MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 128
OCTOBER 1974, PAGES 1133–1136

A Quadratic Partition of Primes $\equiv 1 \pmod 7$

By Kenneth S. Williams*

Abstract. The solutions of a quadratic partition of primes $p \equiv 1 \pmod 7$, in terms of which the author and P. A. Leonard have given the cyclotomic numbers of order seven and also necessary and sufficient conditions for 2, 3, 5 and 7 to be seventh powers (mod p), are obtained for all such primes < 1000.

Let p be a prime $\equiv 1 \pmod 7$. P. A. Leonard and the author [4] have given necessary and sufficient conditions for 2, 3, 5 and 7 to be seventh powers (mod p) (see also [1], [6]), in terms of the solutions of the following quadratic partition of p:

$$72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \tag{1}$$

$$\begin{aligned}12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 \\ + 48x_3x_4 + 98x_5x_6 = 0,\end{aligned} \tag{2}$$

$$\begin{aligned}12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 \\ + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0.\end{aligned} \tag{3}$$

It was shown in [2], [5] that the system (1)–(3) has exactly eight solutions $(x_1, x_2, x_3, x_4, x_5, x_6)$ with $x_1 \equiv 1 \pmod 7$. (The negatives of these eight solutions, each satisfying $x_1 \equiv -1 \pmod 7$, are the only other solutions.) Of the eight solutions with $x_1 \equiv 1 \pmod 7$, two solutions, namely $(x_1, x_2, x_3, x_4, x_5, x_6) = (-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, where $p = t^2 + 7u^2$, $t \equiv 1 \pmod 7$, are regarded as trivial. If $(x_1, x_2, x_3, x_4, x_5, x_6)$ is one of the six nontrivial solutions with $x_1 \equiv 1 \pmod 7$, all six such solutions are given by (*) where $0 \leqslant k \leqslant 5$. In this paper, a nontrivial solution of (1)–(3) with $x_1 \equiv 1 \pmod 7$ is given for each of the 28 primes $p < 1000$ with $p \equiv 1 \pmod 7$ (see Table 2 below). These solutions were computed from a prime factor λ of p in the unique factorization domain $Z[\alpha]$, $\alpha = \exp(2\pi i/7)$, where the values of λ were obtained from an old

Received November 29, 1973.

AMS (MOS) subject classifications (1970). Primary 10B35; Secondary 10B05, 10C05, 10J05.

*This research was supported by a grant (No. A7233) from the National Research Council of Canada. The author's sabbatical leave at the University of British Columbia was also supported by a N.R.C. travel grant (No. T0259).

$$(*)\qquad (x_1, x_2, x_3, x_4, x_5, x_6)\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & -\frac{1}{2} \end{pmatrix}^k,$$

table of Kummer [3], as follows: for each λ an associate π of λ was found such that

$$(4)\qquad \pi_1\pi_4\pi_5 \equiv -1 \pmod{(1-\alpha)^2},$$

where $\pi_i = \sigma_i(\pi)$ and σ_i is the automorphism of $Q(\alpha)$ defined by $\sigma_i(\alpha) = \alpha^i$ $(1 \leqslant i \leqslant 6)$. Then, if

$$(5)\qquad \pi_1\pi_4\pi_5 = c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 + c_5\alpha^5 + c_6\alpha^6,$$

a solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of (1)–(3) is given by

$$(6)\qquad \begin{aligned} x_1 &= -c_1 - c_2 - c_3 - c_4 - c_5 - c_6 \quad (x_1 \equiv 1 \pmod 7)),\\ x_2 &= c_1 - c_6,\\ x_3 &= c_2 - c_5,\\ x_4 &= c_3 - c_4,\\ 7x_5 &= c_1 + c_2 - 2c_3 - 2c_4 + c_5 + c_6,\\ 7x_6 &= c_1 - c_2 - c_5 + c_6. \end{aligned}$$

(Alternatively, as $\pi_1\pi_4\pi_5$ is a Jacobi sum of order 7, the c_i could have been obtained from tables of Jacobi sums.) The solutions $(x_1, x_2, x_3, x_4, x_5, x_6)$ obtained are listed in Table 2 below and each one was shown directly to satisfy (1)–(3).

In view of the relative inaccessibility of Kummer's paper [3], we list for convenience his values of λ in Table 1.

Two mistakes were noted in Kummer's table. For $p = 337$, he gives the incorrect value $\lambda = 2 + \alpha - \alpha^2 - \alpha^4$ (which is a factor of 344) and, for $p = 617$, he gives the incorrect value $\lambda = 2 + \alpha + \alpha^2 - \alpha^5$ (which is a factor of 113). The respective correct values $\lambda = 3 - 4\alpha + 2\alpha^2 - 5\alpha^4 + 4\alpha^5 - 8\alpha^6$ and $\lambda = 5 + 5\alpha - 4\alpha^3 - 3\alpha^4 + 2\alpha^6$ (given below) are taken from a table of Reuschle [7]. (Kummer's table was used rather than Reuschle's, as Kummer's values of λ are in general simpler than those of Reuschle. Two errors were noted in Reuschle's table: the factor of 29 given is incorrect (it is a factor of 1093), and the twelfth prime p listed should be 421 not 431.)

