MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 192
OCTOBER 1990, PAGES 783–813

PSEUDOPRIMES FOR HIGHER-ORDER LINEAR RECURRENCE SEQUENCES

S. GURAK

ABSTRACT. With the advent of high-speed computing, there is a rekindled interest in the problem of determining when a given whole number $N > 1$ is prime or composite. While complex algorithms have been developed to settle this for 200-digit numbers in a matter of minutes with a supercomputer, there is a need for simpler, more practical algorithms for dealing with numbers of a more modest size. Such practical tests for primality have recently been given (running in deterministic linear time) in terms of pseudoprimes for certain second- or third-order linear recurrence sequences. Here, a powerful general theory is described to characterize pseudoprimes for higher-order recurrence sequences. This characterization leads to a broadening and strengthening of practical primality tests based on such pseudoprimes.

1. INTRODUCTION

Efficient, practical tests for primality have recently been given in terms of pseudoprimes for certain second- or third-order linear recurrences [1, 5, 11]. The utility of these tests rely on the quickness of the algorithm (deterministic linear time) and the scarceness of pseudoprimes in the test range. In a recent paper [9] I refined and strengthened those pseudoprimes that involved Lucas sequences. Here I wish to extend these results to higher-order sequences. The methods developed will enable one to devise much stronger tests (fewer pseudoprimes) of comparable efficiency.

To begin, I review some of the types of pseudoprimes that have appeared in the literature and mention what is known concerning their distribution. The first pseudoprimes studied [15] were based on Fermat's criterion. Let c be an integer greater than 1. An (ordinary) pseudoprime to base c (or psp_c) is a composite number N, $(c, N) = 1$, for which $c^{N-1} \equiv 1 \pmod N$. A strong pseudoprime to base c is an odd composite number N, $(c, N) = 1$, for which either (i) $c^d \equiv -1 \pmod N$ or (ii) $c^{d\cdot 2^r} \equiv -1 \pmod N$ for some r with $0 \le r < s$, where $N - 1 = d \cdot 2^s$, d odd.

Such kinds of pseudoprimes where shown to be rare, but not too scarce. Pomerance [13] has shown for ordinary or strong pseudoprimes, base c, that

Received February 23, 1989; revised October 2, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y11; Secondary 11R37, 11A51, 11B50.

the number of pseudoprimes not exceeding x is bounded above by

$$(1) \qquad x \exp\{-\log x \log\log\log x / 2 \log\log x\}$$

for all sufficiently large x. For the best lower bounds, see Pomerance's work [14].

Baillie and Wagstaff [5] introduced analogs for ordinary pseudoprimes based on Lucas sequences and obtained similar results concerning their distributions. In [9], I strengthened their characterization of pseudoprimes for those Lucas sequences which arise from resolvents of certain irreducible polynomials having dihedral Galois group of order 6, 8, or 12. That treatment defined pseudoprimes using sequence signatures and was motivated in part to fully exploit the periodic and recursive properties of the sequences. I indicated there that the techniques employed had a broader application to higher-order linear recurrence sequences than that of strengthening Kurtz, Shanks, and Williams' characterization [11] of pseudoprimes for certain third-order recurrences. It is this far-reaching generalization that I wish to develop here.

I shall begin by outlining some preliminary results on matrix subrings in §2 which will be critical later on. In §3, I will give suitable higher-order analogs for the classical Lucas sequences. Recall that if β and $\overline{\beta}$ are conjugate irrational roots of $p(x) = x^2 + a_1 x + a_0$, where a_0, a_1 are integers with $a_1 \neq 0$, then the Lucas sequences U and V corresponding to $p(x)$ are given by

$$(2) \qquad U_n = \frac{\beta^n - \overline{\beta}^n}{\beta - \overline{\beta}} \qquad (n \geq 0)$$

and

$$(3) \qquad V_n = \beta^n + \overline{\beta}^n \qquad (n \geq 0).$$

Their higher-order analogs provide the basis for characterizing pseudoprimes for higher-order linear recurrences in §4. In the final section, this characterization of pseudoprimes is further strengthened for sequences which arise from resolvent polynomials. The methods employed rely heavily on the deeper arithmetic properties associated with Lagrange resolvents.

For the sake of simplicity, I shall only treat linear recurrences defined over Q. But the theory can be adapted to the more general setting of linear recurrences defined over an arbitrary number field.

2. Some remarks concerning matrices

In order to characterize pseudoprimes for higher-order sequences, I will need some elementary results from the theory of matrices over commutative rings. Let R denote a commutative ring with unity 1, and R^x the multiplicative group of invertible elements in R. Let $M_m(R)$ be the ring of square $m \times m$ matrices with entries from R, and $\mathrm{GL}_m(R)$ the group of those matrices M with $\det(M)$ in R^x. Consider any monic polynomial $p(x)$ in $Z[x]$ of degree $m > 0$, say

$$p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0,$$

and associate with it an $m \times m$ matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{m-1} \end{bmatrix} \tag{4}$$

considered as an element of $M_m(R)$ in the natural manner. Let $M_A(R)$ be the subset of $M_m(R)$ consisting of those matrices of the form

$$M_x = \begin{bmatrix} x_1 & x_2 & \cdots & x_m \\ (x_1 & x_2 & \cdots & x_m)A \\ & & \vdots & \\ (x_1 & x_2 & \cdots & x_m)A^{m-1} \end{bmatrix}$$

for some $x = (x_1, \dots, x_m)$ in R^m. It is clear that

$$M_x = \sum_{i=1}^{m} x_i M_{e_i},$$

where e_i denotes the vector of R^m with 1 in the ith component and zeros elsewhere. Since $M_{e_j} = A^{j-1}$ $(1 \le j \le m)$ and $p(A) = O_m$, the $m \times m$ zero matrix, one has the following

Proposition 1. *The set $M_A(R)$ is a commutative subring of $M_m(R)$ containing the identity matrix I_m. As an R-module, $M_A(R)$ is spanned by the powers A^{j-1} $(1 \le j \le m)$.*

We remark that in case $p(x)$ is irreducible, say with root β, and $R = Q$, then it can be shown that $M_A(Q) \cong Q(\beta)$ and that the multiplication $M_z = M_x M_y$ is that induced by multiplying

$$\begin{aligned}(x_1 + x_2\beta + \cdots + x_m\beta^{m-1})(y_1 + y_2\beta + \cdots + y_m\beta^{m-1}) \\ = (z_1 + z_2\beta + \cdots + z_m\beta^{m-1})\end{aligned}$$

in $Q(\beta)$ with respect to the basis $\{1, \beta, \dots, \beta^{m-1}\}$.

Now consider any linear recurrence sequence $W = (W_n)$ with values in R satisfying the recursion

$$W_{n+m} + a_{m-1}W_{n+m-1} + \cdots + a_0 W_n = 0 \qquad (n \ge 0). \tag{5}$$

Write

$$\det(W) = \det \begin{bmatrix} W_0 & W_1 & \cdots & W_{m-1} \\ W_1 & W_2 & \cdots & W_m \\ \vdots & \vdots & & \vdots \\ W_{m-1} & W_m & \cdots & W_{2m-2} \end{bmatrix}.$$

Proposition 2. *Let $\overline{W}_0, \overline{W}_1, \dots, \overline{W}_{m-1}$ be any values in R. If* $\det(W) \in R^\times$, *then there is a unique matrix C in $M_A(R)$ satisfying*

$$C \begin{bmatrix} W_0 \\ W_1 \\ \vdots \\ W_{m-1} \end{bmatrix} = \begin{bmatrix} \overline{W}_0 \\ \overline{W}_1 \\ \vdots \\ \overline{W}_{m-1} \end{bmatrix}. \tag{6}$$

Proof. The matrix equation (6) is equivalent to solving

$$\begin{gathered} x_1 W_0 + x_2 W_1 + \cdots + x_m W_{m-1} = \overline{W}_0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1 W_{m-1} + x_2 W_m + \cdots + x_m W_{2m-2} = \overline{W}_{m-1} \end{gathered}$$

for some $C = M_x$ with $x \in R^m$. Since $\det(W) \in R^\times$ by hypothesis, one can use Cramer's rule to find a unique solution $x = (x_1, \dots, x_m)$. □

Before concluding this discussion, I would like to make a remark pertaining to the computation of any sequence $W = (W_m)$ defined over R and satisfying (5). For the most part one wishes to find m consecutive terms $W_N, W_{N+1}, \dots, W_{N+m-1}$, which amounts to finding the matrix power A^N, since

$$A^N \begin{bmatrix} W_0 \\ W_1 \\ \vdots \\ W_{m-1} \end{bmatrix} = \begin{bmatrix} W_N \\ W_{N+1} \\ \vdots \\ W_{N+m-1} \end{bmatrix}.$$

There is, of course, a standard technique to do this, requiring at most $2\log_2 N$ matrix multiplications, which relies on the binary representation of N.

3. Higher-order analogs for Lucas sequences

The Lucas sequences (2), (3) introduced in §1 satisfy fundamental identities found by Lucas. To name two of them,

$$2V_{n+k} = V_n V_k + \Delta U_n U_k \tag{7}$$

and

$$2U_{n+k} = U_n V_k + U_k V_n \tag{8}$$

for $n, k \geq 0$, where $\Delta = a_1^2 - 4a_0$ is the discriminant of $x^2 + a_1 x + a_0$, $a_1 \neq 0$ [12]. The sequence U is a divisibility sequence; that is, $U_0 = 0$, $U_1 = 1$, and if $N | U_\omega$ then $N | U_{k\omega}$ for all $k > 1$. In particular, if N is a positive integer prime to a_0, there is a least positive integer ω for which $N | U_\omega$. (This value

$\omega = \omega(N)$ is called the rank of apparition of N in the Lucas sequence U.) When N is prime and $N \nmid 2a_0\Delta$, it is known that

$$\omega(N) \,\Big|\, N - (\Delta/N) \tag{9}$$

and that

$$\omega(N^r) \,\Big|\, N^{r-1}\omega(N) \quad \text{for } r > 0. \tag{10}$$

The periodicity properties of the sequences U and V are well documented [12, 18]. For a positive integer N with $(N, 2a_0\Delta) = 1$, both sequences have a common period $\pi = \pi(N)$, modulo N and $\omega(N)|\pi(N)$. In addition, the set of values $B = B_N = \{U_{k\omega+1} | 0 < k < \pi/\omega\}$ forms a multiplicative group (mod N), known as the group of multipliers of U for the modulus N. In fact, B_N is cyclic generated by the term $U_{\omega+1}$ (mod N).

My purpose here is to introduce higher-order analogs of the Lucas sequences U and V, which will make particularly convenient choices later in characterizing pseudoprimes for higher-order linear recurrences. The sequences introduced possess properties similar to those just mentioned for Lucas sequences. With this goal in mind, I define sequences $U = (U_n)$ and $V = (V_n)$ by

$$U_n = \begin{vmatrix} \beta_1^n & \cdots & \beta_m^n \\ \beta_1^{m-2} & \cdots & \beta_m^{m-2} \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{vmatrix} \cdot \begin{vmatrix} \beta_1^{m-1} & \cdots & \beta_m^{m-1} \\ \beta_1^{m-2} & \cdots & \beta_m^{m-2} \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{vmatrix}^{-1} \qquad (n \geq 0), \tag{11}$$

$$V_n = \beta_1^n + \cdots + \beta_m^n \qquad (n \geq 0), \tag{12}$$

where the β_i are distinct roots of some monic polynomial

$$p(x) = a_m x^m + \cdots + a_1 x + a_0, \qquad a_m = 1, \tag{13}$$

in $Z[x]$ of discriminant $\Delta = \Delta(p(x))$. Both sequences are integer-valued and satisfy the recursion

$$W_{n+m} + a_{m-1}W_{n+m-1} + \cdots + a_1 W_{n+1} + a_0 W_n = 0 \qquad (n \geq 0). \tag{14}$$

I note that U is a generalized "divisibility" sequence in the sense that $U_0 = U_1 = \cdots = U_{m-2} = 0$, $U_{m-1} = 1$, and if N divides $m - 1$ consecutive terms $U_\omega, U_{\omega+1}, \ldots, U_{\omega+m-2}$, then N divides $U_{k\omega}, U_{k\omega+1}, \ldots, U_{k\omega+m-2}$ for $k > 1$. This divisibility property and other similarities with the Lucas sequence (2) were noted by H. Duparc [8]. I shall give a separate, self-contained treatment of some of these similarities here. The divisibility property is an immediate consequence of the following result.

