H.J.S. SMITH AND THE FERMAT TWO SQUARES THEOREM

F.W. CLARKE, W.N. EVERITT, L.L. LITTLEJOHN, AND S.J.R. VORSTER

This paper is dedicated to Professor P.R. Halmos

ABSTRACT. The two squares theorem of Fermat gives a representation of a prime congruent to 1 modulo 4, as the sum of two integer squares. Fermat (1659) is credited with the first proof of this result, but the first recorded proof is due to Euler (1749). Gauss (1801) showed that the two squares representation is essentially unique. In 1855 the Oxford mathematician Henry Smith gave an elementary proof involving the use of continuants. This paper discusses the Smith proof and shows how his method can be extended to give uniqueness. There is a brief account of the life and achievements of Henry Smith recently called "The mathematician the world forgot".

1. INTRODUCTION

In his remarkable book "A Mathematician's Apology" G.H. Hardy wrote, see [12, Page 97]:

"Another famous and beautiful theorem is Fermat's 'two square' theorem. The primes may (if we ignore the special prime 2) be arranged in two classes; the primes

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ \cdots$$

which leave remainder 1 when divided by 4, and the primes

$$3,\ 7,\ 11,\ 19,\ 23,\ 31,\ \cdots$$

which leave remainder 3. All the primes of the first class, and none of the second, can be expressed as the sum of two squares: thus

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2$$
$$17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2$$

but 3, 7, 11 and 19 are not expressible in this way (as the reader may check by trial). This is Fermat's theorem, which is ranked, very justly, as one of the finest of arithmetic. Unfortunately there is no proof within the comprehension of anybody but a fairly expert mathematician."

The history of this theorem of Fermat is given in detail by Dickson [7, Chapter VI, Pages 224-237]. Dickson names the theorem after Girard who discussed the result in 1632; however the common practice now is to attribute the result to Fermat who stated, in 1659, that he possessed an irrefutable proof by the method of infinite descent; see [7, Chapter VI, Page 228] and [2, Page 89]. The first recorded proof is due to Euler given in 1749, see [7, Chapter

1991 *Mathematics Subject Classification.* Primary 11A41, 11E25; Secondary 15A15.
Key words and phrases. Prime numbers, Fermat, two squares theorem.

VI, Pages 230 and 231]; Bell writes [2, Page 89] "It was first proved by the great Euler in 1749 after he had struggled, off and on, for *seven years* to find a proof.". The first proof that the representation of such prime numbers, as the sum of squares of two positive integers, is unique was given by Gauss in 1801; see [7, Chapter VI, Page 233]. See also the account of the two squares theorem of Fermat in the books by Burton [4, Chapter 12, Section 2], and Hardy and Wright [14, Chapter XX].

The last sentence in the above quotation from Hardy is significant. Hardy had an interest in the classification of proof; see, in particular, [13, Page 6, Section 1.7] in connection with the "elementary" proof of inequalities. In this context the technical use of the word elementary must not be confused with the words obvious or easy; many of the elementary proofs in [13] are subtle, ingenious and far from obvious. When Hardy wrote [12] he was, more than likely, not aware that an elementary proof of this theorem of Fermat had been given in 1855 by H.J.S. Smith, one of the predecessors in the Savilian Chair of Geometry in the University of Oxford. This simple but remarkable proof of Smith is within the comprehension of those with knowledge of elementary algebra, including simple properties of determinants, and the fundamental theorem of arithmetic [6, Chapter I, section 4]. The proof is also remarkable for being both constructable and computable for the integers of the two squares representation.

In this paper we give Smith's proof of the theorem of Fermat and present what is, possibly, a new elementary proof of the uniqueness of the two squares representation, but now using Smith's ideas and method. This uniqueness proof involves the Euler Criterion [8, Section 11] for solutions of the quadratic equation $x^2 \equiv -1 \mod(p)$; we present a new existence proof that leads to a constructable solution of this equation.

The original paper of Smith [20] is (the good news) only 2 pages long but is (the bad news for most of us) written in Latin; see also the collected works of Smith [21], in which [20] appears as the second contribution. The Smith proof has not gone entirely without notice; Chrystal [5, Part II, Page 471] reproduces the proof in English, as does, in part, Dickson [7, Chapter VI, Pages 240 and 241]; Davenport mentions the proof [6, Chapter V, Section 3, Page 122] but does not give complete details. Barnes [1] gives an exposition of Smith's existence theorem, and establishes the connection between the Smith palindromic continuant and the Euler Criterion (see Theorems 1 and 2 and their proofs below).

Both Serret [19] and Hermite [17] use ideas similar to the Smith method [20] to give an algorithm for finding the integers in the two squares representation of the theorem of Fermat. This method was subsequently improved by Brillhart [3] to give an impressively fast numerical procedure to determine the representation; as an example the Brillhart method gives

$$10^{50} + 577 = 761106534380835424545040 1^2 + 648626890687392164224542 4^2.$$

The two squares theorem of Fermat continues to attract attention; see the recent contributions by Ewell [9], Heath-Brown [16], Wagon [22] and Zagier [23].

