Irreducible Quadratic Factors of \( x^{(q^n+1)/2} + ax + b \) over \( \mathbb{F}_q \)

DENNIS R. ESTES AND TETSURO KOJIMA

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113
E-mail address: DESTES@MATH.USC.EDU; KOJIMA@USC.EDU

Communicated by Peter Jan-Shyong Shine

Received July 24, 1995; revised December 20, 1995

Let \( f(x) = x^{(q^n+1)/2} + ax + b \in \mathbb{F}_q[x] \) with \( b \neq 0 \), \( q = p' \) and \( p \) an odd prime. If \( n \) is even or \( a^2 + 1 \) is a square in \( \mathbb{F}_q \), then \( f(x) \) does not have an irreducible quadratic factor in \( \mathbb{F}_q[x] \). If \( f(x) \) has a monic irreducible quadratic factor in \( \mathbb{F}_q[x] \) then it is unique and equal to \( x^2 + 2(b/a)x + b^2/(a^2 + 1) \). A condition that \( x^2 + 2(b/a)x + b^2/(a^2 + 1) \) divides \( f(x) \) is expressed in terms of quadratic and biquadratic symbols which are evaluated for \( a = \pm 1, 0 \) and all \( q \), or \( a = \pm 2, \pm 3 \) and \( q = p \). © 1996 Academic Press, Inc.

Factorization of polynomials over finite fields has gained notoriety over time due in part to connections with coding and cryptography. Factoring algorithms and their complexity have been of central interest (see, e.g., [L]), but related issues such as the degrees of the irreducible factors or factors for polynomials of special type have also been investigated. For example, with \( p \) a prime, \( q = p' \), and \( a \neq 0 \), \( x^q - x - a \) is irreducible over \( \mathbb{F}_q \), and if \( u \) denotes a root of this polynomial then \( x^q - x - au^{q-1} \) is irreducible over \( \mathbb{F}_q(u) \) (see, e.g., [K, Theorems 32, 52]). Such polynomials arise in the study of the additive version of Hilbert’s Theorem 90. They are also special cases of the more general polynomial \( g(x) = cx^{q+1} + dx^q - ax - b \), whose complete factorization was determined implicitly by Ore [O] using his theory of \( p \)-polynomials and linearized polynomials. Ore’s investigation arose in the study of irreducible polynomials whose roots are connected by linear substitutions \( x^q = (ax + b)/(cx + d) \). An alternative presentation, including an explicit determination of the factors of \( g(x) \), was presented in [B] and applied to the construction of normal bases of low complexity for finite fields. Another example occurs in Carlitz’ extension to general \( p \) of work by Mills and Zierler for the case \( q = 2 \) (see [C]). The result is that the degrees of the irreducible factors of \( x^{2q^p+1} + x^{q^p-1} + 1 \)
over \( \mathbb{F}_q \) divide either \( 2n \) or \( 3n \). Somewhat more routine are such factorizations over \( \mathbb{F}_q \) as:

1. \( x^{q-1} - 1 = \prod_{u \in \mathbb{F}_q} (x - u) \) and, for \( q \) odd, \( b \neq 0 \), we have \( x^{(q-1)/2} + b \) is a product of \((q - 1)/2d \) irreducible polynomials each of degree \( d \), the order of \( b^2 \) in \( \mathbb{F}_q^* \);

2. if \( x^{q-1} + ax + b \) has an irreducible quadratic factor then either \( a = 0, b = 1, p \neq 2 \), and \( x^{q-1} + 1 = \prod_{u \in \mathbb{F}_q^2} (x^2 - u) \), or \( a \neq 0, x^2 + ((b - 1)/a) x - (b - 1)/a^2 \) is irreducible and is the unique monic irreducible quadratic dividing \( x^{q-1} + ax + b \);

3. if \( x^{q-1} + ax + b, b \neq 0 \), has an irreducible quadratic factor then \( a = 0 \) and \( x^{q-1} + b = \prod (x^2 + cx - b) \) when \( -b \not\in \mathbb{F}_q^2 \), \( x^{q-1} + b = (x^2 + b) \prod (x^2 + cx - b) \) when \( -b \in \mathbb{F}_q^2 \) and \( p \neq 2 \), and \( x^{q-1} + b = (x + u) \prod (x^2 + cx - b), u^2 = b \), when \( p = 2 \), these products over the quadratic polynomials \( x^2 + cx - b \) which are irreducible; and

4. for \( b \neq 0, x^q + ax + b \) has an irreducible quadratic factor only in the event \( a = 1 \), in which case \( x^q + x + b = (x + b/2) \prod (x^2 + bx + c) \) when \( p \neq 2 \) and \( x^q + x + b = \prod (x^2 + bx + c) \) when \( p = 2 \), the two products taken over the quadratic polynomials \( x^2 + bx + c \) which are irreducible.