Proposition 3. *For any* $\omega, k > 0$,

(i) $\mathrm{GCD}(U_\omega, U_{\omega+1}, \ldots, U_{\omega+m-2}) | \mathrm{GCD}(U_{k\omega}, U_{k\omega+1}, \ldots, U_{k\omega+m-2})$,

(ii) $U_{k\omega+m-1} \equiv U_{r\omega+m-1} \cdot U_{s\omega+m-1}$ (mod $\mathrm{GCD}(U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2})$) *if* $k = r + s$ *with* $r, s \geq 0$, *and*

(iii) $U_{k\omega+m-1} \equiv U^k_{\omega+m-1}$ (mod $\mathrm{GCD}(U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2})$).

Proof. I shall first establish that

$$(15) \qquad U_{\omega+r} \equiv U_{\omega+m-1} \cdot U_r \qquad (\text{mod } \mathrm{GCD}(U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2}))$$

for all $r \geq 0$. Since both (U_r) and $(U_{\omega+r})$ satisfy (14), it suffices to verify that (15) holds for any m consecutive values of r, say $0 \leq r \leq m-1$. But this is immediate, since $U_0 = U_1 = \cdots = U_{m-2} = 0$, $U_{m-1} = 1$.

Now (i) follows easily from (15) using induction on k, as does (iii). To establish (ii), note that for $r, s > 0$

$$U_{r\omega+m-1} \equiv U^r_{\omega+m-1} \quad \text{and} \quad U_{s\omega+m-1} \equiv U^s_{\omega+m-1}$$

mod($\mathrm{GCD}(U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2})$) by (iii). Thus,

$$U_{k\omega+m-1} \equiv U^k_{\omega+m-1} \equiv U^r_{\omega+m-1} \cdot U^s_{\omega+m-1} \equiv U_{r\omega+m-1} \cdot U_{s\omega+m-1}$$

mod($\mathrm{GCD}(U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2})$) for $k = r + s$ with $r, s > 0$. If either r or s is zero, the result (ii) holds trivially. This completes the proof of the proposition. □

The question naturally arises as to whether or not there is a rank of apparition of N in the sequence U. To settle this, one has

Proposition 4. *Suppose* N *is an odd positive integer prime to* a_0, *and that* N *divides* $U_k, U_{k+1}, \dots, U_{k+m-2}$ *and* $U_l, U_{l+1}, \dots, U_{l+m-2}$ *for some* $l, k > 0$. *Then* N *divides* $U_j, U_{j+1}, \dots, U_{j+m-2}$, *where* $j = \mathrm{GCD}(l, k)$.

Proof. It suffices to show that N divides $U_{l-k}, U_{l-k+1}, \dots, U_{l-k+m-2}$, assuming $l > k$. I assert that if $(N, a_0) = 1$, then U_{k+m-1} is prime to N. Suppose otherwise, say $\mathrm{GCD}(N, U_{k+m-1}) = d > 1$. Since $(d, a_0) = 1$, we get $d | U_{k-1}$ from (14). Repeating this argument shows that U is the zero sequence (mod d). This contradicts the fact that $U_{m-1} = 1$, so the assertion that $(U_{k+m-1}, N) = 1$ is valid.

I now show that N divides $U_{l-k}, U_{l-k+1}, \dots, U_{l-k+m-2}$. Observe that since $(U_{k+m-1}, N) = 1$,

$$(16) \qquad U_{l+r} \equiv U_{k+r} \cdot \frac{U_{l+m-1}}{U_{k+m-1}} \qquad (\text{mod } N)$$

for $0 \leq r \leq m-1$. The congruence (16) actually holds for all $r \geq -k$, since both (U_{l+r}) and (U_{k+r}) satisfy the recursion (14), and $(N, a_0) = 1$. In particular, we get $U_{l-k}, U_{l-k+1}, \dots, U_{l-k+m-2} \equiv 0$ (mod N). □

From Proposition 4 it follows that for any N with $(N, a_0) = 1$, there is a least positive integer $\omega = \omega(N)$ for which N divides $U_\omega, U_{\omega+1}, \dots, U_{\omega+m-2}$. (I shall refer to $\omega(N)$ as the rank of apparition of N in the sequence U.) Let $t = t(N)$ be the order of $U_{\omega+m-1}$ (mod N). (Note from the argument in the proof of Proposition 4 above that $(N, U_{\omega+m-1}) = 1$.) It follows from (iii) of Proposition 3 that the set $B = B_N = \{U_{k\omega+m-1} \pmod N) \mid 0 \le k < t\}$ is a cyclic multiplicative group modulo N. Following the classical terminology, we refer to B_N as the group of multipliers of U for the modulus N. The period of U modulo N, denoted $\pi = \pi(N)$, is the product $\omega(N) \times t(N)$. When $p(x)$ is irreducible, it easily follows from properties of finite fields that for a prime $p \nmid \Delta$,

$$\pi(p) \,\Big|\, \delta(p) \tag{17}$$

and

$$\pi(p^r) \,\Big|\, p^{r-1}\pi(p) \quad \text{for } r > 1, \tag{18}$$

where $\delta(p) = \mathrm{LCM}_{\mathfrak{p}|p}\{p^{f(\mathfrak{p})} - 1\}$. Here, the LCM is taken over all $Q(\beta)$-primes $\mathfrak{p}$ lying above p and $f(\mathfrak{p})$ denotes the residue degree of $\mathfrak{p}$ in $Q(\beta)/Q$. More generally, for any modulus N with $(a_0, N) = 1$,

$$\pi(N) = \underset{p^\nu \| N}{\mathrm{LCM}}\, \pi(p^\nu), \tag{19}$$

where p ranges over the distinct prime divisors of N.

For a numerical illustration, consider the polynomial $p(x) = x^3 - x - 1$ of discriminant $\Delta = -23$. The sequence U satisfies $U_{n+3} = U_{n+1} + U_n$. The first 29 terms starting with $n = 0$ are

$$0, 0, 1, 0, 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37,$$
$$49, 65, 86, 114, 151, 200, 265, 351, 465, 616, \dots.$$

The values $\omega(N)$ and $\pi(N)$, and the set B_N, are tabulated below for $N = 2, 3, 4, 7$.

N	$\omega(N)$	$\pi(N)$	B_N
2	7	7	$\{1\}$
3	13	13	$\{1\}$
4	14	14	$\{1\}$
7	16	48	$\{2, 4, 1\}$

Let us now turn to the companion sequence V in (12), demonstrating certain identities relating V with U, including one which is the analog of (7).

Proposition 5. *The sequences U and V satisfy the following identities*:

$$U_n U_k \Delta = \begin{vmatrix} V_{n+k} & V_{n+m-2} & \cdots & V_n \\ V_{k+m-2} & V_{2m-4} & \cdots & V_{m-2} \\ \vdots & \vdots & & \vdots \\ V_k & V_{m-2} & \cdots & V_0 \end{vmatrix} \qquad (n, k \ge 0), \tag{20}$$

$$U_n = \sum_{k=1}^{m} b_k V_{n+k-1} \qquad (n \geq 0), \tag{21}$$

where

$$b_{m-k+1} = \frac{(-1)^{k-1}}{\Delta} \begin{vmatrix} V_{2m-3} & V_{2m-4} & \cdots & V_{2m-(k+2)} & V_{2m-(k+4)} & \cdots & V_{m-2} \\ V_{2m-4} & V_{2m-5} & \cdots & V_{2m-(k+3)} & V_{2m-(k+5)} & \cdots & V_{m-3} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ V_{m-1} & V_{m-2} & \cdots & V_{m-k} & V_{m-(k+2)} & \cdots & V_0 \end{vmatrix}$$
$$(1 \leq k \leq m),$$

and

$$V_n = \sum_{k=1}^{m} k a_k U_{n+k-1} \qquad (n \geq 0). \tag{22}$$

Proof. To establish (20), consider the product

$$\begin{vmatrix} \beta_1^n & \cdots & \beta_m^n \\ \beta_1^{m-2} & \cdots & \beta_m^{m-2} \\ \vdots & & \vdots \\ 1 & & 1 \end{vmatrix} \cdot \begin{vmatrix} \beta_1^k & \beta_1^{m-2} & \cdots & 1 \\ \beta_2^k & \beta_2^{m-2} & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ \beta_m^k & \beta_m^{m-2} & \cdots & 1 \end{vmatrix}$$
$$= \begin{vmatrix} V_{n+k} & V_{n+m-2} & \cdots & V_n \\ V_{k+m-2} & V_{2m-4} & \cdots & V_{m-2} \\ \vdots & \vdots & & \vdots \\ V_k & V_{m-2} & \cdots & V_0 \end{vmatrix}.$$

Since

$$\Delta = \begin{vmatrix} \beta_1^{m-1} & \cdots & \beta_m^{m-1} \\ \beta_1^{m-2} & \cdots & \beta_m^{m-2} \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{vmatrix}^2,$$

it follows from (11) that the right-hand side of (20) is $U_n U_k \Delta$. Now observe that (21) is just (20) with $k = m - 1$, where the right-hand determinant has been expanded by minors using the top row.

It remains to verify (22), but since U and V satisfy the same recursion (14), it is enough to check the identity for $0 \leq n \leq m - 1$. Replacing k by $m-k+1$ in the right-hand side of (22) and then re-indexing yields an equivalent expression

$$\sum_{k=0}^{m-1} (m-k) a_{m-k} U_{n+m-k-1} \qquad (n \geq 0).$$

From Newton's identities [7], each term $(m-k)a_{m-k}$ may be replaced by the sum $\sum_{j=0}^{k} a_{m-k+j} V_j$ $(0 \le k \le m-1)$ to yield

$$\sum_{k=0}^{m-1} \left(\sum_{j=0}^{k} a_{m-k+j} V_j U_{n+m-k-1} \right),$$

or equivalently,

$$\sum_{j=0}^{m-1} V_j \left(\sum_{k=j}^{m-1} a_{m-k+j} U_{n+m-k-1} \right) \tag{23}$$

upon changing the order of summation. I claim that the inner sum, for $0 \le n \le m-1$, is just the delta function δ_{jn} ($\delta_{jn} = 0$ for $j \ne n$ and 1 when $j = n$), so that (23) evaluates to V_n for $0 \le n \le m-1$, thereby proving (22). To verify the assertion, I consider the cases $j \ge n$ and $j < n$ separately.

Case (i): $j \ge n$. Here, direct evaluation yields $\sum_{k=j}^{m-1} a_{m-k+j} U_{n+m-k-1} = 0$ if $j > n$ or $a_m U_{m-1} = 1$ if $j = n$.

Case (ii): $j < n$. Here, one can enlarge the sum $\sum_{k=j}^{m-1} a_{m-k+j} U_{n+m-k-1}$ to $\sum_{k=j}^{m+j-1} a_{m-k+j} U_{n+m-k-1}$, since all additional terms $a_{m-k+j} U_{n+m-k-1}$ are zero. (Note that $m \le k \le m+j-1$ implies $0 < n-j \le n+m-k-1 \le n-1 < m-1$ here.) But since U satisfies (14), the padded sum, as well as the original, are both zero. □

Remark. Identity (20) generalizes the Lucas identity (7), but there seems to be no analog of (8) for higher-order sequences.

The question naturally arises as to when V, or for that matter, any integer-valued sequence W satisfying (14) has the same period as U modulo N. This situation is governed by the following theorem.

Theorem 1. *Suppose W is an integer-valued sequence satisfying* (14). *For any N relatively prime to a_0 and any $k > 0$,*

$$W_{k\omega+r} \equiv U_{k\omega+m-1} W_r \pmod{N} \quad (r \ge 0). \tag{24}$$

Moreover, if also $(N, \det(W)) = 1$, then W has the same period $\pi(N)$ as U modulo N. (Here, $\omega = \omega(N)$ is the rank of apparition of N for the sequence U.)

Proof. For any fixed $k \ge 0$, to demonstrate (24), it is enough to verify that it holds for $0 \le r \le m-1$, since $(W_{k\omega+r})$ and (W_r) both satisfy (14). Observe that this is automatically true when $W = U$ from the definition of $\omega(N)$. Thus, the matrix $C = A^{k\omega}$ satisfies

$$C \begin{bmatrix} U_0 \\ \vdots \\ U_{m-1} \end{bmatrix} \equiv U_{k\omega+m-1} \begin{bmatrix} U_0 \\ \vdots \\ U_{m-1} \end{bmatrix} \pmod{N}. \tag{25}$$

But $C = U_{k\omega+m-1} \cdot I_m$ also satisfies (25), so by Proposition 2, $A^{k\omega} \equiv U_{k\omega+m-1} I_m \pmod{N}$. Thus,

$$A^{k\omega} \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \equiv U_{k\omega+m-1} \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \quad (\text{mod } N),$$

or equivalently, (24) holds for $0 \le r \le m-1$.

