1929

Symmetric Functions of *n*-IC Residues (mod *p*)

T. A. Pierce
University of Nebraska - Lincoln

Published in Bull. Amer. Math. Soc. 35 (1929) 708-710.

SYMMETRIC FUNCTIONS OF n-IC RESIDUES (mod p)†

BY T. A. PIERCE

If p be an odd prime, q is said to be an n-ic residue of p if the congruence $x^n \equiv q \pmod{p}$ has solutions; otherwise q is an n-ic non-residue of p. A necessary and sufficient condition that q be an n-ic residue of p is that

$$q^{(p-1)/\delta} \equiv 1, \pmod{p}, \tag{1}$$

where $\delta = \text{g.c.d.}\ (p-1, n)$. The number‡ of n-ic residues of a given prime p is $(p-1)/\delta$.

It is with the symmetric functions of these n-ic residues that this paper deals.

By means of (1) we readily prove that the product of two n-ic residues is an n-ic residue and that the product of an n-ic residue by an n-ic non-residue is an n-ic non-residue.

Put $(p-1)/\delta = r$ and let $q_1, q_2, \cdots, q_r$ be the set of all distinct n-ic residues of p. Then $q_i q_1, q_i q_2, \cdots, q_i q_r$ is the same set in different order, for the assumption that two members of this last set are congruent leads to the conclusion that two members of the first set are not distinct.

---

* Loc. cit., p. 140.

† Presented to the Society, March 30, 1929.

‡ Dirichlet-Dedekind, *Zahlentheorie*, 4th ed., 1894, p. 74.

Let $S_\nu(q_1, q_2, \cdots, q_r)$ be an integral homogeneous symmetric function of $q_1, q_2, \cdots, q_r$ of total degree ν. Assume that ν is not a multiple of r. Take q_i to be an n-ic residue belonging to the exponent r; such a q_i exists since $\phi(r)>1$. Then by virtue of the homogeneity

$$S_\nu(q_iq_1, q_iq_2, \cdots, q_iq_r) = q_i^\nu S_\nu(q_1, q_2, \cdots, q_r).$$

Moreover

$$S_\nu(q_iq_1, q_iq_2, \cdots, q_iq_r) \equiv S_\nu(q_1, q_2, \cdots, q_r), \pmod{p}.$$

Hence

$$(q_i^\nu - 1)S_\nu(q_1, q_2, \cdots, q_r) \equiv 0, \pmod{p}.$$

Since q_i belongs to the exponent r and ν is not a multiple of r, the first factor is not divisible by p; therefore the second factor is divisible by p. Hence we may state the following theorem.

THEOREM 1. *An integral symmetric function of dimension ν of the n-ic residues of the odd prime p is divisible by p if ν is not a multiple of $(p-1)/\delta$.*

Any symmetric function of the rth powers of the q's may be evaluated by (1). Thus

$$\sum q_i^r \equiv 1 + 1 + \cdots = (p-1)/\delta \equiv -\delta^{p-2}, \pmod{p}.$$

A general theory of symmetric functions whose dimensions are multiples of $(p-1)/\delta = r$ is a desideratum here as it is in the case of ordinary residues when the dimensions are multiples of $p-1$. The two simplest cases will be treated here.

First, since

$$x^{(p-1)/\delta} - 1 \equiv 0, \pmod{p},$$

is satisfied by the $(p-1)/\delta$ distinct n-ic residues this congruence has its full complement of real roots and hence

$$q_1q_2 \cdots q_r \equiv \pm 1, \pmod{p}, \tag{2}$$

according as r is odd or even.

Next assume that $(p-1)/\delta$ is even and greater than 2 and let q belong to the exponent $r/2>1$. Such a q exists since $\phi(r/2)>1$. Then $(q^{r/2})^{\delta}\equiv q^{(p-1)/2}\equiv 1 \pmod{p}$ and q is a quadratic residue of p. Thus the congruence

$$x^2 - q \equiv 0, \pmod{p} \tag{3}$$

has a solution x. This solution x must be an n-ic residue, for from $x^2\equiv q \pmod{p}$ we have $x^r\equiv q^{r/2}\equiv 1 \pmod{p}$, and x satisfies (1).

The fact that (3) has a solution among the set of q's may be expressed

$$(q - q_1^2)(q - q_2^2)\cdots(q - q_r^2) \equiv 0, \pmod{p}.$$

Expanding the left member and omitting intermediate terms whose coefficients are multiples of p, by the theorem above we have

$$q^r + (-1)^{r/2}S_{r/2}(q_1^2, \cdots, q_r^2)q^{r/2} + (q_1\cdots q_r)^2 \equiv 0, \pmod{p}, \tag{4}$$

where $S_{r/2}(q_1^2, \cdots, q_r^2)$ is the sum of the products of $q_1^2, \cdots, q_r^2$ taken $r/2$ at a time. The dimension of $S_{r/2}$ is thus $(p-1)/\delta$. The last term of (4) is unity by (2) and since q belonged to the exponent $r/2$ we have

$$S_{r/2}(q_1^2, \cdots, q_r^2) \equiv (-1)^{r/2+1}\,2, \pmod{p}.$$

This last result corresponds to one due to Glaisher* for ordinary residues.

THE UNIVERSITY OF NEBRASKA

* Glaisher, *Congruences relating to sums of products*, etc., Quarterly Journal of Mathematics, vol. 31 (1900), p. 34.