

# Infinite Descent – but not into Hell!

*Shailesh A Shirali*



Shailesh Shirali has been at the Rishi Valley School (Krishnamurti Foundation of India), Rishi Valley, Andhra Pradesh, for more than ten years and is currently the Principal. He has been involved in the Mathematical Olympiad Programme since 1988.

## Induction and Descent: Complementary Principles

Everyone knows the principle of mathematical induction (PMI for short); it is now standard fare even at the high-school level. Curiously, very few seem to know its close relative { the principle of descent (PD for short); curious, because the two principles are complementary to one another. In this article we study some typical applications of this principle.

The PMI states the following. Let  $S$  be a subset of the set of natural numbers  $N$  with the property that (a)  $1 \in S$ , and (b) if  $k \in S$ , then  $k + 1 \in S$  too. Then it must be the case that  $S = N$ . It can be stated in 'contrapositive form' too. Let  $S$  be a subset of the set of natural numbers  $N$  with the property that (a)  $1 \in S$ , (b) if  $k \notin S$  for some  $k \in N$ ,  $k > 1$ , then  $k - 1 \notin S$ . Then it must be the case that  $S = N$ . The PMI looks 'obvious' but it possesses surprising power, and a great many non-trivial results owe their proofs to it. For a survey of some applications, see [1].

The principle of descent, which was first enunciated and used by Fermat, may be stated in various equivalent ways, e.g.:

1. It is not possible to have an infinite, monotonically decreasing sequence of positive integers.
2. Let  $S$  be a non-empty subset of the set of natural numbers with the property that for any positive integer  $k$  greater than 1, if  $k \in S$  then  $k - 1 \in S$  too. Then it must be the case that  $1 \in S$ .
3. Let  $S$  be a subset of the set of natural numbers with the property that  $1 \notin S$ , and for any positive integer  $k$ ,

### Keywords

Descent, induction, irrationality, regular polygons.



if  $k \in S$  then  $k + 1 \in S$  too. Then  $S$  is the empty set.

The close relationship of these statements to the PMI is easy to see.

Inasmuch as the PMI and the PD are equivalent, it may be wondered whether it is worth our while making a separate study of proofs based on the PD. The answer is: most assuredly, yes! { one must not conceal the richness of the particular under the cloak of the general! Accordingly, we now present various 'case studies' that show the descent principle in action.

### The Unit Fraction Algorithm

Fractions with unit numerator are known as unit fractions, or (more exotically) as Egyptian fractions, because of the practice in ancient Egypt of representing fractions as sums of distinct unit fractions. Thus,  $\frac{5}{13}$  would be written as

$$\frac{5}{13} = \frac{1}{3} + \frac{1}{20} + \frac{1}{780}.$$

It is easy to show that every positive rational number between 0 and 1 can be written in this way, and the algorithm to do so is particularly nice; we simply peel off the largest unit fraction not greater than the given fraction, then do the same for the portion remaining, and so on, recursively. We shall show via the PD that this process necessarily terminates, and so yields the desired representation. (For example, for the fraction  $\frac{5}{13}$ , we first peel off  $\frac{1}{3}$ . The portion left is  $\frac{2}{39}$ , from which we peel off  $\frac{1}{20}$ . Now the portion left is  $\frac{1}{780}$ , itself a unit fraction. So  $\frac{5}{13} = \frac{1}{3} + \frac{1}{20} + \frac{1}{780}$ , as given above.)

The validity of the algorithm may be shown as follows. Let  $r$  be any rational number between 0 and 1, say  $r = \frac{a}{b}$ , where  $a, b$  are integers with  $0 < a < b$ . Let the

Every rational number between 0 and 1 can be represented as a sum of distinct Egyptian fractions.



The algorithm described here for expression as a sum of Egyptian fractions is called the greedy algorithm. There are many algorithms of this kind to be found in mathematics e.g., some implementations of the simplex method used to solve linear programs.

positive integer  $n$  be (uniquely) fixed by the condition

$$\frac{1}{n} \cdot \frac{a}{b} < \frac{1}{n+1}$$

If equality holds on the left side, then there is nothing more to be done. If not, let  $s = r - \frac{1}{n}$ ; then

$$s = \frac{a}{b} - \frac{1}{n} = \frac{na - b}{nb}$$

By definition  $0 < na - b < a$ , so the numerator of  $s$  is strictly less than that of  $r$ . If  $s$  is a unit fraction, then we are through. If not, we repeat the process with  $s$  in place of  $r$  and obtain another fraction  $t$  with a smaller numerator; and so we proceed. As the numerators of  $r; s; t; \dots$  form a strictly decreasing sequence of positive integers, the descent must come to a halt sooner or later. The desired representation is now at hand.

