# QUADRATIC RESIDUES IN FACTORIZATION*

BY MARSHALL HALL

1. *Introduction.* The purpose of this paper is to establish a certain theorem which is useful in the factorization of large numbers. Quadratic residues have been frequently used in factorization, particularly by M. Kraïtchik in volume II of his *Recherches sur la Théorie des Nombres.* Beeger† has proved several propositions on the use of quadratic residues in factorization which Kraïtchik tacitly assumed. Quadratic forms are the most convenient representations of a number which give material information as to the type of its prime factors. The knowledge of several quadratic residues of a number is of great aid in finding its factors, but in identifying a prime by its quadratic residues our proof is negative, in that the same result might come about through an error in the calculation. It is to eliminate much of the calculation involved in identifying a prime, and to make the proof of primality positive in character, that the present paper has been undertaken.

2. *Definition of Apparent Residues and Non-Residues.* Following Kraïtchik,‡ I define (quadratic) apparent residues and apparent non-residues in the following manner. If $a$, $b$ are odd primes $>1$, if $(N/\alpha)=+1$ and if $a'=(-1/a)a$, then $a'$ is said to be an apparent residue of $N$.

If $(N/b)=-1$ and if $b'=(-1/b)b$, then $b'$ is said to be an apparent non-residue of $N$. According as the Jacobian symbol $(-1/N)$ is $+1$ or $-1$, $-1$ is said to be an apparent residue or non-residue of $N$. Similarly the apparent characters of $+2$ and $-2$ with respect to $N$ are defined.

We define compound apparent residues and non-residues by calling the product of two apparent residues or two apparent non-residues an apparent residue, and the product of an apparent residue and an apparent non-residue an apparent non-

* Presented to the Society, March 25, 1932.

† Nieuw Archief voor Wiskunde, (2), vol. 16, No. 4, pp. 37–42.

‡ *Recherches sur la Théorie des Nombres*, vol. 2, 1929, p. 8. For Kraïtchik's "résidu éventuel" I write "apparent residue."