A derivation of a proof by D. Zagier

In The American Mathematical Monthly (Vol. 97, Num. 2, Feb. 1990, p. 144), D. Zagier published a half-page article titled: "A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares". The first sentence of the article is the proof in question, the second sentence reads: "This proof is a simplification of one due to Heath-Brown [...] (inspired, in turn, by a proof given by Liouville)."

I can understand that the author could not resist the temptation to cram his proof into a single sentence, but the sentence became long and he was forced to commit the sin of omission. The latter is compensated by explanatory information in the article's second paragraph. But even when this explanation is taken into account, the author still pulls a number of sizeable rabbits out of his hat. The purpose of this note is the removal of those rabbits.

* * *

We have to prove that (for suitable p) there exists a solution of the equation

(0) $(x,y): x^2 + y^2 = p$.

For the general existence theorem $\langle \exists x :: Q.x \rangle$, there exist two radically different proof forms, viz. the "constructive" and the "nonconstructive" proof.

In a constructive proof, one constructs a value w, or designs an algorithm that constructs a value w, such that by virtue of its construction w can be shown to satisfy Q; in this context, such a w is called a "witness".

In a nonconstructive proof, $\langle \exists x :: Q.x \rangle$ is demonstrated without constructing a witness, typically by translating the demonstrandum into $\langle \underline{N}x :: Q.x \rangle \neq 0$, i.e. by proving the existence by means of a counting argument.

Constructive proofs have a number of potential attractions: they give more (viz. the witness), they can be simpler by avoiding the detour of the counting, and, finally, their design gives us the opportunity to draw on our experience in program construction. This time, however, that same experience suggests a nonconstructive proof that (0) can be solved, for a constructive proof

would via the witness effectively boil down to a factorization - in the complex plane - of p since $x^2+y^2 = (x+yi)(x-yi)$, and all factorization algorithms I know are non-constructive in the sense that they are no more than search algorithms that work equally well if there are no factorizations to be found. So I propose to pursue the demonstrandum in the form

$$(1) \qquad \langle \underline{N}\,(x,y) :: x^2+y^2 = p \rangle \neq 0$$

* * *

In view of our demonstrandum (1), we now focus our attention on the constant 0. What do we know about zero? Well, obviously $x+0 = x$ and $x\cdot 0 = 0$ for all natural x. For our current purpose - the question of how we can conclude difference from 0 - the multiplicative property of zero is more interesting. (Possibly, as the following calculation suggests, this is because the statement of the multiplicative property contains the constant 0 twice.) We observe

$$\begin{array}{ll} & n = 0 \\ \Rightarrow & \quad \{\ x\cdot 0 = 0\} \\ & \langle \forall x :: x\cdot 0 = n \rangle \\ \Rightarrow & \quad \{\ \text{pred. calc.}\} \\ & \langle \forall x :: \langle \exists y :: x\cdot y = n \rangle \end{array} \qquad ;$$

taking the contra-positive, we get

(2) $\langle \exists x :: \langle \forall y :: x.y \neq n \rangle \rangle \Rightarrow n \neq 0$,

i.e. we can conclude that n differs from zero when we have found an x that does not divide n.

* * *

We now focus our attention for a while on one number being a divisor or a multiple of another one. This situation is closely related to periodicity, and a standard way of generating an eventually periodic sequence is by repeated application of an operator defined on a finite domain.

The main purpose of this section is to introduce a metaphor that enables us to discuss these matters in the terminology of directed graphs. The mathematical content of this section is simple and well-known; it was certainly known to Fermat, but I don't know in which terminology he dealt with it.

We consider a domain S and functions f and g from S to S; x and y range over the elements of S. With function f we associate a directed graph whose vertices are the elements of

S and in which $f.x = y$ is captured by a directed edge from x to y ; if you allow me a pictorial representation in a formula, the metaphor is captured by the equivalence

(3) $$f.x = y \quad \equiv \quad \text{“} \underset{x}{\bullet} \longrightarrow \underset{y}{\bullet} \text{”}$$

We have obviously

- in the graph representing a function, each vertex has exactly 1 outgoing edge.

