Fermat was asserting that there exist no positive integers (or equivalently, any rational numbers) x, y, z, such that

$x^n + y^n = z^n$ if n is any integer greater than 2.

There is now a very considerable amount of evidence to suggest that Fermat's statement is true. No exceptions have ever been discovered in the three centuries since Fermat's death. On the other hand for many <u>particular</u> values of n the statement has been proved true. (For example, it has been proved that if n contains any odd prime factor less than 619 there are no integers x, y, z satisfying the equation.)

This being so there remains the question as to whether Fermat did indeed find a "truly marvellous proof". No authority questions the sincerity of Fermat's claim, for in all that is known of the man, and in all else that remains of his writings, he stands revealed as a man of the highest integrity. On other occasions he made guesses about mathematical results, but he made it quite clear that they were guesses, and that he had been unable to prove them. In every other case in which he claimed to have a proof, later mathematicians were able to find a proof using methods known to Fermat.

Nevertheless, the majority of mathematicians today believe that Fermat must have made a mistake, and that the proof he claimed to have found contained a well-concealed fallacy. After all, they point out, even the Fermats of this world do make mistakes, and since that day there have been literally thousands of people (including some very good mathematicians) who believed for a time that they had proved the theorem, only to have an oversight later detected. Opponents of their view are able to point out that in all the history of mathematics it is difficult to find an equal of Fermat

in elementary number theory, and that what he considered a truly marvellous piece of deduction might well escape the notice of men of comparable ability. Well, it is most unlikely that this mystery will ever be cleared up, so you can quite happily opt in favour of which ever conclusion appeals to you.

Fermat had earlier proved the special case of his theorem, $n = 4$. This proof, using Fermat's own method of infinite descent, is included in the appendix at the end of this article. Any $n > 2$ is either a power of 2, and divisible by 4, or it contains some odd prime p, as a factor i.e. $n = 4N$ or $n = pN$ where N is an integer. Any solution in integers of

$x^n + y^n = z^n$ would immediately provide integers

$X = x^N$, $Y = y^N$ and $Z = z^N$ such that

$X^4 + Y^4 = Z^4$ or $X^p + Y^p = Z^p$. Hence it would suffice to prove Fermat's result when n is any odd prime.

Although an enormous amount of unsuccessful effort has been expended on this result, the labour has not been altogether wasted. One of the most determined attacks on the problem was made by the German Ernst Kummer (1810-1893). Not only did Kummer succeed in disposing of the problem for a large class of special primes, but ideas and concepts he introduced in his attempt have proved of tremendous importance in twentieth century algebra.

A few more results of a somewhat more technical nature are left for the appendix.

APPENDIX

Theorem I The general solution in positive integers of $x^2 + y^2 = z^2$, such that $2/x$ and $(x, y) = (x, z) = (y, z) = 1$ is given by

$$x = 2uv, \quad y = v^2 - u^2, \quad z = v^2 + u^2$$

where u, v are any positive integers, such that $v > u$, $(u, v) = 1$.

Proof. This is merely another version of the solution obtained in the article, in a form required in the next theorem. It was shown earlier that every solution satisfying the stated conditions is obtainable in the form

$$x = \frac{s^2 - t^2}{2}, \quad y = st, \quad z = \frac{s^2 + t^2}{2}$$

where s and t are relatively prime odd integers. If in this we put $s = u + v$, $t = v - u$, so that $v \left(= \frac{s + t}{2}\right)$ and $u \left(= \frac{s - t}{2}\right)$ are relatively prime integers, we immediately obtain the solution as stated in the theorem.

Puzzles with cubes.

(1) Is it possible to pass a cube through a hole in a smaller cube!!!? How?

(2) Twelve electrical resistances of 1 ohm each are situated along the edges of a cube, and connected at the vertices of the cube. What is the resistance of the whole system between a pair of diagonally opposite vertices?

(Answer p 32)

Theorem: There are no positive integers a, b, c such that $a^4 + b^4 = c^4$. In fact (a slightly stronger result) there are no positive integers x, y, z such that $x^4 + y^4 = z^2$.

