Reprinted from JOURNAL OF MATHEMATICAL ANALYSIS AND APPLICATIONS. Vol. 15, No 1, July 1966

Printed in Belgium
118-131

Artiads Characterized

EMMA LEHMER

Berkeley, California

Dedicated to H. S. Vandiver on his eighty-third birthday

Almost a hundred years ago Lloyd Tanner [1, 2] constructed a table of what he called "coordinates of the reciprocal factors" of primes $p = 10n + 1$ in the field of fifth roots of unity $\alpha = \exp(2\pi i/5)$.

These coordinates are nothing else but the coefficients of the familiar Jacobi function

$$R(\alpha) = \sum_{s=1}^{p-2} \chi(s)\,\chi(s+1), \tag{1}$$

where the character $\chi(s)$ is defined by

$$\chi(s) = \alpha^{\text{ind}\,s}, \qquad (s, p) = 1, \tag{2}$$

the index of s being taken with respect to some primitive root g.

It is well known that

$$R(\alpha)\,R(\alpha^{-1}) = p, \tag{3}$$

which accounts for the term "reciprocal factor."

When the Jacobi function is expanded in powers of α and normalized so that the sum of the coefficients is -1, so that

$$R(\alpha) = \sum_{i=0}^{4} q_i \alpha^i, \qquad \sum_{i=0}^{4} q_i = -1, \tag{4}$$

then the q's are Tanner's coordinates.

In tabulating the q's Tanner noticed that about twenty per cent of the primes $p = 10n + 1$ are such that

$$q_1 \equiv q_2 \equiv q_3 \equiv q_4 \pmod 5. \tag{5}$$

He called these primes "artiads," presumably after the Greek word *αρτιος* meaning "perfect of its kind," but failed in his attempt to characterize such primes.

It is the purpose of this paper to prove that artiads are primes having the Fibonacci root $\theta = (1 + \sqrt{5})/2$ as a quintic residue, where θ is taken as a solution of the congruence $x^2 - x - 1 \equiv 0 \pmod{p}$.

This condition is then restated in terms of the divisibility by 5 of the number w appearing in the representation of $16p$ by the Dickson form [3, 4]

$$16p = x^2 + 50v^2 + 50v^2 + 125w^2$$

$$xw = v^2 - u^2 - 4uv = (v - 2u)^2 - 5u^2, \qquad x \equiv 1 \pmod 5. \tag{6}$$

We next show that the subset of artiads having 2 and α for quintic residues satisfy the conditions

$$\chi(1 + \alpha^i) = 1 \qquad \text{for} \qquad i = 0, 1, 2, 3, 4 \tag{7}$$

imposed by Professor Vandiver on primes of the form $10n + 1$ in connection with a criterion for Fermat's Last Theorem [5].

Since Professor Vandiver's criterion is stated in general for eth roots of unity, where e is an odd prime and $p = ef + 1$, we can ask ourselves whether the notion of an artiad can be generalized in such a way as to retain its connection with Vandiver's problem and with the eth power character of some algebraic number which can be thought of as a generalization of the Fibonacci root θ. We find that this can be done for $e = 7$ where θ is replaced by $2 \cos 2\pi/7$, but that the analogy fails for $e = 11$ so that we are unable to give a more general discussion.

The tools used here are those of cyclotomy for e a prime and the fundamental ideas and formulas will be found in the two Dickson papers cited above and will be stated without proof.

