

HENRY JOHN STEPHEN SMITH  
AND FERMAT'S  
TWO SQUARES THEOREM

Lance L. Littlejohn

Utah State University, Logan, Utah, U.S.A.

March/April 2005

AbiTUMath Program, Novacella, Italy

Lecture taken from the article “**H. J. S. Smith and the Fermat Two Squares Theorem**” (The American Mathematical Monthly, August/September issue, 1999, pp. 652-665)

Joint work with F. W. Clarke (Wales), W. N. Everitt (England), and S. J. R. Vorster (South Africa)

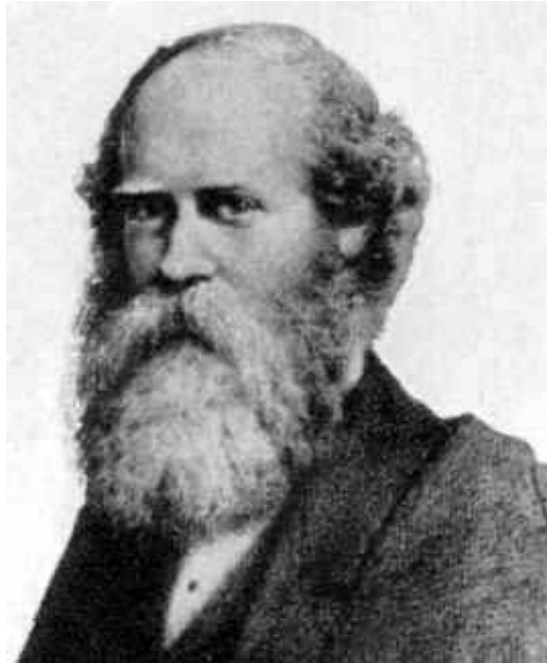


Figure 1: HJS Smith (1826-1883)

- \* Recently, Smith was called "*the mathematician the world forgot*"
- \* **Savilian Professor of Geometry** (chosen over George Boole); succeeded Baden Powell
- \* Elected as a **Fellow of the Royal Society** in 1861 (with James Clerk Maxwell)
- \* 1874-1876: **President of the London Mathematical Society**

\* H. J. S. Smith is the “Smith” of the *Smith normal form* of a matrix (cyclic decomposition theorem for modules, control theory; see “*On systems of linear indeterminate equations and congruences*”, *Philos. Trans. Roy. Soc. Lond.*, 151, 1861, 293-326)

\* 1859-1865: wrote his “**Report on the Theory of Numbers**” described as “*the most complete and elegant monument ever erected to the theory of numbers*”

\* Smith won the *Steiner Prize* of the Royal Academy of Sciences in Berlin for his solution of a geometrical problem

\* He was awarded (posthumously) the *Grand Prix* (shared with H. Minkowski) from the French Academy in 1883 for his work on the number of ways an integer can be represented as a sum of five squares

\* In his paper “*On the integration of discontinuous functions*” (1875), Smith discovered the “*Cantor set*” eight years before Cantor did; generalized result to higher dimensions as well (*Koch snowflake* and the *Sierpinski gasket*)

\* Smith corrected a mistake by Riemann in Riemann's (new) approach to integral calculus and gave an ingenious example to show that the scope of the theory was not quite so great as some had claimed. Smith anticipated a more general integral some 35 years before Lebesgue! In fact, Thomas Hawkins wrote:

“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...”

