On Perron's proof of Fermat's two square theorem

JAROSLAW GRYTCZUK

Abstract. Fermat's two square theorem states that every prime of the form $4m+1$ is the sum of two squares. In this note we give a new proof for this using continued fraction expansion of squareroot of non-square integers.

It is well known that if a natural number d is not a perfect square the simple continued fraction expansion of $\sqrt{d}$ is periodic and has the form $\sqrt{d} =< a_0, \overline{a_1, a_2, \cdots a_s} >$, where $a_i = [(m_i + \sqrt{d})/q_i]$, $m_0 = 0$, $q_0 = 1$ and

$$m_i = a_{i-1}q_{i-1} - m_{i-1}, \tag{1}$$

$$q_i q_{i-1} = d - m_i^2. \tag{2}$$

(See for example in [1]). From these relations and some theorems concerning diophantine equations O. Perron deduces in [2, p.98] the famous result of Fermat: Every prime of the form $4m + 1$ is a sum of two squares.

In this note we will show that it is possible to do the same restricting theoretical tools to the above algorithm.

Proof of the Two Square Theorem. The main idea is the same as Perron's and lies in the palindromatic nature of the fragments $(m_1, \cdots, m_s)$ and $(q_0, \cdots, q_s)$, (see [2, p.76]). In view of this and (2) d is a sum of two squares whenever s is odd. So, we'll be done showing that this is the case for the primes $p = 4m + 1$.

Suppose then, that $p \equiv 1 \pmod 4$ and the length of the shortest period of the continued fraction expansion of $\sqrt{p}$ is even, say $s = 2k$. Then we have $m_k = m_{k+1}$ and after some substitutions;

$$2m_k = a_k q_k \tag{3}$$

and

$$q_k(4q_{k-1} + a_k^2 q_k) = 4p. \tag{4}$$

Analysing the last equation we conclude that $q_k = 2$ or $q_k = 1$. However, the second possibility occurs only if k is a multiple of s [1, p.171]. Hence q_k and q_{k-1} are even a_k is odd and because of (3) so is m_k. From (1) m_{k-1} is odd. too. Actually, the parity of q_i and m_i remains unchanged for further indices $i = k-2, k-3, \ldots, 1, 0$. Indeed, puting (1) to (2) we obtain

$$q_i = q_{i-2} + a_{i-1}(m_{i-1} - m_i) \tag{5}$$

and now looking by turns on (5) and (1) we get the announced effect. But this is contrary to the initial conditions $m_0 = 0$, $q_0 = 1$ and the proof is complete.

References

[1] I. NIVEN and H. ZUCKERMAN, An Introduction to The Theory of Numbers, Third Edition, John Wiley and Sons, (1972).

[2] O. PERRON, Die Lehre von den Kettenbrüchen, Teubner, Stuttgart, (1954).