1. Cyclotomy

Let $p = ef + 1$ be a prime, where e is also an odd prime. Let α be an eth root of unity, $\alpha \neq 1$. Let g be an primitive root of p. Then relations (1) through (3) hold in general. If we now let

$$a_i = q_i - q_0, \tag{8}$$

then the Jacobi function can be written

$$R(\alpha) = \sum_{i=1}^{e-1} a_i \alpha^i, \qquad \text{where} \qquad \sum_{i=1}^{e-1} a_i \equiv -1 \pmod e. \tag{9}$$

It is well known that the a's are connected with the cyclotomic numbers (i, j) giving the number of solutions of the congruence

$$g^{se+i} + 1 \equiv g^{te+j} \pmod{p}. \tag{10}$$

This relation can be written

$$a_i - a_j = \sum_{k=0}^{e-1} [(k, i-k) - (k, j-k)]. \tag{11}$$

We shall also need

$$\sum_{i=0}^{e-1} (a_i a_{i+k} - a_i a_{i+j}) = 0 \qquad (i \neq -j \text{ or } -k) \tag{12}$$

and

$$\text{ind}\,(1 - \alpha^i) \equiv \sum_{j=1}^{e-1} j(i, j) \pmod{e}. \tag{13}$$

The cyclotomic numbers themselves for e odd satisfy the relations

$$(i, j) = (j, i) = (e - i, j - i) \tag{14}$$

and

$$\sum_{j=0}^{e-1} (0\ j) = f - 1, \qquad \sum_{j=0}^{e-1} (i, j) = f \qquad (\text{for } i \neq 0). \tag{15}$$

2. The Case $e = 5$

In this case Eqs. (14) reduce the 25 cyclotomic numbers (i, j) to seven which are subject to conditions (15). These numbers can be taken as $(0, k)$ for $k = 0, 1, 2, 3, 4$ and $(1, 2)$ and $(1, 3)$. They are related to the a's and to the x, u, v, w of the quadratic form (6) by

$$\begin{aligned} 5[(0, 1) - (0, 4)] &= 2a_1 - a_2 + a_3 - 2a_4 = 5v \\ 5[(0, 2) - (0, 3)] &= a_1 + 2a_2 - 2a_3 - a_4 = 5u \\ 5[(1, 3) - (1, 2)] &= a_1 - a_2 - a_3 + a_4 = 5w. \end{aligned} \tag{16}$$

It follows from (16) that $a_1 - a_4 \equiv a_2 - a_5 \equiv 2u - v \pmod 5$, so that

$$a_1 \equiv a_4 \pmod 5, \qquad a_2 \equiv a_3 \pmod 5, \qquad \text{or} \qquad v \equiv 2u \pmod 5 \tag{17}$$

implies that $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 5$, and hence by (8) that Tanner's condition (5) holds. Thus an artiad may be defined by either of the conditions (17). It can also be characterized by:

A prime p is an artiad if and only if $w \equiv 0 \pmod 5$ in (6). (18)

This follows at once from the third condition in (17) and the the second equation in (6).

We are now in a position to prove the following lemma

LEMMA 1. *If θ is a root of $x^2 - x - 1 \equiv 0 \pmod p$, then*

$$2 \operatorname{ind} \theta \equiv a_1 - a_4 \equiv a_2 - a_3 \equiv 2u - v \pmod 5.$$

PROOF. It is clear that θ can be written $\theta = -(\alpha + \alpha^4)$, so that

$$\theta^2 = (\alpha + \alpha^4)^2 = (1 + \alpha^2)(1 + \alpha^3) = (1 - \alpha^4)(1 - \alpha)/(1 - \alpha^2)(1 - \alpha^3)$$

and hence

$$2 \operatorname{ind} \theta = \operatorname{ind}(1 - \alpha) - \operatorname{ind}(1 - \alpha^2) - \operatorname{ind}(1 - \alpha^3) + \operatorname{ind}(1 - \alpha^4).$$

Substituting for $\operatorname{ind}(1 - \alpha^i)$ its value in terms of the cyclotomic numbers from (13) we obtain

$$2 \operatorname{ind} \theta \equiv \sum_{j=1}^{4} j[(1,j) - (2,j) - (3,j) + (4,j)]$$

$$\equiv (0,4) - 2(0,3) + 2(0,2) - (0,1)$$

$$\equiv a_2 - a_3 \equiv a_1 - a_4 \equiv 2u - v \pmod 5 \qquad (18)$$

by (14), (15), and (16).