We make the following remarks before moving on. (a) While the above algorithm certainly yields a representation in the desired form, it does not always do so in the most economical way, i.e., with the least number of summands. (Work out the algorithm with  $r = \frac{47}{60}$  and check for yourself!) (b) The above algorithm, for obvious reasons, is called a 'greedy algorithm'. There are many algorithms of this kind to be found in mathematics (e.g., some implementations of the simplex method used to solve linear programs). (c) A similar analysis can be made for the well-known algorithm of Euclid's that yields the GCD of two given whole numbers; here the step carried out repeatedly is

$$(a; b) \nabla (b; \text{Rem}(a \nabla b));$$

( $\text{Rem}(a \nabla b)$  refers to the remainder when  $a$  is divided by  $b$ ). The remainders form a strictly decreasing sequence of non-negative integers, which therefore must reach 0 at some stage; termination of the algorithm is assured because of this.



## Proofs of Irrationality of Certain Numbers

The classic proof of the irrationality of  $\sqrt{2}$ , due to the Pythagorean school, is well known; it depends ultimately on the fundamental theorem of arithmetic ('prime factorization in  $\mathbb{N}$  is unique'). Much less well known is the proof by descent; its surprising feature is that unique factorization is not used anywhere. Here are the details.

Assuming that  $\sqrt{2}$  is rational, let  $\sqrt{2} = \frac{a}{b}$  where  $a, b$  are positive integers. The equation yields  $b^2 = 2a^2$ , so it follows that the set

$$S = \{n \in \mathbb{N} : n^2 \text{ is an integer}\}$$

is non-empty. Now observe that if  $b \in S$  then  $b^2 \in S$  too, because

$$\frac{b^2}{2} = \frac{2a^2}{2} = a^2 \text{ integer} \Rightarrow \frac{b^2}{2} \in \mathbb{N}$$

also,  $b^2 \in S$  ( $b^2 = b^2(1)$ ) is less than  $b$ . It follows that for each number in  $S$ , there exists another one, smaller than itself. Now we invoke the PD to deduce that  $S$  is empty, in other words that  $\sqrt{2}$  is irrational.

Other square-root irrationalities may be shown in like manner. Thus, to show the irrationality of  $\sqrt{K}$ , where  $K \in \mathbb{N}$  is not square, we let  $c = \lfloor \sqrt{K} \rfloor$ ; then if  $b \in \mathbb{N}$  is such that  $b^2 < K < (b+1)^2$ , the number  $b^2 - K$  is a positive integer smaller than  $b$ . So, by the PD,  $\sqrt{K}$  is irrational.

It may not be too obvious how one could show the irrationality of, say, the cube root of 2 using descent; but see the section on polynomials with integral coefficients.

### Irrationality { Through Geometry!

In some cases a descent proof of irrationality has an elegant geometric analogue. Consider for example the number  $\sqrt{2}$ .



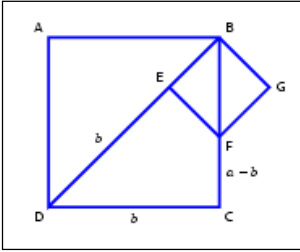


Figure 1.

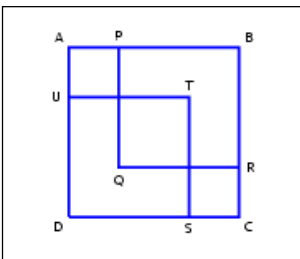
Suppose that  $\sqrt{2}$  is rational; then there exist positive integers  $n$  such that  $n\sqrt{2}$  is integral, so the set  $S$  of positive integers  $n$  such that the diagonal of a square of side  $n$  has integral length is non-empty. Let  $b \in S$ , and let  $ABCD$  be a square with side  $b$ ; then the diagonal  $DB$  has length  $b\sqrt{2} = a$ , say (see Figure 1). Locate a point  $E$  on  $DB$  such that  $DE = b$ ; then  $BE = a - b$ . Construct a square  $BEFG$  on side  $BE$ ; then  $EF = a - b$ . Triangles  $DEF$  and  $DCF$  are congruent, so  $CF = EF = a - b$ , therefore  $BF = b - (a - b) = 2b - a$ . It follows that  $BEFG$  is an integer-sided square whose diagonal has integral length, and it is smaller than the square we started with. Now we invoke the PD to conclude that such a situation is untenable; the irrationality of  $\sqrt{2}$  follows.

