MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 135
JULY 1976, PAGES 649–656

Generalizations of a Classical Theorem in Number Theory

By Richard H. Hudson

Abstract. A classical theorem conjectured by Jacobi asserts that for an odd prime p, the sum of the quadratic residues in the interval $(0, p)$ is less than the sum of the quadratic nonresidues if and only if $p \equiv 3 \pmod 4$. We generalize Jacobi's problem to kth powers (mod p), $k > 2$, and we consider in some detail a generalization of Jacobi's conjecture to quadratic residues and nonresidues (mod n), n an arbitrary integer > 2. From the set of least positive residues (mod n), let c_0 denote the subgroup of quadratic residues (mod n) and let $c_1, c_2, \ldots, c_t$ be the cosets which can be formed with respect to this subgroup. Computer data supports the following generalized Jacobi conjecture: The sum of the elements in c_0 is less than or equal to the sum in any of the other cosets for every integer $n > 2$, a surprising conjecture, especially in view of the fact that counterexamples are easily obtained for $k = 4$, 6, 8, 10, etc. (The coset sums are identical for odd k and prime modulus.) We resolve the generalized Jacobi conjecture in the affirmative when, for example, n is an integer admitting a primitive root, or $n = 2^\alpha$, $\alpha \geqslant 3$. (Here we give explicit formulae for the four coset sums.) For $n = 2p^\alpha$, our proof that the quadratic residues and the quadratic nonresidues (mod n) have the same sum for odd prime p if and only if $p \not\equiv 3 \pmod 8$ is purely elementary. On the other hand, we need Dirichlet's class number formula for quadratic number fields with discriminant $-p \equiv 5 \pmod 8$ to show that the sum of the quadratic nonresidues strictly exceeds the sum of the quadratic residues (mod $2p^\alpha$) if $p \equiv 3 \pmod 8$. Computer data gives rise to a host of interesting problems we are unable to resolve. For example, if $n = 2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, $1 \leqslant i \leqslant r$, we conjecture that a sufficient condition that the coset sums not be identical is that we have $p_i \equiv 3 \pmod 8$ for every i. It is not hard to show that the coset sums are identical if every $p_i \equiv 1 \pmod 4$. However, the problem of finding a necessary condition is very difficult since, e.g., the coset sums are not identical for $n \leqslant 1146$ when $n = 2 \cdot 3 \cdot p$ if $p \equiv 23 \pmod{24}$, but the sums are identical if $p \equiv 7 \pmod{24}$.

1. Introduction and Summary. A classical conjecture generally attributed to Jacobi, see, e.g. [4] asserts that for an odd prime p the number of quadratic residues (mod p) less than $p/2$ exceeds the number greater than $p/2$ if and only if $p \equiv 3 \pmod 4$. This is easily seen to be equivalent to the assertion that for an odd prime p, the sum of the quadratic residues in $(0, p)$ is strictly less than the sum of the quadratic nonresidues in $(0, p)$ if and only if $p \equiv 3 \pmod 4$. As is well known, the classical proof of Dirichlet and all subsequent proofs have been nonelementary [4].

In this paper we consider generalizations of Jacobi's problem in two directions. In Section 2 we generalize the problem to kth power residues and nonresidues, $k >$

Received July 28, 1975; revised October 23, 1975 and November 14, 1975.
AMS (MOS) subject classifications (1970). Primary 10A10, 10A15; Secondary 12A50.

2, and in Section 3 we consider in detail the generalization to composite modulus. I hope the reader will find these generalizations interesting as they raise a host of new problems, provide some surprises, and, hopefully, shed some additional light on Jacobi's original conjecture. I am deeply grateful to James M. Greene for assistance with computer data related to work done in this paper.

Let p be $\equiv 1 \pmod{k}$, p a prime, and k an integer $\geqslant 2$. Then, among the set of least positive residues (mod p), the kth power residues form a proper multiplicative cyclic subgroup (mod p) of order $(p-1)/k$, call it $c_k(p)$. We will frequently call $c_k(p)$, coset 0 or simply c_0 as it is the identity of the cyclic group (mod k) consisting of $c_k(p)$ together with the $k-1$ distinct cosets which can be formed with respect to $c_k(p)$ from the least positive residues (mod p) and with binary operation $\oplus$ defined as follows. Let α, β, and γ be nonnegative integers $\leqslant k-1$. For each fixed k, $c_\alpha \oplus c_\beta = c_\gamma$ if and only if $\forall a \in c_\alpha$ and $b \in c_\beta$, $ab \in c_\gamma$; clearly, we must have $\gamma \equiv \alpha + \beta \pmod{k}$, and this cyclic group (mod k) is generated (additively) by any c_i with $(i, k) = 1$.