Hence by (18) the condition that $\operatorname{ind} \theta = 0$ coincides with the condition (17) for an artiad and gives our main theorem; namely,

THEOREM 1. *A prime p is an artiad if and only if the roots of $x^2 - x - 1 \equiv 0 \pmod p$ are quintic residues of p.*

COROLLARY. *The density of artiads is twenty per cent. The 8 artiads less than 1000 are*

211, 281, 421, 461, 521, 691, 881, 991. (19)

The observed densities are given in the following table:

Limit	No. of artiads	No. of primes	Density	
10000	60	306	.1961	Tanner,
100000	484	2387	.2028	Muskat
1000000	3929	19617	.2003	7094

COROLLARY 2. *The* $(p-1)/5$th *term of the Fibonacci sequence*

$$F_0 = 0, \qquad F_1 = 1, \qquad F_{n+1} = F_n + F_{n-1}$$

is divisible by p *if and only if* p *is an artiad* [6].

Making use of condition (18) we can restate Theorem 1 in the form of a criterion for the quintic character of θ in line with the known [7] criteria for the quintic character of 2 and 3; namely,

2 is a quintic residue of p *if and only if* w *is a multiple of* 4. *3 is a quintic residue of* p *if and only if* x *or* w *is a multiple of* 9. θ *is a quintic residue of* p *if and only if* w *is a multiple of* 5.

The criterion for 5 to be a quintic residue of p takes a slightly different form; namely [8],

5 is a quintic residue of p *if and only if* $u \equiv 2v \pmod 5$.

When this is combined with the criterion for θ, written in the form $v \equiv 2u \pmod 5$, we have $u \equiv v \equiv 0 \pmod 5$ and hence by (6) we have $w \equiv 0 \pmod{25}$ so that

5 and θ *are both quintic residues of* p *if and only if* $w \equiv 0 \pmod{25}$.

We call such primes *hyperartiads* because it follows from (16) that

$$(0, 1) \equiv (0, 4) \pmod 5,$$

$$(0, 2) \equiv (0, 3) \pmod 5, \quad \text{and} \quad (1, 2) \equiv (1, 3) \pmod{25}. \tag{20}$$

This in turn implies by (15) that

$$(0, 1) \equiv (0, 2) \equiv (0, 3) \equiv (0, 4) \pmod 5.$$

The eight hyperartiads less than 10000 are

5081, 5591, 6211, 6271, 8581, 8861, 9011, 9661

5281

A270798
(A271171

corrected
bad)

If the characters of 5 and θ are not related then the ratio of hyperartiads to artiads should be $\frac{1}{5} = .20$. The actual figures are as follows:

Limit	Ratio		Tanner, Muskat 7040
10 000	8/60 = 2/15	= .1333	
100 000	86/484	= .1777	
1 000 000	763/3929	= .1942	

3. Vandiver's Problem

For $e = 5$ the answer to Professor Vandiver's conditions (7) will be found in the following theorem.

Theorem 2. *A prime p satisfies the conditions*

$$\chi(1 + \alpha^i) = 1 \quad \textit{for} \quad i = 0, 1, 2, 3, 4$$

where $\alpha \neq 1$ is a fifth root of unity, if and only if

$$p \equiv 1 \pmod{50} \quad \textit{and} \quad w \equiv 0 \pmod{20}.$$

[*The condition* $w \equiv 0 \pmod{20}$ *may be replaced by* $a_1 \equiv a_4 \pmod{10}$ *by (11)*]

Proof. The condition of the theorem with $i = 0$ implies that 2 is a fifth power residue and hence $w \equiv 0 \pmod 4$. Next since $(1 + \alpha) = \alpha(1 + \alpha^4)$ we must have $\chi(\alpha) = 1$ and this implies that $p \equiv 1 \pmod{50}$. Finally since $\theta = -\alpha(1 + \alpha^3)$, this implies that $\chi(\theta) = 1$. Conversely if 2, α and θ are quintic residues, then (7) is satisfied. This proves the theorem. □

The only primes satisfying the theorem less than 10,000 are $p = 3251$ and $p = 4751$. There are 20 such primes less than 100,000, among them the prime $p = 61051$ cited by Professor Vandiver as an example in [6].

