Fermat and the difference of two squares

STAN DOLAN

1. Introduction

In a previous note [1], Fermat's method of descente infinie was used to prove that the equations

\[ x^4 + y^4 = z^2 \quad x^4 - y^4 = z^2 \quad x^4 + 4y^4 = z^2 \quad x^4 - 4y^4 = z^2 \]

have no positive integer solutions. The geometrically based proof of [1] masked the underlying use of the difference of two squares. In the proofs of this article we shall make its use explicit, just as Fermat did [2, pp. 293-294].

We shall use the elementary idea of the difference of two squares to develop a powerful technique for solving equations of the form \( ax^4 + bx^2y^2 + cy^4 = z^2 \). This will then be applied to three problems of historical interest.

**Problem 1**: Find a square rational number from which, when 5 is added or subtracted, always arises a square rational number.

This problem was posed by Johannes of Palermo to test the mathematical ability of Leonardo of Pisa, who is better known as Fibonacci, [3, pp. 76-81]. The interested reader might like to take up the challenge before reading on!

**Problem 2**: Prove that the equation \( x^7 + y^7 + z^7 = 0 \) has no solution in non-zero integers.

This case of Fermat's last theorem has a surprisingly elementary proof.

**Problem 3**: Which integers can be the areas of right-angled triangles with rational sides?

Figure 1 illustrates that 15 is such an integer.

Integers \( a \) and \( b \) will be termed coprime if the greatest common divisor of \( a \) and \( b \), \((a, b)\), is 1. We shall adopt the convention that 0 and 1 are coprime.

2. New solutions from old

Given a solution to one equation of the form \( ax^4 + bx^2y^2 + cy^4 = z^2 \), we can generate others by using a simple algebraic technique.
Lemma 1: For given integers \(a, b, c\) suppose the equation \(ax^4 + bx^2y^2 + cy^4 = z^2\) has a solution in positive integers, with \(ax^4 \neq cy^4\). Then \(X = z, Y = xy, Z = |ax^4 - cy^4|\) is a solution in positive integers of the equation \(X^4 - 2bX^2Y^2 + (b^2 - 4ac)Y^4 = Z^2\).

Proof: The second equation can be written as \((X^2 - bY^2)^2 = Z^2 + 4acY^4\). The right-hand side is then equal to
\[
(ax^4 - cy^4)^2 + 4acx^4y^4 = (ax^4 + cy^4)^2 = (z^2 - bx^2y^2)^2 = (X^2 - bY^2)^2.
\]

Figure 2 illustrates the effect of applying Lemma 1 twice and then simplifying the resulting equation. In Lemma 1, the solution of the second equation can generally be considered to be larger than the solution of the first equation since \(Y = xy\). To conform to this idea of size and our intended use of "descente", the initial equation is at the bottom of the diagram.

\[
\begin{align*}
x^4 + bx^2y^2 + acy^4 &= z^2 \\
y_{\text{new}} &= 2y \\
x^4 + 4bx^2y^2 + 16acy^4 &= z^2 \\
x_{\text{new}} &= z \\
y_{\text{new}} &= xy \\
z_{\text{new}} &= |x^4 - (b^2 - 4ac)y^4| \\
x^4 - 2bx^2y^2 + (b^2 - 4ac)y^4 &= z^2 \\
x_{\text{new}} &= z \\
y_{\text{new}} &= xy \\
z_{\text{new}} &= |ax^4 - cy^4| \\
ax^4 + bx^2y^2 + cy^4 &= z^2
\end{align*}
\]

FIGURE 2

3. Fibonacci's problem

Fibonacci was asked to find a rational square, \(r^2\), such that
\[
r^2 + 5 = s^2, \quad r^2 - 5 = t^2.
\]
As Figure 3 illustrates, this problem is equivalent to that of finding a right-angled triangle with rational sides and area 5. In fact, 5 is the smallest integral area for which it is possible to construct such a triangle.

\[ s^2 + t^2 = 2r^2 \]
\[ s^2 - t^2 = 10 \]

\[ \text{FIGURE 3} \]

If we let \( s + t = \frac{x}{y} \), where \( x \) and \( y \) are coprime integers, then \( s - t = \frac{10y}{x} \).

