# Explicit Factorization of $x^{2^k}+1$ over $F_p$ with Prime $p \equiv 3 \bmod 4$

Ian F. Blake
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: ifblake@claude2.uwaterloo.ca

Shuhong Gao, Ronald C. Mullin
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: sgao@violet.uwaterloo.ca, rcmullin@watmath.uwaterloo.ca

Revised August 28, 1992

**Abstract.** In this note we give a complete explicit factorization of $x^{2^k}+1$ into irreducible polynomials over $F_p$ for a prime $p \equiv 3 \bmod 4$. As a result we can construct an irreducible polynomial over $F_p$ of degree of any power of 2. Some interesting properties of the coefficients of the irreducibles are noted. We also mention that our results may be useful in applying the Fast Fourier Transform over finite fields.

**Key words:** finite field, irreducible polynomial, primitive root of unity, Fast Fourier Transform (FFT).

**Contact author:** Shuhong Gao, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.

## Introduction

Let $p$ be a prime with $p \equiv 3 \bmod 4$. We consider the problem of completely factoring $x^{2^k}+1$ over $F_p$. As the roots of $x^{2^k}+1$ are primitive $2^{k+1}$th roots of unity (in some extension field of $F_p$), this problem is equivalent to constructing all the minimal polynomials over $F_p$ of primitive $2^{k+1}$th roots of unity for an arbitrary integer $k \geq 1$. Since the degree of any irreducible factor of $x^{2^k}+1$ is known to be a power of 2, it is also related to the problem of constructing an irreducible polynomial of degree $2^e$ for any given integer $e$.

The last problem is considered by Lenstra [4] and Shoup [7]. Let $2^a$ be the highest power of 2 in $p+1$. Then $2^{a+1}$ is the highest power of 2 in $p^2-1$. Let $\alpha \in F_{p^2}$ be of order $2^{a+1}$. Then it is known that $x^{2^e}-\alpha$ is irreducible over $F_{p^2}$ for any integer $e \geq 0$. Thus $(x^{2^e}-\alpha)(x^{2^e}-\alpha^p)$ is irreducible over $F_p$ of degree $2^{e+1}$ and its roots are primitive $2^{a+e+1}$th roots of unity. Both Lenstra and Shoup give simple ways to construct an element of order $2^{a+1}$ in $F_{p^2}$. Since $p \equiv 3 \bmod 4$, $-1$ is a quadratic nonresidue in $F_p$ and therefore $x^2+1$ is irreducible over $F_p$. So $F_{p^2} = F_p(i)$ where $i = \sqrt{-1}$. Let $f$ be the map $f: F_{p^2} \to F_{p^2}$ defined by $f(x) = (1+x)^{(p-1)/2}$. We define $f^{[k]}$ recursively: $f^{[0]}(x) = x$, $f^{[k+1]}(x) = f(f^{[k]}(x)), k \geq 0$. Lenstra [4, page 344] points out that, for every $k$ with $2 \leq k \leq a+1$, $f^{[k-2]}(i) \in F_{p^2}$ has multiplicative order $2^k$, in particular $f^{[a-1]}(i)$ has order $2^{a+1}$. (Actually $f(x)$ is one of the square roots of $x^{-1}$ if $x^{p+1}=1$.) Shoup [7, page 439] suggests taking $a-1$ successive square roots of $i$, then the resulting element is of order $2^{a+1}$. Taking square roots in $F_{p^2}$ can be done using the following formula

$$\sqrt{\alpha} = \begin{cases} i\alpha^{(p+1)/4}, & \text{if } \alpha^{(p-1)/2} = -1, \\ (1+\alpha^{(p-1)/2})^{(p-1)/2}\alpha^{(p+1)/4}, & \text{otherwise,} \end{cases}$$

which holds for any quadratic residue $\alpha$ in $F_p(i)$.