Let f be invertible, i.e. let there exist a function g, such that for all x, y

$$f.x = y \quad \equiv \quad x = g.y \quad ,$$

i.e. the graph representing g is obtained by inverting the direction of all edges in the graph for f ; hence

- in the graph representing an invertible function, each vertex has exactly 1 incoming edge.

Combining our last two findings and restricting ourselves to finite domains, we conclude

- the graph representing an invertible function on a finite domain consists of cycles, such that each vertex lies on one cycle: the cycles partition the domain.

- $\langle \exists n: n \geq 1: \langle \forall x :: x = f^n.x \rangle \rangle$, in which the exponent n denotes n-fold functional composition; a witness for n is the smallest common multiple of the lengths of the cycles occurring in the graph for f.

Conversely, if we are given that, for some positive p, $\langle \forall x :: x = f^p.x \rangle$, then

- f is invertible (since then

$$f.x = y \equiv x = f^{p-1}.y \quad)$$

- for finite domain, each cycle in the graph for f has a length that divides p.

The latter conclusion is of particular interest if the exponent p is prime, since then the domain of f is partitioned into (i) cycles of length p, and (ii) cycles of length 1, i.e. fixpoints of f. Consequently, the number of elements of S and the number of fixpoints of f differ by a multiple of p.

(By constructing a suitable f on a suitable domain, I thus proved for prime p

$$n^p \equiv n \pmod p \quad \text{in EWD740}$$

and $$(p-1)! \equiv (p-1) \pmod p \quad \text{in EWD742}.$$

I am convinced that the device was known to

Pierre de Fermat.)

This theorem will be used below for the simplest case, viz. $p = 2$. In that special case, viz. if $f^2.x = x$ for all x, x is called an "involution".

Remark. An alternative definition of an involution is: a function that is its own inverse; this definition, however, is less attractive because it does not invite the generalization from 2 to any positive integer. (End of Remark.)

That is, we shall use that for involutions on a finite domain, odd/evenness of the size of the domain equivales odd/evenness of the number of fixpoints of the involution. We shall use the equivalence in both directions; calling the two involutions involved "inv0" and "inv1" and the common domain on which they are defined "S", we shall use the following structure

the number of fixpoints of inv0 differs from zero
⇐ the number of fixpoints of inv0 is odd
⇐ the number of elements of S is odd
⇐ the number of fixpoints of inv1 is odd
⇐ inv1 has exactly 1 fixpoint .

* * *

After all these preliminaries, the time has come to return to our obligation of showing that equation (0) has a solution in natural numbers. Our first observation is that, because p is odd, one of the squares is odd while the other one is even; consequently, solvability of (0) is equivalent to solvability of

(4) $\quad (x,y): \; x^2 + 4y^2 = p$.

Remark The transition from (0) to (4) is primarily cosmetic; it is the simplest way of representing our choice that x^2 be the odd square. (End of Remark.)

In order to use the preceding, in particular the way of showing the existence of fixpoints, for showing the existence of solutions of (4), we establish a one-to-one correspondence between the solutions of (4) and the fixpoints of an involution. For the construction of that involution we do something with which every computing scientist is very familiar: replacing in a target relation -here (4)- something by a fresh variable. In more detail, there is a trivial one-to-one correspondence between the solutions of (4) and those of

$$(x,y,z):\ x^2+4y^2=p \ \wedge\ y=z$$

which equation – thanks to Leibniz's Principle – can be rewriten as

(5) $(x,y,z):\ x^2+4yz=p \ \wedge\ y=z$.

Next we create a one-to-one correspondence between the solutions of (5) and fixpoints of an involution, which we call "inv0". The domain S of inv0 consists of the <u>natural</u> solutions of

(6) $(x,y,z):\ x^2+4yz=p$,

so that the truth of the first conjunct of (5) holds for any fixpoint of inv0. Under exploitation of (6)'s symmetry in y & z, we choose for inv0

(7) $(x,y,z) \mapsto (x,z,y)$,

whose fixpoints truthify the second conjunct of (5) because $(x,y,z)=(x,z,y) \equiv y=z$. Our obligation to show that (5) – and hence (4) – has a natural solution has thus been translated in our obligation to show that involution inv0, as defined by (7) on S, has at least 1 fixpoint. Since domain S – the set of natural solutions of (6) – is rather obviously finite, our last obligation can be met by showing that S

contains an odd number of elements, and this we shall demonstrate by defining on S an involution, called "inv1", which has exactly 1 fixpoint. The remainder of this note is devoted to the design of a suitable inv1.