\* After Smith's death, his friend Benjamin Jowett wrote in the *London Times*:

“Henry Smith seems now to be recognized as the greatest English mathematician of the century. I did not know this during his lifetime, and used to think him wanting in originality because his mind was absorbed in the mathematical world”

G.H. Hardy, in his book "*A Mathematician's Apology*", wrote:

"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

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

3, 7, 11, 19, 23, 31

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

$$\begin{aligned} 5 &= 1^2 + 2^2, & 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2, & 29 &= 2^2 + 5^2 \end{aligned}$$

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."**

**Theorem (Fermat)** Suppose  $p$  is a prime number with  $p \equiv 1 \pmod{4}$ . Then there exists unique, co-prime  $u, v \in \mathbb{N}$  such that

$$p = u^2 + v^2.$$

**Example 1**  $p = 17 = 4^2 + 1^2$ .

**Example 2**  $p = 73 = 8^2 + 3^2$ .

**Definition** Let  $n \in \mathbb{N}$  and  $q_1, q_2, \dots, q_n \in \mathbb{N}$ . Define the **continuant** of the ordered  $n$ -tuple  $(q_1, q_2, \dots, q_n)$  to be

$$[q_1] = q_1$$

and

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

**Example 3**  $[4, 5] = \begin{vmatrix} 4 & 1 \\ -1 & 5 \end{vmatrix} = 21.$

**Example 4**  $[1, 2, 3] = \begin{vmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 0 & -1 & 3 \end{vmatrix} = 10;$  in general,  
 $[q_1, q_2, q_3] = q_1q_2q_3 + q_1 + q_3.$

**Properties of Continuants:** Let  $n \in \mathbb{N}$  with  $n \geq 2$ .

- 1)  $[q_1, q_2, \dots, q_n] = q_1[q_2, q_3, \dots, q_n] + [q_3, q_4, \dots, q_n];$
- 2)  $[q_1, q_2, \dots, q_n] \in \mathbb{N};$
- 3)  $[q_1, q_2, \dots, q_n] = [q_n, q_{n-1}, \dots, q_1];$
- 4)  $[q_2, q_3, \dots, q_n] < [q_1, q_2, \dots, q_n];$
- 5)  $\gcd([q_2, q_3, \dots, q_n], [q_1, q_2, \dots, q_n]) = 1;$
- 6)  $[q_1, q_2, \dots, q_{s-1}, q_s, q_{s+1}, q_{s+2}, \dots, q_n] =$   
 $[q_1, q_2, \dots, q_s][q_{s+1}, q_{s+2}, \dots, q_n]$   
 $+ [q_1, q_2, \dots, q_{s-1}][q_{s+2}, q_{s+3}, \dots, q_n].$

## Continuants and the Euclidean Algorithm (EA)

Suppose  $r, s \in \mathbb{N}$  with  $(r, s) = 1$  and  $r < s$ . Then there exists unique  $q_1, \dots, q_n, u, \dots, x, y \in \mathbb{N}$  with

$$\begin{aligned} s/r &= q_1 + u/r \\ r/u &= q_2 + v/u \\ &\vdots \\ x/y &= q_n + 0, \end{aligned}$$

where  $n \geq 2$  and  $q_n \geq 2$ . Moreover,  $s = [q_1, q_2, \dots, q_n]$  and  $r = [q_2, q_3, \dots, q_n]$ .

(Last part is easy to see by Property 1:

$$\begin{aligned} \frac{[q_1, q_2, \dots, q_n]}{[q_2, q_3, \dots, q_n]} &= \frac{q_1[q_2, q_3, \dots, q_n] + [q_3, q_4, \dots, q_n]}{[q_2, q_3, \dots, q_n]} \\ &= q_1 + \frac{[q_3, q_4, \dots, q_n]}{[q_2, q_3, \dots, q_n]} \text{ and use induction.)} \end{aligned}$$

Example 5  $r = 7, s = 10$ . Then

$$\frac{10}{7} = 1 + \frac{3}{7}, \quad \frac{7}{3} = 2 + \frac{1}{3}, \quad \frac{3}{1} = 3 + \frac{0}{1}.$$

Also,  $s = 10 = [1, 2, 3]$  and  $r = 7 = [2, 3]$ .

## Smith's Existence Proof

Let  $p \equiv 1 \pmod{4}$ ; i.e.  $p = 1 + 4r$ .

