Journal of the Minnesota Academy of Science

Volume 64 | Number 1 Article 5

1999

Supplement to "On Translations of Quadratic Residues"

Bruce Brandt

SUPPLEMENT TO "ON TRANSLATIONS OF QUADRATIC RESIDUES"†

BRUCE BRANDT‡

ABSTRACT

Let n and k be arbitrary positive integers. We will tend to be concerned with small k and with n which are several times k!. I stated two conditions on (n, k) in a previous paper; in this paper I restate them and further explore them. In particular, it is proven that if n is the least number satisfying Condition 1 for a certain k, then the least number for k + 1 must be at least 2n + 1. Condition 1 and Condition 2 are rephrased graph-theoretically. A heuristic explanation for why the quadratic residues tend to satisfy Condition 2b is given. A conjecture characterizes n and k which satisfy Condition 2b when n is a prime of the form 4m + 1 and Q are the quadratic residues. The case of the quadratic residues or non-residues with zero appended to them is discussed.

INTRODUCTION

Some background for non-number theorists: **Z**/n**Z** or **Z** mod n, is the set of integers where we ignore multiples of n, that is, where we consider two numbers the same if they differ by a multiple of n. If n is an odd prime, the quadratic residues mod n are the squares mod n (except zero). For example, 2 is a quadratic residue mod 7 because $2 = 3^2 - 7$. The non-residues mod n are the elements of **Z**/n**Z** (beside zero) which are not quadratic residues as non-residues. Also, if n is a prime of the form 4m – 1, and x is a quadratic residue, then –x is a non-residue.

In a previous paper (Brandt 1997), I explored two conditions on positive integers n and k, linking them with the quadratic residues. Condition 1 and Condition 2 are restated below:

Condition 1: The following question is answered positively: Let S be a set of n elements. Does a function exist from S^k to S such that letting x ~ y if x is a member of a k-tuple going to y, we never have x ~ y and y ~ x?

Condition 2: A subset Q of **Z**/n**Z** exists such that:

{2a} $x \in Q \Rightarrow -x \notin Q$

{2b} If $x_1, x_2, \ldots, x_k \in$ **Z**/n**Z**.

Then $x_1 + Q \cap x_2 + Q \cap \ldots \cap x_k + Q \neq \varnothing$.

As mentioned in Brandt (1997), for given n and k, Condition 2 implies Condition 1. Also, given k, if one value of n satifies Condition 1, so does every higher value of n.

1. I will prove an assertion stated without proof in Brandt (1997).

Theorem: If, for k = K, the least value of n satisfying Condition 1 is N, then for k = K + 1, the least value of n satisfying Condition 1 must be at least 2N + 1.

Proof: Suppose the hypothesis and let S be a set satisfying Condition 1 for k = K + 1. Let f be the function from S^{K+1} to S referred to in Condition 1, and let ~ be the associated relation. Let $x_o \in S$. Let T be the set of x such that $x_o \sim x$ and let g be the function from T^K to T such that $g(x_1, x_2, \ldots, x_K) = f(x_o, x_1, x_2, \ldots, x_K)$.

For y, z ∈ T, let us say y*z if y is in a K-tuple which g takes to z. If y * z then y ~ z. Because we can never have y ~ z and z ~ y, we can never have y * z and z * y either. Thus, T satisfies Condition 1 for k = K and so by hypothesis must be of cardinality at least N.

Because this is true for any x_o in S, every element of S must bear the relation ~ to at least N elements of S. Thus, among ordered pairs of unequal elements of S, (x,y), there must be at least $N \bullet |S|$ cases where x ~ y. There must be at least as many cases where it is not true that x ~ y. Since there are a total of $|S|^2 - |S|$ ordered pairs of unequal elements of S, we have,

$|S|^2 - |S| \geq N \bullet |S| + N \bullet |S|$,

so that

$|S| \geq 2N + 1$.

2. Here are graph-theoretic ways of expressing Condition 1 and Condition 2, which may help you see the relationship between them:

Condition 1: Consider n points with at most one directed edge between any two points. Is it possible that any k points in the graph go to a common point via a directed edge?