Throughout the sum of the positive integers $< n$ in a given coset will be called the coset sum. Jacobi's conjecture for odd prime p can now be restated as: the sum in c_0 and the sum in c_1 (there are only two cosets) are equal for $k = 2$ if and only if $p \equiv 1 \pmod{4}$; otherwise, the sum in c_1 strictly exceeds the sum in c_0. In Section 2 we generalize as follows. If $p \equiv 1 \pmod{k}$ the sums in each of the k cosets are identical if and only if $p \equiv 1 \pmod{2k}$, in which case the sum in each coset is precisely $p(p-1)/2k$. When $p \equiv k+1 \pmod{2k}$, however, the number of distinct coset sums must be at least two and may be as great as k. An asymptotic (or exact) formula for estimating the number of distinct coset sums would be interesting. The surprising fact, especially in light of our data for $k = 2$ and composite modulus, is that the sum in c_0 is not necessarily the smallest coset sum when $k > 2$. Indeed, the sum in $c_{k/2}$ is strictly less than the sum in c_0 when, e.g., $p = 29$ and $k = 4$. (The sum in c_0 and the sum in $c_{k/2}$, k even, are independent of the choice of primitive root used to generate the cosets.)

If $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $p_1, \ldots, p_r$ distinct odd primes, the quadratic residues (mod n) form a multiplicative cyclic subgroup of the reduced residues (mod n) of order $\phi(n)/2^{r+\beta}$ where $\beta = 1$ if $\alpha_0 = 0$ or 1, $\beta = 2$ if $\alpha_0 = 2$, and $\beta = 3$ if $\alpha_0 \geqslant 3$ [5, p. 167]. This subgroup is the identity of the group of order $2^{r+\beta-1}$ consisting of the subgroup and $2^{r+\beta-1} - 1$ elements of order 2. (As such, it is noncyclic if $r + \beta - 1 \geqslant 2$, or equivalently, if n does not have a primitive root.) As above, we denote the subgroup by c_0 and the other elements of the group, $c_1, c_2, \ldots, c_t$ where $t = 2^{r+\beta-1} - 1$ are the cosets which can be formed with respect to this subgroup.

In Section 3 we examine the generalization of Jacobi's problem to composite modulus, first considered by Dirichlet. The most surprising result that emerges from our computer data is the fact that for every integer n, $2 < n \leqslant 250$ for which the coset sums are not identical, the sum of the quadratic residues is smaller than the sum in any of the other cosets, a result which we now conjecture holds for all $n > 2$.

We call this the generalized Jacobi conjecture; to date only special cases of this conjecture have been established; see [2, Chapter 6]. Jacobi's conjecture is clearly the special case where n is an odd prime. Recall, from above, that this result is, in general, false if we have $k > 2$ ($n = 29$, $k = 4$; $n = 139$, $k = 6$, etc.), which is precisely the reason we are now restricting our investigation to $k = 2$, although other interesting problems would undoubtedly arise from a generalization to arbitrary k and n where $k \mid \phi(n)$.

If $n = p^\alpha$, p an odd prime, it is easy to show that the sum of the quadratic nonresidues in $(0, p^\alpha)$ strictly exceeds the sum of the quadratic residues in $(0, p^\alpha)$ if and only if $p \equiv 3 \pmod 4$, given the classical result for prime modulus.

If $n = 2p^\alpha$, $\alpha \geqslant 1$, $p \not\equiv 3 \pmod 8$, we prove that the sum of the quadratic residues (mod n) is equal to the sum of the quadratic nonresidues (mod n); moreover, this proof is elementary. Using Dirichlet's formula for the class number of a quadratic number field with discriminant $-p$, we show that the sum of the quadratic nonresidues (mod n) strictly exceeds the sum of the quadratic residues (mod n) for even composite integers admitting a primitive root if and only if $n = 4$ or $n = 2p^\alpha$ where $p \equiv 3 \pmod 8$. If n does not admit a primitive root, the problem is, in general, more difficult. For example, computer data for $n \leqslant 1146$ suggests that the coset sums are identical for $n = 2 \cdot 3 \cdot p$, $p \equiv 7 \pmod 8$, if $p \equiv 7 \pmod{24}$, but not if $p \equiv 23 \pmod{24}$.

