Infinite Descent[*]

Graeme Taylor

March 3, 2006

Infinite Descent is a proof technique of use in solving problems from number theory, ranging from elementary problems to vital theorems of modern algebraic number theory. Infinite Descent was first described by name by the 17th century mathematician Fermat in the paper La mthode de la 'descente infinie ou indfinie.

Proof by Infinite Descent is a special case of proof by contradiction (reductio ad absurdum), although from a mathematical logic point of view it can be seen as equivalent to the axiom of induction, or the well-order property of the natural numbers. The technique is usually employed to demonstrate non-existence of collections of numbers with a particular property. To do so, it is shown that if one set exists, then another exists which is in some sense 'smaller'. In this way, infinitely many successively smaller collections can be found, yet the problem is posed in such a way that there cannot be infinitely many such collections- usually because of the existence of a bound. This is a contradiction, so the assumption of existence of a solution isn't tenable and we thus conclude no solutions exist.

This is probably best understood by way of an example. So consider the following problem:

Show that there is no quadruple (x, y, z, u) of positive integers satisfying

$$x^2 + y^2 = 3(z^2 + u^2)$$

The important thing here is that we are looking for positive integers - the counting numbers $1, 2, 3, \ldots$ - and thus an infinite descent cannot exist: a sequence of such values cannot keep strictly decreasing forever. By contrast, infinite strictly decreasing sequences of rational numbers or real numbers are not inherently paradoxical- the sequence obtained by successive halving $(1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots)$ being an example.

[*] First appeared on Everything2, at *http://www.everything2.com/index.pl?node_id=1790183*

Descent Proof

We proceed therefore to give a proof by infinite descent. Suppose we have four positive integer values x, y, z, u satisfying the required condition. Then, since $3(z^2 + u^2)$ is divisible by three, and $x^2 + y^2$ is equal to that expression, it must be that $x^2 + y^2$ is divisible by 3. Formally, we say that $x^2 + y^2$ is congruent to 0 mod 3, which is a fancy way of saying we are left with remainder 0 after division by 3.

An aside on working mod 3. Here a number is essentially either 0, 1 or 2: 3 is 0 mod 3 (as are 6,9,12 etc.) , 4 is 1 mod 3 (as are 7,10,13,etc) and so on. Addition works as usual except you discard multiples of 3, so, for example, $2 + 2 = 4 = 3 + 1$ *so* $2 + 2 = 1$.

Knowing that $x^2 + y^2 = 0$ mod 3, we conclude that one of three cases holds:

- Both x^2 and y^2 are 0 mod 3
- $x^2 = 1$ mod 3 and $y^2 = 2$ mod 3
- $x^2 = 2$ mod 3 and $y^2 = 1$ mod 3

However, you can easily verify (test all cases!) that the square of any number mod 3 is 0 or 1. That is, there are no numbers which square to 2 mod 3, so the second two cases above are impossible. We know therefore that x^2 and y^2 are both 0 mod 3, meaning they are divisible by 3.

But if the square of an integer can be divided by 3, then the integer itself can be divided by 3. So we can write $x = 3x'$ and $y = 3y'$ for some x' and y'. Since x and y were strictly positive, x' and y' are definitely smaller (x' being a third of x, y' a third of y). We can plug these new versions into the equation to get $(3x')^2 + (3y')^2 = 3(z^2 + u^2)$.

That simplifies to $3 \times 3(x'^2 + y'^2) = 3(z^2 + u^2)$, and cancelling a 3 from each side we get

$$3(x'^2 + y'^2) = z^2 + u^2$$

So we can deduce from the presence of a 3 on the left hand side that $z^2 + u^2 = 0$ mod 3, and by the same reasoning as for x and y earlier can find ourselves z' and u' such that $z = 3z'$ and $u = 3u'$. Plugging into the equation again, we find

$$3(x'^2 + y'^2) = (3z')^2 + (3u')^2$$

So

$$3(x'^2 + y'^2) = 9(z'^2 + u'^2)$$

i.e

$$x'^2 + y'^2 = 3(z'^2 + u'^2)$$

Hence we're right back where we started, except all the numbers are a third of those we started with. There's nothing to stop us applying the same thought process to find a set x'', y'', z'', u''. In fact, we can do this infinitely many times, with the terms strictly decreasing in size each time.

Thus admitting one solution gives rise to an infinite descent, so there can be no solutions.

Direct proof by contradiction

To confirm proof by descent is a contradiction argument in disguise (even though we needn't explicitly appeal to that contradiction to complete a proof; as in the example above the observation of an infinite descent of integers is sufficient), here's a proof of the same result by slightly different means.

Suppose for contradiction there exist positive integer solutions to the problem. Let x, y, z, u be a solution such that $V = x^2 + y^2 = 3(z^2 + u^2)$ is minimal. Then, by the earlier reasoning, we can find x', y, z', u' satisfying the conditions. But they give rise to

$$V' = x'^2 + y'^2 = 3(z'^2 + u'^2) = \frac{V}{9}$$

So $V' < V$, contradicting the minimality of V. So positive integer solutions do not exist.

Constructive proof

One last proof can be given, with a more constructivist feel- it demonstrates that any non-negative integer solution must be the solution $0, 0, 0, 0$. Thus, there cannot be a positive integer solution, since x, y, z, u a solution implies $x = y = z = u = 0$ and x, y, z, u arbitrary positive integers implies x, y, z, u non-zero; the method of proof by contraposition then ensures x, y, z, u aren't a solution and their arbitrary nature proves there are no such solutions.

To reason in this way, let X, Y, Z, U be a non-negative integer solution (so zero is allowed). Then we can construct a new solution X', Y', Z', U' with $X = 3X'$. Repeating, we get X'' st $X = 3X' = 3 \times 3X''$ and so on; concluding that 3^n divides X for every n. But the only number which is infinitely divisible by 3 is zero, so $X = 0$. Further, the same reasoning gives each of Y,ZandU $=0.Wearedone.$

Some notable results by Infinite Descent

Fermat's theorem on sums of two squares (the Christmas Theorem)

An odd prime p can be written as $p = x^2 + y^2$ iff p is congruent to 1 mod 4

Typically for Fermat, he didn't prove this. Euler gave the first proof, by means of infinite descent.

No solution to $x^4 + y^4 = z^2$

This was known to Fermat, and allows an elementary proof of his last theorem in the case $n = 4$ (clearly, if the sum cannot be a square it cannot be a fourth power).

Irrationality of $\sqrt{2}$

That the square root of 2 cannot be rational was known to the Greeks. Euclid gave a proof by infinite descent, so the technique actually predates Fermat by nearly 2000 years! The result generalises to the square root of any prime.