MATHEMATICS OF COMPUTATION
VOLUME 43, NUMBER 167
JULY 1984, PAGES 329-343

Splitting of Quartic Polynomials

By William W. Adams

Abstract. For integers r, s, t, u define the recursion $A(n+4) = rA(n+3) - sA(n+2) + tA(n+1) - uA(n)$ where the initial conditions are set up in such a way that $A(n) = \alpha^n + \beta^n + \gamma^n + \delta^n$ where $\alpha, \beta, \gamma, \delta$ are the roots of the associated polynomial $f(x) = x^4 - rx^3 + sx^2 - tx + u$. In this paper a detailed deterministic procedure using the $A(n)$ for finding how $f(x)$ splits modulo a prime integer p is given. This gives for p not dividing the discriminant of $f(x)$ the splitting of p in the field obtained by adjoining a root of $f(x)$ to the rational numbers. There is an interesting connection between the results here for reciprocal polynomials and some work of D. Shanks.

1. Introduction. Let

$$f(x) = x^d - r_{d-1}x^{d-1} + r_{d-2}x^{d-2} - \cdots + (-1)^d r_0 = (x-\alpha_1)\cdots(x-\alpha_d)$$

be a polynomial with integer coefficients factored over the complex numbers. Set, for $n = 0, 1, 2, \ldots$,

$$A(n) = A_f(n) = \alpha_1^n + \cdots + \alpha_d^n. \tag{1.1}$$

The purpose of this paper is to relate how $f(x)$ splits modulo a prime p, to the congruence properties of $A(n)$ mod p for n near p and for $d \leqslant 4$. Such a criterion is implicitly given for $d = 3$ in [1]. (The case of $d = 2$ is well known, and also may be done by quadratic reciprocity.)

The usual algorithm for finding the splitting of $f(x)$ mod p is due to Berlekamp; see [2], [5]. The current method is completely different from that given by him. The current algorithm can be executed in $O(\log p)$ steps (where "O" depends on $f(x)$)—this is the same as Berlekamp. We note however that Berlekamp's method is not limited to $d \leqslant 4$ as this algorithm currently is.

There is another solution given to this problem by Stefan Schwarz [6] which again is not limited to $d \leqslant 4$. He derives for $d = 4$ a congruence mod p for the number of factors of degree 1 involving a sum of three 3×3 determinants in the $A(n)$. The $A(n)$ must be computed for n near p and $2p$. The current criterion is again quite different and involves less computation.

It is easy to see that $A(n)$ satisfies the recursion

$$A(n+d) = \sum_{j=1}^{d} (-1)^{j-1} r_{d-j} A(n+d-j)$$

Received April 18, 1983; revised August 2, 1983.
1980 *Mathematics Subject Classification.* Primary 12D05; Secondary 10A35.

0025-5718/84 $1.00 + $.25 per page

for the initial conditions

$$A(0) = d, \quad A(1) = r_{d-1}, \quad A(2) = r_{d-1}^2 - 2r_{d-2}, \tag{1.2}$$
$$A(3) = r_{d-1}^3 - 3r_{d-1}r_{d-2} + 3r_{d-3}, \text{ etc.},$$

derived from Newton's identities.

The test to be described involves computing for $n = p - 1$ the so-called *signature* of p, namely the vector $\mathbf{A}_n = [A(n), A(n+1), \ldots, A(n+d-1)]$. If we define the matrix D as the companion matrix of $f(x)$:

$$D = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & & \\ 0 & 0 & 0 & & 1 \\ (-1)^{d-1}r_0 & (-1)^{d-2}r_1 & \cdots & \cdots\cdots & r_{d-1} \end{pmatrix}$$

then we see that $\mathbf{A}_n^t = D\mathbf{A}_{n-1}^t$ and hence

$$\mathbf{A}_n^t = D^n\mathbf{A}_0^t,$$

where $\mathbf{A}_0$ is given by the initial conditions (1.2). It is well known (see [5]) that D^n can be computed in $O(\log n)$ steps. Thus we indeed see that the computation of the signature of p may be done in $O(\log p)$ steps, and so the splitting of p may be quickly determined using the criteria described below.

In [1] it was suggested that these $A(n)$ could be used for a fast pseudoprimality test for $d = 3$. This is based upon a big extension of the following fundamental congruence:

$$A(p) \equiv A(1) \pmod{p} \tag{1.3}$$

for any prime p. (It is very difficult for this congruence to be true when p is not a prime.) Congruence (1.3) may be proved as follows:

Let K be the splitting field of the polynomial $f(x)$ over the rational numbers. Let $\mathfrak{p}$ be a prime of K lying over the prime p. Then $\alpha \to \alpha^p$ is the Frobenius automorphism over $\mathbf{Z}/p\mathbf{Z}$. Hence, mod $\mathfrak{p}$, $\alpha_1^p, \ldots, \alpha_d^p$ is a permutation of $\alpha_1, \ldots, \alpha_d$, and we obtain (1.3) immediately.

There has been no assumption that the polynomial $f(x)$ is irreducible, and, indeed, this is not necessary. We will then be able to deduce the case for $d = 3$ from that for $d = 4$ (by letting α_4 be an appropriate integer).

The paper is organized as follows. In Section 2 the notation for quartic polynomials and the main tools are discussed. In Section 3 we discuss "generalized reciprocal" quartic polynomials, as they must be handled separately. In Section 4 the discussion of Section 3 is continued wherein work of D. Shanks [7] is discussed and, in particular, we see precisely how well the splitting of these dihedral quartics may be determined by congruences. Many of the results stated there were anticipated by L. Carlitz [3] for the special case $a = 1$ in Eq. (3.4). In Section 5 the more "usual" case is discussed, i.e., not the case of Section 3. In Section 6 an ad hoc procedure to determine the splitting of ramified primes is given. In Section 7 the results of Section 5 are applied to derive the analogous results for cubic and quadratic polynomials as well as one case of a degenerate quartic polynomial. Finally, in Section 8 a detailed algorithm is given summarizing the above results on quartic polynomials.

Based upon the algorithm of Section 8 a PASCAL program has been developed which is currently yielding interesting data, cf. [8, Table 1].

I would like to take this opportunity to thank D. Shanks for many helpful discussions and in particular for pointing out to me how one might derive Eq. (4.3).

