A One-Sentence Proof That Every Prime p#1(\mod 4) Is a Sum of Two Squares

D. Zagier

The American Mathematical Monthly, Vol. 97, No. 2. (Feb., 1990), p. 144.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28199002%2997%3A2%3C144%3AAOPTEP%3E2.0.CO%3B2-Q

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/maa.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

http://www.jstor.org
Thu Jun 21 12:17:16 2007

THE TEACHING OF MATHEMATICS

EDITED BY MELVIN HENRIKSEN AND STAN WAGON

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x,y,z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. $\square$

This proof is a simplification of one due to Heath-Brown **[1]** (inspired, in turn, by a proof given by Liouville). The verifications of the implicitly made assertions—that S is finite and that the map is well-defined and involutory (i.e., equal to its own inverse) and has exactly one fixed point—are immediate and have been left to the reader. Only the last requires that p be a prime of the form $4k + 1$, the fixed point then being $(1,1,k)$.

Note that the proof is not constructive: it does not give a method to actually find the representation of p as a sum of two squares. A similar phenomenon occurs with results in topology and analysis that are proved using fixed-point theorems. Indeed, the basic principle we used: "The cardinalities of a finite set and of its fixed-point set under any involution have the same parity," is a combinatorial analogue and special case of the corresponding topological result: "The Euler characteristics of a topological space and of its fixed-point set under any continuous involution have the same parity."

For a discussion of constructive proofs of the two-squares theorem, see the Editor's Corner elsewhere in this issue.

REFERENCE

1. D. R. Heath-Brown, Fermat's two-squares theorem, *Invariant* (1984) 3–5.

Inverse Functions and their Derivatives

ERNST SNAPPER
Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH 03755

If the concept of inverse function is introduced correctly, the usual rule for its derivative is visually so obvious, it barely needs a proof. The reason why the standard, somewhat tedious proofs are given is that the inverse of a function $f(x)$ is