However, for $n = 2^\alpha$, $\alpha \geqslant 3$, we can prove somewhat more than the generalized Jacobi conjecture as we derive explicit formulas for the sums in each of the four cosets. These formulas show that the coset sums are distinct with common difference $2^{\alpha-2}$, and the sum in c_0 is the smallest of the four sums. This result was obtained independently by the aforementioned James M. Greene. Moreover, it is not difficult to show that for $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $\alpha_0 = 0$ or 1, $p_i \equiv 1 \pmod 4$, $1 \leqslant i \leqslant r$, the 2^r coset sums are identical and, furthermore, must have exactly the value $n\phi(n)/2^{r+1}$ while in contrast, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $p_i \equiv 3 \pmod 4$, $1 \leqslant i \leqslant r$, it is easily shown that the coset sums cannot be identical. We conjecture, but are unable to prove that if $4 \mid n$, or if n is odd and has a prime factor $\equiv 3 \pmod 4$, or if the odd prime factors of n are all $\equiv 3 \pmod 8$, then the coset sums cannot be identical. Since there are more than two cosets if n does not have a primitive root it seems worthwhile to distinguish the case where the coset sums have distinct values (no two have the same value), and the case where the coset sums are not identical, but are also not distinct. Computer data supports some surprising conjectures. For example, if $2^2 \mid n$, $2^3 \nmid n$, then we conjecture that the 2^{r+1} coset sums are distinct if the odd prime factors of n are all $\equiv 3 \pmod 8$ in spite of the fact that the coset sums for $n = 2 \cdot 3 \cdot 11$ and for $n = 2^3 \cdot 11$ are not distinct.

Throughout the rest of the paper p will always denote a prime and n and k will denote integers > 1. By the sum of the quadratic residues (mod n) we will always mean the sum of the positive integers less than n and relatively prime to n which are squares (mod n), and similarly for quadratic nonresidues (mod n).

2. The Problem of Jacobi for $k > 2$ and Prime Modulus.

THEOREM 2.1. *Let p be $\equiv 1 \pmod{k}$. Then a necessary and sufficient condition that the coset sums be identical is that p be $\equiv 1 \pmod{2k}$. Moreover, if $p \equiv k + 1 \pmod{2k}$ and coset α is the coset obtained by multiplying the elements of coset β by -1 for some β, $0 \leqslant \beta < k/2$, then*

$$\sum_{a \in c_\alpha} a \neq \sum_{a \in c_\beta} a, \tag{2.1}$$

the sum in each case being taken over the reduced residues (mod p).

Proof. That the condition is sufficient is easy to see. If $p \equiv 1 \pmod{2k}$, then -1 is a kth power residue since for any primitive root g of p $\exists$ an integer α with $p - 1 = 2\alpha k$ and

$$\begin{aligned} g^{(p-1)/2} \not\equiv 1 \pmod{p} &\Rightarrow g^{(p-1)/2} \equiv -1 \pmod{p} \\ &\Rightarrow (g^\alpha)^k \equiv -1 \pmod{p}. \end{aligned} \tag{2.2}$$

Hence, for each integer a, $1 \leqslant a \leqslant p - 1$, a and $p - a$ are in the same coset. Moreover, $(p - 1)/k$ is even, and there are $(p - 1)/k$ elements in each coset. Thus, a and $p - a$ are distinct and letting c_i denote the ith coset,

$$\sum_{a \in c_i} a = p(p - 1)/2k, \qquad i = 0, 1, \ldots, k - 1. \tag{2.3}$$

If, on the other hand, $p \not\equiv 1 \pmod{2k}$, then $p \equiv k + 1 \pmod{2k}$ so that k must be even since p is odd. But, then, $(p - 1)/k$ is odd and -1 is a kth power nonresidue since $(-1)^{(p-1)/k} \equiv -1 \pmod{p}$, see [3, p. 58]. Let α and β be defined as above and denoting cosets α and β by c_α and c_β, respectively, we have

$$\sum_{a \in c_\alpha} a + \sum_{a \in c_\beta} a = p(p - 1)/k. \tag{2.4}$$

Consequently, the proof is complete if each of the sums on the left-hand side of (2.4) is a multiple of p since $(p - 1)/k$ is odd.

