Proceedings of the Iowa Academy of Science

Volume 66 | Annual Issue | Article 49

1959

Waring's Problem, Modulo p, and the Representation Symbol

M. Anne Cathleen Real
Marycrest College

Recommended Citation
Real, M. Anne Cathleen (1959) "Waring's Problem, Modulo p, and the Representation Symbol," *Proceedings of the Iowa Academy of Science, 66(1),* 362-364.
Available at: https://scholarworks.uni.edu/pias/vol66/iss1/49

Waring's Problem, Modulo p, and the Representation Symbol

By SISTER M. ANNE CATHLEEN REAL, C.H.M.

Abstract. The representation symbol [a,b,c] is the statement that an integer of *n*-ic type *a* is congruent to the sum of an integer of *n*-ic type *b* and an integer of *n*-ic type *c*. The symbol is extended to include any definite number of elements. New properties, together with a list of symbols involving the *n*-ic types of specific integers, are derived for use in studying Waring's problem, modulo *p*, for a particular exponent *n*. Let $T_p(n)$ be the least number such that every integer is congruent to the sum of $T_p(n)$ or fewer *n*-ic residues. Then for primes of the form $22k + 1$, $k > 3$, $2 \leqq T_p(11) \leqq 4$.

Waring's problem, modulo *p*, is the determination, for given integers *n* and *p*, of a least *s* depending on *n* and *p* such that for every integer *c*, the equation

$$c = \sum_{i=1}^{s} x_i^n + pq$$

will have a solution where the x_i are integers. The integer *s* shall be denoted by $T_p(n)$.

Throughout this discussion the letter *g* will be used to designate a fixed primitive root for a given prime *p*. An integer *g* is a primitive root of a prime *p* if and only if *p-1* is the least positive integer *t* such that

$$g^t \equiv 1 \pmod{p}.$$

If *c* is an integer not divisible by *p*, then there exists an integer *t* such that $c \equiv g^t \pmod{p}$ where $0 \leqq t < p-1$.

For any given integer *n*, an integer *a* is called the *n*-ic type, modulo *p*, of the integer *c*, if $t = nq + a$, where $0 \leqq a < n$. If $a = 0$, then *c* is called an *n*-ic residue since $c \equiv (g^q)^n \pmod{p}$.

Waring's problem, modulo *p*, can now be stated as the determination of the least number $T_p(n)$ such that any integer is congruent to the sum of $T_p(n)$ or fewer *n*-ic residues.

The letter *I* denotes a variable integer. In a single expression its value need not be the same if it occurs twice. u_k denotes the *n*-ic type of the integer *k*. Thus $k \equiv g^{nI+u_k} \pmod{p}$.

The representation symbol, [a,b,c], as defined by Torline (1955)[1], is the statement that an integer of *n*-ic type *a* is representable as the sum of an integer of *n*-ic type *b* and an integer of *n*-ic type *c*.

This may be written:

$$[a,b,c] \Longleftrightarrow g^{nI+a} \equiv g^{nI+b} + g^{nI+c} \pmod{p}.$$

The extended representation symbol, $[a_1;a_2,a_3,\ldots,a_s]$, is the statement

$$g^{nI+a_1} \equiv g^{nI+a_2} + g^{nI+a_3} + g^{nI+a_s} \pmod{p}.$$

To justify these definitions it can be shown that all integers of the same *n*-ic type are representable as the same number of *n*-ic residues.

The following properties were derived by Torline:

Property 1. If [a,b,c] holds and if integers of *n*-ic types *b* and *c* can be written as the sum of t_1 and t_2 *n*-ic residues respectively, then integers of *n*-ic type *a* are representable as the sum of $t_1 + t_2$ *n*-ic residues.

Property 2. Since -1 is an *n*-ic residue for primes of the form $2nk + 1$, permutations of the elements in the representation symbol do not change the validity of the symbol for these primes. Thus,

$$[a,b,c] <=> [b,c,a] <=> [c,a,b].$$

Property 3. $[a,b,c] <=> [a+r,b+r,c+r]$ since by multiplying the congruence

$$g^{nI+a} \equiv g^{nI+b} + g^{nI+c} \pmod{p}$$

by g^r, we get the congruence

$$g^{nI+a+r} \equiv g^{nI+b+r} + g^{nI+c+r} \pmod{p}.$$

The following theorem utilizes the symbol which has more than three elements.