Incidentally, the congruence (24) readily implies that the period $\pi_W(N)$ of W modulo N divides $\pi(N)$. Now suppose that N is prime to $\det(W)$, too. Since

$$A^{\pi_W(N)} \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \equiv \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \quad (\text{mod } N),$$

it follows from Proposition 2 that $A^{\pi_W(N)} \equiv I_m \pmod{N}$. But then, $U_{\pi_W(N)+r} \equiv U_r \pmod{N}$ for $0 \le r \le m-1$, so $\pi(N)$ divides $\pi_W(N)$. Thus $\pi_W(N) = \pi(N)$. The proof of the theorem is now complete. □

4. Pseudoprimes for the sequences U and V

In this section I shall characterize pseudoprimes for higher-order linear recurrence sequences. It is convenient to consider the sequence V first; so again, let

$$p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

be irreducible in $Z[x]$, as in the previous section, with discriminant Δ. (The coefficients a_i may be rational but are chosen here to be integral to simplify the exposition.) Denote the splitting field of $p(x)$ by L and its Galois group by $G = G(L/Q)$. Let $\Delta(L)$ be the discriminant of L/Q. For $\sigma \in G$, set

$$(26) \qquad V_{\sigma,r} = \sum_{i=1}^{m} \sigma(\beta_i)\beta_i^r \qquad (0 \le r \le m-1).$$

If p is a prime not dividing $a_0\Delta \cdot \Delta(L)$, then the m consecutive terms $V_p, \ldots, V_{p+m-1}$ satisfy

$$(27) \qquad V_{p+r} \equiv V_{\sigma,r} \quad (\text{mod } \tilde{\mathfrak{p}}) \qquad (0 \le r \le m-1)$$

for any L-prime $\tilde{\mathfrak{p}}$ lying above p with Frobenius symbol $((L/Q)/\tilde{\mathfrak{p}}) = \sigma$. This fact easily follows from the definition of the Frobenius symbol, since, in particular,

$$(28) \qquad \beta_i^p \equiv \sigma(\beta_i) \quad (\text{mod } \tilde{\mathfrak{p}}) \qquad (1 \le i \le m).$$

The congruence (27) actually holds in k_σ, the subfield of L fixed by the centralizer $Z_G(\sigma)$ of σ in G, since the values $V_{\sigma,r}$ are seen to lie in k_σ.

There is an equivalent way to express (27) in terms of certain matrices C_σ in $M_A(k_\sigma)$ $(\sigma \in G)$. For $\sigma \in G$, let $x_\sigma = (x_1, \dots, x_m)$ be the unique solution of the linear system

$$\sum_{j=1}^{m} x_j \beta_i^{j-1} = \sigma(\beta_i) \qquad (1 \le i \le m). \tag{29}$$

(Here $\Delta \neq 0$, so one may use Cramer's rule to find that the values Δx_j $(1 \le j \le m)$ are integral in L.) Applying any τ in $Z_G(\sigma)$ to both sides of (29) yields

$$\sum_{j=1}^{m} \tau(x_j)(\tau(\beta_i))^{j-1} = \tau\sigma\tau^{-1}(\tau(\beta_i)) = \sigma(\tau(\beta_i)) \qquad (1 \le i \le m),$$

which shows that $\tau(x_\sigma)$ also solves (29). Since (29) has a unique solution, $\tau(x_\sigma) = x_\sigma$; thus x_σ is fixed by $Z_G(\sigma)$ and the x_j lie in k_σ. Now set

$$C_\sigma = M_{x_\sigma} \quad \text{for } \sigma \in G. \tag{30}$$

Observe that, from (29),

$$C_\sigma \begin{bmatrix} 1 \\ \beta_i \\ \vdots \\ \beta_i^{m-1} \end{bmatrix} = \sigma(\beta_i) \begin{bmatrix} 1 \\ \beta_i \\ \vdots \\ \beta_i^{m-1} \end{bmatrix} \qquad (1 \le i \le m), \tag{31}$$

so that

$$C_\sigma \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_{m-1} \end{bmatrix} = \begin{bmatrix} V_{\sigma,0} \\ V_{\sigma,1} \\ \vdots \\ V_{\sigma,m-1} \end{bmatrix}. \tag{32}$$

It is also clear from (29) or (31) that the C_σ $(\sigma \in G)$ are mutually distinct, and that

$$\rho(C_\sigma) = C_{\rho\sigma\rho^{-1}} \quad \text{for any } \sigma, \rho \in G. \tag{33}$$

Now since

$$A^p \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_{m-1} \end{bmatrix} = \begin{bmatrix} V_p \\ V_{p+1} \\ \vdots \\ V_{p+m-1} \end{bmatrix},$$

it follows from Proposition 2 that (27) is equivalent to the congruence

$$A^p \equiv C_\sigma \pmod{\mathfrak{p}}, \tag{34}$$

where $\mathfrak{p}$ is the k_σ-prime lying between p and $\tilde{\mathfrak{p}}$.

Before introducing the pseudoprimes for the sequence V, I first specify certain sequence signatures. The m-term sequence $V_{\sigma,r}$ $(0 \le r \le m-1)$ in (26) shall be referred to as an admissible signature for V corresponding to σ. (Actually, r need only run over any fixed set of m consecutive integers in (26) and (27), but I have chosen $0, 1, \ldots, m-1$ for the sake of simplicity. I relax this requirement later in some of the examples.) The comment concerning congruence (27) prompts the following definition. Let N be any composite with $(N, 2a_0\Delta) = 1$. Call N a pseudoprime with respect to V, denoted psp_V, if the terms $V_N, V_{N+1}, \ldots, V_{N+m-1}$ match some admissible signature for V modulo $\tilde{\mathfrak{n}}$ for some L-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap \mathbf{Z} = (N)$. Equivalently, N is a psp_V if

$$V_{N+r} \equiv V_{\sigma, r} \pmod{\mathfrak{n}} \qquad (0 \le r \le m-1) \tag{35}$$

for some $\sigma \in G$ and k_σ-ideal $\mathfrak{n}$ satisfying $\mathfrak{n} \cap \mathbf{Z} = (N)$. If N satisfies (35), one says N is a psp_V of type $C(\sigma)$, where $C(\sigma)$ denotes the conjugacy class of G that contains σ. Observe that if (35) holds, then for any $\rho \in G$,

$$V_{N+r} \equiv V_{\rho\sigma\rho^{-1}, r} \pmod{\rho(\mathfrak{n})} \qquad (0 \le r \le m-1),$$

where $\rho(\mathfrak{n})$ is an ideal of $k_{\rho\sigma\rho^{-1}} = \rho(k_\sigma)$.

That (35) has equivalents analogous to (28) and (34) is the key in this study of pseudoprimes.

Theorem 2. *A composite N with $(N, 2a_0\Delta) = 1$ satisfies (35) if and only if*

$$A^N \equiv C_\sigma \pmod{\mathfrak{n}} \tag{36}$$

if and only if

$$\beta_i^N \equiv \sigma(\beta_i) \pmod{\tilde{\mathfrak{n}}} \qquad (1 \le i \le m) \tag{37}$$

for any L-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap k_\sigma = \mathfrak{n}$.

Proof. I will show that (37) → (35) → (36) → (37) to prove the theorem.

(37) → (35): This direction is immediate from (26).

(35) → (36): If (35) holds, then A^N satisfies

$$A^N \begin{bmatrix} V_0 \\ \vdots \\ V_{m-1} \end{bmatrix} \equiv \begin{bmatrix} V_{\sigma,0} \\ \vdots \\ V_{\sigma,m-1} \end{bmatrix} \quad \pmod{\mathfrak{n}} \text{ in } k_\sigma .$$

Since N is prime to $\det(V) = \Delta$, it follows from Proposition 2 that $A^N \equiv C_\sigma \pmod{\mathfrak{n}}$.

(36) → (37): If $A^N \equiv C_\sigma \pmod{\mathfrak{n}}$, then from (31)

$$A^N \begin{bmatrix} 1 \\ \beta_i \\ \vdots \\ \beta_i^{m-1} \end{bmatrix} = \beta_i^N \begin{bmatrix} 1 \\ \beta_i \\ \vdots \\ \beta_i^{m-1} \end{bmatrix} \equiv \sigma(\beta_i) \begin{bmatrix} 1 \\ \beta_i \\ \vdots \\ \beta_i^{m-1} \end{bmatrix} \pmod{\tilde{\mathfrak{n}}} \qquad (1 \le i \le m)$$

for any L-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap k_\sigma = \mathfrak{n}$. In particular, the congruences (37) hold modulo any such L-ideal $\tilde{\mathfrak{n}}$. □

Theorem 2 has several interesting consequences which will be developed in the remainder of this section. Among the more obvious ones is the following.

Corollary 1. *Any* $\mathrm{psp}_V\, N$ *is a* psp_{a_0}.

Proof. Suppose N is a psp_V of type $C(\sigma)$. Then from Theorem 2,

$$\beta_i^N \equiv \sigma(\beta_i) \pmod{\tilde{\mathfrak{n}}} \qquad (1 \le i \le m)$$

for some L-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap \mathbf{Z} = (N)$. Thus, $((-1)^m a_0)^N \equiv (-1)^m a_0 \pmod{N}$. Since N is odd, $a_0^N \equiv a_0 \pmod{N}$. □

This is an apt time to remark about the distribution of pseudoprimes with respect to V. Let $\pi(x, V)$ count the number of psp_V's less than or equal to x. In view of Corollary 1 one immediately gets an upper bound for $\pi(x, V)$ from (1).

Corollary 2. $\pi(x, V) < x\exp\{-\log x \log\log\log x/2\log\log x\}$ *for all sufficiently large* x, *if* $|a_0| \neq 1$.

Virtually nothing else is known about the distribution of the psp_V's when $m > 2$. It is not even known whether there is such a sequence V for which $\pi(x, V) \to \infty$ as $x \to \infty$. (I exclude here certain degenerate sequences which arise when β is a multiple of a root of unity ζ, say $\beta = t\zeta$, with t in Z, or even t a real quadratic unit; cf. [16].) More intriguing is to determine precisely what role the Galois group G plays. One naturally expects pseudoprimes will be rarer when G is larger. But for sequences of identical order m, each with Galois group of order m, how does the structure of G influence the distribution of pseudoprimes, if at all? I give some examples next that demonstrate that pseudoprimes for higher-order sequences are indeed very rare. Unfortunately, the search range (up to 2^{31}) is too narrow, and the examples too few, to shed any light concerning the questions just raised. More comprehensive testing is planned, and the findings will be reported at a later date.

I first ought to mention that for a given $\sigma \in G$, there may be composites N which are psp_V's of type $C(\sigma)$ for any sequence V in (12) that is defined in terms of the minimal polynomial $p(x)$ for some integral element β in L, $(a_0\Delta(p(x)), N) = 1$, which generates L. Such composites, when they exist, will be called L-Carmichael numbers. In view of Theorem 2, I formally define L-Carmichael numbers as follows:

A composite N, $(N, \Delta(L)) = 1$, is said to be an L-Carmichael number of type $C(\sigma)$ if for all $\beta \in L$, $(\beta, N) = 1$ and β integral,

$$\beta^N \equiv \sigma(\beta) \pmod{\tilde{\mathfrak{n}}} \tag{38}$$

for some L-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap \mathbf{Z} = (N)$.

The smallest example is $561 = 3 \cdot 11 \cdot 17$, which is easily seen to be a $Q(\sqrt{-13})$-Carmichael number of type $C(1)$.

Since an L-Carmichael number is clearly a Q-Carmichael or ordinary Carmichael number, it follows [6] that any L-Carmichael number N is odd and square-free. An equivalent characterization for L-Carmichael numbers is given next.

For any prime $p \nmid \Delta(L)$, let $((L/Q)/p)$ denote the Artin class of p in L/Q and $f(p)$ the residue degree of p in L/Q. Given a conjugacy class C of G and any integer $\nu > 0$, let C^ν be the conjugacy class consisting of the νth powers of elements in C.