More generally, the following type of analysis can be used to start the investigation of irreducible quadratic factors over \( \mathbb{F}_q \) of polynomials which are sums of trinomials of the type \( ax^{eq - 1} + bx^{eq} + cx^{eq - 1}, e = 0, 1, 2 \). The key and simple observation is that the Galois group of \( \mathbb{F}_q^2/\mathbb{F}_q \) is generated by \( x \rightarrow x^q \) of order 2. Thus, if \( \theta \) is quadratic over \( \mathbb{F}_q \) then \( \theta, \theta^q \) are the two roots of the monic irreducible \( x^2 - (\theta + \theta^q)x + \theta \theta^q \in \mathbb{F}_q[x] \).

Cases (3) and (4) are special cases of Ore’s polynomial, but no special technique is needed for our cases. For example, to prove the factorization (4) in the case \( p = 2 \), first observe that the trace map, \( x \rightarrow x^q + x \), from \( \mathbb{F}_q^2 \) to \( \mathbb{F}_q \) is onto and hits the value \( -b \neq 0 \) exactly \( q \) times and none of the preimages are in \( \mathbb{F}_q \) since \( b \neq 0 \). Thus, for each \( b \neq 0 \), there are \( q/2 \) irreducible quadratic polynomials of the type \( x^2 + bx + c \) in \( \mathbb{F}_q \) and each has a root in common with \( x^q + x + b \). A similar approach using the norm instead of the trace establishes (3) (see the next example).

Another example is that of Carlitz, Mills, and Zierler, namely \( f(x) = x^{2e(q-1)} + x^{eq - 1} + 1 \). Let \( \theta \) denote a root of \( f(x) \) and assume that \( \theta \) is quadratic over \( \mathbb{F}_q \). One needs to examine the two cases \( n \) odd and \( n \) even; with \( n \) odd, \( \theta^{2n} = \theta^n \) and with \( n \) even, \( \theta^{2n} = \theta \). First, when \( n \) is even, we have \( f(\theta) = \theta^n + 2 = 0 \). Now \( x^3 + 2 \) has an irreducible quadratic factor if and only if \( p \) is odd, \( p \neq 3 \), and 3 does not divide \( q - 1 \) (the last condition ensures that \(-2 \not\in \mathbb{F}_q^2 \) and \( \mathbb{F}_q \) does not contain the cube roots of 1). In the case \( n \) is odd, \( 0 = f(\theta) = \text{norm}(\theta) \theta^2 + \theta^q + 1 \), and \( \text{norm}(\theta^2) + \theta^q + \theta = 0 \); i.e., \( \text{trace}(\theta) = -\text{norm}(\theta)^2 \). The irreducible for \( \theta \) in \( \mathbb{F}_q[x] \) therefore
has the form $x^2 + c^2x + c, c \neq 0$. By considering the derivative, one can show that $f(x)$ has no multiple roots which have degree 2 over $\mathbb{F}_q$. It follows therefore that $f(x) = h(x)g(x)$, where $g(x) = \prod(x^2 + c^2x + c)$ and $h(x)$ is a polynomial having no irreducible quadratic factors in $\mathbb{F}_q[x]$ and the product is over the irreducible polynomials of type $q(x) = x^2 + c^2x + c$. The degree of $g(x)$ can be calculated using Carlitz’ results in [C]. (Much of the analysis for this case can be circumvented by observing that the number of such polynomials $q(x)$ is the same as the number of irreducible quadratics of type $r(x) = x^2 + x + u^3$, as is seen by replacing $x$ in $g(x)$ with $1/\alpha$. If, for example, $p$ is odd then the polynomials $r(x)$ correspond to points not on the elliptic curve $1 - 4u^3 = v^2$. The number of points on the latter curve is determined by standard use of Jacobi sums.)

Our purpose in this paper is the inclusion of the special polynomial $f(x) = x^{(q^n+1)/2} + ax + b \in \mathbb{F}_q[x]$ to the above lore. Galois theory of finite fields cannot alone resolve the quadratic factors of this polynomial due to a squaring which introduces a sign difficulty, and number theory is used to overcome the difficulty. In particular, biquadratic residues play a central role in our analysis as to whether $f(x)$ has irreducible quadratic factors.

The case $a = 0$, i.e., $f(x) = x^{(q^n+1)/2} + b$, already requires more scrutiny than (1)–(4) above. However, Euler’s criteria for testing that an element in a finite field is an $n$th power suffices to resolve the factors of $f(x)$. First we present some notation and reductions.

Let $F$ denote a finite field and set $(w|F)_r = w^{(|F|^{-1})/r}$ for $r$ dividing $|F| - 1$ and $w \in F$. For $p$ odd, we set $(w|F)_2 = (w|F)_1$ which has value $\pm 1$ for $w \neq 0$. In the theorem below, we take $F = \mathbb{F}_q$ or $\mathbb{F}_{q^2}$ and let $i$ (resp. $\sqrt{a^2 + 1}$) denote a root of $x^2 + 1$ (resp. $x^2 - (a^2 + 1)$) in $\mathbb{F}_{q^2}$. Note that when $r|q-1$, $(w|\mathbb{F}_{q^r}) = (\text{norm}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(w)|\mathbb{F}_q)_r, \ w \in \mathbb{F}_{q^r}$.

