Mathematica Pannonica
8/2 (1997), 293–295

A SHORT PROOF OF FERMAT'S TWO-SQUARE TEOREM GIVEN BY JÁNOS BOLYAI

Elemér **Kiss**

Department of Mathematics, University "Petru Maior" of Tg. Mureş, str. N. Iorga 1, 4300 Tg. Mureş, Romania

Dedicated to Prof. I. Gy. Maurer on the occasion of his 70^{th} birthday

Received: March 1997

MSC 1991: 01 A 55, 11 A 41

Keywords: The two-square theorem, integers of Gauss.

Abstract: This paper presents the short proof of Fermat's two-square theorem given by János Bolyai about 140 years ago.

The two-square theorem — which sais that all prime numbers of form $4k+1$ are the sum of two squares — is considered by the history of mathematics to belong to P. Fermat (1601–1665). The theorem has been proved for the first time by L. Euler (1707–1783) in 1754, but mathematicians are still interested in it. In the last decades, and moreover, in the last years many works have been published, the authors of which attempted to give shorter and more simple proofs ([1], [2], [6], [7], [8], [11], [12]).

It probably sounds surprising, but János Bolyai, who is known as the inventor of non-euclidean geometry, was also engaged with Fermat's theorem, and proved it in many ways. Three of these proofs have already been presented in [9], but as a result of the most recent examinations of his manuscripts, a fourth short proof appeared, too. In this proof he applied the theory of complex integers, which has also been worked out by him independently of Gauss [9], [10]. In the followings we will present this proof.

János Bolyai starts from the theorem, that if p is a prime number of form $4k+1$, then there exists such an integer x, that $\frac{x^2+1}{p}$ is an integer. By writing this fraction in the form $\frac{(x+i)(x-i)}{p}$, he proves first, that p as complex integer cannot be a prime number ([3], 1332/1). So $p=(a+bi)(c+di)$, where a, b, c and d are nonzero integers. But then $p=(a-bi)(c-di)$, so $p^2=p\cdot p=(a^2+b^2)(c^2+d^2)$, and because $a^2+b^2>1$ and $c^2+d^2>1$, it results $p=a^2+b^2=c^2+d^2$ ([3], $1333/1^v$).

Bolyai noted this proof in a letter addressed to his father in the middle 1850's. Before him, only G. Eisenstein (1823–1852) proved Fermat's theorem using complex integers, in 1844, but Bolyai did not know Eisenstein's work. By comparing Eisenstein's proof ([4], [5]) with Bolyai's above presented procedure, we can easily conclude, that the two proofs are different.

Finally we remark, that Bolyai's 140 years old thoughts can be found nowadays in many school-books.

References

[1] BARNES, C. W. The representation of primes of the form $4n+1$ as the sum of two squares, *Enseignement Math.* **18**/2 (1972), 289–299.

[2] BARNES, C. W.: Primes of the form $4n+1$ which can be written as the sum of two squares, *J. Elisha-Mitchell-Sci. Soc.* **89** (1973), 226–227.

[3] BOLYAI J.: Manuscripts, Teleki-Bolyai Library, Târgu-Mureş.

[4] DICKSON, L. E.: History of the Theory of Numbers, Chelsea, New York, 1952.

[5] EISENSTEIN, G.: Beiträge zur Kreisteilung, *Jour. für Math.* **27**/3 (1844), 269–278.

[6] EWELL, J. A.: A simple proof of Fermat's two-square theorem, *Amer. Math. Monthly* **90**/9 (1983), 635–637.

[7] FINE, B.: A note on the two-square theorem, *Canad. Math. Bull.* **20**/1 (1977), 93–94.

[8] GILLETT, J. R.: An alternative representation of sums of two squares, *Math. Gaz.* **55** (1971), no. 391, 59–60.

[9] KISS, E.: Bolyai János vizsgálatai a $4m+1$ alakú prímszámok két négyzet összegére való felbontásáról, *Polygon* (Szeged) **6**/2 (1996), 1–8.

[10] KISS, E, Kérdések Bolyai János kutatásairól, *Természet Világa* (Budapest) **127**/11 (1996), 522–523.

[11] VAROUCHAS, I.: Une démonstration élémentaire du théorème des deux carrés, *I. R. E. M. Bull.* **6** (1984), 31–39.

[12] ZAGIER, D.: A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly* **97**/2 (1990), 144.