Condition 2: Same as Condition 1 except assume the points are arranged in a circle and the graph is symmetric with respect to rotation of $2\pi/n$ radians.

(To see that this formulation of Condition 2 is the

† Independent contribution.

‡ 13 27th Avenue Southeast, Minneapolis, MN 55414-3101

same as the one given in Brandt [1997], first number the points 0, 1, 2, ..., n-1, in order around the circle, and define Q as {y - x mod n: x goes to y via a directed edge}.)

3. To simplify language, let us call a set which has a translation which is a subset of another set, a "translational subset" of the other set. Yet another way of expressing Condition 2b:

Condition 2b: Every subset T of $\mathbf{Z}/n\mathbf{Z}$ with k elements is a translational subset of Q.

4. I have discovered something which removes some of the mystery as to why quadratic residues of primes of the form 4m - 1 tend to satisfy Condition 2b.

Let Q be the quadratic residues of a prime n of the form 4m-1, and let T be a subset of $\mathbf{Z}/n\mathbf{Z}$. Let $y \neq 0$. Then

$T + x \subset Q \Leftrightarrow y^2T + y^2 x \subset y^2 Q = Q.$

Thus, T is a translational subset of Q if and only if y^2T is. Similarly, -T is a translational subset of Q if and only if $(-y^2)T$ is. So if z is a nonzero element of $\mathbf{Z}/n\mathbf{Z}$ (which must be of the form $\pm y^2$), $\pm$ T are translational subsets of Q if and only if $\pm$ zT are.

These considerations imply that when Q is the quadratic residue of a prime of the form 4m - 1, one has to test considerably fewer T in Condition 2b, for example one may assume $\{0,1\} \subset T$. Because that assumption greatly reduces computational time, I have verified that for k = 5, n = 331 satisfies Condition 2.

5. When n is a prime of the form 4m + 1, we cannot assume that $\{0,1\} \subset T$, but it is still true that if T is multiplied by a quadratic residue, whether T is a translational subset of the quadratic residues or of the non-residues does not change. Upon investigating primes of the form 4m + 1, we find the following:

Conjecture: Given k, a prime n of the form 4m + 1, satisfies Condition 2b for Q the quadratic residues (or the non-residues), if and only if $n > \pi(k!)$. (verified for $k \leq 4$ and several n)

(The symbol π refers to the transcendental number, not the function counting primes. You may ask, why π? There does appear to be a number b such that $n > b(k!)$ is the relevant condition. When k = 4, n = 73 fails but n = 89 succeeds, so $3.04 < b < 3.71$. When k = 5, n = 373 fails, so $b > 3.10$. Thus π is the anly "aesthetic" number in the correct range. Recall that in Brandt (1997), a similar conjecture was made for n of the form 4m – 1 and b = e.)

6. I have also investigated Q of the form {x: x is a quadratic residue} $\cup$ {0}, or {x: x is a non-residue} $\cup$ {0}, when n is a prime of the form 4m - 1, or of the form 4m + 1. Note that such sets, also, are preserved upon multiplication by a quadratic residue.

The following conjectures appear to hold for such Q just as they do when Q does not contain 0:

Conjecture: It never makes a difference whether you use the quadratic residues or non-residues (verified for $k \leq 4$ and several n).

Conjecture: Given k, if Condition 2b is true of one n, it is true of every greater n that has the same value mod 4 (verified for $k \leq 4$ and several n).

Conjecture: Given k, let n be the least number of the form 4m - 1 satisfying Condition 2b for Q the quadratic residues union {0}. Then no other Q of the same cardinality (up to translation and reflection satisfies Condition 2b (verified for k = 2, n = 3 and k = 3, n = 11).

This last statement does not hold when n is of the form 4m + 1, just as when Q does not contain 0.

However, unlike when Q does not contain 0, for neither n of the form 4m - 1 nor of the form 4m + 1 is there a number b such that n and k satisfy Condition 2b if and only if $n > b(k!)$.

REFERENCE

Brandt, B. 1997. On Translations of Quadratic Residues. J. Minn. Acad. Sci. 62:7.