**Proposition 1.** Let $f(x) = x^{(q^n+1)/2} + ax + b \in \mathbb{F}_q[x]$ and assume that $b \neq 0$. Then

1. $f(x)$ has no irreducible quadratic factors in $\mathbb{F}_q[x]$ when $n$ is even and
2. $f(x)$ has the same irreducible quadratic factors in $\mathbb{F}_q[x]$ as $g(x) = x^{(q^n+1)/2} + eax + eb$ when $n$ odd, $e = (a^2 + 1|\mathbb{F}_q)^{(n-1)/2}$.

**Proof.** Assume first that $n$ is even and that $\theta$ is a root of $f(x)$ which has degree 2 over $\mathbb{F}_q$. Now $\mathbb{F}_q \subset \mathbb{F}_{q^2} \subset \mathbb{F}_{q^n}$. Thus, $\theta^{(q^n+1)/2} = \theta\theta^{(q^n-1)/2} = \theta\theta^{(q^n-1)/2} = \theta(\theta^{(q^n-1)/2})$. It now follows that $a = -(\theta|\mathbb{F}_{q^2})$ and $b = 0$, a contradiction.

Now for the case $n$ odd, note that $\theta^{(q^n+1)/2} = \theta^2$ while $\theta^{q^n} = \theta$. It follows that $\theta^{(q^n+1)/2} = (\theta^{q^n-1}q^{n-2}q^{n-4}q^{n-6}q^{n-7})^{(q+1)/2} = (\theta^{q^n-1}q^{n-2}q^{n-4}q^{n-6}q^{n-7})^{(q+1)/2} = (\theta^{q^n-1}q^{n-2}q^{n-4}q^{n-6}q^{n-7})^{(q+1)/2} = \theta^{q^n-1}q^{n-2}q^{n-4}q^{n-6}q^{n-7}$. The equality $e = (\text{norm}_{\mathbb{F}_{q^{q^n}}}(\theta)|\mathbb{F}_q)^{(n-1)/2}$ when $a = 0$ follows from $\text{norm}_{\mathbb{F}_{q^{q^n}}}(\theta) = \theta^2\theta = b^2$ and when $a \neq 0$ it is derived.
in the proof of Theorem 1. Therefore \( \theta \) is a root of \( f(x) \) if and only if \( \theta \) is a root of \( g(x) \).

**Proposition 2.** If \( p \) is odd, \( f(x) = x^{(q+1)/2} + b, b \neq 0, \varepsilon = (b|\mathbb{F}_q) \), and \( i = 0, 1 \) according as \( \varepsilon = 1, -1 \), then

1. for \( q = 3 \mod 4 \),

\[
f(x) = (x - b^2)^i \prod_{(d|q)=1, (d+4|\mathbb{F}_q)=-1} x^2 - (2\varepsilon + d)bx + b^2,
\]

2. for \( q = 1 \mod 4 \),

\[
f(x) = (x + \varepsilon b) \prod_{(d|q)=1, (d+4|\mathbb{F}_q)=-1} x^2 - (2\varepsilon + d)bx + b^2.
\]

**Proof.** The change of variables \( x \rightarrow by \) replaces \( f(x) \) with \( b(q+1)/2(x^{(q+1)/2} + (b|\mathbb{F}_q)) \) and we can assume for the proof that \( f(x) = x^{(q+1)/2} \pm 1 \). Since the roots of \( f(x) \) are roots of unity for the exponent \( q + 1 \) and all such roots reside in \( \mathbb{F}_q \), the irreducible factors of \( f(x) \) are either linear or quadratic. If \( x - u \) is a linear factor of \( x^{(q+1)/2} \pm 1 \) then \( u^{(q+1)/2} = u(u|\mathbb{F}_q) = \pm 1 \) and therefore \( u = \pm 1 \). Now 1 is a root of \( f(x) \) if and only if \( f(x) = x^{(q+1)/2} - 1 \) and \( -1 \) is a root of \( f(x) \) if and only if \( f(x) = x^{(q+1)/2} + 1 \) and \( (q + 1)/2 \) is odd or \( f(x) = x^{(q+1)/2} - 1 \) and \( (q + 1)/2 \) is even.

