

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

great as  $R$ . The method may be applied to  $\kappa R$ , and we have the following theorem :

**THEOREM :** *If no denominator of odd rank, after the first, in the complete quotients obtained by expanding  $\sqrt{\kappa R}$  in a continued fraction, turns out to be a perfect square, the expansion being carried out until the numerator of the last convergent is greater than  $\kappa R$ , then the factors of  $\kappa R$  differ by more than  $2\sqrt[4]{\kappa R}$ .*

As an example of the application of this theorem to the discovery of prime factors, take Jevons's\* number  $8616460799 = R$ . No perfect square appears in the denominators of the complete quotients obtained in expanding  $\sqrt{R}$ , whence one infers that the factors differ by more than  $608 = 2\sqrt[4]{R}$ . Similar failure attends the expansion of  $\sqrt{2R}$ ,  $\sqrt{6R}$ , and  $\sqrt{30R}$ . On expanding  $\sqrt{210R}$ , however, the third denominator is found to be the square  $11881 = 109^2$ . The numerator of the second convergent is 2690321; we know then that the numbers  $2690321 \pm 109$  contain the desired factors of the given number. The factors are 89681 and 96079.

The most advantageous value of  $\kappa$  to take is the product of the smallest distinct primes. Thus if  $\kappa = 30$  and the factors of  $R$  are  $p$  and  $q$ , then the factors will be discovered if  $p - 30q$ ,  $2p - 15q$ ,  $3p - 10q$ , or  $5p - 6q$  are less than  $2\sqrt[4]{30R}$ .

BERKELEY, CAL.

---

## PROJECTIONS OF THE GLOBE APPROPRIATE FOR LABORATORY METHODS OF STUDYING THE GENERAL CIRCULATION OF THE ATMOSPHERE.

BY PROFESSOR CLEVELAND ABBE.

THE general circulation of the atmosphere is controlled by the general distribution of land and water, and by the insolation, with its resultant temperature, evaporation and clouds. In the analytic treatment of this problem, beginning with D'Alembert, Ferrel, and Erman, as well as in the more elegant works

---

\* Jevons, Principles of science, p. 123, "Can the reader say what two numbers multiplied together will produce the number 8616460799? I think it unlikely that anyone but myself will ever know." I think that the number has been resolved before, but I do not know by whom.