But letting g be a primitive root of p we have

$$\sum_{a \in c_i} a \equiv g^i + g^{i+k} + \cdots + g^{i+(p-1-k)} \pmod{p}, \tag{2.5}$$

since $g^\alpha \in c_i$ if and only if $\alpha \equiv i \pmod{k}$. This geometric progression sums to

$$g^i(g^{p-1} - 1)/(g^k - 1). \tag{2.6}$$

However, $g^k \not\equiv 1 \pmod{p}$ if $p > k + 1$ since g is primitive, and $p \mid g^{p-1} - 1$ by Fermat's theorem, i.e., the numerator in (2.6) is divisible by p and the denominator is not. This completes the proof since if $p = k + 1$ each coset consists of one distinct integer and we take this to be the sum.

Remark 1. Let p be $\equiv k + 1 \pmod{2k}$. It is not true that the sum in c_0 is always less than the sum in $c_{k/2}$. (Coset $k/2$ is always the coset obtained by multiplying the elements of c_0 by -1.) In particular, it is not true when $p = 29$ and $k = 4$, $p = 139$ and $k = 6$, $p = 137$ and $k = 8$, $p = 131$ and $k = 10$, $p = 277$ and $k = 12$, $p = 547$ and $k = 14$. We have not found an example in which the sum in c_0 ex-

ceeds the sum in all the other cosets. Let d denote the number of distinct coset sums. Clearly, $d = 2$ if $(p-1)/k = 3$ since only two coset sums are possible, namely, p and $2p$. It is reasonable to conjecture that d/k increases as $p/k \longrightarrow \infty$ and d/k may even increase monotonically as p increases (k fixed) or k decreases (p fixed). However, an informative expression for d as a function of p and k appears hard to obtain.

3. Generalizations of the Conjecture of Jacobi for Composite Moduli.

THEOREM 3.1. *If $n = p^\alpha$, p odd, then the sum of the quadratic nonresidues* (mod n) *exceeds the sum of the quadratic residues* (mod n), *if and only if* $p \equiv 3$ (mod 4).

Proof. If $p \not\equiv 3 \pmod 4$, the two sums are identical by Theorem 3.4. If $p \equiv 3 \pmod 4$, then r is a quadratic residue or nonresidue of p^α, $\alpha \geqslant 1$, $1 \leqslant r < p^\alpha$, if and only if it is a quadratic residue or nonresidue of p since $x^2 \equiv r \pmod{p^\alpha} \Rightarrow x^2 \equiv r \pmod p$ while if $(r/p) = 1$ then (r/p^α) is the product of α Legendre symbols all with value $+1$; and consequently, r is a quadratic residue of p^α. Thus, the quadratic residues of p^α are precisely $r_1, r_1 + p, \ldots, r_1 + (p^{\alpha-1} - 1)\,(p), r_2, r_2 + p, \ldots, r_2 + (p^{\alpha-1} - 1)p, \ldots, r_{(p-1)/2}, r_{(p-1)/2} + p, \ldots, r_{(p-1)/2} + (p^{\alpha-1} - 1)p$, where $r_1, r_2, \ldots, r_{(p-1)/2}$ are the quadratic residues (mod p). But the quadratic nonresidues of p^α are $n_1, \ldots, n_1 + (p^{\alpha-1} - 1)p, \ldots, n_{(p-1)/2}, \ldots, n_{(p-1)/2} + (p^{\alpha-1} - 1)p$ and the result is seen to be an immediate consequence of the known result for prime modulus.

