

be completely defined by giving its elements in order. That is, the expression 'commutator of s and t ' should not have a double meaning. For the most important applications which have been made of commutators any one of the given definitions seems just as good as any other, but there are applications in which the last definition seems to be the most convenient. It may be added that the definition of commutator in the *Encyclopädie der Mathematischen Wissenschaften*, Volume I 1, page 210, is rendered meaningless by typographical errors.

A THEOREM IN THE THEORY OF NUMBERS.

BY PROFESSOR D. N. LEHMER.

(Read before the San Francisco Section of the American Mathematical Society, December 19, 1903.)

LAGRANGE has shown that if the indeterminate equation $x^2 - Ry^2 = \pm D$ is resolvable in integers, D being less than \sqrt{R} , and x and y being relative primes, then D is a denominator of a complete quotient in the expansion of \sqrt{R} in a continued fraction. (For a proof of this theorem, see Chrystal's *Algebra II*, page 451.) Making use of this result, we may prove the following interesting theorem, which is sometimes very effective in finding the factors of large numbers.

If R is the product of two factors which differ by less than $2\sqrt[4]{R}$, these two factors may be found directly from the expansion of \sqrt{R} in a continued fraction.

Let the two factors be p and q , so that $R = pq$. Then $R = [\frac{1}{2}(p+q)]^2 - [\frac{1}{2}(p-q)]^2$, and the equation $x^2 - Ry^2 = [\frac{1}{2}(p-q)]^2$ is resolvable in integers. If now $[\frac{1}{2}(p-q)]^2$ is less than \sqrt{R} , then by the theorem quoted above, there will be a denominator of a complete quotient in the expansion of \sqrt{R} equal to $[\frac{1}{2}(p-q)]^2$. Since $[\frac{1}{2}(p-q)]^2 < \sqrt{R}$, then $p - q < 2\sqrt[4]{R}$. Moreover the values of the indeterminates in the equation $x^2 - Ry^2 = \pm D$, are furnished by the numerator and denominator of the convergent which immediately precedes the complete quotient having D for a denominator. Hence it follows that the expansion of \sqrt{R} need not be carried farther than is sufficient to make the numerator of the convergent as