Here is another such proof, even simpler than the one above (it was featured in [3]). Suppose that  $\sqrt{2} = \frac{a}{b}$  where  $a, b \in \mathbb{N}$ . Let  $ABCD$  be a square of side  $a$ . Draw squares  $BPQR$  and  $DSTU$  each with side  $b$  inside square  $ABCD$  (see Figure 2). The equation  $a^2 = 2b^2$  implies that the area of square  $ABCD$  is the sum of the areas of squares  $BPQR$  and  $DSTU$ . This means that the area of the central square, with side  $b - (a - b) = 2b - a$ , equals the sum of the areas of the two small squares at the corners (with side  $a - b$ ); so  $\sqrt{2} = \frac{(2b - a)}{(a - b)}$ . Now we invoke the PD as earlier to reach the same conclusion.

### Irrationality of the Golden Ratio

The same idea can be used to show the irrationality of the 'golden ratio'  $\phi$  (the number  $\phi = \frac{1}{2}(\sqrt{5} + 1)$ ). Here we use the fact that in a regular pentagon, the ratio of the diagonal to the side is  $\phi$ . Suppose that  $\phi$  is rational, say  $\phi = \frac{a}{b}$ , where  $a, b \in \mathbb{N}$ . Let  $ABCDE$  be a regular pentagon with side  $b$ ; then each diagonal has length  $a$ . Let the diagonals  $AC, BD, CE, DA, EB$  be drawn. Each diagonal gets divided into three parts, with lengths

Figure 2.



$x; y; x$ , say, where  $y < x$  (the length of the small portion in the middle is  $y$ ). We see that  $b = x + y$  and  $a = 2x + y$ . Solving for  $x; y$  we get  $x = \frac{a}{3} - \frac{b}{3}$  and  $y = \frac{2b}{3} - \frac{a}{3}$ ; so  $x$  and  $y$  are integers! The (small) inner pentagon is now seen to be integer-sided (with side  $y$ ), and its diagonal has integral length (equal to  $x$ ). Now using this observation recursively, we get an endless sequence of smaller and smaller integer-sided regular pentagons, clearly an impossibility.

### Regular Polygons in Lattices

We shall show the following non-existence results in this section.

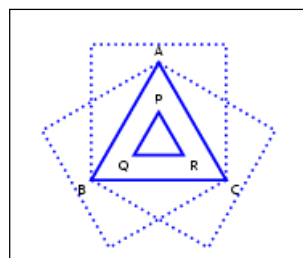
(a) An equilateral triangle cannot be imbedded in the square lattice  $L = \mathbb{Z}^2$ . In other words, it is not possible to find distinct lattice points  $A; B; C$  in the coordinate plane  $\mathbb{R}^2$  such that triangle  $ABC$  is equilateral.

(b) A square similarly cannot be imbedded in an equilateral lattice.

To prove (a), we use the observation that a quarter-turn centered at any point of the square lattice  $L$  maps the lattice back onto itself.

Suppose that there exists an equilateral triangle  $ABC$  with  $A; B; C$  distinct points of  $L$ . Let its side be  $s$ . Consider the squares erected on sides  $BC; CA; AB$  respectively, each one overlapping with the given triangle; let their centers be  $P; Q; R$  (see Figure 3). The vertices of the squares lie at lattice points, so the coordinates of  $P; Q; R$  are half-integers. Triangle  $PQR$  is clearly equilateral. Computations show that its side  $t$  is  $\frac{1}{2}(\sqrt{3} - 1)s$ . An enlargement about the origin by a factor of 2 now yields a lattice point equilateral triangle  $P^0Q^0R^0$ , with side  $t^0 = (\sqrt{3} - 1)s \approx 0.73s$ . We thus get another lattice point equilateral triangle, with sides less than  $\frac{3}{4}$  of the original one. Recursively continuing this process, we get an infinite sequence of lattice point equilateral triangles,

Figure 3.