Proposition 6. *Let N be an odd, square-free composite relatively prime to $\Delta(L)$, and $\sigma \in G$ be of order f. Then N is an L-Carmichael number of type $C(\sigma)$ if and only if for all primes $p|N$ there is an integer $\nu(p)$, $0 \le \nu(p) < f(p)$, such that*

$$(39) \qquad C(\sigma) \subseteq \left(\frac{L/Q}{p}\right)^{\nu(p)} \quad \textit{and} \quad N - p^{\nu(p)} \equiv 0 \pmod{p^{f(p)} - 1}.$$

Proof. ($\leftarrow$) Let p be any prime dividing N. If (39) holds, then there is an L-prime $\mathfrak{P}_p$ lying above p with $((L/Q)/\mathfrak{P}_p)^{\nu(p)} = \sigma$. In particular, for any integral β in L, $(\beta, N) = 1$,

$$(40) \qquad \beta^N \equiv \beta^{p^{\nu(p)}} \equiv \sigma(\beta) \pmod{\mathfrak{P}_p},$$

since $N - p^{\nu(p)} \equiv 0 \pmod{p^{f(p)} - 1}$. Thus, if $\mathfrak{n} = \prod_{p|N} \mathfrak{P}_p$, then $\beta^N \equiv \sigma(\beta) \pmod{\mathfrak{n}}$. Since $\mathfrak{n} \cap \mathbf{Z} = (N)$, one finds that N is an L-Carmichael number of type $C(\sigma)$.

($\rightarrow$) Suppose N is an L-Carmichael number of type $C(\sigma)$ satisfying (38) for some L-ideal $\mathfrak{n}$, and p a prime dividing N. Let $\mathfrak{P}$ be an L-prime lying above p which divides $\mathfrak{n}$. Since (38) implies that the map $z \rightarrow z^N$ is an automorphism for the finite field of $p^{f(p)}$ elements, it follows that $N \equiv p^{\nu(p)} \pmod{p^{f(p)} - 1}$ for some integer $0 \le \nu(p) < f(p)$. In particular, $((L/Q)/\mathfrak{P})^{\nu(p)} = \sigma$, again from (38). □

For the case of a quadratic field L one immediately has

Corollary 3. *Let L be a quadratic field and $N > 1$ be odd, square-free, and prime to $\Delta(L)$. Then*

(i) *N is an L-Carmichael number of type $\sigma = 1$ if and only if $p^2 - 1 | N - 1$ for each inert $p|N$ and $p - 1 | N - 1$ for each $p|N$ which splits in L;*

(ii) *N is an L-Carmichael number of type $\sigma \ne 1$ if and only if each $p|N$ is inert and $p^2 - 1 | N - p$.*

Using Corollary 3, it is easily checked that $7{,}045{,}248{,}121 = 821 \cdot 1231 \cdot 6971$ and $24{,}306{,}384{,}961 = 19 \cdot 53 \cdot 79 \cdot 89 \cdot 3433$ are $Q(\sqrt{-23})$-Carmichael numbers of type $C(1)$.

One also has the following lower bound on the number of prime factors of L-Carmichael numbers.

Corollary 4. *Suppose N is an L-Carmichael number of type $C(\sigma)$, where* $\operatorname{ord}_G \sigma = f$. *Then N has at least $f + 2$ prime factors.*

Proof. For each prime $p|N$, one has from Proposition 6 that $N \equiv p^{\nu(p)} \pmod{p^{f(p)} - 1}$ with $0 \leq \nu(p) < f(p)$ and $((L/Q)/\mathfrak{P})^{\nu(p)} = \sigma$ for some L-prime $\mathfrak{P}$ lying above p. In fact, $f(p) = f\cdot(\nu(p), f(p))$. Set $\delta = \max\{\nu(p), 1\}$. Then $N/p \equiv p^{\delta-1} \pmod{p^f - 1}$, since, if $\nu(p) = 0$, then $f = 1$ and already $N/p \equiv 1 \pmod{p-1}$. In particular, since $(N/p, p) = 1$, one has $N/p \geq p^{\delta-1} + p^f - 1$ or $N/p > p^f$. Taking the product over all prime divisors of N, one finds $N^{g-1} > N^f$, where g is the number of prime divisors of N. Thus $g > f + 1$. □

Very little is known concerning the distribution of ordinary Carmichael numbers, much less L-Carmichael numbers. For a given normal extension L and conjugacy class C of $G(L/Q)$, it is not even known whether there exists an L-Carmichael number of type C. From the remark preceding Proposition 6, an affirmative answer here would immediately imply that there are infinitely many ordinary Carmichael numbers.

Example 1. Consider $p(x) = x^3 - x - 1$ with roots β_1, β_2, and β_3. Here, $L = Q(\beta_1, \sqrt{-23})$ with $G = S_3$, say, generated by the automorphisms σ and τ induced by mappings:

$$\sigma\colon \begin{array}{l} \beta_1 \to \beta_2 \\ \beta_2 \to \beta_3 \\ \beta_3 \to \beta_1 \end{array} \qquad \tau\colon \begin{array}{l} \beta_1 \to \beta_1 \\ \beta_2 \to \beta_3 \\ \beta_3 \to \beta_2 \end{array}$$

The admissible signatures for the sequence $V_n = \beta_1^n + \beta_2^n + \beta_3^n$ $(n \geq 0)$ with fixed choice $r = -1, 0, 1$ are as follows:

r	$V_{1,r}$	$V_{\sigma,r}$	$V_{\sigma^2,r}$	$V_{\tau,r}$	$V_{\tau\sigma,r}$	$V_{\tau\sigma^2,r}$
-1	3	α	$\overline{\alpha}$	β_1	β_2	β_3
0	0	0	0	0	0	0
1	2	-1	-1	$3\beta_1^2 - 2$	$3\beta_2^2 - 2$	$3\beta_3^2 - 2$

Here, α and $\overline{\alpha}$ are conjugate roots of $x^2 - 3x + 8$. The characterization of pseudoprimes for V in terms of the sequence signatures above can be checked using integer arithmetic modulo N, and is equivalent to that given by Adams and Shanks [1]. Kurtz, Shanks, and Williams [11] showed that $\pi(2^{31}, V) = 10$ and $\pi(50 \times 10^9, V) = 55$.

Example 2. Consider $p(x) = x^6 + x^5 + 3x^4 + 11x^3 + 44x^2 + 36x + 32$, which has a root $\beta_1 = \zeta_{31} + \zeta_{31}^2 + \zeta_{31}^4 + \zeta_{31}^8 + \zeta_{31}^{16}$. Here, $L = Q(\beta_1)$ is the unique cyclic field of degree six and conductor 31, so $G = Z_6$ is generated by the automorphism σ which is induced by the mapping $\zeta_{31} \to \zeta_{31}^3$. The admissible signatures for the corresponding sequence V for the fixed choice $r = -2, -1, 0, 1, 2, 3$ are as follows:

r	$V_{1,r}$	$V_{\sigma,r}$	$V_{\sigma^2,r}$	$V_{\sigma^3,r}$	$V_{\sigma^4,r}$	$V_{\sigma^5,r}$
-2	$-9/8$	$83/64$	$145/64$	$114/64$	$238/64$	$-413/64$
-1	6	$17/8$	$-45/8$	$-7/4$	$-7/4$	$17/8$
0	-1	-1	-1	-1	-1	-1
1	-5	-5	-5	26	-5	-5
2	-25	-25	-25	6	37	37
3	-125	61	61	-32	-1	61

Since G is Abelian, each term $V_{\rho,r}$ $(\rho \in G,\ -2 \le r \le 3)$ lies in Q. Up to 2^{31}, there are only two psp_V's; namely $775{,}368{,}901 = 373 \cdot 1117 \cdot 1861$ and $955{,}134{,}181 = 311 \cdot 1303 \cdot 2357$, both L-Carmichael of type $C(1)$.

Example 3. Next consider $p(x) = x^6 - (49/36)x^4 - (143/216)x^3 + x^2 + (11/6)x + 1$ with roots so ordered that its Galois group $G = S_3$ is generated by the permutations $\sigma = (123)(456)$ and $\tau = (14)(26)(35)$ as a subgroup of S_6. The admissible signatures for the corresponding sequence V with fixed choice $r = -2, -1, 0, 1, 2, 3$ are as follows:

r	$V_{1,r}$	$V_{\sigma,r}$	$V_{\sigma^2,r}$	$V_{\tau,r}$	$V_{\tau\sigma,r}$	$V_{\tau\sigma^2,r}$
-2	$-\frac{11}{6}$	$11(\alpha-1)/6$	$11(\overline{\alpha}-1)/6$	$\frac{143}{216}(3\gamma_1^2-\gamma_1-2)$	$\frac{143}{216}(3\gamma_2^2-\gamma_2-2)$	$\frac{143}{216}(3\gamma_3^2-\gamma_3-2)$
-1	6	2α	$2\overline{\alpha}$	$49\gamma_1/36$	$49\gamma_2/36$	$49\gamma_3/36$
0	0	0	0	0	0	0
1	$\frac{49}{18}$	$-\frac{49}{36}$	$-\frac{49}{36}$	$2(3\gamma_1^2-2)$	$2(3\gamma_2^2-2)$	$2(3\gamma_3^2-2)$
2	$\frac{143}{72}$	$143\alpha/216$	$143\overline{\alpha}/216$	$11\gamma_1/6$	$11\gamma_2/6$	$11\gamma_3/6$
3	$-\frac{191}{648}$	$\frac{191}{1296}$	$\frac{191}{1296}$	$\frac{49}{36}(3\gamma_1^2-2)$	$\frac{49}{36}(3\gamma_2^2-2)$	$\frac{49}{36}(3\gamma_3^2-2)$

where α, $\overline{\alpha}$ satisfy $x^2 - 3x + 8 = 0$ and γ_1, γ_2, and γ_3 satisfy $x^3 - x - 1 = 0$. There are only two psp_V's $< 2^{31}$, namely, $517{,}697{,}641 = 6311 \cdot 82031$ and $855{,}073{,}301 = 16883 \cdot 50647$, both of type $C(1)$.

Example 4. Consider $p(x) = x^4 - 8x + 4$ with Galois group S_4, splitting field L and roots

$$\begin{aligned}
\beta_1 &= \alpha_1^{1/2} + \alpha_2^{1/2} + \alpha_3^{1/2}, \\
\beta_2 &= \alpha_1^{1/2} - \alpha_2^{1/2} - \alpha_3^{1/2}, \\
\beta_3 &= -\alpha_1^{1/2} - \alpha_2^{1/2} + \alpha_3^{1/2}, \\
\beta_4 &= -\alpha_1^{1/2} + \alpha_2^{1/2} - \alpha_3^{1/2},
\end{aligned}$$

where the α_i satisfy $x^3 - x - 1 = 0$. The automorphisms of L corresponding to the permutations $\rho = (12)(34)$ and $\tau = (13)(24)$ generate the Klein subgroup H of S_4 with fixed field $Q(\alpha_1, \sqrt{-23})$. The admissible signatures for the sequence $V_n = \beta_1^n + \beta_2^n + \beta_3^n + \beta_4^n$ $(n > 0)$, of type $C(\sigma)$ for $\sigma \in H$, with fixed choice $r = -1, 0, 1, 2$ are:

r	$V_{1,r}$	$V_{\rho,r}$	$V_{\rho\tau,r}$	$V_{\tau,r}$
-1	4	$4/\alpha_1$	$4/\alpha_2$	$4/\alpha_3$
0	0	0	0	0
1	0	$8\alpha_1$	$8\alpha_2$	$8\alpha_3$
2	24	-8	-8	-8

One such pseudoprime for V is $970,355,431 = 22027 \cdot 44053$ of type $C(1)$. I have not computed the psp_V's up to 2^{31}, but this may be the only one.