Now let \( \theta \) denote a root of \( f(x) \) of degree 2 over \( \mathbb{F}_q \). Since \( \text{norm}_{\mathbb{F}_q}[\theta] = \theta^{q+1} = 1 \), the monic irreducible for \( \theta \) in \( \mathbb{F}_q[x] \) has the form \( x^2 + cx + 1, (c^2 - 4|\mathbb{F}_q) = -1 \). Since \( \theta \) has square norm, \( \theta \) is a square in \( \mathbb{F}_q \); by the observation just prior to the statement of the proposition. Set \( \theta = \delta^2, \delta \in \mathbb{F}_q \), and let \( x^2 + ux + v \in \mathbb{F}_q[x] \) denote the irreducible for \( \delta \). Taking norms gives \( v = \pm 1 \) with \( \theta \) a root of \( x^{(q+1)/2} + 1 \) when \( v = -1 \) and \( \theta \) a root of \( x^{(q+1)/2} - 1 \) when \( v = 1 \). Now \( x^2 + ux + v \) divides \( x^2 + cx + 1, \) and hence \( c = 2 - u^2 \) when \( v = 1 \) and \( c = -2 - u^2 \) when \( v = -1 \). Note that \( c^2 - 4 = u^4(2^2 + 4\varepsilon) \). Set \( d = u^2 \). The proof is now completed with the observation that \( f(x) \) has no multiple roots and that if \( \theta \) is a root of an irreducible polynomial \( x^2 + cx + 1 \) in \( \mathbb{F}_q[x] \), then \( \theta^{q+1} = \text{norm}(\theta) = 1 \) and therefore \( \theta \) is a root of either \( x^{(q+1)/2} + 1 \) or \( x^{(q+1)/2} - 1 \).

The situation for \( f(x) = x^{(q+1)/2} + ax + b, ab \neq 0 \) is quite different from above in that the root \( \theta \) is no longer a square. Here 4th power symbols cannot be avoided.

**Theorem 1.** Let \( p \) be an odd prime, \( q = p' \). Let \( f = x^{(q+1)/2} + ax + b \in \mathbb{F}_q[x], ab \neq 0 \). Set \( A = (ab|\mathbb{F}_q)a \) and \( \sigma = 1 + Ai \).
(1) If \((a^2 + 1\|q) \neq -1\) then \(f\) does not have an irreducible quadratic factor in \(\mathbb{F}_q[x]\).

(2) A monic irreducible quadratic factor of \(f\), should one exist, is unique and equal to \(x^2 + 2(b/a)x + b^2/(a^2 + 1)\).

(3) If \((a^2 + 1\|q) = -1\) then \(h(x) = x^2 + 2(b/a)x + b^2/(a^2 + 1)\) is irreducible in \(\mathbb{F}_q[x]\) and a necessary and sufficient condition that \(f\) have \(h\) as a factor is that

\[
(-1\|q) \left( \frac{\sigma}{\sqrt{a^2 + 1\|q}} \right) = i.
\]

Proof. First note that the change of variables \(x \to (b/a)x\) transforms \(f\) to \((b/a)^2)((b/a)F, F = x^{(q+1)/2} + Ax + A\) with \(A = (ba\|q) a; g = x^{(q+1)/2} - \frac{ax - b}{(b/a)^2}((b/a)G, G = x^{(q+1)/2} - Ax - A\) and \(h = x^2 + 2(b/a)x + b^2/(a^2 + 1)\) to \((b/a)^2 H, H = x^2 + 2x + A^2/(A^2 + 1)\). Hence, for the purpose of proof of the theorem, we can replace \(f, h\) by \(F, H\), respectively. Assume that \(FG = x^{q+1} - A^2(x + 1)^2\) has an irreducible quadratic factor and let \(\theta \in \mathbb{F}_q^2 - \mathbb{F}_q\) be a root of this factor. Now \(N := \text{norm}_{2/\mathbb{F}_q}(\theta) = \theta^{q+1} = A^2(\theta + 1)^2\). It follows that \(\theta\) is a root of \(x^2 + 2x + (A^2 - \frac{N}{A^2})\). Hence, \((A^2 - N)/A^2 = N, A^2 + 1 \neq 0, and N = A^2/(A^2 + 1)\). Thus, \(H(x) = x^2 + 2x + A^2/(A^2 + 1)\) is the irreducible for \(\theta\) over \(\mathbb{F}_q\) and its irreducibility implies that \((A^2 + 1\|q) = -1\). Conversely, if \((A^2 + 1\|q) = -1, H(x)\) is irreducible and any root of \(H(x)\) is a root of \(FG\) of multiplicity one (take derivatives). Hence \(FG\) has an irreducible quadratic factor in \(\mathbb{F}_q[x]\) only in the event \((A^2 + 1\|q) = -1\) and in this event \(H(x)\) is the unique monic quadratic irreducible factor of \(FG\). Moreover, if \(\theta \in \mathbb{F}_q^2\) is a root of \(H(x)\) then \(H(x)\) is the unique monic quadratic factor of \(F(x)\) whenever \(\theta^{q+1}/2 = -A(\theta + 1)\) and otherwise \(H(x)\) is the unique monic irreducible factor of \(G(x)\). Thus we need only determine the sign \(s\) for which \(\theta^{q+1}/2 = sA(\theta + 1).\) We can take \(\theta = -1 + 1/\sqrt{A^2 + 1}\).