In Section 2 we give formal statements of the results to be proved by the Smith methods. In Section 3 we give a brief account of the life of Henry Smith. In Section 4 there is a definition and statement of the properties of continuants. The remaining Sections are devoted to proofs of the results. Lastly, in an Appendix, we reproduce the two-page paper, in Latin, of the original Smith paper [20].

2. Statement of results

Let $\mathbb{N} := \{1, 2, 3, \cdots\}$ and $\mathbb{P} := \{p \in \mathbb{N} : p \text{ is a prime number}\}$.

Theorem 1 (Fermat and Gauss)**.** *Let $p \in \mathbb{P}$ with $p \equiv 1 \bmod(4)$; then there exist two unique, positive, co-prime integers $u, v \in \mathbb{N}$ such that*

$$p = u^2 + v^2. \tag{2.1}$$

Proof. See Sections 6 and 7 below. □

Theorem 2 (The Euler Criterion)**.** *Let $p \in \mathbb{P}$ with $p \equiv 1 \bmod(4)$. Then*

1. The quadratic equation

$$x^2 \equiv -1 \bmod(p) \tag{2.2}$$

has two unique solutions $x_0, x_1 \in \mathbb{N}$ such that

$$1 < x_0 < (p-1)/2 \quad \textit{and} \quad (p-1)/2 < x_1 < p, \tag{2.3}$$

with $x_1 = p - x_0$.

2. All other solutions of (2.2) are congruent to x_0 or $x_1 \bmod(p)$.

Proof. See Section 8 below. □

Remark 1. *For a detailed discussion on the Euler Criterion see the book by Dudley* [8, Section 11, Pages 85-86].

3. Henry John Steven Smith

Henry Smith was born on 02 November 1826 in Dublin, Ireland. His father died soon afterwards and the widow moved with her family to England. Smith was educated first by his mother and then by a succession of private tutors, before spending three years at Rugby School; from this School he gained entry to the University of Oxford, in 1844, by winning the top scholarship to Balliol College. In 1848 at Oxford he gained first class honours in both classics and mathematics; he also won the major University prizes in both these subjects, the Ireland scholarship in classics and the Senior Mathematical Scholarship in mathematics.

In 1849 the Balliol College fellowships in classics and mathematics fell vacant; until this time Smith seems to have been undecided as to whether to follow a career in classics or mathematics, but seems to have settled at this time on mathematics. His first paper, on geometry, dates from the next year.

The first paper by Smith on number theory was completed in 1854 and published the following year in Crelle's Journal, see [20]. Unusually, even for that time, it was written in Latin, perhaps in homage to Karl Friedrich Gauss, whose *Disquisitiones arithmeticae* served as an inspiration.

In 1859 Smith was elected to Fellowship of the Royal Society of London and then, in 1860, to the Savilian Chair of Geometry in the University of Oxford; two of his eventual successors to this Chair were G.H. Hardy and E.C. Titchmarsh.

Henry Smith died in Oxford in 1883.

One of the puzzling features when one looks at the work of Henry Smith is why his name is so little known, even amongst those who make regular use of the ideas that he

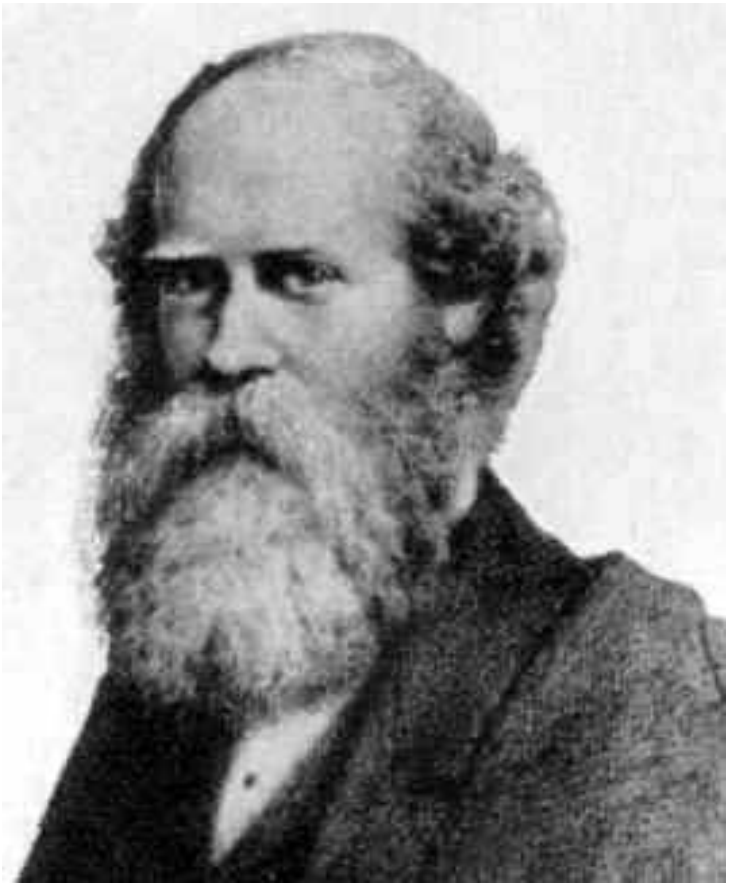

FIGURE 1. Henry John Stephen Smith (1826-1883)