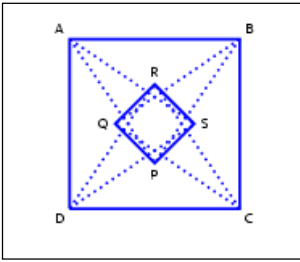


Figure 4.

with side tending to 0. This is clearly not possible. We conclude that such triangles do not exist at all.

The proof of (b) is similar; now we use the observation that a  $60^\circ$  turn about any point of an equilateral lattice E maps the lattice back onto itself.

Suppose that ABCD is a square with A; B; C; D  $\in$  E; let its side be s. We locate points P; Q; R; S within the square such that triangles PAB, QBC, RCD, SDA are equilateral (see Figure 4); then P; Q; R; S are lattice points, and PQRS is a square. Computations show that its side is  $(\sqrt{3} - 1)s = \frac{1}{2}(\sqrt{3} - 1)s$ . Now arguing as we did earlier, we conclude that a square cannot be imbedded in E.

We leave it to the reader to find a proof by descent showing that the lattice L does not contain a regular n-sided polygon for any  $n > 4$ .

In the three-dimensional lattice  $Z^3$ , equilateral triangles do indeed exist; e.g., the triangle with vertices at (1; 0; 0), (0; 1; 0) and (0; 0; 1) is equilateral! The reader should find out why and where the proof given above fails in this case.

### Diophantine Equations

There are many diophantine equations which possess no solutions in integers and sometimes the non-existence of solutions may be shown in a nice manner via the PD. We consider two examples.

(a) The equation  $x^2 + y^2 + z^2 = 2xyz$  possesses no solution in positive integers.

Suppose that there exist positive integers x; y; z such that  $x^2 + y^2 + z^2 = 2xyz$ . Then either just one or all three of x; y; z are even. If just one of them were even, then we would have  $2xyz \equiv 0 \pmod{4}$ ,  $x^2 + y^2 + z^2 \equiv 2 \pmod{4}$ , an absurdity; so all of x; y; z must be even. Write  $(x; y; z) = 2(a; b; c)$ ; then a; b; c are positive inte-



gers and  $4(a^2 + b^2 + c^2) = 16(abc)$ , so  $a^2 + b^2 + c^2 = 4abc$ . The argument just given can now be repeated verbatim to conclude that  $a; b; c$  themselves are even integers. Using this step recursively and invoking the PD, we deduce the stated assertion.

(b) The equation  $x^2 + y^2 = 3z^2$  possesses no solution in positive integers.

Suppose that  $x; y; z$  are positive integers satisfying the given relation. Since  $3 \mid 3z^2$ , if one of  $x; y$  is a multiple of 3, then the other one must be, too. If neither of  $x; y$  is a multiple of 3, then we get  $x^2 + y^2 \equiv 2 \pmod{3}$ , which cannot be, so  $3 \mid x; y$  and therefore  $9 \mid x^2 + y^2$ . This implies that  $3 \mid z$ , so  $3 \mid x; y; z$ . Writing  $(x; y; z) = 3(a; b; c)$ , where  $a; b; c$  are positive integers, we get  $a^2 + b^2 = 3c^2$ , and now the same reasoning applies all over again, verbatim. The stated assertion follows.

### Polynomials with Integral Coefficients

Here is a proposition about polynomials over  $\mathbb{Z}$  that we prove using descent: If  $\alpha$  is a rational root of a monic polynomial  $f$  with integral coefficients, then  $\alpha$  is an integer.

Suppose not; let  $\alpha$  be a rational but non-integral root of a monic  $n^{\text{th}}$  degree polynomial with integral coefficients. The following statements may now be made: (i)  $\alpha^n$  and all higher powers of  $\alpha$  are integral linear combinations of  $\alpha^i$  for  $i = 0, 1, 2, \dots, n-1$ ; (ii) there exists a positive integer  $k$  such that  $k\alpha^i$  is integral for  $i = 0, 1, 2, \dots, n-1$ ; (iii) the set of natural numbers  $k$  such that  $k\alpha^i$  is an integer for all natural numbers  $i$  is nonempty; (iv) for any element  $k$  of this set, the number  $k^0 = k(\alpha; \alpha)$  is a positive integer smaller than  $k$ , and with the same property. Now, via the PD, we are done.

An immediate corollary of this result is that any number of the form  $n^{1/k}$ , with  $n; k \in \mathbb{N}$ , is either an integer or is irrational; it cannot be a non-integral rational number.