Suppose  $\mu \in \{2, 3, \dots, 2r\}$ ; from EA, there exists  $n = n(p, \mu) \in \mathbb{N}$ ,  $q_1, q_2, \dots, q_n \in \mathbb{N}$  such that

$$p = [q_1, q_2, \dots, q_n], \mu = [q_2, q_3, \dots, q_n] \text{ and}$$

$$\frac{p}{\mu} = \frac{[q_1, q_2, \dots, q_n]}{[q_2, q_3, \dots, q_n]}.$$

Moreover,  $q_1 \geq 2$  and  $q_n \geq 2$ . Notice, from the symmetry of continuants that  $p = [q_n, q_{n-1}, \dots, q_1]$ . Put  $v = [q_{n-1}, q_{n-2}, \dots, q_1]$ .

Claim:  $v \in \{2, 3, \dots, 2r\}$ :

First, by Property 1,

$$\begin{aligned} v &= [q_{n-1}, q_{n-2}, \dots, q_1] = [q_1, q_2, \dots, q_{n-1}] \\ &= q_1[q_2, q_3, \dots, q_{n-1}] + [q_3, q_4, \dots, q_{n-1}] \geq q_1 \geq 2. \end{aligned}$$

Secondly, also by Property 1,

$$\begin{aligned}\frac{p}{v} &= \frac{[q_n, q_{n-1}, \dots, q_1]}{[q_{n-1}, q_{n-2}, \dots, q_1]} \\ &= \frac{q_n [q_{n-1}, q_{n-2}, \dots, q_1] + [q_{n-2}, q_{n-3}, \dots, q_1]}{[q_{n-1}, q_{n-2}, \dots, q_1]} \\ &= q_n + \frac{[q_{n-2}, q_{n-3}, \dots, q_1]}{[q_{n-1}, q_{n-2}, \dots, q_1]} \geq q_n \geq 2\end{aligned}$$

so that  $v \leq \frac{p}{2} = 2r + \frac{1}{2}$  and hence  $v \leq 2r$ .

**To summarize:** Associated with every  $\mu = [q_2, q_3, \dots, q_m] \in \{2, 3, \dots, 2r\}$  is a unique *mate*  $v = [q_{m-1}, q_{m-2}, \dots, q_1] \in \{2, 3, \dots, 2r\}$ , where  $\{q_1, q_2, \dots, q_m\} \subset \mathbb{N}$  is such that  $p = [q_1, q_2, \dots, q_m]$ . Notation:  $\mu \sim v$ .

**Example 6**  $p = 13 = 4(3) + 1$  so  $r = 3$  and we consider  $\mu \in \{2, 3, 4, 5, 6\}$ .

$$\frac{13}{2} = \frac{[6, 2]}{[2]}, \quad \frac{13}{3} = \frac{[4, 3]}{[3]}, \quad \frac{13}{4} = \frac{[3, 4]}{[4]}$$

$$\frac{13}{5} = \frac{[2, 1, 1, 2]}{[1, 1, 2]}, \quad \frac{13}{6} = \frac{[2, 6]}{[6]}$$

Moreover,  $2 \sim 6$ ,  $3 \sim 4$ , and  $5 \sim 5$ .

In general, since there is an odd number of elements in  $\{2, 3, \dots, 2r\}$ , this means at least one element - say  $\lambda$  - must mate with itself.

$$\text{i.e. } \lambda = [q_2, q_3, \dots, q_m] = [q_{m-1}, q_{m-2}, \dots, q_1];$$

We call such a  $\lambda$  a **Smith number** associated with  $p$ .