The corresponding problem of finding primes for which

$$\chi(1 - a^i) = 1 \quad \text{for} \quad i = 1, 2, 3, 4 \tag{21}$$

leads to the following theorem.

Theorem 3. *A prime p satisfies conditions (21) if and only if*

$$p \equiv 1 \pmod{50} \quad \text{and} \quad w \equiv 0 \pmod{25}.$$

PROOF. As in Theorem 2 we must have $\chi(\alpha) = 1$, next since

$$(1 + \alpha^i) = (1 - \alpha^{2i})(1 - \alpha^i)$$

we have $\chi(1 + \alpha^i) = 1$ for $i = 1, 2, 3, 4$, and therefore $\chi(\theta) = 1$. Finally since $5 = [(\alpha - \alpha^4)(\alpha^2 - \alpha^3)]^2$ we have $\chi(5) = 1$, and $w = 0 \pmod{25}$. Conversely, if 5, α and θ are all fifth power residues, then (21) is satisfied. Hence the solutions are hyperartiads of the form $50n + 1$.

There are 17 solutions of Theorem 3 less than 100,000, the least one being 13451 among the 86 hyperartiads less than this limit.

A271210

In concluding this section we mention a few simple properties of artiads; namely,

Every artiad has a run of at least four consecutive quintic residues:

$$\theta - 2, \quad \theta - 1, \quad \theta, \quad \theta + 1.$$

Every hyper-artiad has a run of at least six consecutive quintic residues:

$$\theta - 3, \quad \theta - 2, \quad \theta - 1, \quad \theta, \quad \theta + 1, \quad \theta + 2.$$

If θ is a quintic, but not a higher power residue, then all the quintic residues of p can be obtained by addition as follows:

$$r_1 = 1, \qquad r_2 = \theta, \qquad r_n = r_{n-1} + r_{n-2}.$$

We now consider the effect of imposing Tanner's condition (5) for an artiad with respect to some other prime modulus $\pi \neq 5$. The author has conjectured and Muskat gave an unpublished proof that such primes π are eth power residues of p (with some possible exceptions). We give here a proof of a slightly stronger theorem for $e = 5$.

THEOREM 4. *If $a_1 \equiv a_4 \pmod{\pi}$ and $a_2 \equiv a_3 \pmod{\pi}$, where $\pi \neq 5$ is a prime then π is a quintic residue of p.*

PROOF. By (16) it follows that $u \equiv v \equiv w \equiv 0 \pmod{\pi}$ and by (6) that $16p \equiv x^2 \pmod{\pi}$. Substituting these into the period equation considered as a congruence modulo π [7], we obtain

$$F(z) \equiv z^5 - 10pz^3 - 5pxz^2 - 15p^2z - p^2x \pmod{\pi}.$$

For $z \equiv x \pmod{\pi}$, we have

$$F(x) = x^5 - 15px^3 - 16p^2x = x(x^2 + p)(x^2 - 16p) \equiv 0 \pmod{\pi}.$$

But by Kummer's theorem all the factors of numbers represented by the period equation are quintic residues of p. This proves the theorem.

4. The Case $e = 3$

The question now arises as to whether the notion of an artiad is peculiar to quintic residues. The problem did not arise in the cubic case because the two coefficients of the Jacobi function are always congruent modulo 3, and hence every prime is a cubic artiad.

