MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 136
OCTOBER 1976, PAGES 847–853

Explicit Criteria for Quintic Residuacity

By Kenneth S. Williams*

Abstract. Let p be a prime $\equiv 1 \pmod 5$. Necessary and sufficient conditions are determined for the prime q ($q \leqslant 19$) to be a quintic residue of p. The results for $q \leqslant 7$ are known, the rest are new.

Throughout this paper k is an odd prime and p is a prime $\equiv 1 \pmod k$ say, $p = kf + 1$. The f-nomial periods are defined by

$$\eta_s = \sum_{r=0}^{f-1} \exp(2\pi i g^{kr+s}/p) \quad (s = 0, 1, \ldots, k-1), \tag{1}$$

where g is a primitive root (mod p). The period equation $P_k(t)$ of degree k is defined by

$$P_k(t) = \prod_{s=0}^{k-1} (t - \eta_s). \tag{2}$$

It is well known that $P_k(t)$ has integral coefficients (see for example [12, p. 194]). Since replacing the primitive root g in (1) by another primitive root merely permutes the η_i, the coefficients of $P_k(t)$ are independent of the choice of g. The discriminant D_k of $P_k(t)$ is also an integer independent of g given by

$$D_k = \prod_{0 \leqslant r < s \leqslant k-1} (\eta_r - \eta_s)^2. \tag{3}$$

The following is essentially a theorem of Kummer [6] (see also Lehmer [8], [10]).

THEOREM 1. (i) *A prime q ($\neq p$) not dividing D_k is a kth power residue of p if and only if the congruence $P_k(t) \equiv 0 \pmod q$ is solvable.*

(ii) *Every prime q ($\neq p$) dividing D_k is a kth power residue of p.*

When $k = 3$ it is well known (see for example [12, p. 223]) that

$$P_3(t) = t^3 + t^2 - \frac{1}{3}(p-1)t - \frac{1}{27}(pL + 3p - 1), \qquad D_3 = p^2M^2, \tag{4}$$

where the integers L, M satisfy

$$4p = L^2 + 27M^2, \qquad L \equiv 1 \pmod 3). \tag{5}$$

Theorem 1 can be used in conjunction with (4) and (5) to give explicit necessary and sufficient conditions for a prime q to be a cubic residue of p in terms of congruences

Received March 27, 1975; revised October 16, 1975.
AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 12C20.
Key words and phrases. Quintic residue, primitive root, f-nomial periods, period equation.
*Research supported under National Research Council of Canada Grant No. A-7233.

(mod q) involving L and M. For example, we find that 2 is a cubic residue of p if and only if $M \equiv 0 \pmod 2$, that 3 is a cubic residue of p if and only if $M \equiv 0 \pmod 3$, that 5 is a cubic residue of p if and only if L or $M \equiv 0 \pmod 5$, etc. Such conditions have been given by Jacobi [5] for $q \leqslant 37$ and for $q \leqslant 47$ by Cunningham and Gosset [2].

In this note we consider the case $k = 5$. Lehmer [7] has shown that

$$P_5(t) = t^5 + t^4 + c_3t^3 + c_2t^2 + c_1t + c_0, \tag{6}$$

where the integers c_0, c_1, c_2, c_3 are given by

$$\left\{\begin{aligned} 5c_3 &= -2(p-1), \\ 25c_2 &= -(6p + px - 2), \\ 500c_1 &= -[p(x^2 - 125w^2 + 8x - 4p + 24) - 4], \\ 25000c_0 &= -p[x^3 + 10x^2 - 1250w^2 + 625w(u^2 - v^2) + 40x + 80] \\ &\quad + 8p^2(x+5) + 8, \end{aligned}\right. \tag{7}$$

where (x, u, v, w) is a solution of

$$\left\{\begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \qquad x \equiv 1 \pmod 5, \\ xw &= v^2 - 4uv - u^2. \end{aligned}\right. \tag{8}$$