So far, I have defined pseudoprimes with respect to the sequence V. Let us consider now any integer-valued sequence $W = (W_n)$ satisfying the same recurrence as V. It follows from (28) and the argument of Theorem 2 that if p is a prime not dividing $2a_0\Delta \cdot \Delta(L)$, then $A^p \equiv C_\sigma \pmod{\tilde{\mathfrak{P}}}$, where $\tilde{\mathfrak{P}}$ is any L-prime above p and $((L/Q)/\tilde{\mathfrak{P}}) = \sigma$. In particular,

$$W_{N+r} \equiv W_{\sigma,r} \pmod{\tilde{\mathfrak{P}}} \qquad (0 \le r \le m-1), \tag{41}$$

where

$$\begin{bmatrix} W_{\sigma,0} \\ \vdots \\ W_{\sigma,m-1} \end{bmatrix} = C_\sigma \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix}. \tag{42}$$

The sequence $W_{\sigma,r}$ $(0 \le r \le m-1)$ is the analogous admissible signature for W corresponding to σ. The values $W_{\sigma,r}$ lie in k_σ, so (41) actually holds in k_σ as before. A composite N with $(N, 2a_0\Delta) = 1$ is called a pseudoprime with respect to W (or psp_W) of type $C(\sigma)$ if

$$W_{N+r} \equiv W_{\sigma,r} \pmod{\mathfrak{n}} \qquad (0 \le r \le m-1) \tag{43}$$

for some k_σ-ideal $\mathfrak{n}$ satisfying $\mathfrak{n} \cap \mathbf{Z} = (N)$. For the sequence U, the admissible sequence signatures are given by

$$U_{\sigma,r} = \sum_{j=1}^{m} \frac{\sigma(\beta_j)\beta_j^r}{p'(\beta_j)}, \tag{44}$$

where $p'(x)$ denotes the derivative of $p(x)$.

Whether one characterizes pseudoprimes using the sequences U or V, the notions turn out to be equivalent. More generally one has

Theorem 3. *Suppose $W = (W_n)$ is an integer sequence satisfying* (14). *For N with $(N, 2a_0\Delta\det(W)) = 1$, N is a psp_W of type $C(\sigma)$ if and only if N is a psp_V of type $C(\sigma)$.*

Proof. Now N is a psp_W of type $C(\sigma)$ if and only if

$$A^N \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \equiv \begin{bmatrix} W_{\sigma,0} \\ \vdots \\ W_{\sigma,m-1} \end{bmatrix} \pmod{\mathfrak{n}} \tag{45}$$

for some k_σ-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$. Since N is prime to $a_0 \Delta \det(W)$, one finds from (42) and Proposition 2 that (45) is equivalent to

$$A^N \equiv C_\sigma \pmod{\mathfrak{n}}. \tag{46}$$

But from the argument of Theorem 2, (46) holds if and only if N is a psp_V of type $C(\sigma)$. □

5. Stronger pseudoprimes associated with resolvent sequences

Let $L/k/Q$ be any normal tower of finite extensions with Galois groups $\Gamma = G(L/Q)$ and $H = G(L/k)$. Suppose χ is a linear character of H of order $s > 1$ and K/k the cyclic subextension of L/k fixed by annihilator $\text{Ann}(\chi)$. Fix a primitive s-root of unity ζ. I shall assume that $L \cap Q(\zeta) = Q$, so that $\Omega = G(L(\zeta)/Q)$ consists precisely of the maps $\phi_{\rho,e}$ for $\rho \in \Gamma$ and $1 \le e \le s$, $(e, s) = 1$, given by

$$\phi_{\rho,e}|_L = \rho \quad \text{and} \quad \phi_{\rho,e}(\zeta) = \zeta^e.$$

Fix an element σ in the group H whose restriction to K generates $G(K/k) = H/\text{Ann}(\chi)$. To each ψ in H define a function $\lambda = \lambda_\psi$ on Γ by

$$\rho\psi\rho^{-1}(\text{Ann}\,\chi) = \sigma^{\lambda(\rho)}(\text{Ann}\,\chi) \quad \text{in } H/\text{Ann}(\chi) \tag{47}$$

with $0 \le \lambda(\rho) < s$. This map is well defined, since $H \trianglelefteq \Gamma$. The function λ is constant on the cosets of H in Γ.

Now fix a generator θ for K/k and form the Lagrange resolvents

$$\begin{aligned} \omega_{\rho,\nu} = \omega_{\rho,\nu}(\theta) = \rho(\theta) + \zeta^{-\nu}\rho\sigma\rho^{-1}(\rho(\theta)) \\ + \cdots + \zeta^{-(s-1)\nu}\rho\sigma^{s-1}\rho^{-1}(\rho(\theta)) \end{aligned} \tag{48}$$

for integers $\nu > 0$ and $\rho \in \Gamma$. As demonstrated in [10], one may, and I will, assume that the generator θ for K/k is chosen so that each of the Lagrange resolvents $\omega_{\rho,\nu} \neq 0$ for $(\nu, s) = 1$ and $\rho \in \Gamma$. For the sake of simplicity, θ will be taken to be integral here. Since $L \cap Q(\zeta) = Q$, these Lagrange resolvents (48) satisfy for any ρ, τ in Γ

$$\phi_{\tau,e}(\omega_{\rho,\nu}) = \omega_{\tau\rho,\nu e}. \tag{49}$$

Also,

$$\omega_{\rho,\nu}(\sigma^e(\theta)) = \zeta^{\nu e}\omega_{\rho,\nu}(\theta) \tag{50}$$

and

$$\rho(\sigma^e(\theta)) = \frac{1}{\phi(s)} \sum_{\nu}{}' \zeta^{\nu e} \omega_{\rho,\nu}(\theta) \tag{51}$$

for $\rho \in \Gamma$ and any integer e, where the primed sum is over a complete system of reduced residues modulo s. To establish (51), just note, since $L \cap Q(\zeta) = Q$ and

$$\sigma^e(\theta) = \frac{1}{\phi(s)} \sum_{\nu}{}' \zeta^{\nu e} \omega_{1,\nu}, \tag{52}$$

that

$$\rho(\sigma^e(\theta)) = \frac{1}{\phi(s)} \sum_{\nu}{}' \zeta^{\nu e} \phi_{\rho,e}(\omega_{1,\nu}) = \frac{1}{\phi(s)} \sum_{\nu}{}' \zeta^{\nu e} \omega_{\rho,\nu}$$

from (49).

Additional, deeper properties will be needed in characterizing the pseudoprimes. To begin, set for each $\nu \geq 0$ and $\rho \in \Gamma$,

$$\beta_\rho(\nu) = (\omega_{\rho,\nu})^s \quad \text{and} \quad \gamma_{\rho,r}(\nu) = \omega_{\rho,\nu r}/(\omega_{\rho,\nu})^r \tag{53}$$

when $(r, s) = 1$.

Proposition 7. *For fixed ν and any $\tau \in H$ and $\rho \in \Gamma$,*

$$\omega_{\rho\tau,\nu} = \zeta^{\nu\lambda} \omega_{\rho,\nu} \quad \textit{if } \tau = \sigma^\lambda \tau' \textit{ with } \tau' \in \operatorname{Ann} \chi. \tag{54}$$

In particular,

$$\omega_{\rho\tau,\nu} = \omega_{\rho,\nu} \quad \textit{if } \tau \in \operatorname{Ann} \chi, \tag{55}$$

$$\beta_{\rho\tau}(\nu) = \beta_\rho(\nu) \quad \textit{if } \tau \in H, \tag{56}$$

$$\gamma_{\rho\tau,r}(\nu) = \gamma_{\rho,r}(\nu) \quad \textit{if } \tau \in H. \tag{57}$$

Proof. To establish (54), observe that

$$\begin{aligned}\omega_{\rho\tau,\nu} &= \rho\tau(\theta) + \zeta^{-\nu} \rho\tau\sigma(\theta) + \cdots + \zeta^{-\nu(s-1)} \rho\tau\sigma^{s-1}(\theta) \\ &= \rho\sigma^\lambda(\theta) + \zeta^{-\nu} \rho\sigma^{\lambda+1}(\theta) + \cdots + \zeta^{-\nu(s-1)} \rho\sigma^{\lambda+s-1}(\theta),\end{aligned}$$

since $\operatorname{Ann}(\chi)$ fixes θ. The last expression is just $\omega_{\rho,\nu}(\sigma^\lambda(\theta))$, or $\zeta^{\nu\lambda}\omega_{\rho,\nu}(\theta)$ by (50). This yields (54). Formulas (55)–(57) now follow. □

It is evident from (49) that the $\beta_\rho(\nu)$ are mutually conjugate over Q in $L(\zeta)$, in fact, in $k(\zeta)$ by (56). If m is the number of distinct conjugates, then the $\beta_\rho(\nu)$ are roots of a minimal polynomial

$$p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \tag{58}$$

as in (13). Let k' be the field generated by $\beta_1(1)$, and T the subgroup of Ω which fixes k'. The next series of results leads to a characterization of the subgroup T and to criteria for determining when $\beta_\tau(\nu) = \beta_\rho(\mu)$.

First let l^* denote the multiplicative inverse $\pmod{s}$ for any l relatively prime to s.

Proposition 8. *There holds* $\omega_{\tau,\nu} = \omega_{1,1}$ *if and only if* $\tau \in N_\Gamma(\operatorname{Ann}\chi)$, $\tau(\theta) = \theta$, *and* $\tau\sigma\tau^{-1} = \sigma^\nu\tau'$ *for some* $\tau' \in \operatorname{Ann}\chi$.

Proof. To prove the implication →, first write $\tau\sigma\tau^{-1} = \sigma^l\tau'$ for some $\tau' \in \operatorname{Ann}\chi$, since $H \trianglelefteq \Gamma$. As $\operatorname{ord}_{H/\operatorname{Ann}\chi}(\tau\sigma\tau^{-1}) = s$, one has $(l, s) = 1$ above.

Next, note that if $\omega_{\tau,\nu} = \omega_{1,1}$, then

$$\begin{aligned}\tau(\sigma^j(\theta)) &= \frac{1}{\phi(s)}\sum_{\mu}{}' \zeta^{j\mu}\omega_{\tau,\mu} = \frac{1}{\Phi(s)}\sum_{\mu}{}' \zeta^{j\mu}\omega_{1,\nu^*\mu} \\ &= \frac{1}{\phi(s)}\sum_{\mu}{}' \zeta^{j\nu^*\mu}\omega_{1,\mu} = \sigma^{j\nu^*}(\theta), \qquad \text{so } \tau(K) = K,\end{aligned}$$

or equivalently, $\tau \in N_\Gamma(\operatorname{Ann}\chi)$. Thus,

$$\begin{aligned}\omega_{\tau,\nu} &= \tau(\theta) + \zeta^{-\nu}\tau\sigma\tau^{-1}(\tau(\theta)) + \cdots + \zeta^{-\nu(s-1)}\tau\sigma^{s-1}\tau^{-1}(\tau(\theta)) \\ &= \theta + \zeta^{-\nu}\sigma^l\tau'(\theta) + \cdots + \zeta^{-\nu(s-1)}(\sigma^l\tau')^{s-1}(\theta) \qquad (59)\\ &= \theta + \zeta^{-\nu}\sigma^l(\theta) + \cdots + \zeta^{-\nu(s-1)}\sigma^{l(s-1)}(\theta) = \omega_{1,\nu l^*}.\end{aligned}$$

In particular, $l = \nu$.

For the reverse direction ←, (59) now holds with $l = \nu$, so $\omega_{\tau,\nu} = \omega_{1,1}$. □

Proposition 9. *One has* $\beta_\tau(\nu) = \beta_1(1)$ *if and only if* $\tau \in N_\Gamma(\operatorname{Ann}\chi)$ *and* $\tau\sigma\tau^{-1} = \sigma^\nu\tau'$ *for some* $\tau' \in \operatorname{Ann}\chi$.

Proof. The equality $\beta_\tau(\nu) = \beta_1(1)$ is equivalent to $\zeta^g\omega_{\tau,\nu} = \omega_{1,1}$ for some $0 \le g < s$, by Proposition 7. Since $\zeta^g\omega_{\tau,\nu} = \omega_{\tau\sigma^{g\nu^*},\nu} = \omega_{1,1}$ by (54), the above holds by Proposition 8 precisely if $\tau\sigma^{g\nu^*}(\theta) = \theta$ and $\tau\sigma^{g\nu^*}\sigma\sigma^{-g\nu^*}\tau^{-1} = \tau^{-1}\sigma\tau = \sigma^\nu\tau'$ for some $\tau' \in \operatorname{Ann}\chi$. Since $\sigma \in N_\Gamma(\operatorname{Ann}\chi)$, this last equivalence implies that $\beta_\tau(\nu) = \beta_1(1)$ if and only if $\tau \in N_\Gamma(\operatorname{Ann}\chi)$ and $\tau\sigma\tau^{-1} = \sigma^\nu\tau'$ for some $\tau' \in \operatorname{Ann}\chi$. □

The next result gives criteria for deciding when $\beta_\rho(\mu) = \beta_\tau(\nu)$. First, put $\chi^\rho(\tau) = \chi(\rho^{-1}\tau\rho)$ for any $\rho \in \Gamma$ and $\tau \in H$.