2. Quartic Polynomials. We now specialize the notation: Let

$$f(x) = x^4 - rx^3 + sx^2 - tx + u \tag{2.1}$$

$$= (x - \alpha)(x - \beta)(x - \gamma)(x - \delta). \tag{2.2}$$

The sequence $A(n) = A_f(n)$ is defined by

$$A(n+4) = rA(n+3) - sA(n+2) + tA(n+1) - uA(n) \tag{2.3}$$

for integers $n \geqslant 0$, and for the initial conditions (1.2)

$$A(0) = 4, \quad A(1) = r, \quad A(2) = r^2 - 2s, \quad A(3) = r^3 - 3rs + 3t. \tag{2.4}$$

This guarantees that

$$A(n) = \alpha^n + \beta^n + \gamma^n + \delta^n. \tag{2.5}$$

For a given rational prime p, there are different ways $f(x)$ may split mod p, five of which are unramified (have no repeated factors). I will label the unramified ones as $S = 1\,1\,1\,1$, $1\,3$, $1\,1\,2$, $2\,2$, $I = 4$, where the indicated digits give the number of distinct *irreducible* factors of $f(x)$ of that degree mod p. Of course, for any given $f(x)$ some of these cases may not occur. For example, if over $\mathbf{Z}$, $f(x)$ is a product of a linear polynomial and a cyclic cubic, then only S and $1\,3$ may occur.

The method of obtaining the results will be through the use of the Frobenius automorphism applied to the splitting field of $f(x)$. So let K be the splitting field of $f(x)$ over the rational numbers Q ($K = Q(\alpha, \beta, \gamma, \delta)$), and let I_K denote its ring of integers. Fix an unramified rational prime p and let $\mathfrak{p}$ be a prime of K lying over p. Then $I_K/\mathfrak{p}$ is a cyclic Galois extension of $\mathbf{Z}/p\mathbf{Z}$, whose Galois group is the decomposition group $G_{\mathfrak{p}}$ of $\mathfrak{p}$ and is generated by the Frobenius automorphism

$$\sigma_{\mathfrak{p}}\colon \eta \to \eta^p \pmod{\mathfrak{p}} \qquad (\eta \in I_K).$$

The splitting types of $f(x)$ are characterized by the action of $\sigma_{\mathfrak{p}}$ on the four roots $\alpha, \beta, \gamma, \delta$ as follows (rearranging $\alpha, \beta, \gamma, \delta$, if necessary):

$$\begin{cases} S & \alpha^p \equiv \alpha, \beta^p \equiv \beta, \gamma^p \equiv \gamma, \delta^p \equiv \delta \pmod{\mathfrak{p}}, \\ 1\,3 & \alpha^p \equiv \alpha, \beta^p \equiv \gamma, \gamma^p \equiv \delta, \delta^p \equiv \beta \pmod{\mathfrak{p}}, \\ 1\,1\,2 & \alpha^p \equiv \alpha, \beta^p \equiv \beta, \gamma^p \equiv \delta, \delta^p \equiv \gamma \pmod{\mathfrak{p}}, \\ 2\,2 & \alpha^p \equiv \beta, \beta^p \equiv \alpha, \gamma^p \equiv \delta, \delta^p \equiv \gamma \pmod{\mathfrak{p}}, \\ I & \alpha^p \equiv \beta, \beta^p \equiv \gamma, \gamma^p \equiv \delta, \delta^p \equiv \alpha \pmod{\mathfrak{p}}. \end{cases} \tag{2.6}$$

Moreover, for $\rho = \alpha$, β, γ or δ, $\rho^p \equiv \rho(\mathfrak{p})$, whenever we have $\rho \equiv k \pmod{\mathfrak{p}}$ for some k in $\mathbf{Z}$, this characterization will be the primary tool (in Section 3 the notation will be changed however).

One other tool is required, namely the sequence going backwards. Since u may not be ± 1 and the reverse sequence will consist of rational (not integral) numbers, we will define the reverse sequence only modulo the prime p.

Let p be any rational prime p such that $p \nmid u$ (the case where $p|u$ will be discussed later, see Corollary 7.2). Define u^* by $uu^* \equiv 1 \pmod{p}$. Define $A(-n)$ $(n \geqslant 0)$ by the recursion

$$A(-n-4) \equiv u^*tA(-n-3) - u^*sA(-n-2) + u^*rA(-n-1) - u^*A(-n) \pmod{p} \tag{2.7}$$

with the initial conditions corresponding to (2.4). Then, of course, for any prime $\mathfrak{p}$ lying over p in K, we have

$$A(-n) \equiv \alpha^{-n} + \beta^{-n} + \gamma^{-n} + \delta^{-n} \pmod{\mathfrak{p}}.$$

Moreover, working mod p, both recurrences (2.3) and (2.7) hold for all integers n (positive, negative or zero) and mod $\mathfrak{p}$, (2.5) holds for all n.

3. Generalized Reciprocal Quartics. Fix a rational prime p ($p \nmid u$). Let $\mathfrak{p}$ be a prime of K lying over p. The quartics satisfying the condition

$$ur^2 \equiv t^2 \pmod{p} \tag{3.1}$$

must be handled separately.

If $p \nmid r$, then u must be a quadratic residue mod p. Let a satisfy

$$a^2 \equiv u \pmod{p} \quad \text{and} \quad ar \equiv t \pmod{p}. \tag{3.2}$$

If $p|r$, then $p|t$ also, and we see that, for any root ρ of $f(x)$, $-\rho$ is also a root. So, say $\alpha^2\beta^2 \equiv u \pmod{\mathfrak{p}}$. We set $a \equiv \pm\alpha\beta$ (either sign). In this case (3.2) still holds (although a may not lie in $\mathbf{Z}/p\mathbf{Z}$).

We now see by induction on n that the following congruence is true for all integers n:

$$A(n) \equiv a^nA(-n) \pmod{p}. \tag{3.3}$$

It should be noted that if $p|r$, then $A(n) \equiv 0$ (p) for all odd n, and thus the congruence (3.3) is in reality a congruence over $\mathbf{Z}$.

The reason (3.1) must be singled out as a special case is that the main criterion uses a comparison between $A(n)$ and $A(-n)$ for $n = p-1$ and $p+1$. This cannot work in the present case because both the sequences $A(n)$ and $A(-n)$ are "essentially" the same. But in the present case $A(p-1)$, $A(p+1)$ and $A(p+2)$ are easily recognized. Moreover, this case exhibits interesting behavior in its own right (see Section 4).

From (3.2) we see that we are now considering

$$f(x) \equiv x^4 - rx^3 + sx^2 - arx + a^2 \pmod{p}. \tag{3.4}$$

We note that if ρ is a root of $f(x)$, then so is a/ρ ($\rho^4 f(a/\rho) \equiv a^2 f(\rho) \equiv 0 \pmod{\mathfrak{p}}$). We see then that $\alpha, \beta, \gamma, \delta$ is a permutation of $a/\alpha, a/\beta, a/\gamma, a/\delta \bmod \mathfrak{p}$.