Proof: Suppose there are solutions and let x, y, z be the solution for which z is least. It is obvious that $(x, y) = (y, z) = (x, z) = 1$ since any common factor could be cancelled out yielding a smaller solution immediately. Since x and y cannot both be odd, let $2/x$. Using Th. I we have

$$x^2 = 2uv \quad (1), \text{ with } (u, v) = 1$$
$$y^2 = u^2 - v^2 \quad (2)$$
$$z = u^2 + v^2 .$$

From (1) uv is even and by considering remainders on division by 4 in (2) we decide $2/v$, $2\nmid u$.

From (1) $u = U^2$, $v = 2V^2$ and (2) becomes

$$y^2 + 4V^4 = U^4$$

Again employing Th. I we have

$$2V^2 = 2rs \quad (3) \text{ where } (r, s) = 1$$
$$y = r^2 - s^2 \quad (4)$$
$$U^2 = r^2 + s^2 \quad (5)$$

From (3) $r = R^2$, $s = S^2$ and (5) becomes

$$U^2 = R^4 + S^4$$

But this is another solution of the equation, with $U \leqslant U^2 = u \leqslant u^2 < u^2 + v^2 = z$. This contradicts our choice of z as the smallest integer for which the equation was solvable, and hence completes the proof.

For more detailed work on the problem it has proved useful to introduce the following terms. If x, y and z are prime to each other and to n, this condition is referred to as Case I of Fermat's last theorem. If x, y and z are prime to each other but one of them is divisible by the prime n, the condition is called Case II of the theorem. (Case I of the theorem is known to be true for all $n < 253,000,000$, but Case II has proved rather harder to tackle).

An example of a criterion for Case I of the theorem which can be proved by quite simple elementary methods is the following:

Theorem III. If n is an odd prime, and there exists an odd prime p such that

$$f^n + g^n + h^n = 0 \pmod{p} \qquad (1)$$

has no integral solutions f, g, h each not divisible by p, and also such that, for every integer u,

$$u^n \not\equiv n \pmod{p} \qquad (2)$$

then

$$x^n + y^n + z^n = 0 \qquad (3)$$

has no integral solutions each prime to n.

Proof: Let x, y, z satisfy (3), and $xyz \not\equiv 0 \pmod{n}$. We may suppose that $(x, y) = (y, z) = (z, x) = 1$ since any common factor can be first cancelled out.

$$(y + z)\varphi(y, z) = -x^n,$$

where $\varphi(y, z) = y^{n-1} - y^{n-2}z + y^{n-3}z^2 \ldots\ldots + z^{n-1}$.

Any prime factor common to $y + z$ and $\varphi(y, z)$ divides

$$nz^{n-1}\left[= \varphi(y, z) - (y+z)(y^{n-2} - 2y^{n-3}z + 3y^{n-4}z^2 \ldots.\right]$$

Proof Cont'd. It cannot divide z since $(y, z) = 1$, and if it is equal to n we have n/x^n contradicting $x \not\equiv 0 \pmod{n}$.

Hence $y + z = a^n$, $\varphi(y, z) = A^n$ where $(a, A) = 1$.

Similarly $z + x = b^n, \varphi(z, x) = B^n$

and $x + y = c^n, \varphi(x, y) = C^n$,

Hence

$$2x = b^n + c^n - a^n,\ 2y = c^n + a^n - b^n,\ 2z = a^n + b^n - c^n.$$

Let p be an odd prime satisfying the conditions.

From (3) and (1), p divides one of x, y and z. We may assume p/x. Since

$2x = b^n + c^n + (-a)^n$ is divisible by p, further use of (1) shows that p divides one of a, b, and c. Both p/b and p/c easily lead to contradiction. But if p/a, we have $y = -z$,

$\varphi(y, z) = ny^{n-1}$, $\varphi(x, y) \equiv y^{n-1} \pmod{p}$ so that $(AC^{-1})^n \equiv n \pmod{p}$, which contradicts (2).

These contradictions establish the result.

The equation $x^n + y^n + z^n = 0$ is used in this theorem instead of $x^n + y^n = z^n$ because of the greater symmetry.

To illustrate how the theorem works, take $n = 11$. Then the prime $p = 23$ satisfies the stated conditions, (since $u^{11} = 0$, 1, or $-1 \pmod{23}$ for each integer u) and it follows from the theorem that Case I of Fermat's Last Theorem is true for $n = 11$.