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."

residue. No apparent character is given to a number not relatively prime to N, as it is our purpose to find the factors of N, which is supposed to be of unknown composition.

If a number N be prime, then its apparent residues are true residues (that is, $x^2 \equiv a \pmod{N}$, a any apparent residue) and the product of any two apparent non-residues, is a true residue.

3. *A Preliminary Theorem.* We shall now establish various preliminary theorems on apparent residues. We show first the following result.

THEOREM 1. *A number which is a quadratic residue of every prime not dividing it is a perfect square.*

As every odd power of 2 is a non-residue of 3, we may assume that such a number contains an odd factor. Let N be a quadratic residue of every prime not dividing it, and $N = j^2 n$, where n contains no square factors. Then n is a quadratic residue of the same primes as N.

Let $n = p_1 p_2 \cdots p_r$ and let furthermore a be a quadratic non-residue of p_1 (p_1 odd) and b_i be a quadratic residue of p_i, $(i = 2, \cdots, r)$. The congruences $x \equiv 1 \pmod 4$, $x \equiv a \pmod{p_1}$,

$$x \equiv b_i \pmod{p_i} \equiv 1 \pmod 8 \text{ if } p_i = 2, \quad (i = 2, \cdots, r),$$

then always have a solution s, as the moduli are relatively prime. There are an infinite number of prime values for the general solution $x = 4kn + s$. Choose one not dividing j. Then

$$\left(\frac{x}{p_1}\right) = \left(\frac{p_1}{x}\right) = -1, \left(\frac{x}{p_i}\right) = \left(\frac{p_i}{x}\right) = +1, \quad (i = 2, \cdots, r);$$

hence $(N/x) = (n/x) = -1$, contrary to hypothesis, and N must be a perfect square. We have actually proved more than the theorem, namely, that if N is a quadratic residue of all primes except a finite number, then N must be a perfect square.

4. *Compound Characters.* We shall now show that the product of two prime apparent non-residues of a number N is equivalent to a prime apparent residue.

THEOREM 2. *There exists a prime apparent residue of N which has the same quadratic character with respect to any factor of N as the product of the two given prime apparent non-residues.*

Given p_1 and p_2, two prime apparent non-residues of N; each is then a non-residue of an odd number of prime factors of N. There exists a prime $p=kN+p_1p_2$ which is such that $p\equiv 1 \pmod 4$. This is a non-residue of an even number of prime factors of N, and is consequently an apparent residue of N. For if N has s prime factors, $N=f_1f_2\cdots f_s$ (f's not necessarily distinct), we may arrange the f's in the following way.

Class I. $\left(\frac{p_1}{f_i}\right)=\left(\frac{p_2}{f_i}\right)=+1, \qquad (i=1, 2, \cdots, \lambda).$

Class II. $\left(\frac{p_1}{f_i}\right)=-1, \left(\frac{p_2}{f_i}\right)=+1, \qquad (i=\lambda+1, \lambda+2, \cdots, \mu).$

Class III. $\left(\frac{p_1}{f_i}\right)=+1, \left(\frac{p_2}{f_i}\right)=-1, \qquad (i=\mu+1, \mu+2, \cdots, \nu).$

Class IV. $\left(\frac{p_1}{f_i}\right)=\left(\frac{p_2}{f_i}\right)=-1, \qquad (i=\nu+1, \nu+2, \cdots, s).$

Here p is a residue of Classes I and IV (that is, a residue of every f in these classes), and a non-residue of Classes II and III, that is, a non-residue of $\nu-\lambda$ factors of N. The prime p_1 is a non-residue of Classes II and IV, that is, $\mu-\lambda+s-\nu$ factors; p_2 is a non-residue of Classes III and IV, that is, $s-\mu$ factors, and $\nu-\lambda\equiv s-\mu+\mu-\lambda+s-\nu \pmod 2$. As $s-\mu$ and $\mu-\lambda+s-\nu$ are odd, then $\nu-\lambda$ is even and p is an apparent residue of N. Also $p\equiv p_1p_2 \pmod{f_i}$ for any prime factor of N and has the same quadratic character as the product for any factor.

In like manner, it may be shown that the product of two prime apparent residues is equivalent to a prime apparent residue, and the product of a prime apparent residue and a prime apparent non-residue is equivalent to a prime apparent non-residue. Consequently, we may treat compound apparent residues and non-residues as if they were the equivalent primes. In this connection, it may be worth while to mention that a prime $p\equiv 3 \pmod 4$ is considered compound. For example, $+3=-1\cdot -3$ is a compound apparent residue of 35.

5. *Uniqueness of Apparent Residues.*

THEOREM 3. *If the apparent residues of a number A are included in the apparent residues of a number B, not a square, both their apparent residues and their apparent non-residues will coincide.*

For if b is an apparent residue of B, but not of A, and c is an apparent non-residue of both, then bc is an apparent residue of A, but not of B. Such a c must exist, for if all the non-residues of A were residues of B, then B would be a quadratic residue of every prime except a finite set (divisors of A or B) and B would be a perfect square, contrary to the assumption. Hence the product AB is a square, and consequently, aside from squared factors, a number is uniquely determined by its prime apparent residues.

6. *A Test for Primality.* We are now in a position to prove Theorem 4.

THEOREM 4. *If all the apparent residues of a number N are true residues, then the number N is either a prime or a power of a prime.*

PROOF. Let $R=r_1, r_2, r_3, \cdots$ be the set of prime apparent residues of the given number N, and $S=s_1, s_2, \cdots$ be the set of prime apparent non-residues. The sets R and S contain all primes except those dividing N. All primes of the set R are by definition true residues of N. As by Theorem 2 any product $s_i s_j$ has the same character with respect to every factor of N as some r, that is, a residue, if we hold s_i fixed and let s_j vary, we see that the quadratic character, with respect to any prime factor of N, of all s's is determined by a single one.