Dickson [3] has shown that (8) is always solvable; and that if (x, u, v, w) is a solution, all the solutions are (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$ and $(x, -v, u, -w)$. If the condition $x \equiv 1 \pmod 5$ is dropped, the only other solutions of (8) are the negatives of those given above. In [10] Lehmer gives

$$256D_5 = p^4[w^2(4v - 3u) - u(u-v)^2]^2[w^2(3v + 4u) + v(u+v)^2]^2. \tag{9}$$

Theorem 1 can be used in conjunction with (6), (7), (8), (9) to give explicit necessary and sufficient conditions for a prime q to be a quintic residue of p in terms of congruences (mod q) involving x, u, v, w. As there are a great many cases involved (depending on the residue classes (mod q) of p, x, u, v, w) in doing this even for small primes q, Carleton University's Xerox Data Systems Sigma-9 computer was programmed to carry out the details for $q = 2, 3, 5, 7, 11, 13, 17, 19$. As the results are known for $q = 2, 3, 5, 7$ (by different methods), we illustrate the ideas involved by just giving some of the details in the case $q = 11$. In order to do this we introduce the following notation. If a, b, c, d are any integers, we let

$$\begin{aligned} [a, b, c, d] = \{&(a, b, c, d), (a, -b, -c, d), (a, c, -b, -d), (a, -c, b, -d), \\ &(-a, -b, -c, -d), (-a, b, c, -d), (-a, -c, b, d), (-a, c, -b, d)\} \end{aligned} \tag{10}$$

and write $(x, u, v, w) \in [a, b, c, d] \pmod q$ to mean $(x, u, v, w) \equiv (f, g, h, i) \pmod q$ for some $(f, g, h, i) \in [a, b, c, d]$. The computer showed in the case $q = 11$, $p \equiv 1 \pmod{11}$, that $D_5 \equiv 0 \pmod{11}$ if and only if

$$(x, u, v, w) \in [0, 0, 0, 2],\ [4, 0, 0, 0] \quad \text{or} \quad [4, 2, 4, 6] \pmod{11},$$

q	$\left(\frac{p}{q}\right)$	$w \equiv 0 \pmod q$	$w \not\equiv 0 \pmod q$ $(u/w,\ v/w) \pmod q$
2		$x \equiv u \equiv v \equiv 0$	
3	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	
	-1		(0, 0)
5	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	(1, 3)
7	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	(1, 2)
	-1		(0, 0), (0, 2)
11	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	(0, 0), (0, 4), (3, 4)
	-1	$x \equiv 0,\ u \equiv 2v$	(1, 1), (1, 4)
13	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	(0, 6), (1, 4), (3, 8), (4, 7)
	-1		(0, 0), (1, 8), (2, 8), (3, 6), (3, 7)
17	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$	(1,11), (2,2), (2,6), (2,14), (3,3) (3,12), (4,9)
	-1		(0,0), (1,14), (2,7), (2,9), (2,10) (4,7), (4,10), (5,9)
19	+1	$x \not\equiv 0,\ u \equiv v \equiv 0$ $x \equiv 0,\ u \equiv 7v$	(0,0), (0,9), (1,6), (1,7), (1,9) (4,9), (5,11), (6,8), (7,7), (8,9)
	-1	$x \not\equiv 0,\ u \equiv 7v$	(0,4), (1,1), (1,12)*, (1,13), (2,7) (2,11), (6,7), (6,12), (9,9)

*In this case $x \equiv 0 \pmod{19}$.

All congruences are taken modulo q. We note that when q is odd and $u \equiv v \equiv 0$, $w \not\equiv 0 \pmod q$ then $x \equiv 0 \pmod q$.

and that $D_5 \not\equiv 0 \pmod{11}$ with $P_5(t) \equiv 0 \pmod{11}$ solvable, if and only if

$$(x, u, v, w) \in [1, 0, 3, 9] \pmod{11},$$

where (x, u, v, w) is *any* solution of (8). Thus, in this case, by Theorem 1, 11 is a quintic residue of p if and only if

$$(x, u, v, w) \in [0, 0, 0, 2],\ [4, 0, 0, 0],\ [1, 0, 3, 9] \quad \text{or} \quad [4, 2, 4, 6] \pmod{11};$$

that is, if and only if *some* solution (x, u, v, w) of (8) satisfies

$$u \equiv v \equiv 0 \pmod{11}$$

or

$$u \equiv 0, \quad v \equiv 4w, \quad w \not\equiv 0 \pmod{11}$$

or

$$u \equiv 3w, \quad v \equiv 4w, \quad w \not\equiv 0 \pmod{11}.$$

In this manner the following theorem was obtained.