* * *

Before starting the design of inv1, we investigate properties of the individual elements of S, i.e. direct consequences for a natural triple (x,y,z) that solves (6) for prime p of the form $4k+1$. It so happens that here we only use
(i) p is odd
(ii) p is not a square (note that $p=1$ is excluded because 1 is not considered a prime number).
Our first lemma is that for $(x,y,z) \in S$

(8) $\quad x>0 \;\wedge\; y>0 \;\wedge\; z>0$.

Proof
$$
\begin{array}{ll}
 & x>0 \\
\Leftarrow & \quad \{(x,y,z)\in S, \text{ hence } x \text{ is natural}\} \\
 & x \text{ is odd} \\
= & \quad \{(x,y,z)\in S, \text{ hence (6)}\} \\
 & p \text{ is odd} \\
= & \quad \{(i)\} \\
 & \text{true}
\end{array}
$$

$$
\begin{array}{ll}
 & y>0 \;\wedge\; z>0 \\
\Leftarrow & \quad \{(x,y,z)\in S, \text{ hence } y,z \text{ are natural}\}
\end{array}
$$

$$
\begin{array}{ll}
 & y \neq 0 \ \wedge \ z \neq 0 \\
= & \quad \{ \text{arithmetic} \} \\
 & 4yz \neq 0 \\
= & \quad \{ (x,y,z) \in S \text{, hence (6)} \} \\
 & x^2 \neq p \\
= & \quad \{ \text{(ii)} \} \\
 & \text{true}
\end{array}
$$

(End of Proof)

Our next lemma – in the same vein – is that for $(x,y,z) \in S$

(9) $\quad x \neq y-z \ \wedge \ x \neq z-y$

Proof

$$
\begin{array}{ll}
 & x \neq y-z \ \wedge \ x \neq z-y \\
= & \quad \{ \text{arithmetic} \} \\
 & x^2 \neq (y-z)^2 \\
= & \quad \{ \text{arithmetic} \} \\
 & x^2 + 4yz \neq (y+z)^2 \\
= & \quad \{ (x,y,z) \in S \text{, hence (6)} \} \\
 & p \neq (y+z)^2 \\
= & \quad \{ \text{(ii)} \} \\
 & \text{true}
\end{array}
$$

(End of Proof)

Now we are ready to embark on our design of inv1, which should be an involution on S with a single fixpoint. To begin with, we ignore most of these requirements and concentrate our attention on the elaborate (6): can we think of operators on

(x,y,z) for which $x^2+4yz = p$ is an invariant, i.e. that transforms a solution of (6) into a solution of (6) ?

In order that we look beyond inv0 (as given by (7)) we investigate operators

(10) $$(x,y,z) \mapsto (x+\Delta x, y+\Delta y, z+\Delta z)$$

in which Δx is not identically zero. Because any solution to (6) has an <u>odd</u> value of x, we can confine our attention to <u>even</u> Δx; we do justice to this fact by parameterizing

(11) $$\Delta x = 2b \quad .$$

The requirement that $x^2+4yz = p$ be an invariant of (10) now translates into

$$\begin{aligned}
& \Delta(x^2 + 4yz) = 0 \\
= & \quad \{ \Delta\text{-calculus} \} \\
& \Delta(x^2) = -4\Delta(yz) \\
= & \quad \{ \Delta\text{-calculus} \} \\
& 2x(\Delta x) + (\Delta x)^2 = -4\Delta(yz) \\
= & \quad \{ (11), \text{arithmetic} \} \\
& b\cdot(x+b) = -\Delta(yz) \\
= & \quad \{ \Delta\text{-calculus} \} \\
& b\cdot(x+b) = -y\cdot\Delta z - z\cdot\Delta y - \Delta y\cdot\Delta z \quad .
\end{aligned}$$

The simplest way of finding solutions is by eliminating 2 of the 3 products at

the right-hand side by choosing, say,

(12) $\Delta y = 0$,

thus simplifying the relation between b and Δz to

(13) $b \cdot (x+b) = -y \cdot \Delta z$.