Indeed, assuming that $f(x)$ is unramified at p (as we do in this section), we may assume that mod $\mathfrak{p}$ the roots of $f(x)$ are

$$\alpha, \quad a/\alpha, \quad \beta, \quad a/\beta. \tag{3.5}$$

For the next discussion we assume that $r \not\equiv 0 \pmod{p}$ so that a is an integer. For a polynomial over $\mathbf{Z}$ of the shape (3.4) we see that its Galois group G (viewed as a permutation group of its roots (3.5)) must be a subgroup of the dihedral group D_4 of permutations of the square of Figure 1, i.e.

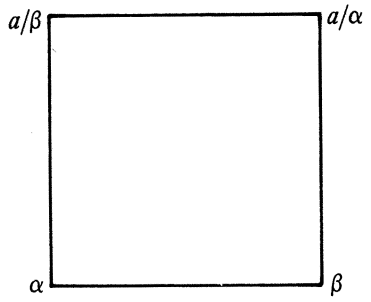

FIGURE 1

(3.6) $G < D_4 = \{\mathrm{id}, (\alpha, a/\alpha), (\beta, a/\beta), (\alpha, \beta)(a/\alpha, a/\beta), (\alpha, a/\beta)(\beta, a/\alpha), (\alpha, a/\alpha)(\beta, a/\beta), (\alpha, \beta, a/\alpha, a/\beta), (\alpha, a/\beta, a/\alpha, \beta)\}$.

Let $G_\mathfrak{p}$ be the decomposition group of $\mathfrak{p}$. Then we have the following standard criteria for the splitting type of p:

(3.7) S if and only if $G_\mathfrak{p} = \{\mathrm{id}\}$,

(3.8) 1 1 2 if and only if $G_\mathfrak{p} = \langle(\alpha, a/\alpha)\rangle$ or $\langle(\beta, a/\beta)\rangle$,

(3.9) 2 2A if and only if $G_\mathfrak{p} = \langle(\alpha, a/\alpha)(\beta, a/\beta)\rangle$,

(3.10) 2 2B if and only if $G_\mathfrak{p} = \langle(\alpha, \beta)(a/\alpha, a/\beta)\rangle$ or $\langle(\alpha, a/\beta)(\beta, a/\alpha)\rangle$,

(3.11) I if and only if $G_\mathfrak{p} = \langle(\alpha, \beta, a/\alpha, a/\beta)\rangle$.

(Here $\langle \cdots \rangle$ means the group generated by $\cdots$.)

Following D. Shanks [7] we distinguish here between two types of 2 2 splittings. Namely we say p has a 2 2A splitting if and only if $G_\mathfrak{p} = \langle(\alpha, a/\alpha)(\beta, a/\beta)\rangle$ and a 2 2B splitting otherwise. This corresponds, in D_4, to permutations which are, in Figure 1, planar rotations or not. We will see that, as in Shanks paper, this distinction is necessary.

Now $G_\mathfrak{p}$ is the Galois group of the residue class field of $\mathfrak{p}/p$ and so is cyclic and is generated by the Frobenius automorphism $\rho \to \rho^p$. Thus, for example, if p is 1 1 2 and $G_\mathfrak{p} = \langle(\alpha, a/\alpha)\rangle$, we have the relations

(3.12) $\alpha^p \equiv a/\alpha$ and $\beta^p \equiv \beta \pmod{\mathfrak{p}}$.

We note that a 1 3 splitting cannot occur (there are no 3-cycles in D_4).

We are now ready to prove the following splitting criteria.

THEOREM 3.1. *Let $f(x)$ be the polynomial* (3.4), *and let p be a prime. Assume that $a \not\equiv 0$ and $r \not\equiv 0 \pmod{p}$ and $f(x)$ does not have multiple roots* mod p. *Then $f(x)$ cannot have a* 1 3 *splitting, and the following table characterizes the possible splittings of $f(x)$* mod p.

Type	$A(p-1)$	$A(p+1)$	$aA(p-1)+A(p+1)$	$A(p+2)$
S	4	r^2-2s	$r^2-2s+4a$	$r^3-3rs+3ar$
1 1 2	$\not\equiv 4$	$\not\equiv 4a$	$r^2-2s+4a$	—
2 2A	$a^*(r^2-2s)$	$4a$	$r^2-2s+4a$	ar
2 2B	$\not\equiv a^*(s-2a)$	$\not\equiv s-2a$	$2(s-2a)$	—
I	$a^*(s-2a)$	$s-2a$	$2(s-2a)$	—

(a^* is defined by $aa^* \equiv 1 \pmod{p}$.)

Proof. To check the table for S splitting we trivially have $A(p-1) \equiv A(0)$, $A(p+1) \equiv A(2)$ and $A(p+2) \equiv A(3) \pmod{p}$, and so the result follows from (2.4) and (3.2).

Now assume $f(x)$ is split 1 1 2 mod p and by symmetry $G_{\mathfrak{p}} = \langle(\alpha, a/\alpha)\rangle$ so that (3.12) holds. Then

$$A(p-1) \equiv \alpha^{p-1} + (a/\alpha)^{p-1} + \beta^{p-1} + (a/\beta)^{p-1} \equiv a/\alpha^2 + \alpha^2/a + 2$$

and

$$A(p+1) \equiv \alpha^{p+1} + (a/\alpha)^{p+1} + \beta^{p+1} + (a/\beta)^{p+1} \equiv 2a + \beta^2 + (a/\beta)^2.$$

Hence

$$aA(p-1) + A(p+1) \equiv 4a + A(2) \pmod{p},$$

as desired. Moreover, $A(p+1) \equiv 4a \pmod{p}$ implies $(\beta - a/\beta)^2 \equiv 0 \pmod{\mathfrak{p}}$, which means p is ramified. Similarly $A(p-1) \not\equiv 4 \pmod{p}$.

Now consider the case where $f(x)$ is split 2 2. In the case 2 2A (3.9) we have

$$\alpha^p \equiv a/\alpha \quad \text{and} \quad \beta^p \equiv a/\beta \pmod{\mathfrak{p}}.$$

Hence

$$A(p-1) \equiv a/\alpha^2 + \alpha^2/a + a/\beta^2 + \beta^2/a \equiv a^* A(2)$$
$$A(p+1) \equiv 4a$$
$$A(p+2) \equiv a\alpha + a(a/\alpha) + \alpha\beta + a(a/\beta) = aA(1).$$

Switching to the case 2 2B (3.10), by symmetry we may assume that $\alpha^p = \beta$ and $\beta^p = \alpha$. Then

$$A(p-1) \equiv \beta/\alpha + \alpha/\beta + \beta/\alpha + \alpha/\beta = 2(\alpha/\beta + \beta/\alpha)$$

and

$$A(p+1) \equiv 2(\alpha\beta + a^2/\alpha\beta).$$

Hence

$$aA(p-1) + A(p+1) \equiv 2(\alpha(a/\beta) + \beta(a/\alpha) + \alpha\beta + (a/\alpha)(a/\beta))$$
$$= 2(s - 2a) \pmod{p}.$$

Moreover, $A(p+1) \equiv s - 2a$ implies $\alpha\beta + a^2/\alpha\beta - a\alpha/\beta - a\beta/\alpha \equiv 0$ or $(\alpha - a/\alpha)(\beta - a/\beta) \equiv 0 \pmod{\mathfrak{p}}$. This implies that $\mathfrak{p}$ is ramified, which we have assumed is not the case. Similarly, $A(p-1) \not\equiv a^*(s-2a) \pmod{p}$.

Finally, assume that $f(x)$ is inert mod p (3.11). Again by symmetry we may assume that $\alpha^p \equiv \beta$, and $\beta^p \equiv a/\alpha$. Then

$$aA(p-1) \equiv a\beta/\alpha + a\alpha/\beta + a^2/\alpha\beta + \alpha\beta = s - 2a$$

and

$$A(p+1) \equiv \alpha\beta + a/\alpha\beta + \beta a/\alpha + \alpha a/\beta = s - 2a.$$

It remains to show that the table of Theorem 3.1 characterizes the splitting type. Checking the table we see that the only confusion that could occur is when $r^2 - 2s + 4a \equiv 2(s-2a) \pmod{p}$ or, when this is not the case, the only remaining possible ambiguity is between S and 2 2A. Both of these possibilities imply multiple roots as we see in Lemma 3.2. Thus Theorem 3.1 is completely proved once Lemma 3.2 is proved. □

LEMMA 3.2. *Let* $f(x)$ *be the polynomial of* (3.4) *with* $a \not\equiv 0 \pmod p$. *Then*

(1) $r^2 - 2s + 4a \equiv 2(s - 2a) \pmod p$ *if and only if, for some integer* r_1, $f(x) \equiv (x^2 - r_1x + a)^2 \pmod p$.

(2) (a) $r \equiv 0 \pmod p$ *and* $r^2 - 2s \equiv 4a \pmod p$ *if and only if* $f(x) \equiv (x^2 - a)^2 \pmod p$.

(b) $r \not\equiv 0 \pmod p$ *and* $r^2 - 2s \equiv 4a \pmod p$ *and* $ar \equiv r^3 - 3rs + 3ar \pmod p$ *if and only if* $f(x) \equiv (x - r/4)^4 \pmod p$.

Proof. In (1) if $p = 2$, let $r_1 = s$, and if $p > 2$, let $r_1 = r/2$. Part (2)(a) is immediate. In part (2)(b) we see $p \neq 2$ (so $r/4$ is defined). Since $r \not\equiv 0$, we may solve $2s = r^2 - 4a$ and $3s \equiv r^2 + 2a$ to obtain $s \equiv 6a$ and $r^2 \equiv 16a$, from which the result is straightforward. □

It remains to consider the case where $r \equiv 0 \pmod p$ so that, by (3.1), $t \equiv 0 \bmod p$. Now, if ρ is a root, so is $-\rho$. The roots may be taken to be α, $-\alpha$, β, $-\beta$. Then we have $G < D_4$, where D_4 is the group of permutations of the square in Figure 2.

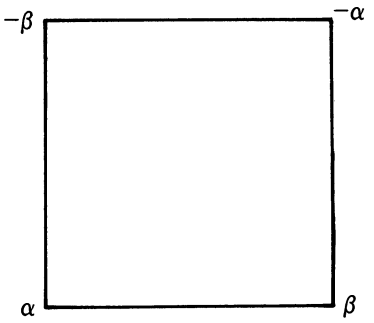

FIGURE 2

With this modification the discussions of the splitting of $f(x)$ and the decomposition groups is the same. For example, 2 2A now means $G_\mathfrak{p} = \langle(\alpha, -\alpha)(\beta, -\beta)\rangle$. We may now state

THEOREM 3.3. *Let* $f(x) \equiv x^4 + sx^2 + u \pmod p$. *Assume* $f(x)$ *does not have multiple roots* mod p (*so* $u \not\equiv 0 \pmod p$). *Then* $p \neq 2$ *and* p *cannot have a* 1 3 *splitting. Moreover, the following tables characterize the possible splittings of* $f(x)$ mod p.

	$s \not\equiv 0 \pmod p$		$s \equiv 0 \pmod p$		
Type	$A(p-1)$	$A(p+1)$	$A(p-1)$	$A(p+1)$	$(A(p+1)/4)^2$
S	4	$-2s$	4	0	—
1 1 2	0	$\not\equiv 0$	0	$\not\equiv 0$	$-u$
2 2A	-4	$2s$	-4	0	—
2 2B	$\not\equiv 0$	$\not\equiv \pm 2s, 0$	0	$\not\equiv 0$	u
I	$\not\equiv 0$	0	$\not\equiv 0, \pm 4$	0	—

Proof. The table obviously characterizes the splitting once we know it is correct. We do not assume anything about s until it is necessary. For an S prime we have $A(p-1) \equiv A(0) \equiv 4$ and $A(p+1) \equiv A(2) \equiv -2s \pmod p$. For a 1 1 2 prime we

may assume by symmetry that $G_{\mathfrak{p}} = \langle(\beta, -\beta)\rangle$, and so $\alpha^p \equiv \alpha$, $\beta^p \equiv -\beta$. Then $A(p-1) \equiv 2 - 2 = 0$ and $A(p+1) \equiv 2(\alpha^2 - \beta^2)$. If $A(p+1) \equiv 0$, then $\alpha \equiv \pm\beta$, violating the assumption of no multiple roots. Finally, $(A(p+1)/4)^2 \equiv ((\alpha^2+\beta^2)^2 - 2\alpha^2\beta^2)/2 \equiv -u$ if $s \equiv 2(\alpha^2+\beta^2) \equiv 0$.

For a 2 2A prime we have $\alpha^p \equiv -\alpha$, $\beta^p \equiv -\beta$, and so $A(p-1) \equiv -4$ and $A(p+1) \equiv -2(\alpha^2+\beta^2) \equiv -A(2)$. For a 2 2$B$ prime we may assume by symmetry that $\alpha^p \equiv \beta$ and $\beta^p \equiv \alpha$. Then

$$A(p-1) \equiv 2(\beta/\alpha + \alpha/\beta) = 1/\alpha\beta, \qquad A(2) = -2s/\alpha\beta \equiv 0 \pmod{p}$$

if and only if $s \equiv 0 \pmod{p}$. Also $A(p+1) \equiv 4\alpha\beta \not\equiv 0 \pmod{p}$. Moreover, $(A(p+1)/4)^2 \equiv \alpha^2\beta^2 \equiv u$.

For an I prime we may assume, by symmetry, that $\alpha^p \equiv \beta$, and $\beta^p \equiv -\alpha$. Then $A(p+1) \equiv 2(\alpha\beta - \beta\alpha) \equiv 0$. Also $A(p-1) \equiv 2(\beta/\alpha - \alpha/\beta) \equiv 0 \mod p$ if and only if $\alpha \equiv \pm\beta$, which violates our assumptions. □

4. Comparison to Some Work of D. Shanks. We now compare the situation in Section 3 with the similar discussion given by D. Shanks [7].

For simplicity we assume the polynomial $f(x)$ in (3.4) is irreducible. We have, (3.5), the roots of $f(x)$ given by α, a/α, β, a/β and the Galois group G of f in (3.6) with $G < D_4$. We identify the subgroups of order 4 in D_4:

$$C_4 = \langle(\alpha, \beta, a/\alpha, a/\beta)\rangle,$$
$$V_4 = \{\mathrm{id}, (\alpha,\beta)(a/\alpha, a/\beta), (\alpha, a/\alpha)(\beta, a/\beta), (\alpha, a/\beta)(\beta, a/\alpha)\},$$
$$V_4' = \{\mathrm{id}, (\alpha, a/\alpha), (\beta, a/\beta), (\alpha, a/\alpha)(\beta, a/\beta)\}.$$

Let Δ = discriminant of $f(x)$. Let A_4 = alternating subgroup of the symmetric group $S_4 = S_4(\alpha, a/\alpha, \beta, a/\beta)$.

We note that $\sqrt{\Delta} \in \mathbf{Q}$ if and only if $G < A_4 \cap D_4 = V_4$. Moreover, if $\sqrt{\Delta} \in \mathbf{Q}(\alpha) - \mathbf{Q}$, then $G \not\subseteq A_4$, $\mathbf{Q}(\sqrt{\Delta})$ is the fixed field of $A_4 \cap G$ while $\mathbf{Q}(\alpha)$ is the fixed field of $\{\mathrm{id}, (\alpha, a/\alpha)\} \cap G$; hence $G = C_4$. Conversely, $G = C_4$ implies $\sqrt{\Delta} \in K = \mathbf{Q}(\alpha)$, and $(\alpha, \beta, a/\alpha, a/\beta)(\sqrt{\Delta}) = -\sqrt{\Delta}$ implies $\sqrt{\Delta} \notin \mathbf{Q}$. Finally, if $\sqrt{\Delta} \notin \mathbf{Q}(\alpha)$, then $[K : \mathbf{Q}] = 8$, and so $G = D_4$. We have

$$G = V_4 \quad \text{if and only if} \quad \sqrt{\Delta} \in \mathbf{Q},$$
$$G = C_4 \quad \text{if and only if} \quad \sqrt{\Delta} \in \mathbf{Q}(\alpha) - \mathbf{Q},$$
$$G = D_4 \quad \text{if and only if} \quad \sqrt{\Delta} \notin \mathbf{Q}(\alpha).$$

Set

$$\Delta_1 = r^2 - 4s + 8a, \qquad \Delta_2 = (s + 2a)^2 - 4ar^2.$$

Then, using the identities $r = \alpha + a/\alpha + \beta + a/\beta$ and $s = 2a + \alpha\beta + a\alpha/\beta + a\beta/\alpha + a^2/\alpha\beta$, we easily derive

$$\Delta_1 = -a^{-1}(\alpha - \beta)(a/\alpha - a/\beta)(\alpha - a/\beta)(\beta - a/\alpha), \tag{4.1}$$

$$\Delta_2 = [(\alpha - a/\alpha)(\beta - a/\beta)]^2. \tag{4.2}$$

Thus we immediately deduce that

$$\Delta = a^2\Delta_1^2\Delta_2. \tag{4.3}$$

Now K contains the quadratic subfield $\mathbf{Q}(\alpha + a/\alpha) = \mathbf{Q}(\sqrt{\Delta_1})$, since

$$(x - (\alpha + a/\alpha))(x - (\beta + a/\beta)) = x^2 - rx + s - 2a$$

is a quadratic polynomial with discriminant Δ_1. It is the fixed field of $V_4' \cap G$. Hence, for a rational prime p and a prime $\mathfrak{p}$ of K lying over p, we have $\alpha + a/\alpha \equiv$ rational integer mod $\mathfrak{p}$ if and only if $G_{\mathfrak{p}}$ fixes $\alpha + a/\alpha$ if and only if $G_{\mathfrak{p}} < V_4'$. Checking the decomposition groups (3.7)–(3.11), we see that this is equivalent to p being S, 1 1 2 or 2 2A. Similarly, let $\rho = (\alpha - a/\alpha)(\beta - a/\beta)$, so that $\rho^2 = \Delta_2$. ρ is fixed by V_4, and so $(\Delta_2/p) = 1$ if and only if $G_{\mathfrak{p}} < V_4$ if and only if p is S or 2 2. Thus we have the following splitting criteria:

$$(4.4)\qquad \begin{cases} S \text{ or } 2\,2A & \text{if and only if } \left(\dfrac{\Delta_1}{p}\right) = \left(\dfrac{\Delta_2}{p}\right) = 1, \\ 2\,2B & \text{if and only if } \left(\dfrac{\Delta_1}{p}\right) = -1, \left(\dfrac{\Delta_2}{p}\right) = 1, \\ 1\,1\,2 & \text{if and only if } \left(\dfrac{\Delta_1}{p}\right) = 1, \left(\dfrac{\Delta_2}{p}\right) = -1, \\ I & \text{if and only if } \left(\dfrac{\Delta_1}{p}\right) = \left(\dfrac{\Delta_2}{p}\right) = -1. \end{cases}$$

We see that we may distinguish between all splitting types except S and 2 2A by congruences. Hence, if it is convenient, Theorem 3.1 need only be applied to those primes p such that both Δ_1 and Δ_2 are quadratic residues mod p.

Another distinction between the 2 2A and 2 2B primes may be noted. Namely, $\mathbf{Q}(\alpha)$ contains the quadratic subfield $\mathbf{Q}(\alpha + a/\alpha)$ whose primes p are split or inert according as $(\Delta_1/p) = 1$ or not. A split prime may move up to $\mathbf{Q}(\alpha)$ as an S, 1 1 2 or 2 2 prime, and an inert prime may move up as an 2 2 or I prime. Noting (4.4), we get the following more precise version:

$\mathbf{Q}(\alpha + a/\alpha)$	$\mathbf{Q}(\alpha)$
Split	S, 2 2A, 1 1 2
Inert	I, 2 2 B.

Finally, to tie in with the section on ramified primes, Section 6, we note that the decomposition (4.3) for Δ gives some information on the splitting type of a ramified prime. So let $p|\Delta$, $p \nmid a$ be a prime, and let $\mathfrak{p}$ lie over p. Using the expressions (4.1) and (4.2) for Δ_1 and Δ_2, it is easy to verify the following criteria:

$p|\Delta_1$ and $p|\Delta_2$ if and only if all roots are the same mod $\mathfrak{p}$,

$p|\Delta_1$ and $p \nmid \Delta_2$ if and only if two pairs of roots are the same mod $\mathfrak{p}$,

$p \nmid \Delta_1$ and $p|\Delta_2$ if and only if there are exactly three distinct roots mod $\mathfrak{p}$.

The first is Case I in Table 6.1, the second is Cases III, IV and the third is Cases V, VI (Case II cannot occur).

5. Nonreciprocal Quartics. We now give the criteria for polynomials and primes not covered by Theorem 3.1, for which $p \nmid u$.

THEOREM 4.1. *Let $f(x) = x^4 - rx^3 + sx^2 - tx + u$ be a polynomial with integer coefficients. Let p be a rational prime. We assume that $f(x)$ does not have multiple roots* mod p, *$p \nmid u$ and $ur^2 \not\equiv t^2$* (mod p). *Then the following table characterizes the splitting of $f(x)$* mod p.

Type	$A(p-1) \equiv A(-p+1)(p)$?	$A(p+1) \equiv uA(-p-1)(p)$?	$A(p-1) \equiv 4(p)$?
S	Yes	No	Yes
1 1 2	Yes	No	No
1 3	No	No	
2 2	Yes	Yes	
I	No	Yes	

Proof. The table clearly characterizes the cases. So we need only prove it is valid. We use the criteria (2.6). Recall that the reverse sequence ($A(n)$ for negative n) is defined in (2.7).

If p is an S prime, then trivially $A(p-1) \equiv A(-p+1) \equiv 4$, $A(p+1) \equiv A(2) \equiv r^2 - 2s$ and $A(-p-1) \equiv A(-2) \equiv (u^*t)^2 - 2u^*s \pmod{p}$. We see that $A(p+1) \equiv A(-p-1) \pmod{p}$ is equivalent to $ur^2 \equiv t^2 \pmod{p}$.

For the remainder of the proof it is convenient to make the following observation. Set

$$\begin{aligned} f_k(x) &= (x-\alpha^k)(x-\beta^k)(x-\gamma^k)(x-\delta^k) \\ &= x^4 - A(k)x^3 + S(k)x^2 - u^kA(-k)x + u^k \end{aligned}$$

for some integer $S(k)$. Then let p be an unramified prime with $\mathfrak{p}$ above it as before. First we have

$$f_{p-1}(x) \equiv x^4 - A(p-1)x^3 + S(p-1)x^2 - A(-p+1)x + 1 \pmod{p},$$

and so we see

$$\text{(5.1)} \qquad \begin{cases} A(p-1) \equiv A(-p+1) \pmod{p} & \text{if and only if} \\ \{\alpha^{p-1}, \beta^{p-1}, \gamma^{p-1}, \delta^{p-1}\} \\ \equiv \{1/\alpha^{p-1}, 1/\beta^{p-1}, 1/\gamma^{p-1}, 1/\delta^{p-1}\} \pmod{\mathfrak{p}}.* \end{cases}$$

Moreover,

$$f_{p+1}(x) \equiv x^4 - A(p+1)x^3 + S(p+1)x^2 - u^2A(-p-1)x + u^2 \pmod{p}.$$

Thus, as we saw in Section 3,

$$\text{(5.2)} \qquad \begin{cases} A(p+1) \equiv uA(-p+1) \pmod{p} & \text{if and only if} \\ \{\alpha^{p+1}, \beta^{p+1}, \gamma^{p+1}, \delta^{p+1}\} \\ \equiv \{u/\alpha^{p+1}, u/\beta^{p+1}, u/\gamma^{p+1}, u/\delta^{p+1}\} \pmod{\mathfrak{p}}. \end{cases}$$

Now, if p is a 1 1 2 prime, then $A(p-1) \equiv 1 + 1 + \delta/\gamma + \gamma/\delta \equiv A(-p+1) \pmod{p}$ and $A(p-1) \not\equiv 4 \pmod{p}$, or else $\gamma \equiv \delta$. If $A(p+1) \equiv uA(-p-1) \pmod{p}$, then (5.2) yields

$$\{\alpha^2, \beta^2, \gamma\delta, \gamma\delta\} \equiv \{u/\alpha^2, u/\beta^2, u/\gamma\delta, u/\gamma\delta\} \pmod{\mathfrak{p}},$$

from which we easily deduce that $(\gamma\delta)^2 \equiv u \pmod{\mathfrak{p}}$. Then $\alpha\beta\gamma\delta = u$ implies

* Here we mean that the two sets are the same mod $\mathfrak{p}$, counting multiplicities.

$(\alpha\beta)^2 \equiv u \pmod p$ as well, and we see that

$$t^2 = u^2(\alpha^{-1} + \beta^{-1} + \gamma^{-1} + \delta^{-1})^2 \tag{5.3}$$
$$= \frac{u^2}{(\alpha\beta)^2}(\alpha + \beta + \gamma + \delta)^2 \equiv ur^2 \pmod p,$$

violating the hypothesis.

If p is a 1 3 prime, then from (5.1) we see that $A(p-1) \equiv A(-p+1) \pmod p$ implies

$$\left\{1, \frac{\gamma}{\beta}, \frac{\delta}{\gamma}, \frac{\beta}{\delta}\right\} \equiv \left\{1, \frac{\beta}{\gamma}, \frac{\gamma}{\delta}, \frac{\delta}{\beta}\right\} \pmod{\mathfrak{p}},$$

which is trivially seen to imply that two of β, γ, δ are the same mod $\mathfrak{p}$. If $A(p+1) \equiv uA(-p-1) \pmod p$, then (5.2) yields $\{\alpha^2, \beta\gamma, \gamma\delta, \delta\beta\} \equiv \{u\alpha^{-2}, u/\beta\gamma, u/\gamma\delta, u/\delta\beta\} \pmod{\mathfrak{p}}$. It is then easily checked that this implies that two of α, β, γ, δ are the same (mod $\mathfrak{p}$).

If p is a 2 2 prime, it is trivially seen that the sets in (5.1) and (5.2) are the same.

Finally, if p is an I prime, it is again clear that the two sets in (5.2) are the same. If, on the other hand, $A(p-1) \equiv A(-p+1) \pmod p$, then

$$\left\{\frac{\beta}{\alpha}, \frac{\gamma}{\beta}, \frac{\delta}{\gamma}, \frac{\alpha}{\delta}\right\} \equiv \left\{\frac{\alpha}{\beta}, \frac{\beta}{\gamma}, \frac{\gamma}{\delta}, \frac{\delta}{\alpha}\right\} \pmod{\mathfrak{p}}.$$

Since p is unramified, there are two possibilities. First, $\alpha/\beta \equiv \beta/\alpha$ implies that $\delta/\gamma \equiv \gamma/\delta$, and so $\alpha \equiv -\beta$ and $\gamma \equiv -\delta$ which implies, since $\alpha\beta\gamma\delta = u$, that $(\alpha\gamma)^2 \equiv u$; and then exactly as in (5.3) we get $ur^2 \equiv t^2 \pmod p$. Second, $\alpha/\beta \equiv \delta/\gamma$ or $\alpha\gamma \equiv \beta\delta \pmod{\mathfrak{p}}$; again using $\alpha\beta\gamma\delta = u$, we derive a contradiction as in (5.3). □

6. Ramified Quartics. The above procedures have all assumed that $f(x)$ does not have multiple roots mod p, i.e. p is unramified. We now outline an ad hoc procedure to deal with the ramified primes.

The discriminant Δ of $f(x)$ is given by (see [4, p. 184])

$$27\Delta = 4(s^2 - 3rt + 12u)^3 - (2s^3 - 72su + 27r^2u - 9rst + 27t^2)^2.$$

Here we continue to assume Eq. (2.1): $f(x) = x^4 - rx^3 + sx^2 - tx + u$ (but we allow $p|u$). Of course, p is ramified if and only if $p|\Delta$, which we assume from now on in this section.

Determining the splitting type of $f(x)$ mod p amounts to determining the degree of each factor (f) and the power to which it occurs (e). There are six possibilities which are summarized in Table 6.1. The first column list the e's and f's. The second gives the explicit factorization of $f(x)$ over $\mathbf{Z}/p\mathbf{Z}$: here all the factors listed are assumed irreducible and distinct. The third column shows the greatest common divisor of $f(x)$ and its derivative $f'(x)$, while the fourth simply gives the degree of $\gcd(f, f')$. The table is valid for $p > 3$. The cases $p = 2, 3$ are easy to deal with separately.

TABLE 6.1

	$efefef$	$f(x)$	$\gcd(f, f')$	$\deg \gcd(f, f')$
I	4 1	$(x-a)^4$	$(x-a)^3$	3
II	3 1 1 1	$(x-a)^3(x-b)$	$(x-a)^2$	2
III	2 2	$(x^2-vx+w)^2$	x^2-vx+w	2
IV	2 1 2 1	$(x-a)^2(x-b)^2$	$(x-a)(x-b)$	2
V	2 1 1 1 1	$(x-a)^2(x-b)(x-c)$	$x-a$	1
VI	2 1 1 2	$(x-a)^2(x^2-vx+w)$	$x-a$	1

After establishing that $p|\Delta$, the next step is to compute $g(x) = \gcd(f(x), f'(x))$. Now the totally ramified case is detected ($\deg g = 3$), and Cases II, III, IV ($\deg g = 2$) are separated from Cases V, VI ($\deg g = 1$).

Write $g(x) = x^2 - vx + w$ in Cases II, III, IV. Then we may distinguish between these three cases simply by computing $D = v^2 - 4w$. Indeed, $D \equiv 0 \pmod p$ if and only if we are in Case II. Otherwise, the Legendre symbol $(D/p) = 1$ if and only if we are in Case IV.

Finally, to distinguish between Cases V, VI we simply compute $f(x)/g(x)^2 = x^2 - vx + w$ and again check the value of $((v^2 - 4w)/p)$.

7. Cubic and Quadratic Polynomials. Let

$$g(x) = x^3 - vx^2 + wx - q \tag{7.1}$$

be a cubic polynomial with integer coefficients. Define $A_g(n)$ as in (1.1). Let p be a prime, $p \nmid q$, such that $g(x)$ is unramified mod p. Then for $p \geqslant 7$ we may choose an integer i such that $(iq/p) = -1$ and $f(x) = g(x)(x - i)$ is unramified mod p. The first condition guarantees $f(x)$ is not a generalized reciprocal quartic (condition (3.1)). We have

$$A_f(n) \equiv i^n + A_g(n) \pmod p$$

for any integer n. In particular, $A_f(p-1) \equiv 1 + A_g(p-1)$ and $A_f(-p+1) \equiv 1 + A_g(-p+1) \pmod p$. Moreover, the splitting type of f and g are directly related:

g	f
S	S
1 2	1 1 2
I	1 3

where, as usual, S means split completely and I means irreducible (or inert). Thus we may apply Theorem 4.1 to obtain the following theorem (the cases of $p = 2, 3, 5$ are easily verified).

THEOREM 7.1. *Let $g(x)$ be given by* (7.1) *with integer coefficients. Let p be a rational prime such that $g(x)$ has no multiple roots* mod p *and $p \nmid q$. Then the following table characterizes the splitting of $g(x)$* mod p *(here $A_g(n) = A(n)$).*

Type	$A(p-1) \equiv A(-p+1)(p)$?	$A(p-1) \equiv 3(p)$?
S	Yes	Yes
1 2	Yes	No
I	No	

This theorem is implicit in [1]. Ramified primes can be handled as in Section 6.

We now go back to the quartic polynomial $f(x) = x^4 - rx^3 + sx^2 - tx + u$ of (2.1). Before we assumed that $p \nmid u$, so we now assume $p|u$. If $p|t$ as well, then $f(x)$ is ramified, and we discussed this case in Section 6. Set $g(x) = x^3 - rx^2 + sx - t$. Then g is unramified if f is. Moreover, $A_g(n) \equiv A_f(n) \pmod{p}$ for any integer n. Hence we conclude.

COROLLARY 7.2. *Let $f(x)$ be given by* (2.1) *as usual. Assume that p is a rational prime, $p|u$, $p \nmid t$ and $f(x)$ is not ramified at p. Then the following table characterizes the splitting of $f(x) \bmod p (A_f(n) = A(n))$.*

Type	$A(p-1) \equiv A(-p+1)(p)$?	$A(p-1) \equiv 3(p)$?
S	Yes	Yes
1 1 2	Yes	No
1 3	No	

Applying precisely the same procedure as above for deducing Theorem 7.1 from the quartic case, we obtain the following result, trivially derived independently.

THEOREM 7.3. *Let $h(x) = x^2 - vx + w$ be a polynomial with integer coefficients. Let p be a rational prime such that $p \nmid w$ and $h(x)$ is not ramified* mod p. *Define $A(n)$ for $h(x)$ as above* (*Eq.* (1.1)). *Then $h(x)$ splits* mod p *if and only if* $A(p-1) \equiv 2 \pmod{p}$.

8. Algorithm for Quartic Splitting. In this section we will compile the results of the previous sections and present the complete procedure for determining the splitting type of a quartic polynomial modulo a prime. The notation is given in Eqs. (2.1), (2.3), (2.4), and (2.7). We assume that we are given the polynomial $f(x)$ and the prime p in advance. All computations below are done mod p.

Case I. The discriminant $\Delta \equiv 0 \pmod{p}$.

Compute $g(x) \equiv \gcd(f(x), f'(x))$.
If $\deg g = 3$ then f, p is totally ramified $e = 4, f = 1$ else
If $\deg g = 2$ write $g(x) = x^2 - vx + w$
  If $v^2 \equiv 4w$ then $f(x) \equiv (x-a)^3(x-b)$
  else if $((v^2 - rw)/p) = 1$ then $f(x) \equiv (x-a)^2(x-b)^2$
    else $f(x) \equiv (x^2 - vx + w)^2$
else $\deg g = 1$, write $f(x)/g(x)^2 \equiv x^2 - vx + w$
  If $((v^2 - 4w)/p) = 1$ then $f(x) \equiv (x-a)^2(x-b)(x-c)$
  else $f(x) \equiv (x-a)^2(x^2 - vx + w)$.

Case II. $\Delta \not\equiv 0 \pmod{p}$ and $p|u$.

Compute $A(p-1), A(-p+1)$
If $A(p-1) \equiv A(p+1)$ then
  if $A(p-1) \equiv 3$ then p is an S prime
  else p is 1 1 2 prime
else p is 1 3 prime.

Case III. $\Delta \not\equiv 0 \pmod p$, $u \not\equiv 0 \pmod p$ and $r \equiv s \equiv t \equiv 0 \pmod p$.
Compute $A(p-1), A(p+1)$
If $A(p+1) \equiv 0$ then
if $A(p-1) \equiv 4$ then p is S
else if $A(p-1) \equiv -4$ then p is $2\ 2A$
else p is I
else if $(A(p+1)/4)^2 \equiv u$ then p is $2\ 2B$
else p is $1\ 1\ 2$.

Case IV. $\Delta \not\equiv 0 \pmod p$, $u \not\equiv 0 \pmod p$ and $r \equiv t \equiv 0 \pmod p$, $s \not\equiv 0 \pmod p$.
Compute $A(p-1), A(p+1)$
If $A(p-1) \equiv 0$ then p is $1\ 1\ 2$
else if $A(p+1) \equiv 0$ then p is I
else if $A(p+1) \equiv 2s$ then p is $2\ 2A$
else if $A(p+1) \equiv -2s$ then p is S
else p is $2\ 2B$.

Case V. $\Delta \not\equiv 0 \pmod p$, $u \not\equiv 0 \pmod p$, $r \not\equiv 0 \pmod p$ and $ur^2 \equiv t^2 \pmod p$.
Compute $a \equiv t/r, A(p-1), A(p+1), A(p+2), A \equiv aA(p-1) + A(p+1)$
If $A \equiv 2(s - 2a)$ then
if $A(p+1) \equiv s - 2a$ then p is I
else p is $2\ 2B$
else if $A(p-1) \equiv 4$ then
if $r^2 - 2s \equiv 4a$ then
if $A(p+2) \equiv ar$ then p is $2\ 2A$
else p is S
else p is S
else if $A(p+1) \equiv 4a$ then p is $2\ 2A$
else p is $1\ 1\ 2$.

Case VI. $\Delta \not\equiv 0 \pmod p$, $u \not\equiv 0 \pmod p$, $ur^2 \not\equiv t^2 \pmod p$.
Compute $A(p-1), A(-p+1), A(p+1), A(-p-1)$
If $A(p-1) \equiv A(-p+1)$ then
if $A(p+1) \equiv uA(-p-1)$ then p is $2\ 2$
else if $A(p-1) \equiv 4$ then p is S
else p is $1\ 1\ 2$
else if $A(p+1) \equiv uA(-p-1)$ then p is I
else p is $1\ 3$.

Department of Mathematics
Institute for Physical Sciences and Technology
University of Maryland
College Park, Maryland 20742

1. W. W. ADAMS & D. SHANKS, "Strong primality tests that are not sufficient," *Math. Comp.*, v. 39, 1982, pp. 255–300.
2. E. BERLEKAMP, "Factoring polynomials over finite fields," *Bell System Tech. J.*, v. 46, 1967, pp. 1853–1859.
3. L. CARLITZ, "A special quartic congruence," *Math. Scand.*, v. 4, 1956, pp. 243–246.

4. B. N. DELONE & D. K. FADEEV, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., 1964.

5. D. E. KNUTH, *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1980.

6. S. SCHWARZ, "Sur le nombre des racines et des facteurs irréductibles d'une congruence donnée," *Časopis Pěst. Mat. Fys.*, v. 69, 1940, pp. 128–145.

7. D. SHANKS, "Dihedral quartic approximations and series for π," *J. Number Theory*, v. 14, 1982, pp. 397–423.

8. D. SHANKS, *Prime-Splitting in Associated Cubic and Quartic Fields: Some Implications and Some Techniques*. (To appear.)