Any number of the form  $n^{1/k}$ , with  $n, k \in \mathbb{N}$ , is either an integer or is irrational; it cannot be a non-integral rational number.



## Two IMO Problems

We top off this survey of case studies with two challenging and pretty problems from the International Mathematical Olympiads of 1986 and 1988 (held in Poland and Australia, respectively). The latter problem was considered for long to be the most difficult problem ever to be asked in an IMO. (However, it has since lost this title!)

### IMO 1986/3.

To each vertex of a regular pentagon an integer is assigned in such a way that the sum of all the negative numbers is positive. If three consecutive vertices are assigned the numbers  $x; y; z$  respectively and if  $y < 0$ , then the following operation is allowed: the numbers  $x; y; z$  are replaced by  $x + y; |y|; z + y$ , respectively. Such an operation is performed repeatedly as long as at least one of the negative numbers is negative. Determine whether this procedure necessarily comes to an end after a finite number of steps.

We note first that the sum  $s$  of the numbers at the vertices stays the same all through, because  $(x + y) + (|y|) + (z + y) = x + y + z$ .

Experimentation suggests that the procedure cannot be continued indefinitely. If we are to prove that the procedure necessarily terminates, we must find a non-negative integer-valued function of the vertex numbers that strictly decreases at each stage. Finding such a function entails a bit of hit-and-trial, but in the end we obtain the following candidate for the function,  $f$ : if the numbers at the vertices are  $x; y; z; u; v$ , read in cyclic order, then

$$f(x; y; z; u; v) = (x - z)^2 + (y - u)^2 + (z - v)^2 + (u - x)^2 + (v - y)^2.$$

Observe that  $f$  is non-negative and integer-valued, as required.

Assuming that  $y < 0$ , let the step  $(x; y; z; u; v) \rightarrow (x +$



$y; i; y; z + y; u; v$  be performed. Let us now see what effect it has on  $f$ . We have,

$$f(x + y; i; y; z + y; u; v) = (x - z)^2 + (u + y)^2 + (z + y - v)^2 + (x + y - u)^2 + (v + y)^2:$$

Simplifying, we get the following expression for  $\Delta f$ , the change in  $f$ :

$$\Delta f = 2y(x + y + z + u + v) = 2ys < 0 \quad (\text{since } s > 0; y < 0):$$

It follows that the  $f$ -value strictly decreases as a result of the operation. So the operation cannot be performed infinitely often; sooner or later the numbers at the vertices will all be non-negative.

Remark. What happens if the numbers placed at the start at the vertices are not integers? So long as they are rational, exactly the same idea works (we simply scale up everything by the LCM of the denominators). But what happens if some of the numbers are not rational? It turns out that in this case too the procedure must terminate; however, the proof has to be worded very differently now. Here is a possible approach. Let the vertices be numbered 0, 1, 2, 3, 4, let the label on vertex  $i$  be  $x_i$ , and for  $i = 0, 1, 2, 3, 4$  and  $j > i$  let the sums  $a_{i;j}$  be computed as follows:

$$a_{i;j} = x_i + x_{i+1} + \dots + x_{j-1};$$

with  $x_5 = x_0, x_6 = x_1$ , and so on. Note that there are infinitely many such sums, but only a finite number of them can be negative, because on cycling around the full set of vertices we add  $s$  to the sum, and  $s$  is positive.

Now suppose that  $x_r < 0$  and  $(x_{r-1}; x_r; x_{r+1}) \nabla (x_{r-1} + x_r; i; x_r; x_{r+1} + x_r)$ . Let us check what happens to the various sums  $a_{i;j}$ . For convenience we write  $b_{i;j}$  for the updated sums.



If all three indices  $r-1; r; r+1$  are part of the range  $[i; j]$ , or none of them is, then  $b_{i;j} = a_{i;j}$ . Now suppose that either one or two of the indices  $r-1; r; r+1$  are part of the range  $[i; j]$ . We now get:

$$b_{i;r} = a_{i;r} + x_r = a_{i;r+1}; \quad b_{i;r+1} = a_{i;r};$$

$$b_{i-1;r+1} = x_{r-1} = a_{r-1;r}; \quad b_{r;r+1} = j \cdot x_r = j \cdot a_{r;r+1};$$

We observe that in the infinite multiset of the sums  $a_{i;j}$ , most of the elements stay unchanged, some elements swap places with others, and precisely one element is replaced by its negative. As a negative number is replaced by a positive number each time, the sequence of operations necessarily terminates. Indeed, we can say more: the number of steps needed for termination does not depend on the order in which the steps are carried out! { it equals the number of negative elements in the initial multiset of values of  $a_{i;j}$ . An elegant and pretty result indeed.

