FERMAT'S LAST CONJECTURE AND POLYNOMIALS

BY BOB HART, HAWKER COLLEGE

About 1637 Pierre Fermat wrote the following famous note in the margin of Bachet's translation of Diophantus' Arithmetica:

It is impossible to write a cube as the sum of two cubes, a fourth power as the sum of two fourth powers and, in general, any power beyond the second as a sum of two similar powers. For this I have discovered a truly wonderful proof but the margin is too small to contain it.

Fermat did write out proofs that the Diophantine equations $x^4 + y^4 = z^2$ and hence $x^4 + y^4 = z^4$ had no solutions but mathematicians have been searching for his "truly wonderful proof" of the general case without success for over 300 years. The search has not been totally fruitless, for many new techniques in number theory and abstract algebra have been developed as a result.

Readers will be aware of the parallel properties between the integers and polynomials

- each is closed, commutative and associative under addition and multiplication.

- each follows the division algorithm, i.e. given x and y there exist unique q and r such that $x = qy + r, 0 \leq r < y$ or, more precisely for polynomials, deg $r <$ deg y. (Here deg p denotes the degree of p, i.e., the order of the highest power in p).

- the integers contain primes, the polynomials contain irreducibles (see the footnote).

Theorem. *If $x(t), y(t)$ and $z(t)$ are polynomials such that*

(i) no non-constant polynomial divides all three and

(ii) at least one is non constant, then it is impossible for

$$[x(t)]^n + [y(t)]^n = [z(t)]^n \text{ if } n \geq 3.$$

Proof: For this proof I will write x for $x(t), y$ for $y(t)$ and z for $z(t)$.

From assumption (i) it follows that no two of the polynomials x, y, z have a common factor; for if they had, they would also have a common irreducible factor, which then divides the third polynomial (see footnote), contrary to assumption (i).

The proof is by contradiction.

Suppose that $x^n + y^n = z^n$ (I)

Differentiate: $nx^{n-1}x' + ny^{n-1}y' = nz^{n-1}z'$

(where $x' = dx/dt, y' = dy/dt$ and $z' = dz/dt$)

Divide by n: $x^{n-1}x' + y^{n-1}y' = z^{n-1}z'$

Multiply by x: $x^nx' + xy^{n-1}y' = xz^{n-1}z'$ (II)

Multiply (I) by x': $x^nx' + y^nx' = z^nz'$ (III)

Subtract (II) - (III): $y^{n-1}(xy' - yx') = z^{n-1}(xz' - zx')$ (A)

Similarly: $z^{n-1}(yz' - zy') = x^{n-1}(yx' - xy')$ (B)

: $x^{n-1}(zx' - xz') = y^{n-1}(yz' - zy')$ (C)

Without loss of generality, let $\deg(x) \leq \deg\,(y) \leq \deg\,(z)$ (because of the symmetry of equations (A), (B), (C) the proof goes through in the same fashion for any other ordering of the degrees).

Also, note that $zy' - yz'$ and all other similar terms in the equations (A), (B) and (C) must be non zero:

Because, if $zy' - yz' = 0$,

then $zy' - yz' = 0$, i.e. $(y/z)' = 0$.

Therefore $y/z = k$, a constant, or $y = kz$, or $z|y$.

Now, $z^{n-1}|z^{n-1}(yz' - zy')$. ($\alpha|\beta$ abbreviates "α divides β")

Hence, $z^{n-1}|x^{n-1}(yx' - xy')$ (equation B)

But z and x have no common factor, therefore

$$z^{n-1}|(yx' - xy')$$

and so $\deg (z^{n-1} \leq \deg (yx' - xy')$ (D)

Now $\deg (z^{n-1}) = (n-1) \deg z$

$\deg (yx') = \deg (xy') = \deg(x) + \deg (y) - 1$

and so $\deg (yx' - xy') \leq \deg (x) + \deg (y) - 1.$

Therefore, from equation (D)

$$(n-1) \deg (z) \leq \deg (x) + \deg (y) - 1$$

Remember $\deg (x) \leq \deg (z)$ and $\deg (y) \leq \deg (z)$

Hence, $(n-1) \deg (z) \leq 2\deg(z) - 1$, or $(n-3) \deg (z) \leq -1$

This is clearly impossible if $n \geq 3$ and the proof is complete.

If we still wish to prove Fermat's last conjecture, this result obviously makes us wonder what is the equivalent of "degrees" for an integer and what is the equivalent of "differentiation" in the integers.

Any ideas?

Footnote: A real polynomial p is irreducible if whenever it factors as $p = qr$ (where q, r are polynomials) one of the factors q or r must be a constant. So $t^2 + 1$ is irreducible whilst $t^2 + 5t + 6 = (t+3)(t+2)$ is reducible. The fact that if an irreducible p divides x^n then it must divide x can be proved like the corresponding fact for integers. The "unique prime factorization theorem" is valid for polynomials just like for integers.

The above proof was shown to me by Professor Koch at the University of Oregon as part of a fascinating course entitled "The History of Analytical Geometry" in 1975.

* * * * * * * *

FERMAT THE MAN

Pierre Fermat (1601-1665) is often known as the *Prince of the Amateurs* (see E.T. Bell "Men of Mathematics"). He was one of the intellectual giants of the 17th century and, as a pure mathematician, was the equal of Newton. This is all the more amazing since he worked as a lawyer or magistrate in Toulouse, only doing his mathematics in his spare time. To-day he is fondly remembered for "Fermat's last theorem" but perhaps he is equally as well known for "Fermat's Principle". His "principle" asserts that a photon of light will always follow the path of shortest time between any two points. Snell's law (which was discovered in 1621) then becomes a trivial consequence of his principle so you can see what amazing insight he had into the nature of light. His most substantial contributions mathematically were in number theory – he essentially founded modern number theory – and in the calculus. Sometimes he is identified, along with Newton and Leibniz, as one of the founders of the calculus, and, in addition, he could make a substantial claim to be the true founder of "Cartesian" geometry. In fact there was a degree of enmity between René Descartes (1596-1650) and Fermat in which most of the bad behaviour emanated from Descartes.