introduced; see the paper *The mathematician the world forgot* by Keith Hannabuss [10]. Several historians of mathematics have ranked him with Cayley and Sylvester among the great pure mathematicians of the nineteenth century. His remarkable contributions to, and his panoramic knowledge of, the theory of numbers can be seen in the monumental *Report on the theory of numbers*, reproduced in [21]. In this area, in 1868, he shared in the Steiner Prize of the Royal Academy of Sciences, in Berlin, for his solution of a geometric problem but involving the representation of integers as a sum of squares.

Not so well known is Smith's early contribution to measure theory and integration in his paper of 1875 *On the integration of discontinuous functions*; see Paper 25 in [21]. In this paper, Smith introduced the first example of what is now called a Cantor set; Cantor's own example appeared eight years later and was not presented as his own discovery. Smith's example divides an interval into m, with $m > 2$, subintervals, and then keeps repeating this process to each remaining subinterval, except the last. Smith also seems to have been the first mathematician to perceive the connection between measure and integral. However, his paper received less attention than it deserved, owing to an inaccurate review in the *Fortschritte der Mathematik*. In his history of integration, see [15, Pages 37 and 40], Thomas Hawkins has remarked:

"Probably the development of a measure-theoretic viewpoint within integration theory would have been accelerated had the contents of Smith's paper been known to mathematicians whose interest in the theory was less tangential than Smith's."
For an informed discussion on the contents of this paper of Smith, and for the development of the ideas therein to higher dimensions, see the papers of Hannabuss [10] and, especially, [11].

4. Continuants

Continuants are closely connected with continued fractions as is indicated by Smith at the beginning of his paper [20]. There is a detailed and elegant account of this connection in Chrystal [5, Chapter XXXIV]; see in particular [5, Chapter XXXIV, Sections 4 to 11]. However Smith uses only continuants in his paper and defines them in terms of determinants; for this definition see [5, Chapter XXXIV, Section 11] and the reference therein to the remarkable history of determinants by Muir and Metzler [18, Chapters III and XIII]. We follow Smith and make the

Definition 1. *For $n \in \mathbb{N}$ let $q_r \in \mathbb{N}$ $(r = 1, 2, \cdots, n)$; then define $[\cdots] : \mathbb{N}^n \to \mathbb{N}$ by the determinant*

$$[q_1, q_2, q_3, \cdots, q_{n-1}, q_n] := \begin{vmatrix} q_1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & -1 & q_n \end{vmatrix}. \tag{4.1}$$

We note that

$$[q_1] = q_1, \quad [q_1, q_2] = q_1 q_2 + 1, \quad [q_1, q_2, q_3] = q_1 q_2 q_3 + q_1 + q_3. \tag{4.2}$$

Lemma 1. *Let $n \in \mathbb{N}$ with $n \geq 2$; then continuants have the following properties:*

(1) $[q_1, q_2, \cdots, q_n] = [q_1][q_2, q_3, \cdots, q_n] + [q_3, \cdots, q_n]$
(2) $[q_1, q_2, \cdots, q_n] \in \mathbb{N}$
(3) $[q_1, q_2, \cdots, q_n] = [q_n, \cdots, q_2, q_1]$
(4) $[q_2, q_3, \cdots, q_n] < [q_1, q_2, \cdots, q_n]$
(5) $[q_2, q_3, \cdots, q_n]$ *and* $[q_1, q_2, \cdots, q_n]$ *are co-prime integers*
(6)

$$[q_1, \cdots, q_{s-1}, q_s, q_{s+1}, q_{s+2}, \cdots, q_n] = [q_1, \cdots, q_{s-1}, q_s][q_{s+1}, q_{s+2}, \cdots, q_n] + [q_1, \cdots, q_{s-1}][q_{s+2}, \cdots, q_n].$$

Proof. Note that if in any formula in Lemma 1 an empty continuant appears then it is convenient, and consistent, to give such a continuant the value 1.

(1) Expand the determinant (4.1) by the first row.
(2) Use (4.2), property 1 and mathematical induction.
(3) Standard property of determinants.
(4) Use properties 1 and 2.

(5) Use property 1.
(6) Use the Laplace expansion on (4.1) centred on row s; see also the proof given by Chrystal [5, Chapter XXXIV, Section 6].