Another change of variables facilitates the proof. Set \(\lambda = (-1 + A\|i)/\sqrt{A^2 + 1}\). Since \((1 + \lambda)^2 = -(2\lambda - \theta^{q+1}/2) = (1 + \lambda)^{q+1}/(2\lambda)^{(q+1)/2} = sA(\sqrt{A^2 + 1}).\)

Case \((-1\|q) = -1\). Thus, \(q = 3 \mod 4\). Since \((-A^2 + 1\|q) = 1, i\sqrt{A^2 + 1} \in \mathbb{F}_q.\) Thus \((1 + \lambda)^{q+1} = (-1 + A\|i)/\sqrt{A^2 + 1})\) \((1 + A\|i)/\sqrt{A^2 + 1}) = 2Ai/\sqrt{A^2 + 1}\). Hence, we have \((2\|q)\lambda^{(q+1)/2} = s.\) Since \((q - 1)/2\) is odd, \((2\|q)\lambda^{(q+1)/2} = (2\|q)\lambda^{(q+1)/2} = (2\|q)\lambda^{(q-1)/2} = (2\|q)\lambda^{(q-1)/2} = s.\) Now \((2i)^{q+1}/2 = (1 + i)^{q+1}/2 = (1 - i)/2 = i\). Thus \(-1\|q) = i.\) And \(s = (-1\|q)i(\lambda\|q)\). It follows that \(s = -1\) if and only if \((-1\|q) = i.\)

Case \((-1\|q) = 1.\) Then \((1 + \lambda)^{q+1} = (1 + A\|i)/\sqrt{A^2 + 1})/(1 - A\|i)/\sqrt{A^2 + 1}) = (-2Ai/\sqrt{A^2 + 1}) = (-2Ai/\sqrt{A^2 + 1}) = -s.\) Hence \((2\|q)i\lambda^{(q-1)/2} = s.\)
Now \((2i)^{(q-1)/2} = (1 + i)^{q-1} = 1\) since \(i \in \mathbb{F}_q\) in this case. Thus, \((2i_{q^2}) = (-i)^{(q-1)/2}\). Since \((q - 1)/2\) is even and \((q + 1)/2\) is odd, \(s = (i)^{(q+1)/2}\) \(\lambda^{-(q-1)/2(q+1)/2}\) and therefore \(s = i(\lambda|\mathbb{F}_q)^{q+1}/2\), which is \(-1\) if and only if \((\lambda|\mathbb{F}_q)^{q+1}/2 = i\).

Finally, note that 
\[\lambda^{-1} = -\sigma/\sqrt{A^2 + 1}\]
and since \((-1|\mathbb{F}_q) = 1\), (3) follows. 

The condition in (3) of the above theorem is not that easy to check. We will specialize to the case \(q = p\) in a moment and show how to determine the symbol \((-\mathbb{F}_p)\) in terms of power residue symbols and how to use reciprocity to determine the value in (3) for fixed \(a, b \in \mathbb{Z}\) and variable \(p\). However, the theorem above suffices for the case \(a = \pm 1\) since the value \(\lambda\) is then an 8th root of unity and its powers are evident. We leave the computations to the reader and record the conclusions as:

**Corollary 1.** Let \(p\) be an odd prime, \(a = \pm 1, b \in \mathbb{F}_q^\times\), and set \(A = 1\) or \(-1\) according as \(a(ab|\mathbb{F}_q) = 1\) or \(-1\). The polynomial \(f(x) = x^{(q+1)/2} + ax + b \in \mathbb{F}_q[x]\) has an irreducible quadratic factor if and only if \(t\) is odd, \(p = \pm 3 \mod 8\) and \(t = A \mod 4\) when \(p = -3, 11 \mod 16\) or \(t = -A \mod 4\) when \(p = 3, -11 \mod 16\).

We assume for the remainder of this article that \(q = p\), i.e., \(t = 1\). Our immediate goal is to replace the power symbols in Theorem 1 with residue symbols defined over number fields. First, a quick review of \(n\)th power residue symbols is in order. Such symbols are defined for a number field \(K\) containing the \(n\)th roots of unity. Let \(P\) denote an ideal in the ring \(\mathcal{O} = \mathcal{O}_K\) of integers in \(K\) and assume that \(P\) is prime to \(n\). The \(n\)th power residue symbol \((\alpha|\mathcal{O})_n\) is defined for all \(\alpha \in \mathcal{O}\) prime to \(P\) and has the following properties [CF, Ex. 1.1–1.4, pp. 348, 349]:

1. \((\alpha|\mathcal{O})_n\) is the unique \(n\)th root of unity in \(K\) determined by Euler’s criterion \((\alpha|\mathcal{O})_n = \alpha^{N(P^{n-1})}\) mod \(P, N(P) = |\mathcal{O}/P|\) and
2. \((\alpha PP^n)_n = (\alpha|\mathcal{O})_n (\alpha|P^n)_n\) and \((\alpha\beta|\mathcal{O})_n = (\alpha|\mathcal{O})_n (\beta|\mathcal{O})_n\).

The \(n\)th power residue symbol induces a multiplicative character of order \(n\) modulo \(P\). In our application, the cases considered are \(n = 2\) defining the quadratic residue symbol and \(n = 4\) defining the biquadratic residue symbol. In the event \(K = \mathbb{Q}, P = p\mathbb{Z}\), \(n = 2\), the quadratic residue symbol \((-p)^2 = (-p)\) is just the Legendre symbol. We define \((\alpha\beta|\mathcal{O})_n\) to be \((\alpha|\mathcal{O})_n\) whenever \(P = \beta\mathcal{O}\) is a principal prime ideal. We record three additional properties of power residues for later use. If \(*\) denotes complex conjugation then

1. \((\alpha|\mathcal{O})_n^{-1} = (\alpha^*|\mathcal{O}^*)_n\).