THEOREM 3.2. *If $n = 2^\alpha$, $\alpha \geqslant 1$, no two coset sums have the same value. Moreover, if $\alpha \geqslant 3$, the coset sums can be arranged in strictly increasing order with common difference $2^{\alpha-2}$. The smallest of these four coset sums is the sum in c_0 which is precisely $2^{\alpha-3}(2^{\alpha-1} - 3)$ for all $\alpha \geqslant 3$.*

Proof. If $n = 2$, there is only one coset and if $n = 4$, 1 belongs to c_0 and 3 belongs to c_1. Hence, we may assume $\alpha \geqslant 3$. Then there are four cosets formed with respect to the cyclic subgroup of quadratic residues (mod n); see [5, p. 167]. The quadratic residues (mod 2^α) are clearly $\equiv 1 \pmod 8$ since the square of each odd integer is $\equiv 1 \pmod 8$, and the modulus is $\equiv 0 \pmod 8$. Conversely, it is well known [3, p. 54] that 5 is an element of the group of reduced residues (mod 2^α) of order $2^{\alpha-2}$. Thus, the $2^{\alpha-3}$ even powers of 5 are distinct quadratic residues (mod 2^α). But, among the odd integers less than 2^α, exactly $2^{\alpha-3}$ (¼ of the odd integers) are $\equiv 1 \pmod 8$. Hence, an integer cannot be $\equiv 1 \pmod 8$ and fail to be a quadratic residue.

Without loss of generality, arrange the cosets so that 3 belongs to coset 1, 5 belongs to coset 2, and 7 belongs to coset 3. Then the elements of coset 1 are $\equiv 3 \pmod 8$, of coset 2 are $\equiv 5 \pmod 8$, and of coset 3 are $\equiv 7 \pmod 8$. Since $\phi(n) = 2^{\alpha-1}$, each coset must have $2^{\alpha-1}/4$ elements and summing these $2^{\alpha-1}/4$ elements in the arithmetic progressions $8n + 1$, $8n + 3$, $8n + 5$, and $8n + 7$, respectively, and denoting the ith coset by c_i, we have

$$\sum_{a \in c_i} a = 2^{\alpha-3}(2^{\alpha-1} - 3) + i(2^{\alpha-2}), \qquad i = 0, 1, 2, 3. \tag{3.1}$$

Remark 2. If $\alpha \geqslant 4$, although 3 and 5 are elements of order $2^{\alpha-2}$ and, consequently, generators of cyclic subgroups of the reduced residues (mod 2^α) with index 2, 7 has order less than $2^{\alpha-2}$. Thus, if $\alpha \geqslant 4$, it is not possible to form cosets with respect to any cyclic subgroup of the reduced residues (mod 2^α) for which the coset sums are all the same. We mention this lest the reader is tempted to create identical coset sums by combining coset 0 and coset 3. Although the combined sum in clearly equal to the combined sum in cosets 1 and 2, the combination of coset 0 and coset 3 does not form a cyclic subgroup of the reduced residues (mod 2^α) if $\alpha \geqslant 4$.

THEOREM 3.3. *If* $n = 2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *is the prime factorization of* n, *then there are* $2^{r+\beta-1}$ *cosets which can be formed with respect to the subgroup of quadratic residues* (mod n); $\beta = 1$ *if* $\alpha_0 = 0$ *or* 1, $\beta = 2$ *if* $\alpha_0 = 2$, $\beta = 3$ *if* $\alpha_0 \geqslant 3$. *If the coset sums are all equal, each must have the value* $(n \cdot \phi(n))/2^{r+\beta}$.

Proof. The first assertion is proved in [5, p. 167]. The second follows immediately from the observation that the sum of the reduced residues (mod n) is $(n \cdot \phi(n))/2$ since there are $\phi(n)$ such integers, and each such integer $a < n/2$ can be paired with $n - a$ yielding $\phi(n)/2$ pairs each summing to n (proved by Crelle in 1845).

Remark 3. A proof that the coset sums cannot be identical if $4 \mid n$, which we are able to obtain only in special cases, combined with Theorem 3.3 would yield the result: A necessary and sufficient condition that the coset sums be identical is that the integers in each coset sum to $(n \cdot \phi(n))/2^{r+1}$. For each n not divisible by 4, and not containing a prime factor $\equiv 3 \pmod 4$, we prove this result in the next theorem. We also note that our computer data indicates that for all n, the coset sums are identical if and only if the sum of the quadratic residues (mod n) is $(n \cdot \phi(n))/2^{r+1}$, a slightly stronger assertion.

THEOREM 3.4. *If* $n = 2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *with* $p_i \equiv 1 \pmod 4$ $\forall i$, $1 \leqslant i \leqslant r$, *and if* $\alpha_0 = 0$ *or* 1, *then the sum in each coset is* $(n \cdot \phi(n))/2^{r+1}$.