□

5. The Euclidean algorithm

Algorithm 1. *Let $r, s \in \mathbb{N}$ be co-prime with $s < r$; then write*

$$\begin{aligned} \frac{r}{s} &= q_1 + \frac{t}{s} \quad 0 < t < s \\ \frac{s}{t} &= q_2 + \frac{u}{t} \quad 0 \leq u < t \\ &\vdots \\ \frac{v}{w} &= q_n + \frac{0}{w} = q_n \end{aligned}$$

for some $n \in \mathbb{N}$ with $n \geq 2$, $q_i \in \mathbb{N}$ $(i = 1, 2, \cdots, n)$ and $q_n \geq 2$.

Thus the rational number $r/s > 1$ has associated with it a set of positive integers $\{q_1, q_2, \cdots, q_n\}$ with the above properties. Conversely we have

Lemma 2. *Given a set of positive integers $\{q_1, q_2, \cdots, q_n\}$ with $n \geq 2$ and $q_n \geq 2$ then there is a unique rational number $r/s > 1$ whose Euclidean algorithm yields the set $\{q_1, q_2, \cdots, q_n\}$; moreover, r/s is determined by*

$$\frac{r}{s} = \frac{[q_1, q_2, \cdots, q_n]}{[q_2, q_3, \cdots, q_n]}. \tag{5.1}$$

Here r and s are co-prime and given by

$$r = [q_1, q_2, \cdots, q_n] \quad \text{and} \quad s = [q_2, q_3, \cdots, q_n]. \tag{5.2}$$

Proof. Define r/s by (5.1) and apply property 1 of Lemma 1 n times.
The result (5.2) follows from property 5 of Lemma 1. □

6. The Smith proof of the Fermat theorem

Proof. Let $p \in \mathbb{P}$ with $p \equiv 1 \mod(4)$ and write $p = 4r + 1$. Let the number μ be taken arbitrarily from the set of positive integers $\{1, 2, \cdots, 2r\}$ and consider the corresponding set of rational numbers $\{p/\mu\}$, noting that $2 < p/\mu \leq p$. From Algorithm 1 applied to p/μ we have, say,

$$\frac{p}{\mu} = \frac{[q_1, q_2, \cdots, q_n]}{[q_2, \cdots, q_n]} \tag{6.1}$$

noting that the integer n and the set $\{q_1, q_2, \cdots, q_n\}$ depend upon the particular choice of μ. From property 5 of Lemma 1 we obtain

$$p = [q_1, q_2, \cdots, q_n] \quad \text{and} \quad \mu = [q_2, \cdots, q_n]. \tag{6.2}$$

From Algorithm 1 and from property 1 of Lemma 1, since $p/\mu > 2$, it follows that, in the representation (6.2),

$$q_1 \geq 2 \quad \text{and} \quad q_n \geq 2. \tag{6.3}$$

Now take one of the rational numbers p/μ with

$$\mu \in \{2, 3, \cdots, 2r\}; \tag{6.4}$$

then we have the following chain of argument, using property 3 of Lemma 1 and (6.1),

$$\frac{p}{\mu} = \frac{[q_1, q_2, \cdots, q_n]}{[q_2, \cdots, q_n]} \Rightarrow [q_1, q_2, \cdots, q_n] = p = [q_n, q_{n-1}, \cdots, q_1] \Rightarrow \frac{[q_n, q_{n-1}, \cdots, q_1]}{[q_{n-1}, \cdots, q_1]} = \frac{p}{\nu}, \tag{6.5}$$

(say). It follows from (6.3), Lemma 2 and property 1 of Lemma 1 that

$$1 < \nu < p/2,$$

so that $\nu \in \{2, 3, \cdots, 2r\}$. Thus the chain of argument that gave (6.5) can be reversed, starting with ν and finishing with μ.

This argument pairs off the elements of the set $\{2, 3, \ldots, 2r\}$ giving each member μ of the set a unique mate ν in the set. However this set contains an odd number of elements so that there must exist at least one member, say λ, that mates with itself in the chain (6.5). For this λ then we obtain from (6.5)

$$\frac{[q_1, q_2, \cdots, q_n]}{[q_2, \cdots, q_n]} = \frac{p}{\lambda} = \frac{[q_n, q_{n-1}, \cdots, q_1]}{[q_{n-1}, \cdots, q_1]}. \tag{6.6}$$

Now apply Algorithm 1 to both sides of (6.6) to give a representation

$$p = [q_1, q_2, \cdots, q_n], \tag{6.7}$$

with the palindromic property, and with (6.3) holding,

$$q_i = q_{n+1-i} \quad (i = 1, 2, \cdots, n). \tag{6.8}$$

If, in (6.8), $n = 2t + 1$ is odd then $n \geq 3$ and the representation (6.7) takes the form, for $s \geq 2$,

$$p = [q_1, \cdots, q_{s-1}, q_s, q_{s-1}, \cdots, q_1].$$

Now apply property 6 of Lemma 1 to give

$$\begin{aligned} p = &[q_1, \cdots, q_{s-1}, q_s][q_{s-1}, \cdots, q_1] \\ &+ [q_1, \cdots, q_{s-1}][q_{s-2}, \cdots, q_1], \end{aligned}$$

and then

$$p = [q_1, \cdots, q_{s-1}]\{[q_1, \cdots, q_{s-1}, q_s] + [q_{s-2}, \cdots, q_1]\}$$

on using other properties of Lemma 1. This last result represents the prime number p as the product of two factors that, using (6.3), are both greater than 1; this is a contradiction to $p \in \mathbb{P}$.