A little elementary algebra then shows that any solution to Fibonacci's problem is of the form \( r = \frac{z}{2xy} \) where

\[ x^4 + 100y^4 = z^2. \]

While this equation has no immediately obvious solution, Lemma 1 can be used to generate infinitely many solutions, using obvious solutions to other, related, equations.

For given integers \( b \) and \( d \), Lemma 1 demonstrated an important connection between the solutions of equations of the two forms:

\[ ax^4 + bx^2y^2 + cy^4 = z^2, \quad ac = d \]
\[ Ax^4 - 2bx^2y^2 + Cy^4 = z^2, \quad AC = b^2 - 4d. \]

In the case of Fibonacci's problem, the related equations are

\[ ax^4 + cy^4 = z^2, \quad ac = -25 \text{ or } 100. \]

Several of these equations have obvious solutions. For example,

\[ 5x^4 + 20y^4 = z^2 \]

has solution \( x = y = 1, z = 5 \).

We can therefore generate solutions of Fibonacci's problem as Figure 4 sets out:
Starting with the solution \((1, 1, 5)\) we obtain \((5, 2, 15)\) and then \((15, 10, 1025)\) which we can simplify to \((3, 2, 41)\).

This gives the solution obtained by Fibonacci

\[
\left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2, \quad \left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2.
\]

Continuing the iteration from \((3, 2, 41)\) we obtain \((41, 12, 1519)\) and then \((1519, 492, 3344161)\). This gives us a second solution to Fibonacci's problem, \(\left(\frac{3344161}{1494696}\right)^2\), and so on.

We shall return, in a more general way, to Fibonacci's problem in Section 6. For now, there are a couple of points arising in the above derivation which are worth noting.

In the solution of Fibonacci's problem, the solution \((15, 10, 1025)\) was simplified to \((3, 2, 41)\). More generally, we have the following results.

**Lemma 2:** A positive integer solution of the equation \(ax^4 + bx^2y^2 + cy^4 = z^2\) can be transformed into one with \((x, y) = 1\).

**Proof:** \((x, y)^4\) is a factor of \(z^2\) and so we can replace \(x, y\) and \(z\) by \(\frac{x}{(x, y)}\), \(\frac{y}{(x, y)}\) and \(\frac{z}{(x, y)^2}\), respectively.
Lemma 3: A positive integer solution of the equation $ax^4 + bx^2y^2 + cy^4 = z^2$ can be transformed into one of an equation $a'x^4 + bx^2y^2 + c'y^4 = z^2$, with $a'c' = ac$ and $x, y$ and $z$ pairwise coprime.

Proof: By Lemma 2 we can suppose $(x, y) = 1$. If $(x, z) \neq 1$, then $(x, z)^2$ is a factor of $cy^4$ and therefore of $c$. Replace $x, z, a$ and $c$ by $\frac{x}{(x, z)}, \frac{z}{(x, z)}, a' = a(x, z)^2$ and $c' = \frac{c}{(x, z)^2}$, respectively. The case $(y, z) \neq 1$ can be treated in the same way.

Many of the equations considered in this section have been of the form $ax^4 + bx^2y^2 + cy^4 = z^2$, with $a = 1$. In the next section we shall make use of the following result.

Lemma 4: If $a$ is a positive square, a positive integer solution of the equation $ax^4 + bx^2y^2 + cy^4 = z^2$ can be transformed into one of $x^4 + bx^2y^2 + acy^4 = z^2$ with the same value of $y$.

Proof: Let $X = x\sqrt{a}$ and $Z = z\sqrt{a}$. Then
\[
ax^4 + bx^2y^2 + cy^4 = z^2
\Rightarrow a^2x^4 + abx^2y^2 + acy^4 = az^2
\Rightarrow X^4 + bx^2y^2 + acy^4 = Z^2.
\]

4. Descente infinie

We have seen that (some) solutions of an equation of the form $ax^4 + bx^2y^2 + cy^4 = z^2$ can be generated from (generally smaller) solutions of related equations. So that we can apply Fermat's method of descente, we need to establish precisely when this can be done.

First we shall use the difference of two squares to prove the converse of Lemma 1.

Lemma 5: For given integers $b$ and $d \neq 0$, suppose the equation
\[
X^4 - 2bX^2Y^2 + (b^2 - 4d)Y^4 = Z^2,
\]
has a solution with $X, Y$ and $Z$ positive integers with $(X, Y) = 1$. Then there are integers $a$ and $c$ such that $ac = d$ and positive, pairwise coprime integers $x, y$ and $z$ such that
\[
ax^4 + bx^2y^2 + cy^4 = z^2,
\]
where $(X, Y, Z) = (z, xy, |ax^4 - cy^4|)$.