Proof. By Theorem 3.3 there are 2^r cosets and, consequently, $\phi(n)/2^r$ elements in each coset. But $p_i \equiv 1 \pmod 4$ clearly $\Rightarrow 4 \mid \phi(p_i^{\alpha_i})$ for each i, $1 \leqslant i \leqslant r$. Consequently, $4^r \mid \phi(n)$, and we have easily that $\phi(n)/2^r$ is even. Moreover, -1 is a quadratic residue of n since -1 is a quadratic residue of each p_i and of 2^{α_0} when $\alpha_0 = 1$. Thus, for each coset, say c_i, $a \in c_i$, if and only if $n - a \in c_i$. Since $\phi(n)/2^r$ is even, a and $n - a$ are distinct, yielding $\phi(n)/2^{r+1}$ pairs in each coset each summing to n and, thus, the sum in each coset must be $(n \cdot \phi(n))/2^{r+1}$.

In contrast to Theorem 3.4 we have the following theorem.

THEOREM 3.5. *If* $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *with* $p_i \equiv 3 \pmod 4$ $\forall i$, $1 \leqslant i \leqslant r$, *then the coset sums are not identical.*

Proof. If $p_i \equiv 3 \pmod 4$, then $2 \mid \phi(p_i^{\alpha_i})$ but $4 \nmid \phi(p_i^{\alpha_i})$ for each i. Thus, $2^r \mid \phi(n)$ but $2^{r+1} \nmid \phi(n)$ which $\Rightarrow (n \cdot \phi(n))/2^{r+1}$ is not an integer; and the result follows from the second part of Theorem 3.3 since $\beta = 1$.

Remark 4. As indicated in the introduction the problem of deciding when the coset sums are identical and when they are not is far more interesting and difficult than is suggested by the relatively trivial Theorems 3.4 and 3.5. In particular, n may have a prime factor $\equiv 3 \pmod 4$; and yet all coset sums may be identical, contrasting

the situation for prime modulus. Indeed, if n is even, all odd prime factors of n can be $\equiv 3 \pmod 4$ and all coset sums be identical, e.g. $n = 42 = 2 \cdot 3 \cdot 7$. However, in the following two theorems we resolve the generalized Jacobi conjecture for integers which admit a primitive root by showing that for composite integers $n = 2p^\alpha$, p odd, the sum of the quadratic nonresidues (mod n) exceeds the sum of the quadratic residues (mod n) if and only if $p \equiv 3 \pmod 8$.

THEOREM 3.6. *If* $n = 2p^\alpha$, $\alpha \geqslant 1$, $p \equiv 3 \pmod 8$, *then the sum of the quadratic nonresidues* (mod n) *exceeds the sum of the quadratic residues* (mod n).

Proof. Let η = the number of quadratic nonresidues of p^α in the interval $(p^\alpha/2, p^\alpha)$ minus the number of quadratic nonresidues of p^α in the interval $(0, p^\alpha/2)$. Since 2 is a quadratic nonresidue of p^α, η = the number of odd quadratic residues of p^α minus the number of odd quadratic nonresidues as is readily seen by multiplying the integers in the interval $(p^\alpha/2, p^\alpha)$ by 2 and reducing modulo the odd integer p^α. Since -1 is a quadratic nonresidue of p^α, η = the number of even quadratic residues of p^α minus the number of even quadratic nonresidues.

Now each odd quadratic residue (or nonresidue) of p^α is a quadratic residue (or nonresidue) of $2p^\alpha$ whereas t is an even quadratic residue (or nonresidue) of p^α if and only if $t + p^\alpha$ is a quadratic residue (or nonresidue) of $2p^\alpha$. Because of Theorem 3.1 we must have $\eta > 0$ and the result follows at once. Indeed, if the sum of the quadratic nonresidues (mod p^α) minus the sum of the quadratic residues (mod p^α) is s, then the sum of the quadratic nonresidues (mod $2p^\alpha$) minus the sum of the quadratic residues (mod $2p^\alpha$) is exactly $s + \eta p^\alpha$.