Then for any prime factor p of N we have the following result. Every prime in R is a residue of p and either (1) all primes of S are non-residues of p, or (2) all primes of S are residues of p.

In the first case, a single *prime* is determined by Theorem 3. In the second case, there is no prime at all, as this is the characterization of a square by Theorem 1. Hence N is divisible only by a single prime, and the theorem follows.

7. *Applications.* In an actual problem of factorization, it is impracticable to determine the true quadratic character of every number. But if all the apparent residues considered are shown to be true residues, the problem is essentially this.

In the two sets

$$A = a_1, a_2, a_3, \cdots, a_r, \qquad B = b_1, b_2, b_3, \cdots, b_s,$$

A and B contain all primes less than some p (-1 considered a prime), we know that every a_i is a true residue, and that every

b_ib_j is a true residue of the number N under consideration. We wish to know what restriction this information places upon possible factors of N.

8. *A Practicable Test for Primality.* We define L_p as the least number, not a square, which is a quadratic residue of all primes $\leqq p$. In other terms, every number less than L_p which has

$$-1,\ 2,\ -3,\ \cdots,\ (-1/p)p$$

as apparent residues must be a perfect square. (Numbers with factors less than p are excluded by the definition of apparent residues.)

THEOREM 5. *If all the factors (not necessarily prime factors) of N lie below L_p, and if $-1, 2, \cdots, (-1/p)p$ may be divided into two classes $A(a_1, a_2, \cdots, a_r)$, the apparent residues of N, and $B(b_1, b_2, \cdots, b_s)$, the apparent non-residues of N, such that every a_i is a true residue of N, and every b_ib_j is a true residue, then N is either a prime or a power of a prime.*

PROOF. For any prime factor q of N we have one of two cases:

CASE I. Every prime in A is a residue of q and every prime in B is a non-residue of q.

CASE II. Every prime in A is a residue of q and every prime in B is a residue of q.

Case II is to be rejected as $-1, 2, \cdots, (-1/p)p$ would be apparent residues of q, and q lies below L_p. This would make q a square, though also a prime.

If q_1 is a prime divisor of N belonging to Case I, then $(q_1/p_i) = (N/p_i)$ for p_i any of $-1, 2, \cdots, (-1/p)p$. In this event $([N/q_1]/p_i) = +1$ and as $N/q_1 < L_p$, it follows that N/q_1 must be a square. Hence q_1 is contained in N to an odd power. If q_2 were another prime dividing N, we would also have N/q_2 a square though divisible by an odd power of q_1. Hence N must be either a prime or the power of a prime.

The numbers L_p seem to increase rapidly as p increases. Lehmer* has found the values up to L_{61} which is 48,473,881. By Theorem 1 it follows that L_p tends to infinity with p.

An asymptotic formula for L_p or some lower bound, such as $2^{p/2}$, would be quite valuable in applying this last theorem.

* American Mathematical Monthly, vol. 35, p. 121. See also Kraitchik, *Recherches sur la Théorie des Nombres*, vol. 1, p. 46.

EXAMPLE. $N=22,253,377$. We find the following quadratic forms.

1. $N = (2361)^2 + (4084)^2.$

2. $N = (3467)^2 + 2(2262)^2.$

3. $N = (3905)^2 + 3(1528)^2.$

4. $N = (4703)^2 + 2^{12}\cdot 3\cdot 11.$

5. $N = (4714)^2 + 3^2\cdot 11^2\cdot 29.$

6. $N = (4736)^2 - 3^2\cdot 11\cdot 13\cdot 137.$

$N = (4717)^2 + 2^3\cdot 3\cdot 137.$

7. $N = (4723)^2 - 2^3\cdot 3^3\cdot 13\cdot 19.$

8. $N = (4777)^2 - 2^4\cdot 3^4\cdot 19\cdot 23.$

This gives us the set $A(-1, 2, -3, -11, 13, -19, -23, 29)$ and shows them to be true residues. For the set B we find:

9. $5N = (10, 525)^2 + 2^2\cdot 11^2\cdot 5\cdot 7\cdot 29.$

10. $3N = (8174)^2 - 7^2\cdot 5\cdot 13\cdot 17.$

11. $3N = (7919)^2 + 2\cdot 5\cdot 7\cdot 17\cdot 41\cdot 83.$

$N = (4722)^2 - 23^2\cdot 83.$

12. $3N = (8206)^2 - 5\cdot 7\cdot 13\cdot 31\cdot 41.$

13. $5N = (10, 533)^2 + 2^2\cdot 17\cdot 47\cdot 101.$

$N = (4705)^2 + 2^7\cdot 3^2\cdot 101.$

14. $5N = (10, 547)^2 + 2^2\cdot 11\cdot 17\cdot 37.$

This gives us the set $B(5, -7, 17, -31, 37, 41, -47)$, and b_ib_j is a residue. As N is not divisible by 2 or 3, any factor must lie below 9, 257, $329 = L_{47}$; hence, if of Case II type, must be a perfect square. Consequently N is a prime or a power of a prime. As $N\equiv 2 \pmod 5$ and $\equiv 3 \pmod{13}$, it is neither a square nor a cube. Having no factor under 50, it cannot be a higher power. Hence N is identified as a prime.

TRINITY COLLEGE, CAMBRIDGE