Proposition 10. *For any* $1 \le \mu, \nu \le s$, $(\mu\nu, s) = 1$ *and* $\rho, \tau \in \Gamma$,

$$\beta_\rho(\mu) = \beta_\tau(\nu) \tag{60}$$

if and only if

$$(\chi^\rho)^\mu = (\chi^\tau)^\nu \quad \text{on } H, \tag{61}$$

which in turn holds if and only if

$$\mu\lambda_\psi(\rho^{-1}\phi) \equiv \nu\lambda_\psi(\tau^{-1}\phi) \pmod{s} \tag{62}$$

for all $\psi \in H$ *and* $\phi \in \Gamma$.

Proof. I shall verify the implications (60) → (61) → (62) → (60) to prove the proposition.

(60) → (61): If $\beta_\rho(\mu) = \beta_\tau(\nu)$, then $\beta_{\tau^{-1}\rho}(\nu^*\mu) = \beta_1(1)$, so $\tau^{-1}\rho \in N_\Gamma(\operatorname{Ann}\chi)$ and $\tau^{-1}\rho\sigma\rho^{-1}\tau = \sigma^{\nu^*\mu}\tau'$ for some $\tau' \in \operatorname{Ann}\chi$ by Proposition 9. Thus, for any element $\psi \in \rho H \rho^{-1}$, say $\psi = \rho\sigma^l\bar{\tau}\rho^{-1}$ for some $0 \le l < s$ and $\bar{\tau}$ in $\operatorname{Ann}\chi$, $\chi^\rho(\psi)^\mu = \chi(\sigma^l\bar{\tau})^\mu = \chi(\sigma^l)^\mu$ and

$$\begin{aligned}\chi^\tau(\psi)^\nu &= \chi(\tau^{-1}\rho\sigma^l\bar{\tau}\rho^{-1}\tau)^\nu = \chi((\sigma^{\nu^*\mu}\tau')^l\tau^{-1}\rho\bar{\tau}\rho^{-1}\tau)^\nu \\ &= \chi(\sigma^l)^\mu\chi(\tau^{-1}\rho\bar{\tau}\rho^{-1}\tau) = \chi(\sigma^l)^\mu.\end{aligned}$$

Since $H = \rho H \rho^{-1}$, one has $(\chi^\rho)^\mu = (\chi^\tau)^\nu$ on H.

(61) → (62): If $(\chi^\rho)^\mu = (\chi^\tau)^\nu$ on H, then for any $\psi \in H$

$$\chi(\rho^{-1}\psi\rho)^\mu = \chi(\tau^{-1}\psi\tau)^\nu.$$

Replacing ψ by $\phi\psi\phi^{-1}$ for any $\phi \in \Gamma$ yields

$$\chi(\rho^{-1}\phi\psi\phi^{-1}\rho)^\mu = \chi(\tau^{-1}\phi\psi\phi^{-1}\tau)^\nu. \tag{63}$$

But (63) holds if and only if $(\rho^{-1}\phi\psi\phi^{-1}\rho)^\mu \operatorname{Ann}\chi = (\tau^{-1}\phi\psi\phi^{-1}\tau)^\nu \operatorname{Ann}\chi$, or

$$\sigma^{\mu\lambda_\psi(\rho^{-1}\phi)} = \sigma^{\nu\lambda_\psi(\tau^{-1}\phi)}. \tag{64}$$

This last condition is equivalent to (62).

(62) → (60): Suppose now that (62) holds. Then for all $\phi \in \Gamma$ and $\psi \in H$,

$$\rho^{-1}\phi\psi^{\mu\nu^*}\phi^{-1}\rho \operatorname{Ann}\chi = \tau^{-1}\phi\psi\phi^{-1}\tau \operatorname{Ann}\chi.$$

Choosing $\phi = \rho$ gives

$$\psi^{\mu\nu^*} \operatorname{Ann}\chi = \tau^{-1}\rho\psi\rho^{-1}\tau \operatorname{Ann}\chi \quad \text{for all } \psi \in H. \tag{65}$$

In particular, $\tau^{-1}\rho(\operatorname{Ann}\chi)\rho^{-1}\tau = \operatorname{Ann}\chi$, so $\tau^{-1}\rho \in N_\Gamma(\operatorname{Ann}\chi)$. Now write $\tau^{-1}\rho\sigma\rho^{-1}\tau = \sigma^l\tau'$ for some $0 \le l < s$ and $\tau' \in \operatorname{Ann}\chi$. Then from (65), $\sigma^{\mu\nu^*} \operatorname{Ann}\chi = \tau^{-1}\rho\sigma\rho^{-1}\tau \operatorname{Ann}\chi = \sigma^l \operatorname{Ann}\chi$, so $l \equiv \mu\nu^* \pmod{s}$. By Proposition 9 one now has $\beta_{\tau^{-1}\rho}(\mu\nu^*) = \beta_1(1)$, so $\beta_\rho(\mu) = \beta_\tau(\nu)$. □

Returning to the situation at hand, first observe that the subgroup T of Ω fixing $\beta_1(1)$ has the form

$$T = \{\phi_{\tau,\nu} \mid \tau \in N_\Gamma(\operatorname{Ann}\chi) \text{ and } \tau\sigma\tau^{-1} = \sigma^\nu\tau' \text{ for some } \tau' \in \operatorname{Ann}\chi\}. \tag{66}$$

Thus, $|T| = |N_\Gamma(\operatorname{Ann}\chi)|$, so the index

$$m = [\Omega : T] = |\Gamma|\phi(s)/|T| = [\Gamma : N_\Gamma(\operatorname{Ann}\chi)] \cdot \phi(s).$$

Fix a set $\mathscr{C}$ of right coset representatives $\tau_1 = 1, \tau_2, \dots, \tau_{m/\phi(s)}$ for $N_\Gamma(\operatorname{Ann}\chi)$ in Γ. It follows from (66) that the set

$$\{\phi_{\tau,\nu} \mid \tau \in \mathscr{C},\ 1 \le \nu \le s,\ (\nu, s) = 1\} \tag{67}$$

is a complete set of right coset representatives for T in Ω. Consequently, the linear sequence V given by

$$V_n = \sum_{\nu}{}' \sum_{\tau \in \mathscr{C}} \beta_\tau(\nu)^n \qquad (n \geq 0) \tag{68}$$

is integer-valued and satisfies the recursion

$$W_{n+m} + a_{m-1} W_{n+m-1} + \cdots + a_0 W_n = 0 \qquad (n \geq 0). \tag{69}$$

It has order m dividing $[k : Q] \cdot \phi(s)$. If K/Q is normal and split at k, then θ may be chosen so that $m = \phi(s)$, since $N_\Gamma(\operatorname{Ann}\chi) = \Gamma$, so $\mathscr{C} = \{1\}$. Now set

$$V_{\psi,r,l} = \sum_{\nu}{}' \sum_{\tau \in \mathscr{C}} \gamma_{\tau,r}(\nu) \zeta^{r\nu\lambda_\psi(\tau^{-1})} \beta_\tau(\nu)^l \qquad (0 \leq l \leq m-1). \tag{70}$$

I claim that the values $V_{\psi,r,l}$ lie in k. Since the $\gamma_{\tau,r}(\nu)$ and $\beta_\tau(\nu)$ lie in k by (56) and (57), it is enough to show that the automorphisms $\phi_{1,e}$ of Ω fix each $V_{\psi,r,l}$. But

$$\begin{aligned} \phi_{1,e}(V_{\psi,r,l}) &= \sum_{\nu}{}' \sum_{\tau \in \mathscr{C}} \gamma_{\tau,r}(\nu e) \zeta^{re\nu\lambda_\psi(\tau^{-1})} \beta_\tau(\nu e)^l \\ &= \sum_{\nu}{}' \sum_{\tau \in \mathscr{C}} \gamma_{\tau,r}(\nu) \zeta^{r\nu\lambda_\psi(\tau^{-1})} \beta_\tau(\nu)^l = V_{\psi,r,l}. \end{aligned}$$

I wish to give a stronger characterization of pseudoprimes with respect to resolvent sequences, such as V in (68), than was developed in the previous section. To this end, I first establish some properties V satisfies for prime moduli.

Let p be a rational prime not dividing $sa_0\Delta \cdot \Delta(L)$ and $\tilde{\mathfrak{p}}$ any prime in L lying above p. Suppose $\mathfrak{p}$ is the prime in k lying between p and $\tilde{\mathfrak{p}}$, say of residue degree f. From the usual transport of structure properties of the Frobenius map, one finds that the Artin symbol $((K/k)/\rho(\mathfrak{p}))$ satisfies

$$\left(\frac{K/k}{\rho(\mathfrak{p})}\right) = \sigma^{\lambda(\rho)} \operatorname{Ann}\chi \quad \text{for any } \rho \in \Gamma, \tag{71}$$

where λ is the function (47) corresponding to $\psi = ((L/k)/\tilde{\mathfrak{p}})$.

Now express $q = p^f = st + r$ with $0 < r \leq s$ and $(r, s) = 1$. By the lemma in [10, p. 425], it follows that for any τ, ρ in Γ,

$$\beta_\tau(\nu) = \omega_{\tau,\nu}^q / (\omega_{\tau,\nu})^r \equiv \gamma_{\tau,r}(\nu) \zeta^{\nu r \lambda(\tau^{-1}\rho)} \pmod{\rho(\tilde{\mathfrak{p}})} \text{ in } k(\zeta). \tag{72}$$

Taking $\rho = 1$ in (72) and summing, one finds that for $0 \leq l \leq m-1$,

$$V_{t+l} \equiv V_{\psi,r,l} \pmod{\mathfrak{p}} \text{ in } k, \tag{73}$$

since, as was previously noted, the $V_{\psi,r,l}$ lie in k.

There is an equivalent way to express (73) in terms of matrices $C_{\psi,r}$ in $M_A(k)$ for $\psi \in H$ and $1 \leq r \leq s$ with $(r, s) = 1$. Let $x_{\psi,r} = (x_1, \ldots, x_m)$

be the unique solution of the linear system

$$(74)\quad \sum_{j=1}^{m} x_j(\beta_\tau(\nu))^{j-1} = \gamma_{\tau,r}(\nu)\zeta^{r\nu\lambda_\psi(\tau^{-1})} \qquad (\tau \in \mathscr{C},\ 1 \le \nu \le s,\ (\nu, s) = 1).$$

(As before in (29), one finds that the values Δx_j are integral, but now in $k(\zeta)$.) Applying any automorphism $\phi = \phi_{1,e}$ in Ω to both sides of (49) for any fixed τ and ν yields, by (49), the equation

$$\sum_{j=1}^{m} \phi(x_j)\beta_\tau(\nu e)^{j-1} = \gamma_{\tau,r}(\nu e)\zeta^{r\nu e\lambda_\psi(\tau^{-1})}.$$

Thus, $\phi(x_{\psi,r})$ also solves (74). Hence, $\phi(x_{\psi,r}) = x_{\psi,r}$ from uniqueness, and therefore the x_j lie in k. Now set

$$(75)\qquad C_{\psi,r} = M_{x_{\psi,r}} \quad \text{for } \psi \in H \text{ and } 1 \le r \le s,\ (r, s) = 1.$$

Observe that from (74),

$$(76)\qquad C_{\psi,r}\begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix} = \gamma_{\tau,r}(\nu)\zeta^{r\nu\lambda_\psi(\tau^{-1})}\begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix}$$

$(\tau \in \mathscr{C},\ 1 \le \nu \le s,\ (\nu, s) = 1)$, so that

$$(77)\qquad C_{\psi,r}\begin{bmatrix} V_0 \\ \vdots \\ V_{m-1} \end{bmatrix} = \begin{bmatrix} V_{\psi,r,0} \\ \vdots \\ V_{\psi,r,m-1} \end{bmatrix}.$$

Evidently, from (76), the $C_{\psi,r}$ $(\psi \in H,\ 1 \le r \le s,\ (r, s) = 1)$ are seen to be distinct, and for any $\psi \in H$, $\rho \in \Gamma$,

$$(78)\qquad \rho(C_{\psi,r}) = C_{\rho\psi\rho^{-1},r}.$$

It also follows from (76) that

$$(79)\qquad C_{\psi,r}^{s}\begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix} = \frac{\beta_\tau(\nu r)}{\beta_\tau(\nu)^{r}}\begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix},$$

so

$$(80)\qquad C_{\psi,r}^{s}A^{r} = C_\eta,$$

where $\eta = \eta_r$ is that element of the Galois group G of the polynomial (58) given by mapping each $\beta_\tau(\nu)$ to $\beta_\tau(\nu r)$.