Proof: $(X, Y) = 1$ and therefore $(Y, Z) = 1$. Then
\[
(X^2 - bY^2)^2 - Z^2 = 4d
\]
FERMAT AND THE DIFFERENCE OF TWO SQUARES 485

\[
\Rightarrow \left( \frac{X^2 - bY^2 - Z}{2} \right) \left( \frac{X^2 - bY^2 + Z}{2} \right) = dY^4.
\]

The two bracketed expressions differ by \(Z\) and are therefore integers having no mutual common factor with \(Y\). Hence there are integers \(a\) and \(c\) and coprime positive integers \(x\) and \(y\) such that

\[
ac = d, \quad Y = xy \quad \text{and} \quad \left\{ \frac{X^2 - bY^2 \pm Z}{2} \right\} = \{ax^4, cy^4\}
\]

\[
\Rightarrow Z = |ax^4 - cy^4| \quad \text{and} \quad ax^4 + cy^4 = X^2 - bY^2
\]

\[
\Rightarrow ax^4 + bx^2y^2 + cy^4 = z^2, \quad \text{where} \quad z = X.
\]

Hence \((X, Y, Z) = (z, xy, |ax^4 - cy^4|)\) and \((x, z) = 1\) since \((X, Y) = 1\).

Now suppose either \(a\) or \(c\) is a square number. Since \(ax^4\) and \(cy^4\) are interchangeable in the above proof we can assume that \(a\) is a square. Furthermore, if both \(a\) and \(c\) are square numbers then we can assume that \(a \leq c\). Good use of this final point will be made in Section 6.

We can now combine Lemmas 4 and 5 to establish the relevant process of descent into. For any positive integer solution we use Lemma 3 to obtain a solution in positive and pairwise coprime integers. Then Theorem 1 allows us to reverse the process introduced in Section 2.

**Theorem 1:** Let \(a, b\) and \(c\) be integers such that \(d \neq 0\) and \(b^2 - 4d \neq 0\), where \(d = ac\). If \(a\) is a square and if there is a positive and pairwise coprime integer solution of equation (1), then there is a positive and pairwise coprime integer solution of equation (2), with \(AC = b^2 - 4ac\). If \(A\) is a square and if there is a positive and pairwise coprime integer solution of equation (2), then there is a positive and pairwise coprime integer solution of equation (2), with \(a'c' = d\). The solution of (1) can be generated from the solution of (3) as shown in Figure 5.

\[
\begin{align*}
ax^4 + bx^2y^2 + cy^4 &= z^2, \quad ac = d \\
2x\sqrt{a} &= (y, 2)Z \\
y &= (y, 2)XY \\
4z\sqrt{a} &= (y, 2)\sqrt{AX^4 - CY^4} \\
AX^4 - 2bX^2Y^2 + CY^4 &= Z^2, \quad AC = b^2 - 4d \\
X\sqrt{A} &= z' \\
Y &= x'y' \\
Z\sqrt{A} &= |a'(x')^4 - c'(y')^4| \\
d' (x')^4 + b' (x')^2(y')^2 + c'(y')^4 &= (z')^2, \quad a'c' = d
\end{align*}
\]

**FIGURE 5**
Proof: First consider a positive and pairwise coprime integer solution \((X, Y, Z)\) of equation (2), with \(A\) a square. Then \((Y, Z) = 1\) and so \((Y, AX) = 1\). By Lemma 4, \(\left(X\sqrt{A}, Y, Z\sqrt{A}\right)\) is a solution of \(x^4 - 2bxy^2 + ACy^4 = z^2\). Since \((X\sqrt{A}, Y) = 1\), Lemma 5 can now be applied to give the required solution.

Now consider a positive and pairwise coprime integer solution \((x, y, z)\) of equation (1), with \(a\) a square. Then \(\left(\frac{2x}{y}, \frac{y}{2}, \frac{4z}{y}\right)\) is a positive and pairwise coprime integer solution of the equation \(ax^4 + 4bx^2y^2 + 16cy^4 = z^2\). The proof now follows as in the above treatment of equation (2).