Apply the Euclidean Algorithm to:

$$\frac{p}{\lambda} = \frac{[q_1, q_2, \dots, q_m]}{[q_2, q_3, \dots, q_m]} = \frac{[q_m, q_{m-1}, \dots, q_1]}{[q_{m-1}, q_{m-2}, \dots, q_1]}.$$

$$\frac{p}{\lambda} = q_1 + \frac{u}{\lambda} = q_m + \frac{u}{\lambda} \text{ so } q_1 = q_m$$

$$\frac{\lambda}{u} = q_2 + \frac{v}{u} = q_{m-1} + \frac{v}{u} \text{ so } q_2 = q_{m-1}$$

$$\frac{u}{v} = q_3 + \frac{x}{v} = q_{m-2} + \frac{x}{v} \text{ so } q_3 = q_{m-2},$$

⋮

$$\frac{x}{y} = q_m + \frac{0}{y} = q_1 + \frac{0}{y}; \text{ i.e. as before, } q_m = q_1.$$

In general, for this choice of  $\lambda$ ,  $q_i = q_{m-i+1}$  ( $i = 1, 2, \dots, m$ ) and  $p = [q_1, q_2, \dots, q_2, q_1]$  is **palindromic**.

Suppose that  $m$  is odd; i.e.  $m = 2t + 1$ .

Then, from Property 6,

$$\begin{aligned} p &= [q_1, q_2, \dots, q_m] = [q_1, q_2, \dots, q_t, q_{t+1}, q_t, \dots, q_2, q_1] \\ &= [q_1, q_2, \dots, q_{t+1}][q_t, q_{t-1}, \dots, q_1] \\ &\quad + [q_1, q_2, \dots, q_t][q_{t-1}, q_{t-2}, \dots, q_1] \\ &= [q_1, q_2, \dots, q_t] \{ [q_1, q_2, \dots, q_{t+1}] + [q_{t-1}, q_{t-2}, \dots, q_1] \}. \end{aligned}$$

But this says that  $[q_1, q_2, \dots, q_t]$  divides  $p$ , contradicting the fact that  $p$  is prime.

Consequently  $m$  is even; i.e.  $m = 2t$  and  $p$  has the form

$$\begin{aligned}
 p &= [q_1, q_2, \dots, q_{t-1}, q_t, q_t, q_{t-1}, \dots, q_2, q_1] \\
 &= [q_1, q_2, \dots, q_t][q_t, q_{t-1}, \dots, q_1] \\
 &\quad + [q_1, q_2, \dots, q_{t-1}][q_{t-1}, q_{t-2}, \dots, q_1] \\
 &= [q_1, q_2, \dots, q_t]^2 + [q_1, q_2, \dots, q_{t-1}]^2 \text{ when } t > 1.
 \end{aligned}$$

where we have used Properties 3 and 6 of continuants. Moreover, from Property 5,  $[q_1, q_2, \dots, q_t]$  and  $[q_1, q_2, \dots, q_{t-1}]$  are co-prime.

If  $t = 1$ , then  $p = [q_1, q_1] = q_1^2 + 1$  which is the sum of two squares.

This completes Smith's existence proof!

**Example 7**  $p = 13$ . In this case,  $\lambda = 5 = [1, 1, 2]$  and

$$\begin{aligned} p = [2, 1, 1, 2] &= [2, 1][1, 2] + [2][2] \\ &= [2, 1]^2 + 2^2 \\ &= 3^2 + 2^2. \end{aligned}$$

Observe that  $\lambda^2 \equiv -1 \pmod{13}$ .

**Example 8**  $p = 41$ . In this case,  $\lambda = 9 = [1, 1, 4]$  and

$$\begin{aligned} p = [4, 1, 1, 4] &= [4, 1][1, 4] + [4]^2 \\ &= [4, 1]^2 + 4^2 \\ &= 5^2 + 4^2. \end{aligned}$$

Observe that  $\lambda^2 \equiv -1 \pmod{41}$ .

## Uniqueness of the Representation

**Fact** Every palindromic continuant representation of  $p$  (and we know it has at least one, namely the Smith number  $\lambda$  found by the existence proof)

$$p = [t_1, t_2, \dots, t_m, t_m, \dots, t_2, t_1],$$

is such that

$$x := [t_2, t_3, \dots, t_m, t_m, \dots, t_2, t_1]$$

satisfies the congruence  $x^2 \equiv -1 \pmod{p}$ .