Is this a proof by descent? Oh yes! { but the descent principle has been used in a rather more subtle manner.

IMO 1988/6.

Let  $a$  and  $b$  be positive integers such that the quantity

$$c = \frac{a^2 + b^2}{ab + 1}$$

is an integer. Show that  $c$  is a square.

Solution. We shall prove a stronger statement: Let  $a; b; c$  be positive integers such that  $1 \cdot a^2 + b^2 \mid abc \cdot c + 1$ ; then the quantity  $a^2 + b^2 \mid abc$  is a square.

Let  $d$  denote the value of  $a^2 + b^2 \mid abc$ ; thus  $1 \cdot d \cdot c + 1$ . If  $c = 1$  then  $d = 1$  or  $2$ . If  $d = 1$ , there is nothing to prove; and  $d = 2$  cannot happen at all, for  $a^2 + b^2 \mid ab$  is odd if at least one of  $a, b$  is odd, and is a multiple of 4 if  $a, b$  are both even. If  $c = 2$ , then the result follows



trivially, with  $d = (a - b)^2$ . In the discussion below we assume that  $c > 2$ .

If  $d = 1$ , there is nothing to prove. If  $d > 1$ , we consider the curve  $\Gamma_d \subset \mathbb{R}^2$  defined by

$$\Gamma_d := f(x; y) : x^2 + y^2 - cxy = d;$$

This is the equation of a hyperbola symmetric in the lines  $y = \pm x$ . Our interest lies in the lattice points on  $\Gamma_d$ , of which  $(a; b)$  is one such. The crucial observation that we make is this: from a single lattice point of  $\Gamma_d$  one can by descent generate infinitely many such points. The descent is accomplished as follows.

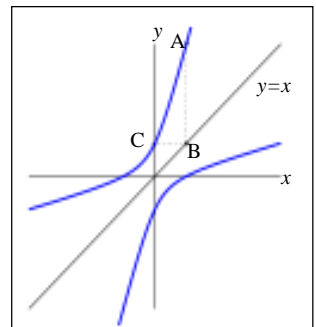
Let  $A(u; v)$  be a lattice point on the upper branch of  $\Gamma_d$ ; then  $v > u$ . We move vertically down from  $A$  to the line  $y = x$  (see Figure 5), meeting it at  $B(u; u)$ ; then we move horizontally (to the left) from  $B$  to  $\Gamma_d$ , meeting it at  $C$ . To find the coordinates of  $C$ , note that the image of  $A$  under reflection in the line  $y = x$  is the point  $A^0(v; u)$ . So one point of intersection of the curve and the line  $y = u$  is  $(v; u)$ ; that is, one root of the quadratic equation

$$x^2 - cux + (u^2 - d) = 0$$

is  $x = v$ . Since the sum of the roots of the equation is  $cu$ , the other root must be  $x = cu - v$ , implying that  $C = (cu - v; u)$ . Since  $c; u; v$  are integers, it follows that  $C$  is a lattice point. Note that  $C$  and  $A$  lie on the same branch of the curve.

So we have moved from the lattice point  $(u; v)$  to the lattice point  $(cu - v; u)$ ; this is the descent step, which we iterate. Each such step carries us from one lattice point of  $\Gamma_d$  to another one, on the same branch. As the curve has positive slope at every point, the movement results in a strict decrease in both coordinates. The descent results in an eventual passage into the third quadrant.

Figure 5.



The proof that the continued fraction approach yields all possible non-negative integral solutions to Pell's equation is another example of a task that can be accomplished elegantly via the PD.

Since  $d \cdot c + 1$ , the curve cannot have any lattice points in the interiors of the second and fourth quadrants; for if  $(x; y)$  were such a lattice point, then  $xy \cdot j \cdot 1$  and  $x^2 + y^2 \cdot 2$ , and so  $2 \cdot x^2 + y^2 = cxy + d \cdot 1$ , which is absurd.