In Theorem 1, equations (1) and (3) are of the same form and so Theorem 1 can be applied repeatedly unless and until an equation is obtained such that the coefficients of \(x^4\) and \(y^4\) are both non-squares.

As noted earlier, when one of the coefficients is a square there is no loss of generality in supposing that it is the coefficient of \(x^4\) which is square. Also as noted earlier, when both of the coefficients are squares there is no loss of generality in supposing that the coefficient of \(x^4\) is no greater than the coefficient of \(y^4\).

When Theorem 1 is applied repeatedly, the value of \(y\) is non-increasing as one proceeds down the diagram. It was in just such a situation as this that Fermat famously wrote:

"... there cannot be an infinite series of [positive integers] smaller than any given integer we please. The margin is too small to enable me to give the proof completely and with all detail." [2, p. 293].

For the equations of Theorem 1, there are therefore just two possibilities:

- there is a loop of solutions with \(y\) constant;
- all the solutions are generated from positive integer solutions of equations of the form

\[Ax^4 + Bx^2y^2 + Cy^4 = z^2,\]

where neither \(A\) nor \(C\) are squares and where either \(B = b\) and \(AC = ac\) or \(B = -2b\) and \(AC = b^2 - 4ac\).

As we shall see in Section 6, the first of these possibilities occurs relatively rarely. For now it is sufficient to note that the equations that arise from this possibility can be dealt with very easily.

**Lemma 6:** If the equations of Theorem 1 have a loop of solutions with \(y\) constant, then there is a solution, with \(y\) odd, of a deterministic equation of the form \(a + by^2 + \frac{d}{y}y^4 = A\), where \(a\) is a square factor of \(d\) and \(A\) is a square factor of \(b^2 - 4d\).
Proof: Using the notation of Theorem 1, for \( y \) to be constant, we must have \((y, 2) = X = x' = 1\).

Then \( \sqrt{A} = z' \) and equation (3) is an equation of the required form.

Theorem 1 therefore enables us to restrict our attention to equations of the form \( ax^4 + bx^2y^2 + cy^4 = z^2 \), where neither \( a \) nor \( c \) is a square. For such an equation, modular arithmetic can often be used to good effect. This will prove extremely useful in the later sections of this paper.

5. Fermat's last theorem for \( n = 7 \)

The proof of Lemma 7 provides a good illustration of how the methods of Section 4 can be applied to specific equations.

Lemma 7: The equation \( 7^2x^4 + 6.72x^2y^2 - 7y^4 = z^2 \) has no solution in positive integers.

Proof: From Lemma 3, Theorem 1 and Lemma 6, it is sufficient to check three cases:

- \( a - 3.7^2y^2 + cy^4 = A, ac = 2^4.7^3, A \) is a square factor of \(-7^3\) and \( y \) is odd.

All odd square numbers are congruent to 1 modulo 8 and so \( a - 3 + c \equiv 1 \pmod{8} \) i.e. \( a + c \equiv 4 \pmod{8} \). Since 16 is a factor of \( ac \) both \( a \) and \( c \) would have to be multiples of 4 with one being a multiple of 8. This contradicts the fact that 32 is not a factor of \( ac \).

- \( ax^4 - 3.7^2x^2y^2 + cy^4 = z^2, ac = 2^4.7^3, \) neither \( a \) nor \( c \) is square.

\( z^2 \) is positive and so \( a \) and \( c \) must both be positive. If both \( a \) and \( c \) were even, then \( x^2y^2 \equiv z^2 \pmod{2} \) and so \( x, y \) and \( z \) would all be odd. Then \( a + c \equiv 4 \pmod{8} \) leads to a contradiction, as above. Therefore \( 2^4 \) divides \( a \) or \( c \) and one of these must be a square.

- \( ax^4 + 6.7^2x^2y^2 + cy^4 = z^2, ac = -7^3, \) neither \( a \) nor \( c \) is square.

\( 7^2 \) is a factor of precisely one of \( a \) or \( c \) and, without loss of generality, we can suppose \( 7^2 \) is a factor of \( c \). Then \( z^2 \equiv ax^4 \pmod{7^2} \). Now 7 cannot be a common factor of \( x \) and \( z \) and \( 7^2 \) is not a factor of \( a \). Therefore \( a \) is a non-zero square modulo 7. Then \( a = 1 \) a square.