However, the condition $(0, 1) \equiv (0, 2) \pmod 3$ for a hyperartiad requires that

$$M = (0, 1) - (0, 2) \equiv 0 \pmod 3,$$

where $4p = L^2 + 27M^2$. It is well known, however, that M is a multiple of 3 if and only if 3 is a cubic residue of p. Vandiver's problem for $e = 3$ requires that 2 and ω are cubic residues. This implies that $p = 18n + 1$ and $L \equiv -2, \pmod{18}$.

5. The Case $e = 7$

In order to arrive at a reasonable generalization of artiads to seventh power residues we first give a generalization of Lemma 1.

Lemma 2. *Let $\alpha \neq 1$ be a seventh root of unity and let $\theta_k = \alpha^k + \alpha^{-k}$ be the roots of the congruence*

$$x^3 + x^2 - 2x - 1 \equiv 0 \pmod p,$$

then

$$\text{ind } \theta_k \equiv k(a_{3k} - a_{7-3k}) \pmod 7 \qquad (k = 1, 2, 3), \tag{22}$$

where the subscripts are taken modulo 7.

Proof. As in Lemma 1 we can write

$$2 \text{ ind } \theta_\kappa = \text{ind } (1 - \alpha^{4k}) + \text{ind } (1 - \alpha^{3k}) - \text{ind } (1 - \alpha^{2k}) - \text{ind } (1 - \alpha^{5k}).$$

Substituting the expressions for $\text{ind } (1 - \alpha^t)$ from (13) and using (14) and (15), we obtain

$$\text{ind } \theta_1 = (0, 2) - (0, 5) + 2[(0, 3) - (0, 4)] - 2[(1, 3) - (1, 5)]$$

$$\text{ind } \theta_2 = 3[(0, 1) - (0, 6)] - 2[(0, 3) - (0, 4)] + 3[(1, 3) - (1, 5)]$$

$$\text{ind } \theta_3 = -3[(0, 1) - (0, 6)] - [(0, 2) - (0, 5)] - [(1, 3) - (1, 5)]. \tag{23}$$

On the other hand, we find from (11) that

$$\begin{aligned} a_1 - a_6 &= 2[(0,1) - (0,6)] + [(0,3) - (0,4)] + 2[(1,3) - (1,5)] \\ &\equiv 3 \text{ ind } \theta_2 \pmod 7 \\ a_2 - a_5 &= -[(0,1) - (0,6)] + 2[(0,2) - (0,5)] + 2[(1,3) - (1,5)] \\ &\equiv 5 \text{ ind } \theta_3 \pmod 7 \\ a_3 - a_4 &= (0,2) - (0,5) + 2[(0,3) - (0,4)] - 2[(1,3) - (1,5)] \\ &\equiv \text{ind } \theta_1 \pmod 7. \end{aligned} \tag{24}$$

This proves the lemma.

The following theorem is an immediate consequence of Lemma 2.

THEOREM 5. *The three roots of the congruence,*

$$x^3 + x^2 - 2x - 1 \equiv 0 \pmod p,$$

are seventh power residues of $p = 14n + 1$ *if and only if*

$$a_k \equiv a_{7-k} \pmod 7 \quad \textit{for} \quad k = 1, 2 \textit{ and } 3. \tag{25}$$

We will call primes satisfying Theorem 5 *septic artiads*. The first few septic artiads are

14197, 21617, 25801, 24977, 25999, ⋯.

A270800

Their observed densities are as follows:

Limit	No. of septic artiads	No. of primes	Density
100 000	28	1607	.0174
1000 000	240	13063	.0184
2000 000	466	24792	.0188

They are short of the expected density of $\frac{1}{49} = .0204$, assuming that the characters of θ_1 and θ_2 are not related, while that of θ_3 is determined, since their product is equal to 1.

We show that the notion of a hyperartiad also carries over to seventh power residues by proving the following theorem.