I am ready to give the matrix equivalent of (72). Since

$$A^t \begin{bmatrix} V_0 \\ \vdots \\ V_{m-1} \end{bmatrix} = \begin{bmatrix} V_t \\ \vdots \\ V_{t+m-1} \end{bmatrix}, \qquad \text{where } p^f = st + r$$

with $1 \leq r \leq s$, $(r, s) = 1$, it follows from Proposition 2 that (72) is equivalent to the congruence

$$(81) \qquad A^t \equiv C_{\psi, r} \pmod{\mathfrak{p}}.$$

The congruence (72), or its equivalent (81), is the basis upon which to characterize stronger pseudoprimes associated with the resolvent sequence V than were given in §3. For this purpose, I shall henceforth assume that k/Q is Abelian, say of conductor F. Then k is a classfield corresponding to some group $\mathscr{A}$ of norm residues defined modulo F. From classfield theory, if $\mathscr{R}$ is the full group of reduced residues modulo F, then the residue degree f of the prime p is just the order of p in $\mathscr{R}/\mathscr{A}$. I have required that k/Q be Abelian here to facilitate determining the residue degree of p in k. This can be done also for non-Abelian k/Q, but at the expense of introducing certain auxiliary linear sequences that are helpful in deciding the Artin class of p in k/Q (chiefly, on account of (27)).

The sequence $(V_{\psi,r,0}, V_{\psi,r,1}, \dots, V_{\psi,r,m-1})$ in (70) will be referred to as an admissible signature for V of type (ψ, r). Suppose N is a composite prime to $2a_0\Delta\Delta(L)$ and to s. Let f be the order of N in $\mathscr{R}/\mathscr{A}$, and suppose

$$(82) \qquad N^f = st + r, \qquad 1 \leq r \leq s, \ (r, s) = 1.$$

Call N an s-pseudoprime with respect to V, denoted $s\text{-psp}_V$, if the terms $V_t, V_{t+1}, \dots, V_{t+m-1}$ match an admissible sequence signature for V (mod $\mathfrak{n}$) in k for some k-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$; that is, if

$$(83) \qquad V_{t+l} \equiv V_{\psi,r,l} \pmod{\mathfrak{n}} \qquad (0 \leq l \leq m-1)$$

in k for some $\psi \in H$. An $s\text{-psp}_V$ N satisfying (83) is said to be of type (ψ, r).

Actually, one may define admissible sequence signatures $(V_{\psi,r,l})$ using any m fixed consecutive values on l here (and in (70)), not just $0, 1, \dots, m-1$, and then take the corresponding terms (V_{t+l}) to define s-pseudoprimes in the same fashion. In the same way, one may let r run through any fixed complete set of reduced residues (mod s) with the appropriate modifications in the definitions. I shall take this liberty later in some examples. In addition, I will illustrate how to relax the requirement that k/Q be Abelian, using an auxiliary sequence rather than a congruence condition to decide an appropriate "f" for N in expression (82).

Condition (83) defining the s-psp_V's has equivalents analogous to (72) and (81). Namely,

Theorem 4. *A composite* N *with* $(N, 2a_0 s\Delta\cdot\Delta(L)) = 1$ *satisfies* (83) *if and only if*

$$A^t \equiv C_{\psi, r} \pmod{\mathfrak{n}}, \tag{84}$$

which in turn holds if and only if for all $\tau \in \Gamma$ *and* $(\nu, s) = 1$

$$\beta_\tau(\nu) \equiv \gamma_{\tau, r}(\nu)\zeta^{\nu r\lambda(\tau^{-1})} \pmod{\tilde{\mathfrak{n}}} \tag{85}$$

for any $k(\zeta)$*-ideal* $\tilde{\mathfrak{n}}$ *with* $\tilde{\mathfrak{n}} \cap k = \mathfrak{n}$.

Proof. I demonstrate that (85) → (83) → (84) → (85) to prove the result.

(85) → (83): This follows immediately from (70).

(83) → (84): If (83) holds, then, arguing as in the proof of Theorem 2, one has $A^t \equiv C_{\psi, r} \pmod{\mathfrak{n}}$, since N is prime to $\det(V) = \Delta$.

(84) → (85): If $A^t \equiv C_{\psi, r} \pmod{\mathfrak{n}}$, then from (76),

$$A^t \begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix} = \beta_\tau(\nu)^t \begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix}$$
$$\equiv \gamma_{\tau, r}(\nu)\zeta^{\nu r\lambda(\tau^{-1})} \begin{bmatrix} 1 \\ \beta_\tau(\nu) \\ \vdots \\ \beta_\tau(\nu)^{m-1} \end{bmatrix} \pmod{\tilde{\mathfrak{n}}}$$

for all $\tau \in \Gamma$ and $(\nu, s) = 1$, where $\tilde{\mathfrak{n}}$ is any $k(\zeta)$-ideal with $\tilde{\mathfrak{n}} \cap k = \mathfrak{n}$. Thus (85) holds modulo any such $k(\zeta)$-ideal $\tilde{\mathfrak{n}}$. □

Corollary 5. *Any* s-psp_V N *of type* (ψ, r) *with* $f = 1$ *is a* psp_V *of type* η_r *and an ordinary* psp_c, *where* $c = |a_0|^{1/s}$.

Proof. Suppose N is an s-psp_V of type (ψ, r). From Theorem 4, $A^t \equiv C_{\psi, r}$ (mod $\mathfrak{n}$) for some k-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$. Then by (80),

$$A^{N^f} \equiv C^s_{\psi, r} A^r \equiv C_{\eta_r} \pmod{\mathfrak{n}}, \tag{86}$$

so if $f = 1$, N is a psp_V of type η_r. Also from Theorem 4,

$$\beta_\tau(\nu)^t = \omega_{\tau,\nu}^{N^f}/(\omega_{\tau,\nu})^r \equiv \omega_{\tau,\nu}\zeta^{r\nu\lambda_\psi(\tau^{-1})}/(\omega_{\tau,\nu})^r \pmod{\tilde{\mathfrak{n}}}$$

for some $k(\zeta)$-ideal $\tilde{\mathfrak{n}}$ with $\tilde{\mathfrak{n}} \cap k = \mathfrak{n}$. Hence,

$$\omega_{\tau,\nu}^{N^f} \equiv \omega_{\tau,\nu}\zeta^{r\nu\lambda_\psi(\tau^{-1})} \pmod{\mathfrak{N}} \tag{87}$$

for some $L(\zeta)$-ideal $\mathfrak{N}$ with $\mathfrak{N} \cap k(\zeta) = \tilde{\mathfrak{n}}$. Taking the product in (87) over $\tau \in \mathscr{C}$ and $1 \leq \nu \leq s$ with $(\nu, s) = 1$, one obtains

$$(88) \qquad \left(\prod_{\nu}{}' \prod_{\tau} \omega_{\tau,\nu}\right)^{N^f} \equiv \prod_{\nu}{}' \prod_{\tau} \omega_{\tau,\nu} \pmod{\mathfrak{N}}.$$

I assert that $\gamma = \prod'_{\nu} \prod_{\tau\in\mathscr{C}} \omega_{\tau,\nu}$ lies in Q and that $c = |\gamma|$, so that

$$(89) \qquad c^{N^f} \equiv c \pmod{N},$$

since N is odd. Hence N is a psp_c if $f = 1$.

To prove the assertion that γ lies in Q, it is enough to show that any $\phi_{p,e}$ fixes γ. For each $\tau \in \mathscr{C}$, write $\rho\tau = \xi_\tau\bar{\tau}$, where $\xi_\tau \in N_\Gamma(\operatorname{Ann}\chi)$, $\bar{\tau} \in \mathscr{C}$, and $\xi_\tau\sigma\xi_1^{-1} = \sigma^{\nu(\tau)}\tau'$ for $\tau' \in \operatorname{Ann}\chi$ and $0 \leq \nu(\tau) < s$. Then from (49),

$$\begin{aligned} \phi_{p,e}(\gamma) &= \prod_{\nu}{}' \prod_{\mathscr{C}} \omega_{\rho\tau,\nu e} = \prod_{\nu}{}' \prod_{\mathscr{C}} \omega_{\rho\tau,\nu} \\ &= \prod_{\nu}{}' \prod_{\bar{\tau}\in\mathscr{C}} \omega_{\xi_\tau\bar{\tau},\nu} = \prod_{\nu}{}' \prod_{\mathscr{C}} \omega_{\tau,\nu\nu(\tau)^*} = \gamma. \end{aligned}$$

Thus, γ lies in Q; in fact, $\gamma^s = \prod'_{\nu} \prod_{\mathscr{C}} \beta_\tau(\nu) = (-1)^m a_0$, so $c = |\gamma|$. This completes the proof of the corollary. □

From (86) above one immediately has

Corollary 6. *Any s-psp_V N of type (ψ, r) satisfies*

$$V_{N^f+l} \equiv V_{\eta_r,l} \pmod{\mathfrak{n}} \qquad (0 \leq l \leq m-1)$$

for some k-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$.

Now let $\pi(x, V, \phi)$ count the number of s-psp_V's N with Artin symbol $((k/Q)/N) = \phi$ that are less than or equal to x. In view of Corollary 5 one gets an upper bound for $\pi(x, V, 1)$ as before from (1). Namely, if $|a_0| \neq 1$, then

$$(90) \qquad \pi(x, V, 1) < x\exp\{-\log x \log\log\log x/2\log\log x\}$$

for all sufficiently large x.

Actually, Pomerance's argument in the proof of Theorem 2 in [13] extends to give the same upper bound for the number of composites N less than or equal to x which satisfy (89) for a given base $c > 1$ and fixed $f > 1$. Thus, more generally, one finds that

Corollary 7. *For any fixed ϕ in $G(k/Q)$, if $|a_0| \neq 1$, then*

$$\pi(x, V, \phi) < x\exp\{-\log x \log\log\log x/2\log\log x\}$$

for all sufficiently large x.

Aside from the upper bound given above, virtually nothing is known about the distribution of s-psp_V's when $m > 2$.

Example 5. Consider $q(x) = x^5 - 75x^3 - 375x^2 - 625x - 3125/11$ with root θ and splitting field $L = Q(\zeta_{11} + \zeta_{11}^{-1})$. Here, $K = L$, $k = Q$, and $\Gamma = H$ is cyclic of order 5 generated, say, by σ induced by the action $\zeta_{11} \to \zeta_{11}^3$. Taking any nontrivial character χ of H, one sees that $\mathscr{C} = \{1\}$ in (68), since Ω is Abelian. In addition, the function $\lambda_{\sigma^\mu}(\rho) = \mu$ in (47) for any $\rho \in \Gamma$ and $0 \le \mu < s$. Using $\theta/4$ in place of θ to define the Lagrange resolvents (48), one finds from (52) that the conjugates of θ are just

$$\sigma^e(\theta) = \zeta^e \omega_{1,1} + \zeta^{2e} \omega_{1,2} + \zeta^{3e} \omega_{1,3} + \zeta^{4e} \omega_{1,4} \qquad (0 \le e \le 4).$$

The minimal polynomial for $\beta = \omega_{1,1}^5$ is $p(x) = x^4 - 4500x^3/11 + 92500x^2 - 8696875x + 55^5$ and $k' = Q(\zeta)$. The admissible signatures for the sequence $V_n = \beta_1(1)^n + \beta_1(2)^n + \beta_1(3)^n + \beta_1(4)^n$ $(n \ge 0)$ with fixed choice $l = -1, 0, 1, 2$ are as follows:

l	$V_{1,1,l}$	$V_{\sigma,1,l}$	$V_{\sigma^2,1,l}$	$V_{\sigma^3,1,l}$	$V_{\sigma^4,1,l}$
-1	$23/1331$	$-84/6655$	$-153/6655$	$58/6655$	$64/6655$
0	4	-1	-1	-1	-1
1	$4500/11$	$-2525/11$	$4425/11$	$-4550/11$	$-1850/11$
2	$\dfrac{-2135000}{121}$	$\dfrac{-3679000}{121}$	$\dfrac{12607125}{121}$	$\dfrac{-11974750}{121}$	$\dfrac{5181625}{121}$

l	$V_{1,2,l}$	$V_{\sigma,2,l}$	$V_{\sigma^2,2,l}$	$V_{\sigma^3,2,l}$	$V_{\sigma^4,2,l}$
-1	$148/73205$	$-538/73205$	$449/73205$	$-601/73205$	$542/73205$
0	$15/11$	$-9/11$	$2/11$	$-7/11$	$-1/11$
1	185	60	-40	-65	-140
2	$32250/11$	$338750/11$	$78500/11$	$-82125/11$	$-367375/11$

l	$V_{1,-2,l}$	$V_{\sigma,-2,l}$	$V_{\sigma^2,-2,l}$	$V_{\sigma^3,-2,l}$	$V_{\sigma^4,-2,l}$
-1	$59/121$	$-2/121$	$-10/121$	$5/121$	$-52/121$
0	75	-30	-10	-40	5
1	$60300/11$	$-91825/11$	$-56825/11$	$-35075/11$	$123425/11$
2	$\dfrac{-100573750}{121}$	$\dfrac{-237157500}{121}$	$\dfrac{-74741875}{121}$	$\dfrac{153435000}{121}$	$\dfrac{259038125}{121}$

l	$V_{1,-1,l}$	$V_{\sigma,-1,l}$	$V_{\sigma^2,-1,l}$	$V_{\sigma^3,-1,l}$	$V_{\sigma^4,-1,l}$
-1	$15/121$	$5/121$	$9/121$	$-19/121$	$-10/121$
0	30	-10	-5	-5	-10
1	$35875/11$	$-12900/11$	$-34425/11$	$38050/11$	$-26600/11$
2	$\dfrac{-16447625}{121}$	$\dfrac{50381125}{121}$	$\dfrac{-101612000}{121}$	$\dfrac{103903625}{121}$	$\dfrac{-36225125}{121}$

Up to 2^{31}, there are 16 pseudoprimes for V, all of type (1,1) but one. These 5-psp_V's are listed below.

