

THE AMERICAN MATHEMATICAL MONTHLY	
Volume 97, Number 2	February 1990
Contents	
ARTICLES	
A Note on the Newtonian N -Body Problem	DONALD G. SWARTZ 105
The Square-Rooted Primes	W. S. BARNES 107
EDITOR'S CORNER	
The Number $\sqrt{2}$ and the Square Root	STAN GARDNER 109
LETTERS TO THE EDITOR	
UNRESOLVED PROBLEMS	JOSEPH A. DALLARD 115
NOTES	
A Theorem on the Foundations of the Bernoulli Numbers	ALBERT GARDNER 116
A Generalization of the Quadratic Reciprocity Theorem	ROBERT G. JONES 118
On the p -adic Integers	EDWARD A. BECKER, FREDERICK K. HARRIS, and DOUGLAS R. HESTER 119
THE TEACHING OF MATHEMATICS	
A Note on the Teaching of the p -adic Integers	J. J. DALLARD 121
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 122
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 123
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 124
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 125
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 126
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 127
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 128
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 129
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 130
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 131
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 132
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 133
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 134
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 135
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 136
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 137
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 138
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 139
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 140
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 141
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 142
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 143
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 144
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 145
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 146
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 147
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 148
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 149
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 150
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 151
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 152
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 153
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 154
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 155
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 156
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 157
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 158
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 159
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 160
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 161
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 162
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 163
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 164
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 165
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 166
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 167
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 168
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 169
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 170
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 171
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 172
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 173
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 174
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 175
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 176
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 177
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 178
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 179
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 180
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 181
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 182
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 183
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 184
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 185
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 186
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 187
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 188
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 189
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 190
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 191
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 192
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 193
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 194
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 195
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 196
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 197
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 198
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 199
On the Teaching of the p -adic Integers	JOSEPH A. DALLARD 200

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: <https://www.tandfonline.com/loi/uamm20>

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

D. Zagier

To cite this article: D. Zagier (1990) A One-Sentence Proof That Every Prime $p \equiv 1 \pmod{4}$ Is a Sum of Two Squares, The American Mathematical Monthly, 97:2, 144-144, DOI: [10.1080/00029890.1990.11995565](https://doi.org/10.1080/00029890.1990.11995565)

To link to this article: <https://doi.org/10.1080/00029890.1990.11995565>



Published online: 11 Apr 2018.



Submit your article to this journal [↗](#)



Article views: 2



Citing articles: 4 View citing articles [↗](#)

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