THEOREM 6. *A septic artiad has* 7 *for a seventh power residue if and only if*

$$(0,k) \equiv (0, 7-k) \pmod 7 \quad \textit{for} \quad k = 1, 2, 3. \tag{26}$$

PROOF. By Theorem 3 we have $a_k - a_{7-k} \equiv 0 \pmod 7$. The condition for 7 to be a seventh power residue is [8]

$$a_1 - a_6 + 30\,(a_2 - a_5) + 18\,(a_4 - a_3) \equiv 0 \pmod{49}. \tag{27}$$

In our case, this reduces to

$$[(a_1 - a_6) + 2\,(a_2 - a_5) + 3\,(a_3 - a_4)]/7 \equiv 0 \pmod 7. \tag{28}$$

(24) By using (24), this condition becomes

$$(0, 2) - (0, 5) \equiv (0, 4) - (0, 3) \pmod 7.$$

Substituting this back into 24, we obtain

$$(0, 1) - (0, 6) \equiv (0, 2) - (0, 5) \equiv (0, 3) - (0, 4) \pmod 7. \tag{29}$$

In order to complete the proof of (26), we first point out that (25) implies $a_1 \equiv a_2 \equiv \cdots \equiv a_6 \pmod 7$. It follows from (11) that

(25)
$$a_1 + a_6 - (a_2 + a_5) = 7\,[(2, 4) - (1, 4)] \equiv 0 \pmod 7$$

few
$$a_1 + a_6 - (a_3 + a_4) = 7\,[(2, 4) - (1, 2)] \equiv 0 \pmod 7, \tag{30}$$

hence

$$a_1 + a_6 \equiv a_2 + a_5 \equiv a_3 + a_4 \pmod 7, \tag{31}$$

which together with (25), shows that $a_i \equiv a_j \pmod 7$ for all $i, j \neq 0$.

We next write (12) in the form (with $k = 1, j = 2$)

$$\begin{aligned} 4\,(a_1a_6 - a_3a_4) &= 4\,[a_1(a_2 - a_5) + a_6(a_5 - a_4) + (a_3 - a_4)\,(a_2 - a_5)] \\ &= (a_1 + a_6)^2 - (a_1 - a_6)^2 - (a_3 + a_4)^2 + (a_3 - a_4)^2. \end{aligned}$$

Taking this modulo 49 and recalling that for an artiad $a_i \equiv 1 \pmod 7$ by (9), we obtain

$$a_2 + a_5 \equiv a_1 + a_6 \pmod{49}. \tag{32}$$

If we repeat this argument with $k = 1, j = 3$ we obtain

$$a_3 + a_4 \equiv a_1 + a_6 \pmod{49}. \tag{33}$$

Hence for an artiad (31) holds modulo 49. Substituting this into (30), we obtain

$$(1, 2) \equiv (1, 4) \equiv (2, 4) \pmod 7. \tag{34}$$

Using (15) with $j = 1$ and 2, we have

$$2(2, 4) - (1, 2) - (1, 4) = (0, 1) - (0, 2) - (0, 5) + (0, 6),$$

while (15) with $j = 1$ and 4 gives

$$(2, 4) - 2(1, 2) - (1, 4) = (0, 1) - (0, 3) - (0, 4) + (0, 6).$$

Hence by (34) we have

$$(0, 1) + (0, 6) \equiv (0, 2) + (0, 5) \equiv (0, 4) + (0, 3) \pmod 7 \qquad (35)$$

which together with (29) establishes (26).

Conversely, if (26) holds then conditions (24) and (28) are satisfied, and 7 and all the θ's are seventh power residues. This completes the proof of the theorem.