THEOREM 2. *Let p be a prime* $\equiv 1 \pmod 5$, *and let q be one of* 2, 3, 5, 7, 11, 13, 17, 19. *Then q is a quintic residue of p if and only if some solution* (x, u, v, w) *of* (8) *satisfies the conditions given in the preceding table.*

Table of primes $\equiv 1 \pmod 5$ *and* $< 10{,}000$ *having* 2, 3, 5, 7, 11, 13, 17, 19 *as quintic residues*

2			3			5		
151	3881	8831	41	3881	9011	31	4861	9311
241	4211	9041	431	4051	9221	191	5051	9341
251	4751	9091	491	4111	9341	251	5281	9491
431	4861	9431	661	4201	9421	271	5471	9631
571	4871	9461	761	4721	9851	601	5591	9661
641	4931	9511	1021	4801		641	5711	9851
911	5021	9521	1051	4951		761	6211	
971	5381	9781	1091	5351		1091	6271	
1181	5441		1171	5501		1861	6421	
1811	5471		1471	5591		2381	6581	
2011	5581		1511	6011		2521	6701	
2351	5641		1871	6091		2621	6791	
2381	5711		2111	6101		2741	6961	
2411	5821		2131	6301		2851	6971	
2731	5861		2161	6311		3061	6991	
3061	6221		2281	6421		3121	7151	
3121	6361		2441	6481		3461	7691	
3221	6571		2521	6521		3581	7901	
3251	6581		2591	6581		3631	8581	
3301	6791		2621	6701		3701	8681	
3331	6871		2791	6991		4001	8731	
3361	8161		2851	7331		4201	8861	
3391	8191		3191	7451		4261	8951	
3541	8461		3221	7591		4271	8971	
3761	8501		3691	8101		4421	9011	
3821	8681		3851	8831		4591	9221	

7			11			13		
181	3881	9781	61	3881	9341	61	3361	8191
311	4091	9851	191	3931	9391	271	3491	8221
661	4111	9901	241	4001	9661	311	3541	8311
811	4241		311	4111	9811	331	4021	8461
911	4391		541	4211		461	4391	8641
971	4441		661	4241		601	4591	8761
1031	4591		691	4261		761	4621	9091
1151	4861		751	4621		971	4651	9281
1171	5011		911	4951		1021	4751	9421
1201	5051		1181	5381		1061	4831	9491
1321	5261		1231	5431		1091	5011	9511
1621	5441		1291	5441		1151	5231	9521
1811	5591		1301	5471		1381	5281	9781
1861	6451		1481	5531		1481	5431	
1871	6761		1531	5741		1571	5651	
2161	6841		1871	6151		1601	5741	
2371	6871		1931	6311		1741	6301	
2381	7411		2351	6421		1861	6451	
2441	7451		2521	6481		2141	6551	
2741	7561		2591	7211		2251	6581	
2801	8191		2741	7321		2281	6691	
3011	8431		2791	7351		2711	7001	
3361	8861		3001	7541		3001	7321	
3461	9281		3301	7901		3011	7351	
3631	9491		3461	8221		3191	7681	
3691	9511		3701	9001		3221	8171	

The results for $k = 2, 3, 5$ are due to Lehmer [10] (see also [7], [9], [14]). The result for $k = 7$ is a simpler restatement of a restatement due to Lehmer [10] of a theorem of Muskat [13]. The rest are new.

