ON A SYMMETRIC FUNCTION OF THE PRIMITIVE ROOTS OF PRIMES

Joseph B. Dence and Thomas P. Dence

1. Introduction. The elementary symmetric functions of n variables are:

$$s_1 = u_1 + u_2 + \cdots + u_n$$

$$s_2 = u_2u_1 + u_3u_1 + u_3u_2 + \cdots + u_nu_{n-1} = \sum_{i>j} u_iu_j$$

$$s_3 = \sum_{i>j>k} u_iu_ju_k$$

$$\vdots$$

$$s_n = \prod_{i=1}^{n} u_i.$$

In a previous paper [1] we investigated the elementary symmetric function s_1 of the primitive roots of a prime. The principal tool was the use of certain cyclotomic polynomials. The present work continues this line of investigation and considers the function s_2 of the primitive roots. Throughout, p denotes an odd prime, $d \geq 1$ is any divisor of $p-1$, and $\{g_i\}$ is the set of primitive roots of p.

2. Numerical Results. The first few odd primes, beginning with $p = 5$, yield the following simple results: $p = 5$: $s_2 \equiv 1 \pmod p$; $p = 7$: $s_2 \equiv 1 \pmod p$; $p = 11$: $s_2 \equiv 1 \pmod p$; $p = 13$: $s_2 \equiv -1 \pmod p$; $p = 17$: $s_2 \equiv 0 \pmod p$. The residues obtained strongly urge the computation of the residues modulo p of s_2 for many more primes. A sampling of these computations is given in Table 1. Since in [1] it was important to note whether $p-1$ is squarefree or not, Table 1 has been organized so that the primes p in columns (1)–(3) are those where $p-1$ is not squarefree; in columns (4) and (5) $p-1$ is squarefree.

p	(1) $s_2 \pmod p$
5	1
61	1
277	1
373	1
4621	1

p	(2) $s_2 \pmod p$
19	0
37	0
73	0
193	0
457	0

p	(3) $s_2 \pmod p$
29	-1
53	-1
293	-1
421	-1
797	-1

p	(4) $s_2 \pmod p$
31	0
43	0
67	0
79	0
683	0

p	(5) $s_2 \pmod p$
23	1
47	1
59	1
83	1
463	1

Table 1. Residues of the Symmetric Function s_2 of the Primitive Roots of Various Primes p.

The table suggests strongly that for all primes $p \geq 5$ the congruence

$$s_2 \equiv 0 \text{ or } \pm 1 \pmod p$$

holds. Our object is to show this by making a connection with s_1.

3. Sums of Squares of the Primitive Roots. The connection with s_1 is made by considering the sums of squares of the primitive roots. Let

$$S = \sum_{i=1}^{\phi(p-1)} g_i^2;$$

then it follows algebraically that $2s_2 = s_1^2 - S$, and we need the residues modulo p of S in order to compute the residues modulo p of s_2. We do this by again appealing to certain properties of the cyclotomic polynomials.

The nth cyclotomic polynomial, $\Phi_n(x)$, is defined as

$$\Phi_n(x) = \prod_{\zeta}(x - \zeta),$$

where ζ spans all of the primitive nth roots of unity. We recall that the degree of $\Phi_n(x)$ is $\phi(n)$, and all of the coefficients in $\Phi_n(x)$ are integers [4]. Write

$$\Phi_n(x) = \sum_{k=0}^{\phi(n)} c(n, k)x^k,$$

as in [1]. Then if $n = d$, a divisor of $p - 1$, Theorem 3 in [1] shows that the coefficient $c(d, \phi(n) - 1)$ is 0 if d is not squarefree, $+1$ if d is squarefree and contains an odd number of prime factors, and -1 if $d = 1$ or d is squarefree and contains an even number of prime factors. Since the roots of $\Phi_d(x) \equiv 0 \pmod p$ are all of the incongruent integers of order d modulo p, the preceding gives us Theorem 1 [6].

Theorem 1. The sum of the incongruent integers of order d modulo p is congruent to $\mu(d)$, where μ is the Möbius function.

In particular, Theorem 1 gives immediately for any odd prime p,

$$s_1 \equiv \mu(p - 1) \pmod p.$$

But from [2], for any g_i, the integer g_i^2 has order

$$\frac{p - 1}{(2, p - 1)} = \frac{p - 1}{2}.$$

There are

$$\phi\left(\frac{p - 1}{2}\right)$$

incongruent integers of order $(p - 1)/2$, whereas there are $\phi(p - 1)$ primitive roots. Hence, squaring and reducing the primitive roots modulo p produces

$$\frac{\phi(p - 1)}{\phi\left(\frac{p-1}{2}\right)}$$

copies of the integers of order $d = (p-1)/2$. Theorem 2 follows from this and from Theorem 1.

Theorem 2.

$$S \equiv \frac{\phi(p-1)}{\phi\left(\frac{p-1}{2}\right)}\mu\left(\frac{p-1}{2}\right) \pmod{p},$$

if p is any odd prime.

