A THEOREM ON FACTORIZATION*

BY D. N. LEHMER

In a note in this Bulletin† I observed that if $R=pq$ is the product of two odd factors whose difference is less than twice the fourth root of R then the factors of R are obtainable directly from the expansion of $R^{1/2}$ in a continued fraction. This theorem comes from the fact that in view of a theorem due to Lagrange, $(p-q)^2/4$ will appear as a denominator of a complete quotient in that expansion, and that therefore the diophantine equation $x^2-Ry^2=(p-q)^2/4$ will have the integral solution $x=\frac{1}{2}(r+q)$, $y=1$.

The object of the present note is to point out that the method is of much wider application than the above statement would indicate. For consider the identity

$$\left(\frac{mp + nq}{2}\right)^2 - \left(\frac{mp - nq}{2}\right)^2 = mnpq.$$

From this it appears that if mn is a square and if m and n are both odd or both even, we will have an integral solution of the equation

$$x^2 - Ry^2 = \frac{1}{4}(mp - nq)^2,$$

namely

$$x = \frac{1}{2}(mp + nq), \qquad y = (mn)^{1/2}.$$

By Lagrange's theorem, therefore, if $mp-nq<2R^{1/4}$ one of the denominators in the expansion of $R^{1/2}$ will certainly be $(mp-nq)^2/4$ and since the numerator of the preceding convergent will be $(mp+nq)/2$ these two numbers will serve to furnish the factors p and q of R. We have then the following theorem.

* Presented to the Society, San Francisco Section, October 30, 1926.

† Vol. 13 (1906-7), p. 501. Translated in Sphinx-Oedipe, 1911. Given also in Kraitchik's *Recherches sur la Théorie des Nombres*, p. 73.