Thus in (6.8) the integer $n = 2t$ must be even and so (6.7) takes the form, for $s \geq 1$,

$$p = [q_1, \cdots, q_s, q_s, \cdots, q_1] \tag{6.9}$$

with $q_1 \geq 2$ from (6.3). Now apply property 6 of Lemma 1 to give

$$p = [q_1, \cdots, q_s][q_s, \cdots, q_1] + [q_1, \cdots, q_{s-1}][q_{s-1}, \cdots, q_1]$$

and then

$$p = [q_1, \cdots, q_{s-1}]^2 + [q_1, \cdots, q_s]^2. \tag{6.10}$$

From property 1 it follows that $[q_1, \cdots, q_{s-1}]$ and $[q_1, \cdots, q_s]$ are co-prime.

This completes the Smith proof of the Fermat part of Theorem 1. □

7. A Corollary

We have

Corollary 1. *Let $p \in \mathbb{P}$ with $p = 4r + 1$; then there are exactly $2r$ distinct continuant representations of p*

$$p = [q_1, \cdots, q_n]$$

with $q_n \geq 2$.

Proof. Let $\mu \in \{1, 2, \cdots, 2r\}$; then from (6.1)

$$\frac{p}{\mu} = \frac{[q_1, q_2, \cdots, q_n]}{[q_2, \cdots, q_n]} \quad \text{and} \quad p = [q_1, q_2, \cdots, q_n] \tag{7.1}$$

with $q_n \geq 2$; these continuant representations of p are distinct since otherwise, from (7.1), $p/\mu = p/\mu'$ for $\mu \neq \mu'$.

Let p have a representation $p = [q_1, q_2, \cdots, q_n]$ with $q_n \geq 2$. If $n = 1$ then $q_1 = q_n = p$ and we can take $\mu = 1$ in (7.1). If $n \geq 2$ then, since $q_n \geq 2$, from Lemma 1, properties 1 and 3 it follows that $[q_2, \cdots, q_n] \leq (p-1)/2$ so that in (7.1) we have $[q_2, \cdots, q_n] \in \{2, \cdots, 2r\}$. □

8. Proof of Theorem 2

We begin with

Lemma 3. *Given any $n \in \mathbb{N}$ with $n \geq 2$ and any set of positive integers $\{q_1, q_2, \cdots, q_n\}$ define*

$$I_n(q_1, q_2, \cdots, q_n) := [q_1, q_2, \cdots, q_n][q_2, q_3, \cdots, q_{n-1}] - [q_1, q_2, \cdots, q_{n-1}][q_2, \cdots, q_n]. \tag{8.1}$$

Then

$$I_n(q_1, q_2, \cdots, q_n) = (-1)^n. \tag{8.2}$$

Proof. We have, from (4.2),

$$I_2(q_1, q_2) = [q_1, q_2] - [q_1][q_2] = 1. \tag{8.3}$$

For the general case we have, from property 6 of Lemma 1,

$$[q_1, \cdots, q_n] = [q_1, \cdots, q_{n-1}]q_n + [q_1, \cdots, q_{n-2}] \tag{8.4}$$

$$[q_2, \cdots, q_n] = [q_2, \cdots, q_{n-1}]q_n + [q_2, \cdots, q_{n-2}]. \tag{8.5}$$

Multiply (8.4) by $[q_2, \cdots, q_{n-1}]$ and (8.5) by $[q_1, \cdots, q_{n-1}]$ to give, using (8.1),

$$\begin{aligned} I_n(q_1, q_2, \cdots, q_n) &= [q_1, \cdots, q_{n-2}][q_2, \cdots, q_{n-1}] \\ &\quad - [q_2, \cdots, q_{n-2}][q_1, \cdots, q_{n-1}] \\ &= -I_{n-1}(q_1, q_2, \cdots, q_{n-1}). \end{aligned}$$

Repeated application of this last result yields

$$I_n(q_1, q_2, \cdots, q_n) = (-1)^r I_{n-r}(q_1, \cdots, q_{n-r}) \quad (r \in \{1, 2, \cdots, n-2\}); \tag{8.6}$$

taking $r = n - 2$ gives, from (8.3),

$$I_n(q_1, q_2, \cdots, q_n) = (-1)^{n-2} I_2 = (-1)^n$$

and so (8.2) follows, as required. □

Proof of Theorem 2, Part 1.

Proof. Let $p \in \mathbb{P}$ with $p \equiv 1 \bmod(4)$; then from the proof of Theorem 1 p has at least one palindromic continuant representation

$$p = [q_1, \cdots, q_s, q_s, \cdots, q_1] \tag{8.7}$$

with $s \geq 1$ and $q_1 \geq 2$.