Note Choice (12) can be made "without loss of generality", that is, firstly, that the choice of $\Delta z = 0$ would not have given something essentially new since (6) is symmetric in y and z, and, secondly, that it is no restriction to change of the pair (y,z) only one at a time: we can always combine two moves into a single one so as to achieve $\Delta y \neq 0 \wedge \Delta z \neq 0$. (End of Note)

I can think of only 4 ways of satisfying relation (13). The derivations of the 4 operators below have taken (11) and (12) into account:

- $b = -y \wedge x+b = \Delta z$ yields

(14) $(x,y,z) \mapsto (x-2y, y, z+x-y)$;

- $b = y \wedge x+b = -\Delta z$ yields

(15) $(x,y,z) \mapsto (x+2y, y, z-x-y)$;

- $b = \Delta z \wedge x+b = -y$ yields (after

solving b from the second conjunct)

(16) $(x,y,z) \mapsto (-x-2y, y, z-x-y)$;

• $b = -\Delta z \wedge x+b = y$ yields (again after solving b from the second conjunct)

(17) $(x,y,z) \mapsto (2y-x, y, z+x-y)$.

Note that formulae (14) through (17), of the form

(18) $(x,y,z) \mapsto (x',y',z')$

are templates in the sense that, because of (6)'s symmetry in y and z, we are free to interchange y and z, or to interchange y' and z'. For instance, applying the first one to (15) would yield

(19) $(x,y,z) \mapsto (x+2z, z, y-x-z)$,

and applying the second one to (14) would yield

(20) $(x,y,z) \mapsto (x-2y, z+x-y, y)$.

Up till now, we have confined our attention to the invariance of (6). The next constraint to take into account is that $\mathcal{S}$ consists of the natural solutions of (6), i.e. we have to achieve the invariance of (8). This means that transformation (18)

is guarded by

(21) $\quad x'>0 \;\wedge\; y'>0 \;\wedge\; z'>0$.

Of the templates, (16) is identified by this requirement as useless, as it yields $x'<0$ (on account of (8)). This observation restricts our interest to templates (14), (15) and (17).

The time has come to remember that we are looking for an involution inv1 on S with exactly 1 fixpoint, i.e. for which $(x,y,z) = (x',y',z')$ holds for exactly 1 triple. The subtarget $x=x'$ rules out (14) and (15) as $x=x'$ then implies $y=0$, which falsifies (8). Consequently, the requirement that a fixpoint exist focusses our attention on (17).

In the following we shall use that, for $(x0, y0, z0)$ and $(x1, y1, z1)$ points on domain S,

$$x0=x1 \;\equiv\; y0=y1 \;\equiv\; z0=z1 \quad ,$$

which is a consequence of (6) and (8); as a result $(x0,y0,z0) = (x1,y1,z1)$ can be established by 2 of the 3 equalities.

Therefore, because under (17) we have $y=y'$, fixpoints of (17) are characterized by

$x = x'$, i.e. $x = 2y - x$ or, equivalently, $x = y$. Hence, for (x,y,z) a fixpoint of (17), we have on account of (6):

$$x \cdot (x + 4z) = p \quad ,$$

which guarantees for (17) the unique fixpoint $(1,1,k)$ if p is a prime of the form $1+4k$. (The conclusion of the uniqueness of this fixpoint is the only use made of p's primality.)

The next question is whether (17) is an involution, that is, with

$$(x,y,z) \xrightarrow{(17)} (x',y',z') \xrightarrow{(17)} (x'',y'',z'') \quad ,$$

holds $(x,y,z) = (x'', y'', z'')$?

We observe

$$\begin{aligned} & x'' \\ = & \quad \{ (17) \text{ with } x,y := x',y' \} \\ & 2y' - x' \\ = & \quad \{ (17) \} \\ & 2y - (2y - x) \\ = & \quad \{ \text{algebra} \} \\ & x \qquad ; \end{aligned}$$

since $y = y''$ is a trivial consequence of (17), (17) is indeed an involution.