However, from Euler's Criterion, this quadratic congruence has exactly two solutions (modulo  $p$ ):  $\lambda$  and  $p - \lambda$ , where  $\lambda$  is the Smith number from Smith's existence proof.

Also,  $p - \lambda > 2r$  so  $\lambda$  is the only such Smith number in the set  $\{1, 2, \dots, 2r = (p - 1)/2\}$ .

Now suppose  $p \equiv 1 \pmod{4}$  and there are two co-prime, two-squares representations of  $p$  :

$$p = u^2 + v^2 = r^2 + s^2,$$

where  $u < v$  and  $r < s$ . Apply the Euclidean algorithm:

$$1 < \frac{v}{u} = \frac{[q_1, q_2, \dots, q_n]}{[q_2, q_3, \dots, q_n]}$$

and

$$1 < \frac{s}{r} = \frac{[t_1, t_2, \dots, t_m]}{[t_2, t_3, \dots, t_m]}.$$

From Property 6,

$$\begin{aligned} p &= u^2 + v^2 = [q_1, q_2, \dots, q_n]^2 + [q_2, q_3, \dots, q_n]^2 \\ &= [q_n, q_{n-1}, \dots, q_1, q_1, \dots, q_{n-1}, q_n] \end{aligned}$$

$$\begin{aligned} p &= r^2 + s^2 = [t_1, t_2, \dots, t_m]^2 + [t_2, t_3, \dots, t_m]^2 \\ &= [t_m, t_{m-1}, \dots, t_1, t_1, \dots, t_{m-1}, t_m]; \end{aligned}$$

that is, **two palindromic representations of  $p$ .**

Hence

$$\lambda_1 := [q_{n-1}, \dots, q_1, q_1, \dots, q_n]$$

and

$$\lambda_2 := [t_{m-1}, \dots, t_1, t_1, \dots, t_m]$$

both satisfy the congruence  $x^2 \equiv -1 \pmod{p}$ .

**Claim**  $1 \leq \lambda_1, \lambda_2 \leq (p-1)/2 = 2r$

Indeed, from the Euclidean Algorithm, we have  $q_n \geq$

2. Applying Property 1 to

$$p = [q_n, q_{n-1}, q_{n-3}, \dots, q_{n-1}, q_n] = 4r + 1,$$

we see that

$$\begin{aligned} \frac{p}{\lambda_1} &= \frac{q_n[q_{n-1}, \dots, q_n] + [q_{n-3}, \dots, q_n]}{[q_{n-1}, \dots, q_n]} \\ &= q_n + \frac{[q_{n-3}, \dots, q_n]}{[q_{n-1}, \dots, q_n]} \\ &\geq q_n \geq 2, \end{aligned}$$

so  $\lambda_1 \leq 2r$ . Similarly,  $\lambda_2 \in \{1, 2, \dots, 2r\}$ .

From uniqueness, we have

$$\lambda_1 = \lambda_2;$$

that is to say,

$$[q_{n-1}, \dots, q_1, q_1, \dots, q_n] = [t_{m-1}, \dots, t_1, t_1, \dots, t_m] = \lambda.$$

Apply the Euclidean Algorithm to the two representations of  $p/\lambda$

$$\frac{p}{\lambda} = \frac{[q_n, \dots, q_1, q_1, \dots, q_n]}{[q_{n-1}, \dots, q_1, q_1, \dots, q_n]} = \frac{[t_m, \dots, t_1, t_1, \dots, t_m]}{[t_{m-1}, \dots, t_1, t_1, \dots, t_m]}$$

to obtain  $n = m$  and  $q_i = t_i$  for  $i = 1, 2, \dots, n$ . Consequently,

$$u = [q_1, q_2, \dots, q_n] = [t_1, t_2, \dots, t_m] = r,$$

and, similarly,

$$v = [q_2, q_3, \dots, q_n] = [t_2, t_3, \dots, t_m] = s.$$

and this completes the uniqueness proof.