N	Factorization	Type (ψ, r)
5049001	$31 \cdot 271 \cdot 601^*$	$(1, 1)$
5148001	$41 \cdot 241 \cdot 521^*$	$(1, 1)$
49019851	$4951 \cdot 9901$	$(1, 1)$
82929001	$281 \cdot 421 \cdot 701^*$	$(1, 1)$
139952671	$131 \cdot 571 \cdot 1871^*$	$(1, 1)$
216821881	$331 \cdot 661 \cdot 991^*$	$(1, 1)$
382536001	$31 \cdot 71 \cdot 151 \cdot 1151^*$	$(1, 1)$
392099401	$29 \cdot 139 \cdot 211 \cdot 461^*$	$(1, 1)$
625482001	$241 \cdot 1201 \cdot 2161^*$	$(1, 1)$
652969351	$271 \cdot 811 \cdot 2971^*$	$(1, 1)$
1024966801	$12101 \cdot 84701$	$(1, 1)$
1098000091	$23431 \cdot 46861$	$(1, 1)$
1317828601	$41 \cdot 181 \cdot 311 \cdot 571^*$	$(1, 1)$
1515785041	$331 \cdot 991 \cdot 4621^*$	$(1, 1)$
1708549501	$211 \cdot 1741 \cdot 4651^*$	$(1, 1)$
2487941	$911 \cdot 2731$	$(\sigma^3, 1)$

$^*Q(\zeta)$-Carmichael numbers of type $C(1)$.

Example 6. Now consider $k = Q(\beta, \sqrt{-23})$, where β satisfies $x^3 - x - 1 = 0$, and let $K = k(\beta^{1/2})$ with splitting field L. Choose a character χ of H which is nontrivial on $G(K/k)$. Fix σ in H with $\chi(\sigma) \neq 1$, and let δ generate $\operatorname{Ann}\chi$. Then the subgroup $H = G(L/k) \trianglelefteq \Gamma = S_4$ is generated by δ and σ, with

$$\begin{array}{rl} \delta\colon & \beta_1^{1/2} \to \beta_1^{1/2} \\ & \beta_2^{1/2} \to -\beta_2^{1/2} \\ & \beta_3^{1/2} \to -\beta_3^{1/2} \end{array} \quad \text{and} \quad \begin{array}{rl} \sigma\colon & \beta_1^{1/2} \to -\beta_1^{1/2} \\ & \beta_2^{1/2} \to \beta_2^{1/2} \\ & \beta_3^{1/2} \to -\beta_3^{1/2} \end{array}$$

for an appropriate ordering of the roots of $x^3 - x - 1$ with $\beta_1 = \beta$. Using $\theta = \beta^{1/2}/2$ to define the Lagrange resolvents (48), one finds that $\omega_{\rho,1} = \rho(\beta^{1/2})$ for any ρ in Γ.

Next, fix coset representatives $1, \rho, \rho^2, \tau, \tau\rho, \tau\rho^2$ for H in Γ, where

$$\begin{array}{rl} \rho\colon & \beta_1 \to \beta_2 \\ & \beta_2 \to \beta_3 \\ & \beta_3 \to \beta_1 \end{array} \quad \text{and} \quad \begin{array}{rl} \tau\colon & \beta_1 \to \beta_1 \\ & \beta_2 \to \beta_3 \\ & \beta_3 \to \beta_2 . \end{array}$$

The functions λ_ψ on Γ defined by (47) are given in the table below.

coset $\backslash\ \psi$	1	δ	σ	$\delta\sigma$
H	0	0	1	1
ρH	0	1	1	0
$\rho^2 H$	0	1	0	1
τH	0	0	1	1
$\tau\rho H$	0	1	1	0
$\tau\rho^2 H$	0	1	0	1

Now $\Omega = \Gamma$ here, $N_\Gamma(\operatorname{Ann}\chi) = H \cup \tau H$, so $k' = Q(\beta)$. The sequence V in (68) is just $V_n = \beta_1^n + \beta_2^n + \beta_3^n$, which was considered in Example 1. The admissible sequences for V of type $(\psi, 1)$ with fixed choice $l = -1, 0, 1$ are given below:

l	$V_{1,1,l}$	$V_{\delta,1,l}$	$V_{\sigma,1,l}$	$V_{\delta\sigma,1,l}$
-1	3	-1	-1	-1
0	0	$2\beta_1$	$2\beta_2$	$2\beta_3$
1	2	$-2+2\beta_1^2$	$-2+2\beta_2^2$	$-2+2\beta_3^2$

Since k/Q is non-Abelian, it will be necessary here to determine an appropriate choice for f in (82) for composite N in order to define 2-psp_V's. A very convenient strategy is to first test whether or not N is a psp_V. Given a composite N with $(N, 2a_0\Delta \cdot \Delta(L)) = 1$, let us say N is a 2-psp_V of type $(\psi, 1)$ if

(i) N is a psp_V, say of type $C(\gamma)$ for some γ in $G(k/Q)$, and

(ii) $V_{(N^f+2l-1)/2} \equiv V_{\psi,1,l} \pmod{\mathfrak{n}}$ $(l = -1, 0, 1)$ for some k-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$ and ψ in H, where $f = \operatorname{ord}_{G(k/Q)} \gamma$.

It was mentioned in Example 1 that all 55 psp_V's below 50×10^9 are of type $C(1)$. Of these, 42 also satisfy condition (ii) and are thus 2-psp_V's. The exceptions are those numbered 7, 13, 15, 17, 19, 23, 33, 37, 38, 39, 49, 52, and 55 on Kurtz, Shanks and Williams' list [11].

An obvious question to consider here is just how scarce are s-psp_V's compared with psp_V's for the same resolvent sequence V. In Example 5 above I found that up to 2^{31} there were roughly 13 times as many psp_V's as 5-psp_V's. Whereas in Example 6 most of the psp_V's are 2-psp_V's. This scant evidence, combined with observations I made while investigating 3-psp_V's [9], seems to suggest that while s-psp_V's are rarer than psp_V's for the same resolvent sequence, the relative improvement is modest. If one wishes to have far fewer pseudoprimes in a given range, it appears to be much more advantageous to replace the sequence V by another one associated with a polynomial having larger Galois group.

I would now like to extend the notion of higher-order pseudoprimes to other sequences satisfying the same recursion as V. Let us consider an integer sequence $W = (W_n)$ satisfying (69). For a prime p not dividing $2a_0\Delta \cdot \Delta(L)$, say with k-prime $\mathfrak{p}$ lying above p of residue degree f and L-prime $\tilde{\mathfrak{p}}$ above $\mathfrak{p}$, it follows from (74) that

$$W_{t+l} \equiv W_{\psi,r,l} \pmod{\mathfrak{p}} \qquad (0 \le l \le m-1), \tag{91}$$

where

$$\begin{bmatrix} W_{\psi,r,0} \\ \vdots \\ W_{\psi,r,m-1} \end{bmatrix} = C_{\psi,r} \begin{bmatrix} W_0 \\ \vdots \\ W_{m-1} \end{bmatrix} \tag{92}$$

in k^m. Here, $p^f = st + r$ with $1 \le r \le s$, $(r, s) = 1$ as before with $\psi = ((L/k)/\tilde{\mathfrak{p}})$.

The sequence $W_{\psi,r,l}$ $(0 \le l \le m-1)$ is the analogous admissible signature for W of type (ψ, r). A composite N with $(N, 2a_0\Delta \cdot \Delta(L)) = 1$ is called an s-pseudoprime with respect to W, denoted $s\text{-}\mathrm{psp}_W$, of type (ψ, r), if the terms

$$W_{t+l} \equiv W_{\psi,r,l} \pmod{\mathfrak{n}} \qquad (0 \le l \le m-1) \tag{93}$$

for some k-ideal $\mathfrak{n}$ with $\mathfrak{n} \cap \mathbf{Z} = (N)$. (Here again, $N^f = st + r$, $1 \le r \le s$, $(r, s) = 1$, where f is the order of N in $\mathscr{R}/\mathscr{A}$.)

For the sequence U, given by (11) with the conjugates $\beta_\tau(\nu)$ ordered, the admissible signature of type (ψ, r) is given by

$$U_{\psi,r,l} = \sum_{\nu}{}' \sum_{\tau \in \mathscr{C}} \frac{\zeta^{r\nu\lambda_\psi(\tau^{-1})} \gamma_{\tau,r}(\nu) \beta_\tau(\nu)^l}{p'(\beta_\tau(\nu))}. \tag{94}$$

The characterization of these higher-order pseudoprimes using the sequence U or V is essentially the same. More generally, I note

Theorem 5. *Suppose $W = (W_n)$ is an integer sequence satisfying* (69). *For N satisfying $(N, 2a_0\Delta \det(W) \cdot \Delta(L)) = 1$, N is an $s\text{-}\mathrm{psp}_W$ of type (ψ, r) if and only if N is an $s\text{-}\mathrm{psp}_V$ of type (ψ, r).*

I omit the proof of Theorem 5, since the argument is essentially the one used in the proof of Theorem 3, except now one uses (84) instead of (36).

Bibliography

1. W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.
2. W. Adams, *Characterizing pseudoprimes for third-order linear recurrences*, Math. Comp. **48** (1987), 1–15.
3. E. Artin, *Galois theory*, 2nd ed., University of Notre Dame, 1946.

4. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1968.

5. R. Baillie and S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1390–1417.

→ R. Carmichael, *On composite numbers* p*, which satisfy the Fermat congruence*, Amer. Math. Monthly **19** (1912), 22–27.

7. L. E. Dickson, *Elementary theory of equations*, Wiley, New York.

8. H. Duparc, *Periodicity properties of recurring sequences.* II, Indag. Math. **16** (1954), 473–485.

9. S. Gurak, *Cubic and biquadratic pseudoprimes of Lucas type* (to appear).

10. ____, *On the representation theory for full decomposable forms*, J. Number Theory **13** (1981), 421–442.

11. G. Kurtz, D. Shanks, and H. C. Williams, *Fast primality tests for numbers less than* $50 \cdot 10^9$, Math. Comp. **46** (1986), 691–701.

→ E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

13. C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.

14. ____, *A new lower bound for the pseudoprime counting function*, Illinois J. Math. **26** (1982), 4–9.

15. C. Pomerance, J. L. Selfridge, and S. Wagstaff, Jr., *The pseudoprimes to* 25,000,000,000, Math. Comp. **35** (1980), 1003–1026.

16. A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequence*, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys. **21** (1973), 793–797.

17. B. L. van der Waerden, *Modern algebra*, vols. 1, 2, Ungar, New York, 1949–1950.

→ M. Ward, *Arithmetical properties of sequences in finite fields*, Ann. of Math. (2) **39** (1938), 210–219.

Department of Mathematics and Computer Science, University of San Diego, San Diego, California 92110