If \(F \subseteq L\) are number fields, \(\alpha^{2ni/n} \in F, P\) a prime ideal of \(L\), and \(B = \mathfrak{f} \cap F\), then \(\forall \alpha \in F\) prime to \(nP\),

1. \((\alpha|\mathcal{O})_n = (\alpha|B)_n, s = [\mathcal{O}_L/P : \mathcal{O}_L/B].\)
This is from the fact that the Frobenius \( x \rightarrow x^{N(B)} \) generates the Galois group of \( L(P) = \mathcal{C}_L/P \) over \( F(B) = \mathcal{C}_B/B \). Now \( \alpha^N(P-1) = \alpha(N(B)-1) \in \mathcal{N}(B)^{1,2,3,4} \in N(L(P)/F(B))_{\alpha(B)} = (\alpha(B) \mod P)

Let \( m \) be an integer prime to \( p, \pi | p \) a prime divisor in \( \mathbb{Z}[i] \), and \( \xi \in \mathbb{Z}[i] \) with \( \xi \xi^b = m \). Then

\[
(\nu) \left( \frac{\xi}{m} \right)^{(p^2 - 1)/4} = \left( \frac{\xi^2}{m} \right)^{(p^2 - 1)/8} = (\xi | p)_4 (m | p)^{(p - 1)/4} \mod \pi.
\]

For \( p = -1 \mod 4, \pi = \xi p \), and the formula follows from the observation that \((\nu m)^{(p^2 - 1)/4} = m^{(p^2 - 1)/8} = (m | p)^{(p + 1)/4} \mod p\mathbb{Z}[i] \), while \((\xi | p)_4 \equiv \xi^{(p^2 - 1)/4} \mod p\mathbb{Z}[i] \). If \( p = 1 \mod 4, (\nu m)^{(p^2 - 1)/4} = (m | p)_4^{(p + 1)/2} = (m | p)_4 (m | \pi)_4^{(p - 1)/2} \equiv \epsilon(m | \pi)_4 \mod \pi \), where, since \((p - 1)/2\) is even, \( \epsilon = 1 \) if \((m | \pi) = 1 \) and \( \epsilon = (-1)^{(p - 1)/4} \) if \((m | \pi) = -1 \). Also, \( \xi^{(p^2 - 1)/4} = (\xi | \pi)_4 \xi^b \equiv (\xi | \pi)_4 \mod \pi \) since \( x^p = \mod \pi \) for \( x \in \mathbb{Z}[i] \). Thus,

\[
\left( \frac{\xi}{m} \right)_4 = \left( \frac{\xi | \pi}{\pi} \right)_4 \left( \frac{\xi^b | \pi}{\pi} \right)_4 = \epsilon(\xi | \pi)_4 (\xi | \pi)_4 = \epsilon(\xi | p)_4.
\]

The transition from the power symbols used in Theorem 1 to power residue symbols in Theorem 2 below can be accomplished by taking \( \mathbb{F}_{p^2} \) to be the residue class field of a prime deal \( P/p \) in the ring \( \mathcal{C} \) of integers of \( \mathbb{Q}(i, \sqrt{A^2 + 1}) \) and the image of \( i, \sqrt{A^2 + 1} \) in this field to be the choice of roots for \( x^2 + 1, x^2 - (A^2 + 1) \). Note that if \( \mu: \mathcal{C} \rightarrow \mathcal{C}/P \) is the projection then \( \left( \mu(z) \mid \mathbb{F}_{p^2} \right)_4 = \mu((z | P)_4) \).

**Theorem 2.** Let \( p \) denote an odd prime, \( f(x) = x^{(p + 1)/2} + ax + b \in \mathbb{Z}[x] \) with \( ab \) prime to \( p \), and \( \sigma = 1 + Ai \in \mathbb{Z}[i], A = a(ab | p) \). A necessary and sufficient condition that \( f(x) \) have an irreducible quadratic factor modulo \( p \) is that \((a^2 + 1 | p) = -1 \) and \((-2 | p) (\sigma | p)_4 = i \). In the latter event, \( f(x) \) has the unique monic irreducible factor \( x^2 + 2(b/a)x + b^2/(a^2 + 1) \) modulo \( p \).

