A Note on Fermat's Last Theorem
Author(s): J. M. Gandhi
Source: *The American Mathematical Monthly*, Vol. 73, No. 10 (Dec., 1966), pp. 1106-1107
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2314650
Accessed: 24/03/2010 21:25

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp. 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/action/showPublisher?publisherCode=maa.

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.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

http://www.jstor.org

If a cancellation semigroup is not a group, then any identity it satisfies is a consequence of the commutative law

determines the identities a cancellation semigroup can satisfy. More generally, any identity which a nonperiodic semigroup satisfies is a consequence of the commutative law. In this form we see that our result is, in a way, a generalization of Neumann's result in [2], that any identity which a group satisfies may be put in the form

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \cdot c(x_1, x_2, \cdots, x_n) = 1,$$

where $c(x_1, x_2, \cdots, x_n)$ is a complex commutator word in the variables.

References

1. A. H. Clifford and G. B. Preston, The algebraic theory of semigroups, vol. 1, Math. Surveys 7, Amer. Math. Soc., 16 (1962).

2. B. H. Neumann, Identical relations in groups I, Math. Ann., 114 (1937) 506–525.

A NOTE ON FERMAT'S LAST THEOREM

J. M. GANDHI, University of Alberta, Edmonton

Recently D. E. Stone [2] proved the following theorem which pertains to Fermat's Last Theorem (FLT).

THEOREM. *If p and $2p+1$ are odd primes and*

$$a^p + b^p + c^p = 0,$$

where a, b, c are nonzero, pairwise prime integers, then precisely one of the integers a, b, c is divisible by p.

In this note we prove a similar theorem pertaining to FLT.

THEOREM. *If p and $4p+1$ are primes with $p>3$, and $a^p+b^p+c^p=0$, where a, b, c are nonzero, pairwise prime integers, then precisely one of the integers a, b, c is divisible by $4p+1$.*

Proof of Theorem. Assume that $(abc, 4p+1)=1$. Writing (1) as $a^p+b^p=-c^p$ and squaring, we get

$$a^{2p} + b^{2p} + 2a^p b^p = c^{2p}. \tag{1}$$

Since $4p+1$ is prime, and since, by assumption, a, b, c are each prime to $4p+1$, we have by Fermat's "little" theorem,

$$\begin{aligned} &a^{2p} \equiv \pm 1 \pmod{4p+1}, \quad b^{2p} \equiv \pm 1 \pmod{4p+1} \\ &c^{2p} \equiv \pm 1 \pmod{4p+1}. \end{aligned} \tag{2}$$

The sign before the residues is $+$ or $-$ according as $k^2 \equiv a$, $k^2 \equiv b$, $k^2 \equiv c \pmod{4p+1}$ respectively has or has not integral solutions.

Using (2) in (1) we get

$$\pm 1 \pm 1 + 2a^p b^p \equiv \pm 1 \pmod{4p+1}$$

or

$$2a^p b^p \equiv +1, -1, +3 \text{ or } -3 \pmod{4p+1}.$$

Squaring the last congruence and using (2) we get

$$\pm 4 \equiv 1 \text{ or } 9 \pmod{4p+1}.$$

Since p is a prime >3, the last congruence is impossible. This contradicts the assumption $(abc, 4p+1)=1$ and hence one of a, b, c must be divisible by $4p+1$.

The author is on leave from University of Rajasthan, Jaipur.

References

1. L. E. Dickson, History of Theory of Numbers, Vol. II, Chelsea, New York, 1952, 734.
2. D. E. Stone, On Fermat's Last Theorem, this MONTHLY, 70 (1963) 976.

CLASSROOM NOTES

EDITED BY GERTRUDE EHRLICH, University of Maryland

Send manuscripts to R. A. Rosenbaum, Wesleyan University, Middletown, Conn. 06457.

ON PROVING THEOREMS IN PLANE GEOMETRY VIA DIGITAL COMPUTER

RICHARD BELLMAN, University of Southern California

1. Introduction. The development of the digital computer has focused considerable attention upon various types of algorithms, and, in particular, upon those connected with logical processes and decision-making. An offshoot of this has been the set of attempts by various people, with varying degrees of success, to replicate human thought processes with the aid of a digital computer. In this connection, let us cite the work in translation of languages, pattern recognition, chess playing, checker playing, and the proving of logical and geometric theorems.

In pursuing these goals, there are many different approaches that can be pursued. At one extreme, we can imitate what the human mind does; at the other extreme, we can fasten our attention solely upon the capabilities of an analog or digital computer. In between, we have a continuum of man-machine processes. Since it is generally agreed by knowledgeable people that we possess very little understanding of the working of the brain, it is clearly hazardous to follow the first route. We shall restrain ourselves exclusively to a completely rigorous use of the computer in establishing geometric theorems.

The basic idea is quite simple. The structure of Euclidean plane geometry permits us to express geometric theorems as algebraic identities. Algebraic iden-