A more general result than Theorem 2 was stated in [5]. It is clear that the residues of S are restricted to 0, ± 1, ± 2. We illustrate this in Table 2.

p	$\phi(p-1)$	$\phi((p-1)/2)$	$\mu((p-1)/2)$	S	$S \pmod{p}$
11	4	4	-1	153	-1
41	16	8	0	8036	0
53	24	12	1	21944	2
61	16	8	-1	20372	-2
79	24	24	1	61937	1
211	48	48	-1	848008	-1

Table 2. Residues Modulo p of the Sums of Squares of the Primitive Roots of Various Primes p.

4. The Main Result. In view of the relationship between s_1, s_2 and S, and of the result in Theorem 2, the following theorem emerges.

Theorem 3. Let $\{g_i\}$ denote the primitive roots of the prime $p \geq 5$, and let

$$\Phi_{p-1}(x) = \sum_{k=0}^{\phi(p-1)} c(p-1,k)x^k$$

be the $(p-1)$st cyclotomic polynomial. Then

$$s_2 = \sum_{i>j} g_i g_j \equiv c(p-1, \phi(p-1)-2) \pmod{p}$$

$$\equiv \frac{1}{2}\left(\big(\mu(p-1)\big)^2 - \frac{\phi(p-1)}{\phi\left(\frac{p-1}{2}\right)}\mu\left(\frac{p-1}{2}\right)\right) \pmod{p}.$$

That the right-hand side of the last congruence is actually integral can be seen by considering various cases of factorization of $p-1$, $(1/2)(p-1)$.

The formula in Theorem 3 can be presented pictorially (in Figure 1) by considering, in fact, the different cases of factorization of $p-1$, $(1/2)(p-1)$. There are precisely five such cases of factorization; these correspond to the five columns of Table 1.

As a matter of distribution, we observe that among the first 100 primes (beginning with $p=5$) the residues -1, 0, 1 of s_2 occur in the ratios $12:59:29$. The question of what these ratios should be in the limit of infinitely many primes is an interesting one.

Finally, we note in conclusion that although Theorem 3 might be generalizable to an arbitrary elementary symmetric function s_n and to an arbitrary modulus (but one which still has primitive roots), the result is apt to be too complex to permit a simple pictorial presentation analogous to Figure 1. This has long been suspected [3].

References

1. J. B. Dence, "Primitive Roots the Cyclotomic Way," *Missouri Journal of Mathematical Sciences*, 12 (1999), 5–11.

2. J. B. Dence and T. P. Dence, *Elements of the Theory of Numbers*, Harcourt/Academic Press, San Diego, California, 1999.

3. A. R. Forsyth, "Primitive Roots of Prime Numbers and Their Residues," *Messenger of Mathematics*, 13 (1883/1884), 169–192.

4. L. J. Goldstein, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973, 226–227.

5. R. Moller, "Sums of Powers of Numbers Having a Given Exponent Modulo a Prime," *American Mathematical Monthly*, 59 (1952), 226–230.

6. M. A. Stern, "Bemerkungen über hohere Arithmetik," *Journal für Mathematik*, 6 (1830), 147–153.

Joseph B. Dence
Department of Chemistry
University of Missouri
St. Louis, MO 63121

Thomas P. Dence
Department of Mathematics
Ashland University
Ashland, OH 44805
email: tdence@ashland.edu

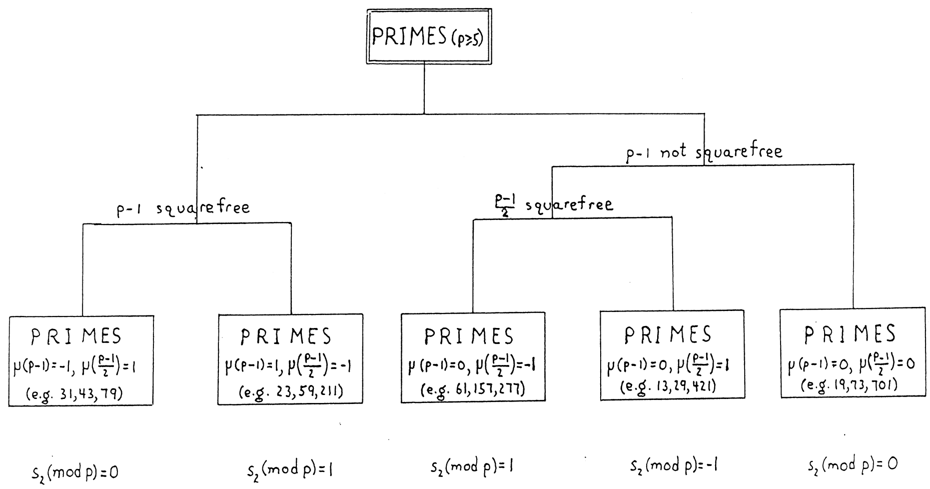

Figure 1.
Classification of the Primes on the Basis of the
Residues Modulo p of the Symmetric Function s_2.