Define $x_0 \in \mathbb{N}$ by

$$x_0 := [q_2, \cdots, q_s, q_s, \cdots, q_1]; \tag{8.8}$$

it follows that, from $q_1 \geq 2$ and property 1 of Lemma 1,

$$1 < x_0 < (p-1)/2. \tag{8.9}$$

Now apply the result of Lemma 3 to the right-hand side of (8.7), with $n = 2s$, to obtain

$$\begin{aligned} &[q_1, \cdots, q_s, q_s, \cdots, q_1][q_2, \cdots, q_s, q_s, \cdots, q_2] \\ &\quad - [q_1, \cdots, q_s, q_s, \cdots, q_2][q_2, \cdots, q_s, q_s, \cdots, q_1] \\ &= (-1)^{2s} = 1. \end{aligned}$$

From (8.7), (8.8) and property 3 of Lemma 1 this last result reduces to

$$p[q_2, \cdots, q_s, q_s, \cdots, q_2] - x_0^2 = 1$$

and so

$$x_0^2 \equiv -1 \bmod(p).$$

This result, together with (8.9) completes the proof of Part 1. □

Proof of Theorem 2, Part 2.

Proof. Suppose that r is another solution of the quadratic equation (2.2) with $r \neq x_0$ and $r \neq p - x_0$; without loss of generality we may suppose that r is a least, positive residue $\bmod(p)$. Then

$$r^2 \equiv x_0^2 \equiv -1 \quad \bmod(p)$$

and hence p divides $r^2 - x_0^2 = (r - x_0)(r + x_0)$; since p is prime p divides $r - x_0$ or $r + x_0$. The former case implies $r \equiv x_0 \bmod(p)$, but since both r and x_0 are least, positive residues

it follows that $r = x_0$. In the latter case $r \equiv -x_0 \equiv p - x_0 \mod(p)$ and since, again, r and $p - x_0$ are least, positive residues it follows that $r = p - x_0$.

This contradiction completes the proof of Part 2. □

9. The ''Smith'' proof of the Gauss theorem

We are now in a position to give a proof, using the methods of Henry Smith, of the Gauss uniqueness result for the Fermat theorem, as presented in Theorem 1.

Proof. Let $p \in \mathbb{P}$ with $p \equiv 1 \mod(4)$ and suppose that there are two, co-prime two squares representations

$$p = u^2 + v^2 \quad \text{and} \quad p = s^2 + r^2$$

with $u < v$, $s < r$.

Apply Algorithm 1 to the rational numbers v/u and r/s to obtain

$$1 < \frac{v}{u} = \frac{[q_1, q_2, \cdots, q_n]}{[q_2, \cdots, q_n]} \quad \text{and} \quad 1 < \frac{r}{s} = \frac{[t_1, t_2, \cdots, t_m]}{[t_2, \cdots, t_m]};$$

then

$$u = [q_2, \cdots, q_n] \quad \text{and} \quad v = [q_1, q_2, \cdots, q_n]$$
$$s = [t_2, \cdots, t_m] \quad \text{and} \quad r = [t_1, t_2, \cdots, t_m].$$

Hence, using property 6 of Lemma 1, we obtain, with $m, n \in \mathbb{N}$,

$$p = u^2 + v^2 = [q_2, \cdots, q_n]^2 + [q_1, q_2, \cdots, q_n]^2 = [q_n, \cdots, q_2, q_1, q_1, q_2, \cdots, q_n] \tag{9.1}$$

and

$$p = s^2 + r^2 = [t_2, \cdots, t_m]^2 + [t_1, t_2, \cdots, t_m]^2 = [t_m, \cdots, t_2, t_1, t_1, t_2, \cdots, t_m]. \tag{9.2}$$

From Part 1 of Theorem 2 we have the result that

$$[q_{n-1}, \cdots, q_1, q_1, \cdots, q_{n-1}, q_n]$$

and

$$[t_{m-1}, \cdots, t_1, t_1, \cdots, t_{m-1}, t_m]$$

are both solutions of the quadratic equation $x^2 \equiv -1 \mod(p)$ satisfying $1 < x < (p-1)/2$. From the uniqueness of this solution we have

$$[q_{n-1}, \cdots, q_1, q_1, \cdots, q_{n-1}, q_n] = [t_{m-1}, \cdots, t_1, t_1, \cdots, t_{m-1}, t_m] = \rho \text{ (say)}. \tag{9.3}$$

From the results (9.1), (9.2) and (9.3) it follows that

$$1 < \frac{p}{\rho} = \frac{[q_n, \cdots, q_2, q_1, q_1, q_2, \cdots, q_n]}{[q_{n-1}, \cdots, q_1, q_1, \cdots, q_{n-1}, q_n]} = \frac{[t_m, \cdots, t_2, t_1, t_1, t_2, \cdots, t_m]}{[t_{m-1}, \cdots, t_1, t_1, \cdots, t_{m-1}, t_m]}. \tag{9.4}$$

An application of Algorithm 1, to both the continuant terms in (9.4), implies that $m = n$ and

$$q_i = t_i \quad (i = 1, 2, \cdots, n);$$

thus $u = s$, $v = t$ and the uniqueness result is established. □

10. Appendix

In this appendix we reproduce the original 1855 paper [20] of Henry Smith.