TABLE 1. *Prime factors* λ *in* $Z[\alpha]$ *of primes* $p \equiv 1 \pmod 7$, $p \leqslant 1000$

p	λ	p	λ
29	$1+\alpha-\alpha^2$	491	$3+\alpha+\alpha^3-\alpha^5$
43	$2+\alpha$	547	$3+\alpha$
71	$2+\alpha+\alpha^3$	617	$5+5\alpha-4\alpha^3-3\alpha^4+2\alpha^6$
113	$2-\alpha+\alpha^5$	631	$2+2\alpha-\alpha^2+\alpha^3+\alpha^6$
127	$2-\alpha$	659	$2+2\alpha-\alpha^2+\alpha^5$
197	$3+\alpha+\alpha^5+\alpha^6$	673	$4+3\alpha+2\alpha^2+\alpha^4+2\alpha^6$
211	$3+\alpha+2\alpha^2$	701	$3+\alpha+\alpha^4-\alpha^5+\alpha^6$
239	$3+2\alpha+2\alpha^2+\alpha^3$	743	$3+2\alpha-\alpha^3-\alpha^4$
281	$2-\alpha-2\alpha^3$	757	$3+2\alpha+\alpha^3$
337	$3-4\alpha+2\alpha^3-5\alpha^4+4\alpha^5-8\alpha^6$	827	$2+2\alpha-\alpha^4-\alpha^6$
379	$3+2\alpha+\alpha^2$	883	$2-\alpha^2-2\alpha^3-\alpha^5$
421	$3+\alpha+\alpha^2$	911	$3+2\alpha-\alpha^3+\alpha^4$
449	$2+\alpha-\alpha^3-\alpha^6$	953	$3+\alpha-\alpha^2-\alpha^3$
463	$3+2\alpha$	967	$2+2\alpha-\alpha^3+2\alpha^5$

TABLE 2. *Solutions of* (1)–(3)

p	x_1	x_2	x_3	x_4	x_5	x_6
29	1	−2	−3	−2	−1	1
43	1	−6	−1	−2	−1	1
71	15	0	3	−2	−3	−1
113	−27	6	−4	3	0	−2
127	29	0	12	−1	−2	0
197	−13	−6	1	−8	−5	1
211	−55	0	13	−4	1	−1
239	57	−11	0	6	3	−1
281	57	6	7	12	−3	−1
337	−13	15	−10	4	−5	−1
379	−13	10	13	−12	−5	1
421	−55	−4	3	18	−5	1
449	−41	0	10	19	−4	2
463	1	0	9	22	−1	−3
491	−69	6	9	20	3	1
547	43	2	15	0	−1	5
617	−55	−6	−1	−16	1	−5

(*continued*)

TABLE 2 (*continued*)

p	x_1	x_2	x_3	x_4	x_5	x_6
631	8	−6	−18	14	−8	0
659	−27	−4	−9	−30	3	1
673	22	20	8	−12	−4	−4
701	−125	20	3	−4	−1	1
743	−27	20	12	−3	−6	4
757	−27	14	−13	4	9	3
827	15	26	3	−6	−3	−5
883	15	−4	−13	−32	3	−3
911	29	−6	−10	−31	−2	4
953	50	12	8	−28	4	4
967	127	15	−6	20	−1	3

From Table 2, we see that x_1 is *even* only for $p = 631, 673, 953$, so that (see [4]) 2 is a seventh power (mod p) for primes $p \equiv 1 \pmod 7$ less than 1000 only for these primes. Indeed, we can show directly that $2 \equiv 196^7 \pmod{631}$, $2 \equiv 128^7 \pmod{673}$, $2 \equiv 120^7 \pmod{953}$.

Department of Mathematics
Carleton University
Ottawa, Ontario, Canada

1. H. P. ALDERSON, "On the septimic character of 2 and 3," *Proc. Cambridge Philos. Soc.*, v. 74, 1973, pp. 421–433.

2. L. E. DICKSON, "Cyclotomy and binomial congruences," *Trans. Amer. Math. Soc.*, v. 37, 1935, pp. 363–380.

3. E. KUMMER, "Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité," *J. Analyse Math.*, v. 12, 1847, pp. 185–212.

4. P. A. LEONARD & K. S. WILLIAMS, "The septic character of 2, 3, 5 and 7," *Pacific J. Math.* (To appear.)

5. P. A. LEONARD & K. S. WILLIAMS, "A diophantine system of Dickson," *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (To appear.)

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

7. K. G. REUSCHLE, "Zerfällung aller Primzahlen innerhalb des ersten Tausend in ihre aus siebenten Wurzeln der Einheit gebildeten complexen Primfactoren," *Monatsh. Kl. Preuss. Akad. Wiss. Berlin*, v. 1859, pp. 694–697.