6. Vandiver's Problem for $e = 7$

Theorem 2 can be generalized to the case $e = 7$ as follows:

Theorem 7. *A prime p satisfies the conditions*

$$\chi(1 + \alpha^i) = 1 \quad \text{for} \quad i = 0, 1, \cdots, 6,$$

where $\alpha \neq 1$ is a seventh root of unity, if and only if

$$p \equiv 1 \pmod{98} \quad \text{and} \quad a_i \equiv a_{7-i} \pmod{14} \quad (i = 1, 2, 3).$$

Proof. The condition of the theorem with $i = 0$ implies that $\chi(2) = 1$ and hence $a_i \equiv a_{7-i} \pmod 2$. Next since $(1 + \alpha) = \alpha(1 + \alpha_6)$ we have $\chi(\alpha) = 1$ and $p = 98n + 1$. Finally, since $\theta_i = \alpha^i(1 + \alpha^{-2i})$, we have $\chi(\theta_i) = 1$. By Theorem 5 we have $a_i = a_{7-i} \pmod 7$ and the conclusion follows. Conversely if $a_i \equiv a_{7-i} \pmod{14}$ then 2 and θ_i are seventh power residues, and if $p = 98n + 1$ so is α and the theorem follows.

Similarly we have an analogue of Theorem 3.

Theorem 8. *A prime p satisfies the conditions*

$$\chi(1 - \alpha^i) = 1 \quad \text{for} \quad i = 0, 1, \cdots, 6$$

where $\alpha \neq 1$ is a seventh root of unity, if and only if

$$p \equiv 1 \pmod{98} \quad \text{and} \quad (0, j) \equiv (0, 7 - j) \pmod 7.$$

Proof. The conditions of the theorem imply that the conditions of Theorem 7 hold for $i \neq 0$. Hence α and θ_κ are seventh power residues, and so is 7, since

$$7 = -\alpha^5[(1 - \alpha)(1 - \alpha^3)(1 - \alpha^5)]^2.$$

Conversely, if α, θ_κ and 7 are seventh power residues, then the conditions of the theorem are satisfied. Hence the subset of hyperartiads of the form $98n + 1$ provides solutions to this problem and the theorem follows from Theorem 6.

It is rather surprising that of the 28 septic artiads $< 10^5$ in Muskat's table, none satisfies Theorem 6 or 7 and therefore 8.

Further calculations on the 7040 at the Computer Center in Berkeley gave the following results:

Out of the 240 artiads less than 10^6 there are seven hyperartiads, namely,

665897, 741413, 794207, 859601, 876611, 892627, 980911.

Of these only 876611 satisfies the conditions of Theorem 8. There are just two solutions of Vandiver's problem for $e = 7$, namely,

874651 and 941879.

Out of the 466 septic artiads less than $2 \cdot 10^6$ there are 34 hyperartiads, four of which satisfy Theorem 8, and there are five solutions of Vandiver's problem. All these figures are considerably smaller than expected, assuming independence of the various characters. This is probably due to the large size of the first solution.

As in the quintic case the artiads enjoy runs of four consecutive seventh power residues. This follows from the fact that

$$\theta_\kappa^2 = \theta_{\kappa+1} + 2 \qquad \text{and} \qquad \theta_\kappa \theta_{\kappa+1} = -(1 + \theta_{\kappa+1}).$$

Hence, as before,

$$\theta_\kappa - 1, \qquad \theta_\kappa, \qquad \theta_\kappa + 1, \qquad \text{and} \qquad \theta_\kappa + 2$$

are all seventh power residues. Similarily the septic hyperartiads have runs of six consecutive residues, since $-7 = (\theta_1 - 2)(\theta_2 - 2)(\theta_3 - 2)$, giving the additional residues $\theta_\kappa - 2$ and $\theta_\kappa + 3$.

Another property of septic artiads which has no analogue in the quintic case is the following:

THEOREM 9. *If $p = 14n + 1$ is a septic artiad then $t \equiv 0 \pmod 7$ in*

$$p = s^2 + 7t^2. \tag{36}$$

PROOF. This follows from the expression for t in terms of the cyclotomic numbers (see [4], p. 376), namely,

$$2t = (0, 1) + (0, 2) + (0, 4) - (0, 3) - (0, 5) - (0, 6) + (1, 5) - (1, 3).$$

But by (23) this is congruent modulo 7 to

$$2t = \text{ind } \theta_\kappa - 2 \text{ ind } \theta_{\kappa+1} . \tag{37}$$

Hence for an artiad $t \equiv 0 \pmod 7$ and the theorem follows.