DE COMPOSITIONE NUMERORUM PRIMORUM FORMAE $4\lambda+1$ EX DUOBUS QUADRATIS

[Crelle's Journal, vol. L. pp. 91, 92; 1855.]

Sit

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}$$

fractio continua, cujus numerator, qui determinanti

$$\begin{vmatrix} q_1, & 1, & 0, & 0, & \cdot & \cdot & \cdot & 0 \\ -1, & q_2, & 1, & 0, & \cdot & \cdot & \cdot & 0 \\ 0, & -1, & q_3, & 1, & \cdot & \cdot & \cdot & 0 \\ 0, & 0, & -1, & q_4, & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ 0, & 0, & 0, & 0, & \cdot & \cdot & -1, & q_n \end{vmatrix}$$

aequalis est, per hujusmodi formulam $(q_1\ q_2\ q_3 \cdots q_{n-1}\ q_n)$ exprimatur. Erit ergo

$$[q_1\ q_2\ \cdots q_{i-1}\ q_i] = [q_i\ q_{i-1} \cdots\ q_2\ q_1]$$

et

$$[q_1 \cdots q_n] = [q_1\ q_2 \cdots q_i] \cdot [q_{i+1} \cdots q_n] + [q_1\ q_2 \cdots q_{i-1}] \cdot [q_{i+2} \cdots q_n];$$

quae aequationes pendent ab illa forma determinantali, ambae autem L. Eulero debentur.

Itaque, si quantitatum q *par* sumatur numerus, ipsaeque ita serie symmetrica disponantur, ut binae inter se aequales fiant, elucet, quantitatem $[q_1\ q_2 \cdots q_i\ q_i \cdots q_2\ q_1]$ summam fore duorum quadratorum inter se primorum; fit enim

$$[q_1 q_2 \cdots q_i q_i \cdots q_2 q_1] = [q_1 q_2 \cdots q_i]^2 + [q_1 q_2 \cdots q_{i-1}]^2 \cdots$$

Contra in numero quotientium *impari,* erit

$$[q_1 \cdots q_{i-1}\ q_i\ q_{i-1} \cdots q_2\ q_1] = (q_1 \cdots q_{i-1}) \cdot \{[q_1 \cdots q_i] + [q_1 \cdots q_{i-2}]\},$$

unde colligis, numerum $[q_1 \cdots q_i \cdots q_1]$ primum esse non posse, nec duplicem numeri primi; si quidem casus excipis, in quibus, aut i unitati aequatur, aut i binario, q unitati.

Sit p numerus integer datus; $\mu_1, \mu_2, \cdots \mu_s$ series numerorum, qui ad p primi sunt, ipsiusque p dimidio minores.

Formentur fractiones continuae $\frac{p}{\mu_1}, \frac{p}{\mu_2}, \cdots \frac{p}{\mu_s}$; quae omnes ita terminentur, ut is quotiens qui in extremo loco ponatur unitatem superet. Hinc patet, quanta fuerit numerorum

$\mu_1, \mu_2, \cdots \mu_s$ multitudo, tantum fore numerum determinantium $[q_1 \cdots q_n]$, qui dato numero p aequales erunt, neque praeter illos ullum dare ejusdem formae determinantem, cujus et primus et extremus quotiens unitate major sit, quique numero p aequalis esse possit.

Jam vero, quum duo determinantes $[q_1 \cdots q_n]$ et $[q_n \cdots q_1]$ aequales sint, quumque ipsum q_n unitate majus sit, apparet $[q_n \cdots q_1]$ ex una aliqua fractionum $\frac{p}{\mu}$ oriri. Unde sequitur, data quavis fractione $\frac{p}{\mu}$, inveniri posse aliam in eadem serie, quae quotientes eosdem, ordine inverso, repraesentet.

Sit p primus, formae $4\lambda + 1$; ut numerus determinantium ipsi p aequalium par existat. Quum ipse p unus e determinantium serie fiat, unus certo alius inveniri poterit in quo quotientium ordo invertendo non mutatur. Cum sit ergo

$$p = [q_1\ q_2 \cdots q_i\ q_i \cdots q_2\ q_1]$$

erit denique

$$p = [q_1 q_2 \cdots q_i]^2 + [q_1 q_2 \cdots q_{i-1}]^2.$$

Quam theorematis Fermatiani demonstrationem maxime elementarem esse patet, quum pendeat a conversione fractionum vulgarium in fractiones continuas.