We are now in a position to give an elementary proof of Fermat's last theorem in the case \( n = 7 \). The following proof is a simplified version of Genocchi's proof as given in [4, pp. 57-62].

Theorem 2: The equation \( x^7 + y^7 + z^7 = 0 \) has no solution in non-zero integers.
Proof: Suppose \( x, y \) and \( z \) to be such a solution. Denote the symmetric functions \( \Sigma x, \Sigma xy \) and \( xyz \) by \( p, q \) and \( r \) respectively, and denote \( \Sigma x^i \) by \( s_i \).

Without loss of generality we can suppose \( x \) and \( y \) to be positive and then \( |z|^7 = x^7 + y^7 < (x + y)^7 \) and so \( |z| < x + y \) and \( p \neq 0 \).

The \( s_i \) satisfy Newton's identities

\[
s_i + 3 = ps_{i+2} - qs_{i+1} + rs_i.
\]

Define \( t_i = \frac{s_i}{p^i}, Q = \frac{q}{p^i} \) and \( R = Q - \frac{r}{p^i} \). Then the \( t_i \) satisfy the equation

\[
t_i + 3 = t_{i+2} - Qt_{i+1} + (Q - R)t_i.
\]

Then

\[
\begin{align*}
t_0 &= 3, \\
t_1 &= 1, \\
t_2 &= 1 - 2Q, \\
t_3 &= 1 - 3R, \\
t_4 &= 1 - 4R + 2Q^2, \\
t_5 &= 1 - 5R + 5RQ, \\
t_6 &= 1 - 6R + 6RQ - 2Q^3 + 3R^2, \\
t_7 &= 1 - 7R(1 - Q + Q^2) + 7R^2 = 0
\end{align*}
\]

Let \( 1 - 2Q = \frac{u}{v} \), where \( u \) and \( v \) are non-zero integers. Then

\[
4 - 7R\left(\frac{u^2}{v^2} + 3\right) + 28R^2 = 0.
\]

The discriminant of this quadratic in \( R \) is \( 7^2\left(\frac{u^2}{v^2} + 3\right)^2 - 448 \). This must be a rational square and so \( 7^2u^4 + 6.7^2u^2v^2 - 7v^4 \) is an integer square.

By Lemma 7 this is not possible and so the equation \( x^7 + y^7 + z^7 = 0 \) has no solution in non-zero integers.

6. The congruent number problem

As we saw in Section 3, solving Fibonacci's problem was equivalent to finding a right-angled triangle with rational sides and area 5. The triangle corresponding to the solution we found (see Figure 6) was actually a scaled version of the familiar \((9, 40, 41)\) triangle.

![Figure 6](https://example.com/figure6.png)

\[
\text{Area} = \frac{1}{2} \times \frac{9}{6} \times \frac{41}{6} = 5.
\]
A positive integer which can be expressed as the area of a right-angled triangle with rational sides is called a congruent number and the general problem of determining which positive integers are congruent numbers is called the congruent number problem. If a number, \( n \), is a congruent number, then any positive integer which is a multiple of \( n \) by a rational square is also a congruent number. Thus we need only consider square-free integers.

The congruent number problem is thus equivalent to the problem of finding solutions in positive integers of the equation \( x^4 + 4n^2y^4 = z^2 \) (see Figure 7).

Pythagorean triples can be used to find specific examples of congruent numbers. For example, the three smallest congruent numbers are 5, 6 and 7; which are obtained from the (9, 40, 41), (3, 4, 5) and (175, 288, 337) triangles, respectively. Fermat himself had made some progress on the opposite problem of determining numbers which are not congruent numbers. For example, the results of [1] show that no number which is a square or twice a square is a congruent number. Although the congruent number problem has still not been completely solved, extensive progress on this problem has been made in recent times through the connection with elliptic curves [6, pp. 3-7].

So far in this article, the method of applying descente together with the difference of two squares has been applied to specific individual equations. We shall now show that the method can be applied in a more general manner by considering three results from the theory of congruent numbers.

**Theorem 3**: Any congruent number, \( n \), can be expressed as the area of infinitely many different right-angled triangles with rational sides.

**Proof**: We can suppose that \( n \) is square-free. Suppose further that it is the area of only finitely many different right-angled triangles with rational sides.