Now it follows from the nature of the descent that we cannot jump from the interior of the first quadrant to the interior of the third quadrant in a single step; for if  $v > u > 0$  then the signs of the second coordinates in  $(u; v)$  and  $(cu \cdot j \cdot v; u)$  are both positive. Also, we are barred from entering the interior of the second quadrant. Therefore in order to reach the interior of the third quadrant, we must step upon both the x-axis and the y-axis, i.e., on the points  $(0; d)$ ,  $(j \cdot d; 0)$ , which consequently must be lattice points. It follows that  $d$  is a square.

Here is another (rather short) proof of the above assertion. We start with natural numbers  $a; b; c$  with  $a^2 + b^2 \cdot j \cdot abc (= t; \text{say})$  between 1 and  $c + 1$ .

If  $t$  is not a square, then  $a \notin b$ ; for  $a = b$  gives  $a^2(2j \cdot c) = t$  which gives in turn  $c = 1$  and  $t = a^2$ , a square.

Assume that it is possible to have  $t$  non-square; assume that the corresponding  $a > b$  has  $b$  the least possible (of course,  $b > 0$ ). Then the 'other' root  $d$  of the equation  $a^2 + b^2 \cdot j \cdot abc = t$ , viewed as a quadratic equation in  $a$ , satisfies the relations  $a + d = bc$ ,  $ad = b^2 \cdot j \cdot t$ . In particular,  $d$  is an integer.

If  $d < 0$ , then we get, in turn,  $db \cdot j \cdot 1$ ,  $dbc \cdot j \cdot c$ ,  $c \cdot j \cdot dbc$ ,  $c + 1 \cdot 1 \cdot j \cdot dbc$ . So  $d^2 + b^2 \cdot j \cdot dbc = t \cdot c + 1 \cdot 1 \cdot j \cdot dbc$ , i.e.,  $d^2 + b^2 \cdot 1$ , an impossibility; so  $d \cdot 0$ .

If  $d = 0$ , then we get  $t = b^2$ , a contradiction; so  $d > 0$ .

Now  $d = bc \cdot j \cdot a$ . If  $d \cdot b$ , then we get, in turn,  $bc \cdot j \cdot a \cdot b$ ,  $bc \cdot j \cdot a + b$ ,  $abc \cdot j \cdot a^2 + ab > a^2 + b^2$ . That is,  $a^2 + b^2 \cdot j \cdot abc < 0$ , which is not possible. Hence  $d < b$ .



Since  $1 \cdot b^2 + d^2 \mid dbc = t \cdot c + 1$ , we obtain a 'smaller' solution  $(b, d)$  in place of  $(a, b)$ , the value of  $t$  being non-square (it is the same  $t$ ). Now PD leads to a contradiction. It follows that  $t$  is a square.

### Family connections

There are many cousins to IMO 1988/6 (in its original form). The reader may enjoy trying to prove the following. (a) If  $a, b$  are positive integers such that the number  $c = (a^2 + b^2)/(ab + 1)$  is an integer, then  $c = 5$ . (b) If  $a$  and  $b$  are positive integers such that  $a^2 + b^2 \mid a$  is divisible by  $2ab$ , then  $a$  is a perfect square.

### Concluding Remarks

We have certainly not exhausted the list of applications of the principle of descent! Other elegant applications include the proof by Fermat of his claim that the equation  $x^4 + y^4 = z^2$  has no solutions in positive integers; the proof by Euler of Fermat's theorem stating that any prime of the form  $1 \pmod{4}$  is a sum of two squares; and the proof by Lagrange of his own theorem that every prime is a sum of four squares. (Euler knew of this result but was not able to prove it. Ironically, the method used by Lagrange is practically the same as that used by Euler to prove Fermat's claim.) (See [2] for details of both proofs.) The proof that the continued fraction approach yields all possible non-negative integral solutions to Pell's equation is another example of a task that can be accomplished elegantly via the PD. More applications could be catalogued, but we leave the task to the reader.

### Acknowledgements

Thanks are due to my friend and colleague Professor B Sury for several helpful suggestions that have been incorporated here.

### Suggested Reading

- [1] B Sury, *Mathematical Induction – an Impresario of the Infinite*, *Resonance*, Vol.3, pp. 69-76, 1998.
- [2] G H Hardy and E M Wright, *Introduction to the Theory of Numbers*, Cambridge University Press, 1960.
- [3] K Puly, *The square root by infinite descent*, *Resonance*, Vol.5, No.8, p.83, 2000.

#### Address for Correspondence

Shailesh A Shirali  
Rishi Valley School  
Chittoor District  
Rishi Valley 517 352  
Andhra Pradesh, India.