Singulos autem formae $1 + x^2$ divisores ex duobus quadratis conflari, eodem modo demonstrare in promptu est. Sit enim

$$\mu\nu = 1 + x^2,$$

apparet fore

$$\mu = [q_1\ q_2 \cdots q_i\ q_i \cdots q_2\ q_1]$$
$$\nu = [q_2\ q_3 \cdots q_i\ q_i \cdots q_3\ q_2]$$
$$x = [q_1\ q_2 \cdots q_i\ q_i \cdots q_2].$$

Oxford, *Maio* 1854.

Acknowledgement 1. *Norrie Everitt thanks his three co-authors for their agreement to dedicate this paper to Paul Halmos who, from afar, has been his guide and mentor in mathematics. This paper should have been completed some years ago for a volume dedicated to Paul Halmos; apologies for the delay but I hope the paper is now the better for subsequent collaboration and extension.*

All four authors thank Keith Hannabuss, Fellow and Tutor in Mathematics of Balliol College in Oxford, for his contribution to the Section on the life of Henry Smith; we have been guided by and quoted from his papers [10] *and* [11]*; additionally we have had access to, and quoted from a yet unpublished account of the life of Henry Smith.*

References

[1] C.W. Barnes. 'The representation of primes of the form $4n + 1$ as the sum of two squares.' *Enseign. Math.* (2) **18** (1972), 289-299.

[2] E.T. Bell. *Men of Mathematics.* (Victor Gollancz Ltd., London; 1937.)

[3] J. Brillhart. 'Note on representing a prime as a sum of two squares.' *Math. Comp.* **26** (1972), 1011-1013.
[4] D.M. Burton. *Elementary Number Theory.* (The McGraw- Hill Companies, Inc., New York; 1998.)
[5] G.E. Chrystal. *Algebra:* **I** and **II**. (Adam and Charles Black, Edinburgh; 1889. The 6th. edition reprinted by Chelsea Publishing Co., New York; 1959.)
[6] H.A. Davenport. *The Higher Arithmetic.* (Hutchinson House, London; 1952.)
[7] L.E. Dickson. *History of the Theory of Numbers:* **II**. (Chelsea Publishing Co., New York; 1966.)
[8] U. Dudley. *Elementary Number Theory.* (2nd. edition. W.H. Freeman and Company, New York; 1978.)
[9] J.A. Ewell. 'A simple proof of Fermat's two-square theorem.' *Amer. Math. Monthly.* **90** (1983), 635-637.
[10] K. Hannabuss. 'The mathematician the world forgot.' *New Scientist.* **97** (1983), 901-903.
[11] K. Hannabuss. 'Forgotten fractals.' *The Mathematical Intelligencer.* **18** (1996), 28-31.
[12] G.H. Hardy. *A Mathematician's Apology.* (Cambridge University Press; 1969).
[13] G.H. Hardy, J.E. Littlewood and G. Pólya. *Inequalities.* (Cambridge University Press; 1952.)
[14] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* (5th edition. Oxford University Press; 1979.)
[15] T. Hawkins. *Lebesgue's Theory of Integration; Its Origins and Development.* (Chelsea Publishing Co., New York; 1975.)
[16] D.R. Heath-Brown. 'Fermat's two-squares theorem.' *Invariant.* (1984), 3-5.
[17] C. Hermite. 'Note au sujet de l'article précedent. *J. Math. Pures Appl.* **13** (1848), 15.
[18] T. Muir and W.H. Metzler. *A Treatise on the Theory of Determinants.* (Dover Publications. Inc., New York; 1960.)
[19] J.-A. Serret. 'Sur un théorème relatif aux nombres entiers.' *J. Math. Pures Appl.* **13** (1848), 12-14.
[20] H.J.S. Smith. 'De Compositione Numerorum Primorum $4\lambda+1$ Ex Duobus Quadratis.' *Crelle's Journal.* **L** (1855), 91-92.
[21] H.J.S. Smith. *The Collected Mathematical Papers of Henry John Stephen Smith:* **I** and **II**. (Edited by J.W.L. Glaisher. The Clarendon Press, Oxford; 1894. Reprinted by Chelsea Publishing Co., New York; 1965.)
[22] S. Wagon. 'The Euclidean algorithm strikes again.' *Amer. Math. Monthly.* **97** (1990), 125-129.
[23] D. Zagier. 'A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.' *Amer. Math. Monthly.* **197** (1990), 144.

F.W. Clarke, Department of Mathematics, University of Wales Swansea, Singleton Park, Swansea SA2 8PP, Wales, UK
E-mail address: f.clarke@swansea.ac.uk

W.N. Everitt, School of Mathematics and Statistics, University of Birmingham, Edgbaston, Birmingham B15 2TT, England, UK
E-mail address: w.n.everitt@bham.ac.uk

L.L. Littlejohn, Department of Mathematics and Statistics, Utah State University, Logan, UT 84322-3900, USA
E-mail address: lance@sunfs.math.usu.edu

S.J.R. Vorster, Department of Mathematics, Applied Mathematics and Astronomy, University of South Africa, P.O. Box 392, 0001 Pretoria, Republic of South Africa
E-mail address: vorstsjr@alpha.unisa.ac.za