The last question about (17) is: "Is it an involution on S?", and here the answer is

negative: constraint (21) tells us that (17) is an involution on the subdomain of $\mathcal{S}$ restricted by

(22) $$2y-x>0 \;\wedge\; z+x-y>0$$

Note that we do not need to check that the target point (x',y',z') lies on the subdomain, as it follows from (17) being an involution:

$$\begin{array}{ll} & 2y'-x'>0 \;\wedge\; z'+x'-y'>0 \\ = & \quad \{(17)\} \\ & x''>0 \;\wedge\; z''>0 \\ = & \quad \{(17) \text{ is an involution}\} \\ & x>0 \;\wedge\; z>0 \\ = & \quad \{(x,y,z) \in \mathcal{S}\} \\ & \text{true} \end{array}$$

We accept (17) restricted to the subdomain (22) of $\mathcal{S}$ as part of inv1, more precisely as the part of inv1 that contains 1 fixpoint. Our remaining task is to complete the definition of inv1, i.e. to design a fixpoint-free involution on the complement of (22); because of odd.x and $x \neq y-z$, that complement is the subdomain of $\mathcal{S}$ restricted by

$$x-2y>0 \;\vee\; y-x-z>0$$

which is equivalent to the subdomain of $\mathcal{S}$ restricted by (23) $\vee$ (24) with

(23) $x - 2y > 0 \;\wedge\; z + x - y > 0$

(24) $y - x - z > 0$.

Note that these conditions are no rabbits: (23) is the guard - corresponding to (21) - for transformations (14) and (20), and (24) is for instance the guard for (19).

In fact, (19) and (20) are suitable candidates for the completion of the definition of inv1; they are, when we can show $(x, y, z) = (x'', y'', z'')$ with

(i) $(x, y, z) \xrightarrow{(19)} (x', y', z') \xrightarrow{(20)} (x'', y'', z'')$

(ii) $(x, y, z) \xrightarrow{(20)} (x', y', z') \xrightarrow{(19)} (x'', y'', z'')$

Proof ad (i) we observe

$x = x'' \;\wedge\; z = z''$

$=$ {(20) with $x, y, z := x', y', z'$}

$x = x' - 2y' \;\wedge\; z = y'$

$=$ {(19)}

$x = x + 2z - 2z \;\wedge\; z = z$

$=$ {algebra}

true .

ad (ii) we observe similarly

$x = x'' \;\wedge\; y = y''$

$=$ {(19) with $x, y, z := x', y', z'$}

$x = x' + 2z' \;\wedge\; y = z'$

$=$ {(20)}

$x = x - 2y + 2y \;\wedge\; y = y$

= {algebra}
true

(End of Proof.)

Summarizing, inv1 is defined by

$(x,y,z) \mapsto$

$(2y-x,\ y,\ z+x-y)$ if $2y>x \wedge z+x>y$
$(x-2y,\ z+x-y,\ y)$ if $x>2y \wedge z+x>y$
$(x+2z,\ z,\ y-x-z)$ if $y>z+x$.

* * *

The remaining question to be answered is how "miraculous" this proof is, how fortunate Zagier has been in the construction of inv1. Since S has an odd number of elements, the existence of involutions with a single fixpoint is no problem; the problem is the choice of an inv1 with compact definition and manageable properties. The linearity of the expressions in (14) through (17) makes the transformations invertible, which is very nice if you are heading for an involution, that fixpoints can only come from (17) and that (14) and (15) are each other's inverse is fairly obvious. But the guards are not mutually exclusive and their disjunction is not true for each point of S. That the latter can be achieved by replacing (14) and (15) via x,y-exchange by (19) and (20), well, that is, as far as I can see, just a hell of a lot of luck. Eager to see my prejudices

confirmed, I interpret this luck of course as the well-deserved reward for keeping things as simple as possible.

Acknowledgements My debt to D. Zagier is obvious. I am also endebted to the undergraduate students that attended my last spring's course on "Mathematical Methodology" and with whom I discussed and designed the above proof in their oral examinations.

Nuenen, 2 August 1993

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA