Irreducible Quartic Polynomials with Factorizations modulo *p*

Eric Driver, Philip A. Leonard, and Kenneth S. Williams

1. INTRODUCTION. In a discussion of irreducibility criteria in their fine algebra text, Dummit and Foote include the following remark [**4**, p. 310]:

> Unfortunately, there are examples of polynomials even in $\mathbb{Z}[x]$ which are irreducible but whose reductions modulo every ideal are reducible.... For example, the polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime...and the polynomial $x^4 - 72x^2 + 4$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every integer.

The matter is then put on hold until Galois theory is treated five chapters later.

The reason for the reducibility modulo p of the cited polynomials is that they have the Klein 4-group V as their Galois groups, so factorization modulo p follows from the cycle structure of permutations in this group [**4**, Corollary 41, p. 622]. But this and the related discussion of density [**4**, pp. 623 ff.] are much more advanced topics. We shall provide an elementary treatment both of the examples cited and of families of related polynomials so that instructors might explore this phenomenon in a bit more detail earlier in the sequence of topics. In the course of doing so, we shall revisit several sources, including a recent Putnam Mathematical Competition question and a few items from the "ancient history" of polynomial factorization. The question of reducibility modulo p can be treated rather easily for the polynomials we consider. For certain families we discuss reducibility modulo every integer in some detail.

2. BIQUADRATIC POLYNOMIALS MODULO *p*. Our attention in this section focuses on monic polynomials f of the form

$$f(x) = x^4 + rx^2 + s,$$

where r and s are integers. Although some authors use "quartic" and "biquadratic" as synonyms, we follow Kappe and Warren [**5**] (among others) and reserve the latter term for polynomials of this special type. We ask which among them are irreducible over $\mathbb{Z}$ yet reducible modulo p for each prime p. We also investigate in section 3 the additional property of being reducible modulo n for every integer n larger than 1.

It is convenient to begin by giving a necessary and sufficient condition for $f(x)$ to be reducible in $\mathbb{Z}[x]$. We prove:

Theorem 1. *Let r and s be integers. Then $f(x) = x^4 + rx^2 + s$ is reducible in $\mathbb{Z}[x]$ if and only if there exist integers a, c, and e satisfying*

$$c + e - a^2 - r = 0, \tag{1}$$

$$a(e - c) = 0, \tag{2}$$

and

$$ce - s = 0, \tag{3}$$

in which case

$$f(x) = (x^2 + ax + c)(x^2 - ax + e). \tag{4}$$

Proof. Suppose that $f(x)$ is reducible in $\mathbb{Z}[x]$. Then $f(x)$ has either a linear factor $x - m$ in $\mathbb{Z}[x]$ or an irreducible quadratic factor $x^2 + ax + c$ in $\mathbb{Z}[x]$. In the former case, if $m \neq 0$ then $f(x)$ also has the second factor $x + m$, making it divisible by $x^2 - m^2$ in $\mathbb{Z}[x]$, whereas if $m = 0$ then $f(x)$ is clearly divisible by x^2. In both cases $f(x)$ has a quadratic factor $x^2 + ax + c$ belonging to $\mathbb{Z}[x]$. Thus

$$x^4 + rx^2 + s = (x^2 + ax + c)(x^2 + tx + e)$$

for integers t and e. Equating coefficients of x^3, we conclude that $t = -a$ and (4) follows. Equating coefficients of x^2, x, and 1, we obtain (1), (2), and (3), respectively.

Conversely, suppose that (1), (2), and (3) hold. Then

$$\begin{aligned}(x^2 + ax + c)(x^2 - ax + e) &= x^4 + (c + e - a^2)x^2 + a(e - c)x + ce \\ &= x^4 + rx^2 + s,\end{aligned}$$

whence $f(x)$ is reducible in $\mathbb{Z}[x]$. ■

We now continue to develop the reducibility criteria for $f(x)$. In what follows, we often write $n = \square$ to indicate that an integer n is a perfect square. Since $r^2 - 4s$ is the discriminant of the quadratic $f(x^{1/2})$, it is reasonable to suspect that whether $r^2 - 4s$ is a perfect square or not will have an effect on if and how $f(x)$ reduces. Indeed, the next two corollaries to Theorem 1 show how the factorization of $f(x)$ depends on the quantity $r^2 - 4s$. In particular, when $r^2 - 4s = \square$, then $f(x)$ factors into a product of two quadratics with no linear terms; and when $r^2 - 4s \neq \square$ and $f(x)$ is reducible, it must factor into two quadratics with linear terms.

Corollary 1. *Let r and s be integers such that $r^2 - 4s$ is a perfect square, say $r^2 - 4s = t^2$ ($t \in \mathbb{Z}$). Then $f(x) = x^4 + rx^2 + s$ is reducible in $\mathbb{Z}[x]$, and*

$$f(x) = \left(x^2 + \tfrac{1}{2}(r - t)\right)\left(x^2 + \tfrac{1}{2}(r + t)\right).$$

Corollary 2. *Let r and s be integers such that $r^2 - 4s$ is not a perfect square. Then $f(x) = x^4 + rx^2 + s$ is reducible in $\mathbb{Z}[x]$ if and only if there exists an integer c such that*

$$c^2 = s, \qquad 2c - r = \square,$$

in which case

$$f(x) = (x^2 + ax + c)(x^2 - ax + c),$$

where a is an integer such that $a^2 = 2c - r$.

As Corollaries 1 and 2 are simple consequences of Theorem 1, we leave their proofs to the reader.

We remark that, if r and s are integers such that $r^2 - 4s \neq \square$ and if $x^4 + rx^2 + s$ is reducible in $\mathbb{Z}[x]$, then the integer c of Corollary 2 satisfies

$$(2c - r)(-2c - r) = r^2 - 4c^2 = r^2 - 4s \neq \square,$$

so that

$$2c - r \neq 0, \qquad -2c - r \neq \square.$$

Since $\pm c$ are the only integers for which $c^2 = s$, this shows that c is unique.

The polynomials cited in the introduction provide good illustrations for this result. In the case of $x^4 + 1$ we have $r = 0$, $s = 1$, and $r^2 - 4s = -4 \neq \square$. Because there does not exist an integer c satisfying $c^2 = 1$ and $2c = \square$, we conclude on the basis of Corollary 2 that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$. With $x^4 - 72x^2 + 4$ we reach the same conclusion: here $r = -72$, $s = 4$, and $r^2 - 4s = 5168 \neq \square$, and there does not exist an integer c such that $c^2 = 4$ and $2c + 72 = \square$.

A nice example of a family of biquadratics for which reducibility in $\mathbb{Z}[x]$ is easily decided was given in a recent Putnam Competition [**8**, Problem A3], where the polynomials

$$P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2 \qquad (m \in \mathbb{Z})$$

were introduced. Here $r = -(2m + 4)$ and $s = (m - 2)^2$, which means that

$$r^2 - 4s = (2m + 4)^2 - 4(m - 2)^2 = 32m$$

is a perfect square if and only if $2m$ is a perfect square. If $2m$ is a square, then $m = 2u^2$ for some integer u and, by Corollary 1, we have

$$P_m(x) = (x^2 - (2u^2 - 4u + 2))(x^2 - (2u^2 + 4u + 2)).$$

If $2m$ is not a perfect square then, again by Corollary 2, $P_m(x)$ is reducible if and only if $\pm 2(m - 2) + 2m + 4 = \square$, which happens if and only if $m = t^2$ for some t in $\mathbb{Z}$, in which case

$$P_m(x) = (x^2 + 2tx + t^2 - 2)(x^2 - 2tx + t^2 - 2).$$

Thus $P_m(x)$ is irreducible in $\mathbb{Z}[x]$ except when m or $2m$ is a perfect square.

So far we have considered the reducibility criteria for $f(x) = x^4 + rx^2 + s$ over $\mathbb{Z}$. We now turn our attention to the other half of the problem, namely, to reducibility criteria for $f(x)$ over $\mathbb{Z}/p^k\mathbb{Z}$, where p is a prime and k is a positive integer. Our next theorem is the direct analog of Theorem 1, and its proof is similar enough to the proof of that result to be left to the reader.

Theorem 2. *Let p be a prime, and let k be a positive integer. Then a polynomial $f(x) = x^4 + rx^2 + s$ in $\mathbb{Z}[x]$ is reducible modulo p^k if and only if there exist integers a, c, and e satisfying*

$$c + e - a^2 - r \equiv 0 \pmod{p^k}, \tag{5}$$

$$a(e - c) \equiv 0 \pmod{p^k}, \tag{6}$$

and

$$ce - s \equiv 0 \pmod{p^k}, \tag{7}$$

in which case

$$f(x) \equiv (x^2 + ax + c)(x^2 - ax + e) \pmod{p^k}. \tag{8}$$

We now give the complete story of the factorization of $f(x)$ modulo an odd prime p. Two special cases are easy to handle. If $s \equiv 0 \pmod{p}$, then (5), (6), and (7) are solvable with $k = 1$, $a = c = 0$, and $e = r$, implying that

$$x^4 + rx^2 + s \equiv x^2(x^2 + r) \pmod{p}$$

is reducible. If $r^2 - 4s \equiv 0 \pmod{p}$ then (5), (6), and (7) are solvable with $k = 1$, $a = 0$, and $c = e \equiv r/2 \pmod{p}$, so

$$x^4 + rx^2 + s \equiv x^4 + rx^2 + r^2/4 \equiv (x^2 + r/2)^2 \pmod{p}$$

is reducible. (Here $1/2$ signifies the inverse of 2 modulo p.)

In describing the rest of the criteria, we use properties of the *Legendre symbol* (k/p), which is defined for an integer k and an odd prime p by

$$\left(\frac{k}{p}\right) = \begin{cases} 1 \text{ if } p \nmid k \text{ and } x^2 \equiv k \pmod{p} \text{ is solvable,} \\ 0 \text{ if } p \mid k, \\ -1 \text{ if } p \nmid k \text{ and } x^2 \equiv k \pmod{p} \text{ is insolvable.} \end{cases}$$

It is well known that

$$\left(\frac{kl}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{l}{p}\right)$$

for all integers k and l, and that

$$\left(\frac{k^2 l}{p}\right) = \left(\frac{l}{p}\right)$$

if $p \nmid k$.

The following result is due to Carlitz [**1**] and can be deduced in an elementary way from Theorem 2:

Theorem 3. *If p is an odd prime and if r and s are integers such that $s \not\equiv 0 \pmod{p}$ and $r^2 - 4s \not\equiv 0 \pmod{p}$, then the following statements hold:*

(i) *$f(x) = x^4 + rx^2 + s$ is the product of two distinct monic linear polynomials and an irreducible monic quadratic polynomial modulo p if and only if*

$$\left(\frac{s}{p}\right) = -1, \qquad \left(\frac{r^2 - 4s}{p}\right) = 1. \tag{9}$$

(ii) *$f(x) = x^4 + rx^2 + s$ is the product of four distinct monic linear polynomials modulo p if and only if*

$$\left(\frac{s}{p}\right) = 1, \qquad \left(\frac{r^2 - 4s}{p}\right) = 1, \qquad \left(\frac{-r - 2t}{p}\right) = 1, \tag{10}$$

where t is an integer such that $s \equiv t^2 \pmod{p}$.

(iii) *$f(x) = x^4 + rx^2 + s$ is the product of two distinct monic irreducible quadratic polynomials modulo p if and only if*

$$\left(\frac{s}{p}\right) = 1, \qquad \left(\frac{r^2 - 4s}{p}\right) = 1, \qquad \left(\frac{-r - 2t}{p}\right) = -1, \tag{11}$$

where t is an integer such that $s \equiv t^2 \pmod{p}$, or

$$\left(\frac{s}{p}\right) = 1, \qquad \left(\frac{r^2 - 4s}{p}\right) = -1. \tag{12}$$

(iv) *$f(x) = x^4 + rx^2 + s$ is irreducible modulo p if and only if*

$$\left(\frac{s}{p}\right) = -1, \qquad \left(\frac{r^2 - 4s}{p}\right) = -1. \tag{13}$$

As a bridge from Theorem 3 to the next result, we consider the irreducibility of $f(x) = x^4 - 10x^2 + 17$ modulo p, where p is again an odd prime. By Theorem 3 (iv) this polynomial is irreducible modulo p if and only if

$$\left(\frac{17}{p}\right) = \left(\frac{32}{p}\right) = -1,$$

that is, if and only if

$$\left(\frac{2}{p}\right) = \left(\frac{17}{p}\right) = -1.$$

In particular, it is irreducible modulo 61. This accounts for the replacement of $x^4 - 10x^2 + 17$ [**3**, p. 303] with $x^4 - 72x^2 + 4$ in the second edition [**4**, p. 310], and points to the condition contained in the next theorem. It is worth noting that, up until this point, all of our arguments have involved only elementary results from number theory. However, the proof of the next result relies on Dirichlet's famous theorem on primes in arithmetic progressions, which states that there are infinitely many primes p with $p \equiv a \pmod{m}$ for any a relatively prime to m.

Theorem 4. *Let r and s be integers such that $r^2 - 4s$ is not a perfect square. Then the polynomial $f(x) = x^4 + rx^2 + s$ is reducible modulo p for every prime p if and only if $s = t^2$ for some integer t.*

Proof. Suppose that $s = t^2$ for an integer t. Consider an odd prime p. If $s \equiv 0 \pmod{p}$ or $r^2 - 4s \equiv 0 \pmod{p}$ then, by the remarks following Theorem 2, $f(x)$ is reducible modulo p. If $s \not\equiv 0 \pmod{p}$ and $r^2 - 4s \not\equiv 0 \pmod{p}$, then $(s/p) = 1$, so $f(x)$ is reducible modulo p (Theorem 3(ii),(iii)). Thus $f(x)$ is reducible modulo every odd prime p. For $p = 2$, there are only the four biquadratic polynomials x^4, $x^4 + 1$, $x^4 +$

x^2, and $x^4 + x^2 + 1$ to consider modulo 2, and it is easy to check that each of these is reducible modulo 2.

Conversely, suppose that $f(x)$ is reducible modulo p for every prime p. Suppose that s is not a perfect square. Then, as both $r^2 - 4s$ and s are nonsquares, by the law of quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes p such that

$$\left(\frac{r^2-4s}{p}\right) = \left(\frac{s}{p}\right) = -1.$$

In view of Theorem 3(iv), $f(x)$ is irreducible modulo each of these primes, a contradiction. Hence s is a perfect square. ■

We are now in a position to state the main result of this section, which gives necessary and sufficient conditions for a polynomial to be irreducible over $\mathbb{Z}$ but reducible modulo p for every prime p. This result is easily obtained by combining Corollaries 1 and 2 with Theorem 4.

Theorem 5. *Let r and s be integers. Then the polynomial $f(x) = x^4 + rx^2 + s$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo p for every prime p if and only if the following are true:*

$$r^2 - 4s \neq \square, \qquad s = \square, \qquad 2\sqrt{s} - r \neq \square, \qquad -2\sqrt{s} - r \neq \square.$$

We return again to the polynomials cited in the introduction. First, for the polynomial $f(x) = x^4 + 1$, we have

$$r = 0, \quad s = 1, \quad r^2 - 4s = -4 \neq \square, \quad \sqrt{s} = 1,$$
$$2\sqrt{s} - r = 2 \neq \square, \quad -2\sqrt{s} - r = -2 \neq \square.$$

Appealing to Theorem 5, we see that $f(x)$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo p for every prime p.

In the case of the polynomial $f(x) = x^4 - 72x^2 + 4$,

$$r = -72, \quad s = 4, \quad r^2 - 4s = 5168 \neq \square,$$
$$\sqrt{s} = 2, \quad 2\sqrt{s} - r = 76 \neq \square, \quad -2\sqrt{s} - r = 68 \neq \square.$$

Thus, by Theorem 5, $f(x)$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo p for every prime p.

As another example consider $f(x) = x^4 - 10x^2 + 1$. Here we have

$$r = -10, \quad s = 1, \quad r^2 - 4s = 96 \neq \square, \quad \sqrt{s} = 1,$$
$$2\sqrt{s} - r = 12 \neq \square, \quad -2\sqrt{s} - r = 8 \neq \square.$$

According to Theorem 5, $f(x)$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo p for every prime p.

Next consider the family of polynomials F_a defined by

$$F_a(x) = x^4 + 2(1-a)x^2 + (1+a)^2 \quad (a \in \mathbb{Z}).$$

Here

$$r = 2(1-a), \quad s = (1+a)^2, \quad r^2 - 4s = -16a,$$
$$\sqrt{s} = 1+a, \quad 2\sqrt{s} - r = 4a, \quad -2\sqrt{s} - r = -4.$$

Theorem 5 implies that $F_a(x)$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo p for every prime p if and only if neither a nor $-a$ is a square. This is a slight generalization of Lee's theorem [**6**].

As yet another example, we revisit the Putnam problem, where

$$P_m(x) = x^4 - (2m+4)x^2 + (m-2)^2 \quad (m \in \mathbb{Z}).$$

Suppose that $m \neq \square$ and $2m \neq \square$. Then from what we showed earlier, $P_m(x)$ is irreducible in $\mathbb{Z}[x]$. By Theorem 4 $P_m(x)$ is reducible modulo p for every prime p.

We now give an example of a one-parameter family of biquadratic polynomials that are irreducible in $\mathbb{Z}[x]$ and reducible modulo p for every prime p for *every* value of the parameter. Let

$$L_k(x) = x^4 - (4k+1)x^2 + 1 \qquad (k \in \mathbb{Z}).$$

In this situation

$$r = -4k - 1, \qquad s = 1, \qquad r^2 - 4s = 16k^2 + 8k - 3.$$

As a square is congruent to 0, 1, or 4 modulo 8, we see that $r^2 - 4s$, $2\sqrt{s} - r$, and $-2\sqrt{s} - r$ are not perfect squares, since

$$r^2 - 4s \equiv 5 \pmod{8}, \qquad \pm 2\sqrt{s} - r \equiv 3 \pmod{4}.$$

Hence, by Theorem 5, the polynomial $L_k(x)$ is irreducible in $\mathbb{Z}[x]$ but reducible modulo p for every prime p independently of k.

We close this section by noting that, when a biquadratic polynomial $x^4 + rx^2 + s$ in $\mathbb{Z}[x]$ is irreducible, its Galois group is the Klein 4-group V if and only if s is a perfect square. This follows, for example, from [**5**, Theorem 1(iii), p. 134]. Thus the biquadratic polynomials

$$x^4 + 1, \quad x^4 - 10x^2 + 1, \quad x^4 - 72x^2 + 4, \quad P_m(x)\ (m, 2m \neq \square),$$
$$F_a(x)\ (\pm a \neq \square), \quad L_k(x)\ (k \in \mathbb{Z})$$

all have the Klein 4-group V as their Galois groups. On the other hand, the biquadratic polynomial $x^4 - 10x^2 + 17$ has the dihedral group D_4 of order 8 as its Galois group. It is the fact that the latter group contains elements permuting the roots of $x^4 - 10x^2 + 17$ in a 4-cycle, together with the Tchebotarov density theorem, that accounts for the existence of (infinitely many) primes p for which the polynomial is irreducible modulo p [**4**, p. 623].

3. BIQUADRATIC POLYNOMIALS MODULO n. We have seen that both $x^4 + 1$ and $x^4 - 72x^2 + 4$ are irreducible in $\mathbb{Z}[x]$ and reducible modulo p for every prime p. These two differ, however, when we consider their reducibility modulo an arbitrary positive integer n.

If we suppose that $x^4 + 1$ is reducible modulo 4, then Theorem 2 establishes the existence of integers a, c, and e such that c and e are odd and $c \equiv e \pmod{4}$. But then $a^2 \equiv c + e \equiv 2c \equiv 2 \pmod 4$, which is impossible. Thus $x^4 + 1$ is not reducible modulo 4.

On the other hand, we claim that $f(x) = x^4 - 72x^2 + 4$ is reducible modulo n for every positive integer n larger than 1. We recall two facts from elementary number theory: if a is an integer such that $a \equiv 1 \pmod 8$, then the congruence $x^2 \equiv a \pmod{2^k}$ is solvable for every positive integer k; if p is an odd prime and b is an integer such that $(b/p) = 1$, then the congruence $x^2 \equiv b \pmod{p^k}$ is solvable for every positive integer k. By the Chinese remainder theorem it suffices to prove that $f(x)$ is reducible modulo p^k for each positive integer k and each prime p. We consider a number of cases.

Case 1: $p = 2$. Since $17 \equiv 1 \pmod 8$, there exists an integer A with $A^2 \equiv 17 \pmod{2^k}$, whence

$$f(x) \equiv (x^2 + 2Ax - 2)(x^2 - 2Ax - 2) \pmod{2^k}.$$

Case 2: $p = 17$. Because $(19/17) = (2/17) = 1$, there exists an integer B such that $B^2 \equiv 19 \pmod{17^k}$, so

$$f(x) \equiv (x^2 + 2Bx + 2)(x^2 - 2Bx + 2) \pmod{17^k}.$$

Case 3: $p = 19$. As $(17/19) = (-2/19) = 1$, there exists an integer C satisfying $C^2 \equiv 17 \pmod{19^k}$. This gives rise to the factorization

$$f(x) \equiv (x^2 + 2Cx - 2)(x^2 - 2Cx - 2) \pmod{19^k}.$$

Case 4: $p \neq 2$, 17, or 19 and $(17/p) = 1$. In this case there exists an integer D such that $D^2 \equiv 17 \pmod{p^k}$ and

$$f(x) \equiv (x^2 + 2Dx - 2)(x^2 - 2Dx - 2) \pmod{p^k}.$$

Case 5: $p \neq 2$, 17, or 19 and $(19/p) = 1$. Here there exists an integer E with $E^2 \equiv 19 \pmod{p^k}$, implying that

$$f(x) \equiv (x^2 + 2Ex + 2)(x^2 - 2Ex + 2) \pmod{p^k}.$$

Case 6: $p \neq 2$, 17, or 19 and $(17/p) = (19/p) = -1$. We have $(323/p) = (17/p)(19/p) = 1$, so there exists an integer F for which $F^2 \equiv 323 \pmod{p^k}$. In this instance

$$f(x) \equiv (x^2 - 36 + 2F)(x^2 - 36 - 2F) \pmod{p^k}.$$

It is now time to see what distinguishes an irreducible polynomial like $x^4 + 1$, which is reducible modulo p for every prime but not modulo n for every integer n greater than 1, from the irreducible polynomial $x^4 - 72x^2 + 4$, which is reducible modulo n for $n = 2, 3, 4, \dots$. We consider a biquadratic polynomial $f(x) = x^4 + rx^2 + s$ in $\mathbb{Z}[x]$ satisfying the conditions of Theorem 5, ensuring that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and reducible modulo p for every prime p. We describe the precise conditions under which $f(x)$ is also reducible modulo n for every integer n bigger than 1. By the Chinese remainder theorem, it suffices to determine the conditions under which $f(x)$ is reducible modulo every prime power p^k.

Theorem 6. *Let $f(x) = x^4 + rx^2 + s$ be a polynomial in $\mathbb{Z}[x]$ such that the following hold:*

$$r^2 - 4s \neq \square, \qquad s = \square, \qquad 2\sqrt{s} - r \neq \square, \qquad -2\sqrt{s} - r \neq \square.$$

Write $s = t^2$ for an integer t, and let p be a prime. Then $f(x)$ is reducible modulo p^k for every positive integer k if and only if $r^2 - 4t^2$ is a square modulo p^k for every positive integer k or $-r + 2t$ is a square modulo p^k for every positive integer k or $-r - 2t$ is a square modulo p^k for every positive integer k.

The proof of Theorem 6, although straightforward, is somewhat technical, so we defer it to the appendix at the end of the article. In order to apply Theorem 6, one requires conditions under which a nonzero integer a is a square modulo p^k for a given prime p and all positive integers k. From results in elementary number theory (see, for example, [**7**, pp. 63–65] for a concise treatment of what is needed), we have the following:

Fact 1. *Let a be a nonzero integer, and write $a = 2^m a_0$, where a_0 is an odd integer and m is a nonnegative integer. Then $x^2 \equiv a \pmod{2^k}$ has solutions for all positive integers k if and only if m is even and $a_0 \equiv 1 \pmod{8}$.*

Fact 2. *Let a be a nonzero integer, let p be an odd prime, and write $a = p^m a_0$, where a_0 is an integer not divisible by p and m is a nonnegative integer. Then $x^2 \equiv a \pmod{p^k}$ has solutions for all positive integers k if and only if m is even and a_0 is a quadratic residue modulo p.*

We need these results in order to exhibit a class of irreducible biquadratic polynomials $x^4 + rx^2 + s$ that are reducible modulo n for every positive integer n greater than 1.

Theorem 7. *If q_1 and q_2 are distinct odd primes such that*

$$q_1 \equiv 1 \pmod{8}, \qquad \left(\frac{q_2}{q_1}\right) = 1,$$

and if $f(x) = x^4 - 2(q_1 + q_2)x^2 + (q_1 - q_2)^2$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ but reducible modulo n for $n = 2, 3, 4, \ldots$.

Proof. Here $r = -2(q_1 + q_2)$, $s = (q_1 - q_2)^2$, and $t = q_1 - q_2$. Thus

$$r^2 - 4t^2 = 16q_1q_2 \neq \square, \quad -r + 2t = 4q_1 \neq \square, \quad -r - 2t = 4q_2 \neq \square.$$

Consider an arbitrary positive integer k. As $q_1 \equiv 1 \pmod{8}$, Fact 1 ensures that the integer $-r + 2t$ is a square modulo 2^k. Because $(q_2/q_1) = 1$, by Fact 2 $-r - 2t$ is a square modulo q_1^k. Now $q_1 \equiv 1 \pmod{8}$ and $(q_2/q_1) = 1$, so by the law of quadratic reciprocity $(q_1/q_2) = 1$. Fact 2 tells us that $-r + 2t$ is a square modulo q_2^k. If p is a prime different from 2, q_1, or q_2 such that $(q_1/p) = 1$, then $-r + 2t$ is a square modulo p^k. Similarly, if $(q_2/p) = 1$, $-r - 2t$ is a square modulo p^k, while if $(q_1/p) = (q_2/p) = -1$, then $(q_1q_2/p) = 1$ and $r^2 - 4t^2$ is a square modulo p^k. Hence, $f(x)$ is irreducible in $\mathbb{Z}[x]$ and reducible modulo p^k for every prime p and every positive integer k (Theorem 6), and by the Chinese remainder theorem $f(x)$ is reducible modulo n for each positive integer n greater than 1. ■

The polynomial $x^4 - 72x^2 + 4$ arises from Theorem 7 by taking $q_1 = 17$ and $q_2 = 19$. We note that, since there are infinitely many primes q_2 with $q_2 \equiv 1 \pmod{2q_1}$ for any prime q_1 such that $q_1 \equiv 1 \pmod 8$, the class of polynomials in Theorem 7 is infinite.

4. STICKELBERGER'S PARITY THEOREM. The "ancient history" of polynomial factorization contains a result that explains the reducibility modulo p of polynomials such as $x^4 + 1$ and $x^4 - 72x^2 + 4$. Originally due to Stickelberger [**10**], it has been rediscovered and studied in more recent times (see [**2**] and [**11**]). We state Stickelberger's theorem in a form convenient for our purposes and encourage the reader to consult Swan's paper [**11**] for a proof and some interesting applications.

Theorem 8. *Let $f(x)$ be a monic polynomial of degree n in $\mathbb{Z}[x]$, and let p be an odd prime not dividing the discriminant $D(f)$ of f. Suppose that*

$$f(x) \equiv f_1(x) f_2(x) \cdots f_r(x) \pmod{p},$$

where the f_j are irreducible polynomials modulo p. Then $n \equiv r \pmod 2$ if and only if $(D(f)/p) = 1$.

As is immediately clear, this result indicates that a polynomial of even degree with (nonzero) square discriminant is always factorable modulo p for all odd primes p not dividing its discriminant.

5. A FAMILY FOR THE ALTERNATING GROUP. In discussing quartics irreducible over the integers but reducible modulo every prime, we have treated biquadratics in some detail. These polynomials have the Klein 4-group as their Galois groups. In this section we introduce a family of polynomials having the alternating group A_4 as their Galois groups, and we invite the reader to explore the same phenomena for these polynomials.

The "ancient history" yields a starting point. Seidelmann [**9**] determined the quartics with rational coefficients having the alternating group A_4 as their Galois groups, namely,

$$[e^3 - (f^2 + 3g^2)(3e + 2f)]x^4 - 6ex^2 - 8x - 3\frac{e^2 - 4f^2 - 12g^2}{e^3 - (f^2 + 3g^2)(3e + 2f)},$$

with e, f, and g rational such that $e^3 - (f^2 + 3g^2)(3e + 2f)$ is not zero. Setting $f = -e - \frac{1}{2}$ and $g = \frac{1}{2}$, we obtain the polynomials

$$f_e(x) = x^4 - 6ex^2 - 8x + (9e^2 + 12e + 12) \qquad (e \in \mathbb{Z}).$$

Each of these can be shown to be irreducible by establishing that

(i) $f_e(x)$ has no linear factors in $\mathbb{Z}[x]$, and
(ii) $f_e(x)$ has no quadratic factors in $\mathbb{Z}[x]$.

We give the details only for (ii). If $f_e(x)$ has a quadratic factor, then it admits a factorization of the form

$$x^4 - 6ex^2 - 8x + (9e^2 + 12e + 12) = (x^2 + Ax + B)(x^2 - Ax + C)$$

for integers A, B, and C. Comparing coefficients leads to the three equations:

$$-A^2 + B + C = -6e, \tag{14}$$

$$A(C - B) = -8, \tag{15}$$

$$BC = 9e^2 + 12e + 12. \tag{16}$$

Examining the powers of 2 in (15), we see that

$$A = \varepsilon 2^r, \qquad B - C = \varepsilon 2^{3-r},$$

where $\varepsilon = -1$ or 1 and r belongs to $\{0, 1, 2, 3\}$. From (14), we deduce that

$$B + C = 2^{2r} - 6e.$$

Solving the two linear equations for B and C shows that r is 1 or 2 and that

$$B = 2^{2r-1} - 3e + \varepsilon 2^{2-r}, \qquad C = 2^{2r-1} - 3e - \varepsilon 2^{2-r}.$$

Inserting these values of B and C into (16), we arrive at

$$(2^{2r-1} - 3e)^2 - 2^{4-2r} = 9e^2 + 12e + 12.$$

However, for $r = 1$ or 2 this equation yields only nonintegral values for e, a contradiction.

Recall now (see, for example, [**4**, p. 595]) that the discriminant D of a quartic polynomial $x^4 + Px^2 + Qx + R$ is given by

$$D = 16P^4R - 4P^3Q^2 - 128P^2R^2 + 144PQ^2R - 27Q^4 + 256R^3. \tag{17}$$

We infer that the discriminant D_e of $f_e(x)$ is

$$D_e = 2^{12}3^4(e^2 + e + 1)^2.$$

Since D_e is a perfect square, Theorem 8 implies that, for any odd prime p not dividing D_e, $f_e(x)$ has an even number of irreducible factors modulo p and so is reducible modulo p. For $p = 2$ we have

$$f_e(x) \equiv (x + e)^4 \pmod 2,$$

for $p = 3$

$$f_e(x) \equiv x(x + 1)^3 \pmod 3,$$

and for p ($\neq 2, 3$) dividing $e^2 + e + 1$

$$f_e(x) \equiv (x + 3(e + 1))(x - (e + 1))^3 \pmod p.$$

Thus $f_e(x)$ is reducible modulo p for every prime p.

For the sake of completeness, we appeal to [**5**] to show that the Galois group of $f_e(x)$ is A_4 for every integer e. As the discriminant of $f_e(x)$ is a perfect square, we know that its Galois group must be a subgroup of the alternating group A_4 [**4**, Proposition 34, p. 592]. We recall that if the quartic polynomial $x^4 + Px^2 + Qx + R$ has roots α_1, α_2, α_3, and α_4 in $\mathbb{C}$, then the cubic polynomial with the roots $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\alpha_1\alpha_4 + \alpha_2\alpha_3$ is the *resolvent cubic* of $x^4 + Px^2 + Qx + R$. It is given by $x^3 - Px^2 - 4Rx + (4PR - Q^2)$ (see, for example, [**5**]). In order to prove that the Galois group of $f_e(x)$ is actually A_4 we must show that the resolvent cubic of $f_e(x)$ has no roots in $\mathbb{Z}$ [**5**, Theorem 1(ii), p. 134]. The resolvent cubic in question is

$$g_e(x) = x^3 + 6ex^2 - 4(9e^2 + 12e + 12)x - 8(3e(9e^2 + 12e + 12) + 8).$$

Suppose that m is an integral root of $g_e(x)$. Clearly m must be even, say $m = 2n$, and (after dividing by 8) we have

$$n^3 + 3en^2 - (9e^2 + 12e + 12)n - (3e(9e^2 + 12e + 12) + 8) = 0.$$

It follows that

$$(n + 3e)n^2 - (n + 3e)(9e^2 + 12e + 12) - 8 = 0, \tag{18}$$

from which it is immediate that $n + 3e$ divides 8, so $n + 3e = \varepsilon 2^w$ with ε in $\{-1, 1\}$ and w in $\{0, 1, 2, 3\}$. Substituting $n = \varepsilon 2^w - 3e$ into (18) yields

$$(\varepsilon 2^w - 6e)2^{2w} - 12(e + 1)\varepsilon 2^w - 8 = 0.$$

The three possibilities $w = 0, 2$, or 3 are easily ruled out by divisibility considerations. It remains to consider the situation for $w = 1$. In this case, after substituting and then dividing by 8, we obtain

$$\varepsilon - 3e - 3e\varepsilon - 3\varepsilon - 1 = 0,$$

which in turn yields

$$-2\varepsilon - 1 = 3e(\varepsilon + 1).$$

This equation shows that $\varepsilon \neq -1$. Thus $\varepsilon = 1$, which leads to $e = -1/2$, contradicting the fact that e is an integer. Therefore the polynomial $g_e(x)$ has no integer roots, whence the Galois group of $f_e(x)$ is A_4.

We leave the reader with the question: Are there integers e for which $f_e(x)$ is reducible modulo n for every integer n greater than 1?

6. APPENDIX: PROOF OF THEOREM 6. ($\Leftarrow$) Suppose first that $u^2 \equiv r^2 - 4t^2 \pmod{p^k}$ has a solution for every positive integer k, where p is an odd prime. Let w denote the inverse of 2 modulo p^k. Then $f(x)$ is reducible modulo p^k, for

$$f(x) \equiv (x^2 + w(r + u))(x^2 + w(r - u)) \pmod{p^k}.$$

Suppose next that $u^2 \equiv r^2 - 4t^2 \pmod{2^h}$ has a solution for every positive integer h. Let k be a positive integer, and let v be a solution of $v^2 \equiv r^2 - 4t^2 \pmod{2^{k+2}}$, so $v \equiv r \pmod 2$. Then $s = \frac{1}{2}(v - r)$ is an integer. Clearly $v = r + 2s$. Also $s(r + s)$ is congruent to $-t^2$ modulo 2^k. Hence $f(x)$ is reducible modulo 2^k: namely,

$$f(x) \equiv x^4 + rx^2 - s(r + s) \equiv (x^2 - s)(x^2 + r + s) \pmod{2^k}.$$

Now assume that $u^2 \equiv -r + 2t \pmod{p^k}$ has a solution for each positive integer k, where p is an arbitrary prime. Then $f(x)$ is reducible modulo p^k with the factorization

$$f(x) \equiv (x^2 + ux + t)(x^2 - ux + t) \pmod{p^k}.$$

Finally, when $u^2 \equiv -r - 2t \pmod{p^k}$ has a solution for each prime p and each positive integer k, then $f(x)$ has the factorization

$$f(x) \equiv (x^2 + ux - t)(x^2 - ux - t) \pmod{p^k},$$

revealing that it is reducible modulo p^k.

($\Rightarrow$) Suppose that $f(x)$ is reducible modulo p^k for every positive integer k. Fix such a k. We first consider the case when p is an odd prime not dividing $r^2 - 4t^2$. If

$$\left(\frac{r^2 - 4t^2}{p}\right) = 1,$$

then $r^2 - 4t^2$ is a square modulo p^k. If

$$\left(\frac{r^2 - 4t^2}{p}\right) = -1,$$

then

$$\left(\frac{-r + 2t}{p}\right)\left(\frac{-r - 2t}{p}\right) = -1,$$

so

$$\left(\frac{-r + 2t}{p}\right) = 1$$

or

$$\left(\frac{-r - 2t}{p}\right) = 1.$$

Accordingly, either $-r + 2t$ or $-r - 2t$ is a square modulo p^k.

Assume next that p is an odd prime dividing $r^2 - 4t^2$. Because $r^2 - 4t^2 \neq \square$, we deduce that $t \neq 0$. Express t as $t = p^l t_0$, where l is a nonnegative integer and t_0 is an integer not divisible by p, and let k be a positive integer. Since $f(x)$ is reducible modulo p^{2k+4l}, Theorem 2 declares the existence of integers a, c, and e such that

$$c + e - a^2 - r \equiv 0 \pmod{p^{2k+4l}}, \tag{19}$$

$$a(c - e) \equiv 0 \pmod{p^{2k+4l}}, \tag{20}$$

$$ce - s \equiv 0 \pmod{p^{2k+4l}}. \tag{21}$$

By adding p^{2k+4l} to a, if necessary, we may suppose that $a \neq 0$. Similarly adding p^{2k+4l} to c, if necessary, we may suppose that $c \neq e$. Let p^{k_1} and p^{k_2} be the exact powers of p dividing a and $c - e$, respectively. Then, by (20), $k_1 + k_2 \geq 2k + 4l$.

Suppose first that $k_1 \geq k + 2l$. Then $a^2 \equiv 0 \pmod{p^{2k+4l}}$. From (19) we infer that

$$c + e \equiv r \pmod{p^{2k+4l}},$$

so (21) leads to

$$r^2 - 4t^2 = r^2 - 4s \equiv (c + e)^2 - 4ce \equiv (c - e)^2 \pmod{p^{2k+4l}}.$$

Thus

$$u^2 \equiv r^2 - 4t^2 \pmod{p^k}$$

is solvable for each k in $\mathbb{N}$.

Now assume that $k_1 < k + 2l$. Then $k_2 \geq 2k + 4l - k_1 > k + 2l$. Set

$$e - c = d_0 p^{k_2}, \qquad p \nmid d_0.$$

Referring to (19), we conclude that

$$2c + d_0 p^{k_2} - a^2 - r = (c + e - a^2 - r) - (e - c - d_0 p^{k_2}) \equiv 0 \pmod{p^{2k+4l}}.$$

As a result

$$-r + 2c \equiv a^2 - d_0 p^{k_2} \pmod{p^{2k+4l}}$$

and, since $k_2 \geq k + 2l + 1$,

$$-r + 2c \equiv a^2 \pmod{p^{k+2l+1}}.$$

Invoking (21), we obtain

$$p^{2l} t_0^2 = t^2 = s \equiv ce \equiv c(c + d_0 p^{k_2}) \equiv c^2 \pmod{p^{k+2l+1}},$$

which implies that

$$t = p^l t_0 \equiv \varepsilon c (\bmod\, p^{k+1})$$

for $\varepsilon = 1$ or -1. Finally,

$$-r + 2\varepsilon t \equiv a^2 \pmod{p^k}.$$

The case $p = 2$ can be treated in a similar manner. We leave the details to the reader.

REFERENCES

1. L. Carlitz, Note on a quartic congruence, this MONTHLY **63** (1956) 569–571.
2. K. Dalen, On a theorem of Stickelberger, *Math. Scand.* **3** (1955) 124–126.
3. D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, N.J., 1991.
4. ———, *Abstract Algebra*, 2nd ed., Prentice-Hall, Upper Saddle River, N.J., 1999.
5. L.-C. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, this MONTHLY **96** (1989) 133–137.
6. M. A. Lee, Some irreducible polynomials which are reducible mod p for all p, this MONTHLY **76** (1969) 1125.
7. W. J. LeVeque, *Topics in Number Theory*, vol. 1, Addison-Wesley, Reading, MA, 1956.
8. 62nd Annual William Lowell Putnam Mathematical Competition, *Math. Magazine* **75** (2002) 72–78.
9. F. Seidelmann, Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebegem Rationalitätsbereich, *Math. Annalen* **78** (1918) 230–233.
10. L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, in *Verhandlungen des I Internationalen Mathematiker-Kongresses*, Zürich, August 1897, F. Rudio, ed., B. G. Teubner, Leipzig, 1898, pp. 182–193.
11. R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* **12** (1962) 1099–1106.

ERIC DRIVER received his M.S.E and Ph.D. degrees in electrical engineering from Arizona State University in 1993 and 1996, respectively. He has worked for Lockheed Martin in Goodyear, Arizona, for the last eight years, designing advanced radar systems. He has always loved mathematics, especially number theory, and is presently pursuing a Ph.D. in mathematics at Arizona State University. His research interests include algebraic number theory, class field theory, and algebraic topology.

700 E. Mesquite Circle N128, Tempe, AZ 85281.
eric.driver@lmco.com

PHILIP A. LEONARD recently retired from Arizona State University, where he served for thirty-six years. His interests have been in number theory and aspects of combinatorics, as well as in working with students preparing to teach mathematics. He received the 2002 MAA Southwestern Section Award for Distinguished College or University Teaching of Mathematics.

Department of Mathematics, Arizona State University, Tempe, AZ 85287-1804.
philip.leonard@asu.edu

KENNETH S. WILLIAMS finished his Ph.D. in mathematics at the University of Toronto in 1965. After a year as a lecturer at the University of Manchester, England, he joined the Department of Mathematics at Carleton University in Ottawa. He became a full professor in 1975 and served as chair of the department from 1980 to 1984 and again from 1997 to 1998. In 1998, when the department became the School of Mathematics and Statistics, he became its first director, serving until 2000. In 2002 he retired as professor emeritus and distinguished research professor. He continues to supervise the theses of graduate students in number theory. His hobbies include birding, hiking and gardening.

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6.
williams@math.carleton.ca

"I even know of a mathematician who slept with his wife only on prime-numbered days . . . ," Graham said.

—*The Man Who Loved Only Numbers* by Paul Hoffman

A mathematician was obsessed with things prime.
He thought about them almost all of the time.
Said to his dear wife, "It truly seems right
That we should only make love on a prime-numbered night."
His wife thought for a bit ('cause she was no dummy),
"At the month's start this does seem quite yummy,
For there's two, three, five, seven
A three-night hiatus and then there's eleven.
But of the month's end I start to be wary
Near the twenty-third day of the month February.
For the next prime day after will be March the first
Such sexual continence might cause me to burst!"
He shook his head sadly, "As it's commonly reckoned,
The next prime day would be found on the second."

—Submitted by John Drost, Marshall University