Theorem: If [a,b,c] holds, then $[2a;2b,u_2+b+c,2c]$ and $[3a;3b,u_3+2b+c,u_3+b+2c,3c]$ hold.

Proof: If [a,b,c] holds, then $g^{nI+a} \equiv g^{nI+b} + g^{nI+c} \pmod{p}$.

By squaring this congruence we have

$$g^{nI+2a} \equiv g^{nI+2b} + 2g^{nI+b}g^{nI+c} + g^{nI+2c} \pmod{p},$$

and cubing the same congruence we have

$$g^{nI+3a} \equiv g^{nI+3b} + 3g^{nI+2b}g^{nI+c} + 3g^{nI+b}g^{nI+2c} + g^{nI+3c} \pmod{p}.$$

Interpreting these congruences as representation symbols, recalling that

$$2 \equiv g^{nI+u_2} \pmod{p} \text{ and } 3 \equiv g^{nI+u_3} \pmod{p},$$

the desired symbols are obtained.

In particular, if [a,0,0] and if $u_2 = 0$, then [2a;0,0,0].

Also, if [a,0,0] and if $u_2 = 0$, then [3a;0,0,0,0].

The simple relation $16 = 15 + 1$ or $2^4 = 5 \cdot 3 + 1$ gives the congruence $$g^{nI+4u_2} \equiv g^{nI+u_5+u_3} + 1 \pmod{p},$$ which is equivalent to the statement A: $[4u_2,u_5+u_3,0]$. Similarly, the following valid symbols, as well as other useful symbols not included here, are obtained.

B: $[u_3,u_2,0]$ C: $[2u_3,3u_2,0]$
D: $[2u_5,2u_3,2u_4]$ E: $[u_5,u_3,u_2,]$

The following theorem, dealing with Waring's problem, modulo *p*, with $n = 11$, makes use of these ideas.

Theorem 2. If *p* is a prime of the form $22k + 1$ where $k>3$, then $2 \leqq T_p(11) \leqq 4$.

For a fixed prime p of the form $22k + 1$, the proof was divided into three cases.

Case: I: $u_2 = 0$, $u_3 = 0$; in which case an argument involving sequences of integers was used together with some of the above theory.

Case II: $u_2 = 0$, $u_3 = a \neq 0$; in which all possible values for u_5 were considered; that is, $u_5 = 0, a, 2a, \ldots, 10a$.

Case III: $u_2 = a \neq 0$; in which case all possible values for u_5 were considered for each possible value for u_3.

The case when $u_2 = 0$, $u_3 = a \neq 0$, and $u_5 = 7a$ will serve as an example of the technique used in cases II and III. By substituting these values in the representation symbols A, B, C, D, and E as given above, the following valid symbols, together with their derived symbols, are obtained.

A: [0,8a,0] <==> [*8a*,0,0] by property 2
=> [*5a*;0,0,0] by theorem 1
B: [*a*,0,0]
C: [*2a*,0,0] => [*4a*;0,0,0] by theorem 1
D: [*3a*,2a,0] <==> [a,0,*9a*] <==> [0,*10a*,8a] by properties 2 and 3
E: [*7a*,a,0] <==> [*6a*,0,10a] by property 3

From the symbols containing italicized elements it may be concluded that integers of n-ic types a, $2a$, and $8a$ are representable as the sum of two n-ic residues. Also integers of n-ic types $3a$, $4a$, $5a$, $7a$, $9a$, and $10a$ are representable as the sum of three n-ic residues, and integers of n-ic type $6a$ are representable as the sum of four n-ic residues. Thus integers of all n-ic types are representable as the sum of not more than four n-ic residues for this particular case. Tables were set up using this basic device for all possible combinations of u_2, u_3, and u_5. In addition, in several cases representation symbols involving the n-ic types of the integers 7, 23, and 67 were used in the proof of the theorem.

Literature Cited

1. Torline, Sister Mary Ferdinand, C.S.J. "Waring's Problem, Modulo p," Unpublished Ph.D. dissertation, Department of Mathematics, Saint Louis University, 1955.

MARYCREST COLLEGE
DAVENPORT, IOWA