A table giving the values of (x, u, v, w) corresponding to primes $p \leqslant 10{,}000$, $p \equiv 1 \pmod 5$ has been deposited by the author in the UMT file of the American Mathematical Society. Using this table and Theorem 2, it was found that out of the 306 primes $p \leqslant 10{,}000$ with $p \equiv 1 \pmod 5$; 60 (resp. 57, 58, 55, 56, 65, 67, 77) of them have 2 (resp. 3, 5, 7, 11, 13, 17, 19) as a quintic residue of p. The actual

17			19		
101	2791	8461	131	3331	7331
181	2801	8581	151	3461	7351
491	3271	8681	181	3631	7621
601	3571	8761	241	3701	7841
701	4091	8831	691	3851	7901
811	4801	8941	701	4051	8011
991	4871	8951	1021	4231	8111
1031	5081	9011	1031	4241	8161
1061	5231	9161	1051	4271	8311
1231	5521	9221	1151	4451	8431
1321	5581	9421	1181	4951	8521
1361	5641	9491	1291	5051	8741
1481	5741	9721	1531	5171	8761
1571	5981	9781	1811	5261	8821
1801	6131	9931	1901	5431	8861
1831	6361		2161	5521	9001
1861	6491		2251	5641	9161
2131	6761		2341	5741	9241
2221	7121		2531	5881	9281
2281	7211		2621	6011	9391
2351	7331		2731	6491	9491
2371	7481		2741	6551	9551
2381	7691		2791	6781	9601
2591	8161		3001	6841	9721
2671	8171		3181	6911	9851
2711	8311		3191	7211	

values of p are given in the accompanying tables. The lists of primes p having 2 or 3 as a quintic residue of p agree with those of Bickmore [1]. The corresponding densities are 0.1960. . . , 0.1862. . . , 0.1895. . . , 0.1797. . . , 0.1830. . . , 0.2124. . . , 0.2189. . . , 0.2516. . ., which are in fair agreement with the asymptotic density $1/5 = 0.2$ (see for example Elliott [4]).

The author would like to acknowledge his indebtedness to Messrs. Barry Lowe and Barry Savage for their help with the programming necessary for this paper.

Finally, we mention that the corresponding problem for eighth powers has been treated recently by von Lienen [11].

Department of Mathematics
Carleton University
Ottawa, Ontario, Canada

1. C. E. BICKMORE, "On the numerical factors of $a^n - 1$. II," *Messenger Math.*, v. 26, 1897, pp. 1–38.

2. A. J. C. CUNNINGHAM & T. GOSSET, "4-tic and 3-tic residuacity tables," *Messenger Math.*, v. 50, 1920, pp. 1–30.

3. L. E. DICKSON, "Cyclotomy, higher congruences, and Waring's problem," *Amer. J. Math.*, v. 57, 1935, pp. 391–424.

4. P. D. T. A. ELLIOTT, "A problem of Erdös concerning power residue sums," *Acta Arith.*, v. 13, 1967/68, pp. 131–149; Corrigendum, *ibid.*, v. 14, 1967/68, p. 437. MR **36** #3741; **37** #4031.

5. K. G. J. JACOBI, "De residuis cubicis commentatio numerosa," *J. Reine Angew. Math.*, v. 2, 1827, pp. 66–69.

6. E. E. KUMMER, "Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen," *J. Reine Angew. Math.*, v. 30, 1846, pp. 107–116.

7. EMMA LEHMER, "The quintic character of 2 and 3," *Duke Math. J.*, v. 18, 1951, pp. 11–18. MR 12, 677.

8. EMMA LEHMER, "Criteria for cubic and quartic residuacity," *Mathematika*, v. 5, 1958, pp. 20–29. MR **20** #1668.

9. EMMA LEHMER, "Artiads characterized," *J. Math. Anal. Appl.*, v. 15, 1966, pp. 118–131. MR **34** #1261.

10. EMMA LEHMER, "On the divisors of the discriminant of the period equation," *Amer. J. Math.*, v. 90, 1968, pp. 375–379. MR **37** #2718.

11. H. von LIENEN, "Primzahlen als achte Potenzreste," *J. Reine Angew. Math.*, v. 266, 1974, pp. 107–117. MR **49** #4916.

12. G. B. MATHEWS, *Theory of Numbers*, 2nd ed., Chelsea, New York, 1961. MR **23** #A3698.

13. J. B. MUSKAT, "Criteria for solvability of certain congruences," *Canad. J. Math.*, v. 16, 1964, pp. 343–352. MR **29** #1170.

14. J. B. MUSKAT, "On the solvability of $x^e \equiv e \pmod{p}$," *Pacific J. Math.*, v. 14, 1964, pp. 257–260. MR **28** #2997.