**Proof.** Theorem 1(3) reduces by \((\nu) \) above to \((-1 | p) (\sigma | p)_4 \equiv (-1 | p)^{(p - 1)/4} \equiv i \). A simple check of possible residues of \( p \) modulo 8 shows that \((-1 | p)^{(p - 1)/4} = (-2 | p). \)

We will require biquadratic reciprocity for the examples to follow. Certain biquadratic reciprocity formulas originated in the works of Eisenstein and a number of specialized formulas have been derived to date. The formula we require is easily derived from a general approach making use of norm residue symbols. We include its derivation for completeness. Set \( \rho = 1 + i \) and let \( k_\rho \) denote the completion of \( k = \mathbb{Q}(i) \) with respect to the valuation
determined by \( \rho \). The norm residue symbol \((\alpha, \beta)_\rho\) is defined for all \( \alpha, \beta \in k_\rho^* \) and has the following properties (see, e.g., [CF, pp. 352, 353]):

- (vi) \((\alpha, \beta)_\rho\) is a 4th root of unity;
- (vii) \((-,-)_\rho\) is bimultiplicative on \( k^*_\rho \times k^*_\rho \);
- (viii) \((\alpha, \beta)_\rho = 1\) if and only if \( \beta \) is a norm from \( k_\rho(\sqrt{\alpha}) \);
- (ix) \((\alpha, \beta)_\rho(\beta, \alpha)_\rho = 1\); and
- (x) (reciprocity) if \( \beta \in k_\rho \) is prime to \( \rho \) then \((\alpha, \beta)_\rho = (\beta|\alpha)_4 \)
  \((\alpha|\beta)_4^{-1} \forall \alpha \in k \text{ prime to } \rho \) and \((\alpha, \beta)_\rho = (\alpha|\beta)_4 \forall \alpha \in k \) that are units or divisible only by \( \rho \).

For \( \beta \in k_\rho, \beta = \rho^{(b)} \gamma \) with \( \gamma \) prime to \( \rho \). Set \( \text{ord}_\rho \beta = e(\beta) \).

**Lemma 1.** Let \( m, t \in \mathbb{Z} \) with \( m = 1 + 8t \). Then \( \forall \beta \in k_\rho^* \), \((m, \beta)_\rho = (-1)^{\text{ord}_\rho \beta} \).

**Proof.** (see e.g. [CF, EX. 2.12]). Hensel’s lemma implies that \( m = b^2 \in \mathbb{Q}_2 \). Set \( b = 1 + 2u \). By replacing \( b \) with \(-b\) if necessary, we can adjust so that \( u = 2v \). Thus \( m = (1 + 4v)^2, 2v^2 + v - t = 0 \). Now \( t = 0 \mod 2 \) implies \( u = 0 \mod 2 \mathbb{Z}_2 \) and hence \( m \) is a 4th power in \( \mathbb{Q}_2 \). In this event, \((m, \beta)_\rho = 1 \forall \beta \in k_\rho^* \). If \( t = 1 \mod 2 \) then \( k_\rho(\sqrt{m}) = k_\rho(\sqrt{1 + 4v}) = k_\rho(\tau), \tau = (1 + \sqrt{1 + 4v})/2 \) a root of \( x^2 - x - v = f(x) \). Since \( f'(x) = 1 \mod \rho, k_\rho(\sqrt{m}) \) is unramified over \( k_\rho^* \). Consequently, \( \beta \) is a norm from \( k_\rho(\sqrt{m}) \) if and only if \( \text{ord}_\rho \beta = e(\beta) \).

**Lemma 2 (Reciprocity).** Let \( \sigma = 1 + Ai \in \mathbb{Z}[i], 1 + A^2 = 2q \) with \( q \) an odd integer. Set \( 1 + Ai = (1 + i)^s \beta, s = \frac{1}{2} \text{trace}(\beta) \) and let \( p \) denote an odd prime not dividing \( 1 + A^2 \). Then

1. \((-2)p(\sigma|p)_4 = p^{(p^2 - 1)/8}(p|\beta)_4 \) if \( p = 1 \mod 8 \),
2. \((-2)p(\sigma|p)_4 = -p^{(p^2 - 1)/8}(-p|\beta)_4 \) if \( p = -1 \mod 8 \),
3. \((-2)p(\sigma|p)_4 = (-1)^p p^{(p^2 - 1)/8}(3p|\beta)_4(\beta|3)_4^{-1} = (-1)^p p^{(p^2 - 1)/8} \) \((-p|\beta)_4 \) if \( p = 3 \mod 8 \), and
4. \((-2)p(\sigma|p)_4 = (-1)^p p^{(p^2 - 1)/8}(-3p|\beta)_4(\beta|3)_4^{-1} = (-1)^p p^{(p^2 - 1)/8} \) \((p|\beta)_4 \) if \( p = -3 \mod 8 \).