If \( n \) is odd, then Theorem 1 can be applied to the equations \( x^4 - n^2y^4 = z^2 \) and \( x^4 + n^2y^4 = z^2 \). From Lemma 6, there is a solution, with \( y \) odd, of an equation of the form \( a - \frac{a^2}{4}y^4 = A \), where \( a \) is a square factor of \( n^2 \) and \( A \) is a square factor of \( 4n^2 \). Then \( a \) and \( \frac{a^2}{4}y^4 \) are odd squares and are therefore congruent to 1 modulo 8. Then \( A \) is divisible by 8 and therefore \( 4n^2 \) is divisible by 8 a contradiction.

Now suppose that \( n \) is even. Then \( n = 2m \) where \( m \) is odd. Theorem 1 can then be applied to the equations \( x^4 + m^2y^4 = z^2 \) and \( x^4 - 4m^2y^4 = z^2 \).
From Lemma 6, there is a solution, with $y$ odd, of an equation of the form $a + \frac{m^2}{a}y^4 = A$, where $a$ is a square factor of $m^2$ and $A$ is a square factor of $4m^2$. Then $A \equiv 2 \pmod{8}$ and $A$ cannot be a square, a contradiction.

**Theorem 4**: No prime of the form $8n + 3$ can be the area of a right-angled triangle with rational sides.

**Proof**: Suppose that such a triangle does exist. Then there is a positive integer solution of the equation $x^4 - p^2y^4 = z^2$. By Theorems 1 and 3, this solution is part of a descending and terminating sequence of solutions. We shall make use of the elementary fact that neither $-1$ nor $2$ is a square modulo $p$ to prove that there is no such sequence.

The penultimate term in the sequence is a pairwise coprime solution to an equation $AX^4 + CY^4 = Z^2$, where $A$ is square and $AC = 4p^2$ or $-16p^2$. Then $p^2$ divides either $A$ or $C$ and $p$ is not a factor of $Z$. If $p^2$ divides $A$, then $C$ is a square modulo $p$ and so $\frac{AC}{p^2}$ is a square modulo $p$. Therefore $AC = 4p^2$. Then both $A$ and $C$ are squares, contradicting the fact that $A > C$. We can therefore conclude that $p$ is not a factor of $A$.

The final term of the sequence is a pairwise coprime solution to an equation $ax^4 + cy^4 = z^2$, where neither $a$ nor $c$ is a square and $ac = 4p^2$ or $-p^2$. Furthermore, $Z\sqrt{A} = |ax^4 - cy^4|$, where $p$ is not a factor of $Z\sqrt{A}$. Hence $p^2$ divides either $a$ or $c$. The only possibility is $2x^4 + 2p^2y^4 = z^2$, contradicting the fact that $2$ is not a square modulo $p$.

The following theorem can be proved in a very similar way, making use of the fact that, for a prime $p$ of the form $8n + 5$ neither $-2$ nor $2$ is a square modulo $p$. The proof is left as an exercise for the reader.

**Theorem 5**: For $p$ a prime of the form $8n + 5$ the area of a right-angled triangle with rational sides cannot be $2p$.

**7. Concluding remarks**

We have seen how relatively sophisticated results can be obtained using the elementary idea of the difference of two squares, when used in conjunction with Fermat's method of descente infinie.

An interesting comment on one particular use of descente infinie in [5] was that it was 'nothing other than induction'. This raises the general issue of precisely how we should consider the relationship between the three methods of proof known as:

- proof by induction;
- proof by contradiction or reductio ad absurdum;
- descente infinie.

The method of proof by contradiction is often greatly strengthened by considering not just any counterexample but one which in some regard is minimal. Induction itself can then be seen as 'nothing other than' a highly
stylised form of proof by minimal counterexample. Furthermore, rather than using descente infinie to produce an infinitely descending series of counterexamples, it is often more sensible to assume from the outset a minimal counterexample.

Thus we can view proof by minimal counterexample as the generic method underlying both descente infinie and induction. However, as we have seen in this article, this is not the whole story. Fermat's method is important for proving some equations to be insoluble but it is also extremely useful for generating solutions to others.

It is difficult to argue with Lagrange's view of descente as:

"...one of the most fruitful methods in the whole theory of numbers." [2, p. 300].

References


STAN DOLAN
126A Harpenden Road, St. Albans, Herts AL3 6BZ