But Eq. (37) proves a little more; namely,

THEOREM 10. *A prime* $p = 14n + 1 = s^2 + 343\tau^2$ *if and only if*

$$a_1 + a_2 + a_4 \equiv a_3 + a_5 + a_6 \pmod 7. \tag{38}$$

PROOF. By (37) the requirement $t = 7\tau$ implies

$$\text{ind } \theta_\kappa = 2 \text{ ind } \theta_{\kappa+1} .$$

Substituting this into (23), we obtain (38). Conversely, if (38) holds, then adding the three equations (24), we obtain

$$-\text{ind } \theta_1 + 3 \text{ ind } \theta_2 + 5 \text{ ind } \theta_3 = 0.$$

But the sum of all the indices is zero, hence $\text{ind } \theta_2 = 2 \text{ ind } \theta_3$ and $t \equiv 0 \pmod 7$ by (37). This proves the theorem.

Of the 228 primes $< 10^5$ satisfying Theorem 10 there are 28 artiads, which is just short of the expected one-seventh.

A271265

5. THE CASE $e = 11$

Theorems 1 and 5 cannot be readily generalized to the case $e = 11$ because Lemmas 1 and 2 lose their simple structure when generalized to $e = 11$. We state without proof this generalization in order to clarify the difficulty which arises at this point:

LEMMA 3. *Let* $\alpha \neq 1$ *be an eleventh root of unity and let* $\theta_k = \alpha^k + \alpha^{-k}$ *be the roots of the congruence*

$$y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1 \equiv 0 \pmod p,$$

then

$$\text{ind } \theta_k - 3 \text{ ind } \theta_{k+1} = 5k(a_{3k} - a_{8k}) - k(a_{4k} - a_{7k})$$

where the subscripts are taken modulo 11.

In is clear from this that if $a_k \equiv a_{11-k} \pmod{11}$ for $k = 1, 2, \cdots, 10$ then

$$\text{ind } \theta_k = 3 \text{ ind } \theta_{k+1} ;$$

but this does not guarantee that the θ's are eleventh power residues. However, if one of the θ's is a residue, then all the θ's are residues in this case. It is quite obvious that for larger values of e the corresponding lemmas would increase in complexity and one could not expect to obtain results comparable in simplicity to those obtained above for the cases $e = 5$ and $e = 7$.

References

1. H. W. Lloyd Tanner. On the binomial equation $x^p - 1$: Quintesection. *Proc. London Math. Soc.* **18** (1886-7), 214-234.
2. H. W. Lloyd Tanner. On complex primes formed with fifth roots of unity. *Proc. London Math. Soc.* **24** (1892-3), 223-262.
3. L. E. Dickson. Cyclotomy, higher congruences and Waring's problem. *Amer. J. Math.* **57** (1935), 391-424.
4. L. E. Dickson. Cyclotomy and trinomial congruences. *Trans. Amer. Math. Soc.* **37** (1935), 363-380.
5. H. S. Vandiver. New types of trinomial congruence criteria applying to Fermat's last theorem. *Proc. Natl. Acad. Sci. U.S.A.* 40 (1954), 248-252.
6. E. Lehmer. On the quadratic character of Fibonacci root. *Fibonacci J.* (to appear).
7. E. Lehmer. The quintic character of 2 and 3. *Duke Math. J.* 18 (1951), 11-18.
8. J. B. Muskat. On the solvability of $x^e \equiv e \pmod{p}$, *Pacific J.* **14** (1964), 257-260.

PRINTED IN BRUGES, BELGIUM, BY THE ST CATHERINE PRESS, LTD.