point of ac with a point of b and join a point of ab with a point of c. Let x_1 in ab, x_2 in ac, be the points where this line meets these spaces. The line then contains x, x_1, x_2 all in a, where although x_1 and x_2 might coincide, neither could be x. But then the line would lie wholly in a, contrary to hypothesis. Hence $x(ab+ac)=0$, and (2) is established. Likewise y cannot be in $ab+bc$. For if it were then $x+y$ would be in $a+ab+bc=a+bc$, contrary to hypothesis. Thus (4) is established, and (6) follows similarly. Hence for a to fail to be distributive in the second sense implies Case A. Conversely given Case A, then a fails to be distributive with respect to b and c in the second sense. Indeed y will then be in $a+b$ and also in $x+y$ which is in $a+c$. But y will not be in $a+bc$. For y is in b, but not in $ab+bc$, hence not in ab nor bc, hence not in a nor bc. If y were yet in $a+bc$, there would be a point u in a, and a point v in bc such that y would be in $u+v$. But y and v are then distinct and are both in b. Hence $u+v$ is in b, and u is in b. Hence u is in ab. Hence y would be in $ab+bc$ contrary to hypothesis. Hence Case A is a necessary and sufficient condition that a fail to be distributive with respect to b and c in the second sense.

Since Case B is necessary and sufficient for a to be distributive with respect to b and c in the first sense and again also in the second sense, Theorem 1 is proved. Since this Case B is symmetric in a, b, and c, Theorem 2 is proved.

BROWN UNIVERSITY

ON FACTORING LARGE NUMBERS*

BY D. H. LEHMER† AND R. E. POWERS

1. *Introduction*. Various non-tentative methods of factoring a given odd number N, based on the expansion of $N^{1/2}$ in a regular continued fraction, have been described.‡ The success of most of these methods depends on the appearance of a perfect square among the denominators of the complete quotients. In practice, however, such an event occurs all too infrequently. More often

* Presented to the Society, April 11, 1931.

† National Research Fellow.

‡ Dickson, *History of the Theory of Numbers*, vol. 1, Chapter 14; and D. N. Lehmer, this Bulletin, vol. 13, p. 501, and vol. 33, pp. 35–36.