Remark 5. For the primes $\equiv 3 \pmod 4$ for which 2 is a quadratic nonresidue, the difference between the coset sums for $n = 2p^\alpha$ is ηp^α greater than the difference for $n = p^\alpha$, a significant magnification. Clearly, the question of whether or not 2 is a quadratic residue of p is central to the problem as the next theorem indicates. This causes us to wonder whether the quadratic residuacity of 3 has a bearing on our conjecture that the coset sums are not identical for any $n = 2 \cdot 3 \cdot p$ if $p \equiv 23 \pmod{24}$, although they are identical (for $n < 1000$) if $p \equiv 7 \pmod{24}$. A natural extension of Theorem 3.6 which we are unable to prove is that if $n = 2p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where $p_i \equiv 3 \pmod 8$ $\forall i$, $1 \leqslant i \leqslant r$, the coset sums cannot be identical.

THEOREM 3.7. *If* $n = 2p^\alpha$, $\alpha \geqslant 1$, p *an odd prime* $\not\equiv 3 \pmod 8$, *the sum of the quadratic residues* (mod n) *and the sum of the quadratic nonresidues* (mod n) *is exactly* $(n \cdot \phi(n))/4$.

Proof. Because of Theorems 3.3 and 3.4 it suffices to show that the coset sums are equal when $p \equiv 7 \pmod 8$. But letting η be the difference between the number of quadratic nonresidues and the number of quadratic residues in the interval $(p/2, p)$, whether positive or negative, it is well known [1, p. 301] that for all $p \equiv 7 \pmod 8$, the difference between the sum of the quadratic nonresidues (mod p) and the quadratic residues (mod p) is ηp. Moreover, the difference is ηp^α if $p \equiv 7 \pmod 8$ and $\alpha > 1$ since a is a quadratic residue (mod p^α) only if it is a quadratic residue of p, and summing over the intervals $(0, p)$, $(p, 2p)$, $\ldots$, $(p^\alpha - p, p^\alpha)$ the difference ηp occurs exactly $p^{\alpha-1}$ times. But 2 is a quadratic residue of p, and so by reasoning

analogous to the proof of Theorem 3.6, the number of even quadratic nonresidues (mod p^α) minus the number of even quadratic residues (mod p^α), is $-\eta$. This completes the proof as each even quadratic residue of p^α, say r, contribute $r + p^\alpha$ to the sum in c_0 for $n = 2p^\alpha$ and each even quadratic nonresidue, say n, contributes $n + p^\alpha$ to the sum in c_1, exactly cancelling the difference between the coset sums for $n = p^\alpha$.

Remark 6. We have separated the proofs of Theorems 3.6 and 3.7 for the fundamental reason that in the proof of Theorem 3.7 we do not need to use that $\eta > 0$ and, consequently, the proof is completely elementary. We note that the coset sums cannot all be the same if $n = 2^{\alpha_0}p_1^{\alpha_1}$, $p_1 \equiv 3 \pmod 4$, for any $\alpha_0 \neq 1$ as a relatively immediate consequence of Theorems 3.3 and 3.5. Indeed, each coset contains $\phi(n)/2^{r+\beta}$ odd integers if $\alpha_0 = 0$, but $\phi(n)/2^{r+\beta}$ is odd so that the sum in each coset must be odd; however, $(n \cdot \phi(n))/2^{r+\beta}$ is even and, hence, the coset sums cannot be identical. Thus, Theorem 3.7 can be phrased: for $n = 2^{\alpha_0}p_1^{\alpha}$, $p_1 \equiv 3 \pmod 4$, the coset sums are all identical if and only if $\alpha_0 = 1$ and $p_1 \equiv 7 \pmod 8$.

Department of Mathematics and Computer Science
University of South Carolina
Columbia, South Carolina 29208

1. RAYMOND AYOUB, *An Introduction to the Analytic Theory of Numbers,* Math. Surveys, no. 10, Amer. Math. Soc., Providence, R. I., 1963. MR **28** #3954.

2. L. E. DICKSON, *History of the Theory of Numbers.* Vol. 3, Washington, 1919.

3. WILLIAM JUDSON LEVEQUE, *Topics in Number Theory.* Vol. 1, Addison-Wesley, Reading, Mass., 1956. MR **18**, 283.

4. LEO MOSER, "A theorem on quadratic residues," *Proc. Amer. Math. Soc.,* v. 2, 1951, pp. 503-504. MR **12**, 804.

5. K. K. NORTON, "Upper bounds for k-th power coset representatives modulo n," *Acta Arith.,* v.15, 1968/69, pp. 161–179. MR **39** #1419.