More mathematical folklore.

> "Fermat's general method, that of "infinite descent", is profoundly ingenious, but has the disadvantage that it is often extremely difficult to apply."
>
> E.T.Bell in "The Development of Mathematics" (1945)

The purpose of this debunking note is to expose a few time-honoured mathematical concepts as mere artefacts of an unfortunate notation. The unfortunate notation writes *non* A => C or *non* C => A instead of the symmetric disjunction A *or* C .

The indirect proof.

Mathematicians call a proof of the theorem A => B "indirect" when, instead of proving A => B "directly", one proves *non* B => *non* A . But you cannot prove the one without proving the other: both are equivalent to *non* A *or* B . The distinction is void.

The reductio ad absurdum.

With C *and* *non* C as the prototype of a contradiction --an "absurdity"-- the reductio ad absurdum proceeds as follows. In order to prove A

0) one proves *non* A => C
1) one proves *non* A => *non* C
2) one concludes *non* A => (C *and* *non* C) , hence A .

But, apart from notation, the above proof *must* be equivalent to

0) proving *non* C => A
1) proving C => A
2) concluding (C *or* *non* C) => A , hence A .

In so-called contrast to the first proof the latter one is called "a proof by case analysis"! The distinction is void. I prefer

0) proving A *or* C
1) proving A *or* *non* C
2) concluding A .

Mathematical induction.

I was taught two patterns for mathematical induction.

Pattern 1:

1.0) prove $P(0)$ ("the base")

1.1) prove $(\underline{A}\ n:\ n \geq 0:\ P(n) \Rightarrow P(n+1))$ ("the induction step")

1.2) conclude $(\underline{A}\ n:\ n \geq 0:\ P(n))$

Pattern 2:

2.1) prove $(\underline{A}\ n:\ n \geq 0:\ (\underline{A}\ i:\ 0 \leq i < n:\ P(i)) \Rightarrow P(n))$

2.2) conclude $(\underline{A}\ n:\ n \geq 0:\ P(n))$

The following are comments on the way in which I was introduced to them-- a way that, I am afraid, is rather standard.

Pattern 1 , which regretfully is the better known one, was postulated and by renaming, substitution, and simplification pattern 2 was derived from it.

My first complaint is that no one pointed out to me that the two are <u>equivalent</u>, i.e. that by suitable renaming, substitution, and simplification the validity of pattern 1 can again be derived from the postulated validity of pattern 2.

My second complaint is that no one ever pointed out to me that the transition from pattern 1 to pattern 2 represents an obviously permissible strengthening of the induction hypothesis, thereby offering the opportunity for a simpler proof obligation.

My third complaint is that no one pointed out to me that for given P pattern 2 is in a sense canonical because the transition from 1 to 2 is idempotent. The moral of the story is that pattern 2 should always be preferred.

Fermat's "infinite descent" consists of proving $(\underline{A}\ n:\ n \geq 0:\ P(n))$ by showing that the assumption $\underline{\text{non}}\ P(n)$ leads to the existence of a natural value $i < n$, such that $\underline{\text{non}}\ P(i)$, which then leads to a contradiction.

I quote from E.T.Bell again --but this time from his "Men of Mathematics"--

"His own account is both concise and clear, so we shall give a free translation from his letter of August, 1659, to Carcavi.

"For a long time I was unable to apply my method to affirmative propositions, because the twist and the trick for getting at them is much more troublesome than that which I use for negative propositions. Thus, when I had to prove that every prime which exceeds a multiple of 4 by 1 is composed of two squares, I found myself in a fine torment. But at last a meditation repeated many times gave me the light I lacked, and now affirmative propositions submit to my method. The course of my reasoning in affirmative propositions is such: if an arbitrarily chosen prime of the form $4n+1$ is not a sum of two squares, [I prove that] there will be another of the same nature, less than the one chosen, and [therefore] next a third still less, and so on. Making an infinite descent of all the numbers of this kind I arrive at the number 5 , the least of all the numbers of this kind [4n+1]. [By the proof mentioned and the preceding argument from it], it follows that 5 is not a sum of two squares. But it is. Therefore we must infer by a reductio ad absurdum that all primes of the form $4n+1$ are sums of two squares." "

But what is Fermat's proof obligation? With

$P(n)$: the n-th prime of the form $4k+1$ is the sum of two squares

he has to prove

$$(\underline{A}\ n\colon n \geq 0 : \underline{\text{non}}\ P(n) \Rightarrow (\underline{E}\ i\colon 0 \leq i < n\colon \underline{\text{non}}\ P(i))) \quad ,$$

but this is <u>identical</u> to 2.1: both are

$$(\underline{A}\ n\colon n \geq 0\colon (\underline{E}\ i\colon 0 \leq i < n\colon \underline{\text{non}}\ P(i))\ \underline{\text{or}}\ P(n)) \quad .$$

Hence Fermat's method of "infinite descent" is nothing but normal mathematical induction in its easiest form. It doesn't deserve a special name and E.T.Bell's appreciation of it as quoted at the beginning of this text is all rubbish.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

1 May 1980
prof.dr.Edsger W.Dijkstra
Burroughs Research Fellow