**Proof.** \((1 + i)p|_4 = (2p)^{(p-1)/4} i^{(p^2 - 1)/8} \) by (v). Also, \((\sigma|p)_4 = (1 + i)p|_4(\beta|p)_4 \) and \((\beta|p)_4 = (p|\beta)_4(\beta|p)_4 \). The proof of the lemma therefore reduces to the computation of \((p, \beta)_\rho \). If \( p = 1 \mod 8 \) the value of the latter symbol is 1 by Lemma 1. If \( p = -1 \mod 8 \), \((p, \beta)_\rho(-1, \beta)_\rho = (-p, \beta)_\rho = 1 \). Thus, \((p, \beta)_\rho = (-1, \beta)_\rho^{-1} \), which by reciprocity is \((-1|\beta)_4^{-1} = (-1|\beta)_4 \). If \( p = \pm 3 \mod 8 \) then \((p, \beta)_\rho = (\pm 3, \beta)_\rho^{-1} = (\pm 3|\beta)_4(\beta|3)_4^{-1} \). Finally, the value \((-3, \beta)_\rho = (-3|\beta)_4(\beta|3)_4^{-1} = (-1)^p \) can be explicitly computed using the techniques in [CF, pp. 348–353]. We leave these computations to the reader.
Remark. Lemma 2 provides a general method for determining those primes $p$ for which for given $a$, $b$, $x^{(p-1)/2} + ax + b$ have an irreducible quadratic factor modulo $p$. For example, when $a$ even, we can ensure that $(-2|p)(p|\beta)_4 = i$ by selecting primes $p \equiv 1 \mod 8$ and $(p|\beta)_4 = i$; $p \equiv -1 \mod 8$ and $(-p|\beta)_4 = -i$; $p \equiv 3 \mod 8$ and $(3p|\beta)_4(\beta|3)^{-1} = i$; or $p \equiv -3 \mod 8$ and $(-3p|\beta)_4(\beta|3)^{-1} = -i$. Thus if $a = 4$ and $p = 31 \mod 2 \times 5$ then $x^{(p-1)/2} + 4x + b$ has an irreducible quadratic factor for each $b$ with $(b|p) = -1$.

Example 1 (Case $a = \pm 2$). We assume in this case that $(5|p) = (p|5) = -1$, i.e., $p = \pm 2 \mod 5$. Note that if $\sigma = 1 + Ai$ then $i = A \mod \sigma$. We have $(w|\sigma)_4 = w^{(5-1)/4} = w \mod \sigma$, $w \in \mathbb{Z}[i]$.

Lemma 2 implies $(-2|p)(\alpha|p)_4 = i$ if and only if $p = A \mod 5$ when $p \equiv \pm 1 \mod 8$ and $p = -A \mod 5$ when $p \equiv \pm 3 \mod 8$. Hence,

Corollary 2. Let $p$ be an odd prime, $a = \pm 2$, $b \in \mathbb{Z}$ with $b$ prime to $p$. A necessary and sufficient condition that $x^{(p-1)/2} + ax + b$ have an irreducible quadratic factor modulo $p$ is that $p = a(2b|p) \mod 5$.

Example 2 (Case $a = \pm 3$). We assume in this event that $(10|p) = -1$, i.e., $p = \pm 7, \pm 11 \pm 17$, or $\pm 19 \mod 40$. Set $\beta = 2 + i$ or $-1 - 2i$ according as $A = 3$ or $A = -3$. Thus, $1 + Ai = (1 + i)\beta$. Note that $i = A \mod \beta$; $(p|\beta)_4 = p \mod \beta$ and $(-1|\beta)_4 = -1$. Lemma 2 gives $(-2|p)(1 + Ai|p)_4 = i(p^{x-1})/8 \mod \beta$ if $p \equiv \pm 1 \mod 8$ and $(-p|p)_4 = i(p+7)/8(3p) \mod \beta$ if $p \equiv \pm 3 \mod 8$. It follows therefore that $(-2|p)$ $(1 + Ai|p)_4 = i$ if and only if $p = i(p-1)/8 \mod \beta$ when $p \equiv \pm 1 \mod 8$ and $p = 2i(p-1)/8 \mod 3 \mod 8$. The respective cases mod 16 for the last quantity are $p = A \mod 5$ when $p = \pm 1 \mod 16$; $p = -A \mod 5$ when $p = \pm 7 \mod 16$; $p = -\text{sign} A \mod 5$ when $p = \pm 3 \mod 16$; $p = \text{sign} A \mod 5$ when $p = \pm 5 \mod 16$. Hence,

Corollary 3. Let $p \neq 3$ be an odd prime, $a = \pm 3$, $b \in \mathbb{Z}$ with $b$ prime to $p$. A necessary and sufficient condition that $x^{(p-1)/2} + ax + b$ have an irreducible quadratic factor modulo $p$ is that when $A = a(b|p) = 3$, $p$ is one of $-23, -17, 7, 11, 19, 21, 33$, or $29 \mod 80$, and when $A = -3$, $p$ is one of $-7, -11, -19, -21, -29, -33, 17, or 23 \mod 80$.

Remark. The map $\phi(f(x)) = x^{\deg(f(x))} f(1/x)$ is an automorphism of the multiplicative semigroup of polynomials in $k[x]$ which do not vanish at zero. Consequently, finding the irreducible factors of $x^n + ax + b, b \neq 0$, is equivalent to finding the irreducible factors of $x^n + ab^{-1}x^{n-1} + b^{-1}$. Thus, our investigation also includes the question as to the quadratic factors of $x^{(q-1)/2} + ax^{(q-1)/2} + b, b \neq 0$. 

212

ESTES AND KOJIMA
ACKNOWLEDGMENT

The authors thank Irving Kaplansky for the question answered herein.

REFERENCES