Both Lenstra's and Shoup's methods construct explicitly one element in $F_{p^2}$ of order $2^k$ for any $k \leq a+1$ by taking square roots. Note that if $\alpha$ is of order $2^k$ then both $\sqrt{\alpha}$ and $-\sqrt{\alpha}$ have order $2^{k+1}$ provided $k > 0$. One may modify their methods

to find all the elements of order $2^k$ recursively by starting at $i = \sqrt{-1}$. In order to factor $x^{2^{k+1}} + 1$, one then needs to compute the minimal polynomials over $F_p$ of all the elements constructed.

We shall show that all the irreducible factors of $x^{2^k}+1$ can be obtained by computing directly their coefficients. As a consequence, we find some interesting properties of the coefficients. All the operations will be in $F_p$.

**Main Results**

We assume that $p$ is a prime such that $2^a|(p+1)$, $2^{a+1} \nmid (p+1)$ with $a \geq 2$. Then $2^{a+1}$ is the highest power in $p^2 - 1$.

**Theorem 1** *Let $H_1 = \{0\}$. Recursively define*

$$H_k = \{\pm(\frac{u+1}{2})^{(p+1)/4} \ : \ u \in H_{k-1}\}$$

*for $k = 2, 3, \cdots, a-1$ and*

$$H_a = \{\pm(\frac{u-1}{2})^{(p+1)/4} \ : \ u \in H_{a-1}\}.$$

*Then, for $1 \leq k \leq a-1$, $H_k$ has cardinality $2^{k-1}$,*

$$x^{2^k} + 1 = \prod_{u \in H_k} (x^2 - 2ux + 1), \tag{1}$$

*and for any integer $e \geq 0$,*

$$x^{2^{a+e}} + 1 = \prod_{u \in H_a} (x^{2^{e+1}} - 2ux^{2^e} - 1). \tag{2}$$

*All the factors in the above products are irreducible over $F_p$.*

*Proof.* First note that $F_{p^2}$ contains all the $2^{a+1}$th roots of unity, since $2^{a+1}|(p^2-1)$. Note that since $2^2 \nmid (p-1)$, for $1 \leq k \leq a$, every primitive $2^{k+1}$th root of unity is of degree 2 over $F_p$. We prove (1) and (2) by induction on $k$.

For $k = 1$, note that $p \equiv 3 \bmod 4$, $-1$ is a quadratic nonresidue in $F_p$. Hence $x^2 + 1$ is irreducible over $F_p$. Therefore (1) is true for $k = 1$.

Assume that (1) is true for $k$ with $1 \leq k < a$. For $k+1$, we prove that (1) is true if $k+1 < a$ and (2) with $e = 0$ is true if $k+1 = a$. Substituting the $x$ in (1) by $x^2$ yields

$$x^{2^{k+1}} + 1 = \prod_{u \in H_k} (x^4 - 2ux^2 + 1).$$

and for a complete factorization it is required to factor

$$x^4 - 2ux^2 + 1 \tag{3}$$

for any $u \in H_k$.

Let $\beta$ be a root of (3). Then $\beta$ is of order $2^{k+2}$. As $k + 2 \leq a + 1$, $\beta$ is of degree 2 over $F_p$. The minimal polynomial of $\beta$ is of the form

$$x^2 - 2rx + s, \tag{4}$$

where $r, s \in F_p$. As $\beta$ is a root of both (3) and (4), we have

$$\beta^2 + s = 2r\beta, \tag{5}$$

and

$$\beta^4 = 2u\beta^2 - 1. \tag{6}$$

Squaring (5) gives

$$\beta^4 = (4r^2 - 2s)\beta^2 - s^2. \tag{7}$$

From (6) and (7) we have

$$(4r^2 - 2s)\beta^2 - s^2 = 2u\beta^2 - 1.$$

As $\beta^2 \notin F_p$ (since $\beta^2$ has order $2^{k+1}$ and $2^{k+1} \nmid (p-1)$), we must have $4r^2 - 2s = 2u$ and $s^2 = 1$. So

$$s = \pm 1, \tag{8}$$

and

$$r = \pm\sqrt{\frac{u+s}{2}} = \pm(\frac{u+s}{2})^{(p+1)/4}. \tag{9}$$

The last equation follows from the fact that if $w$ is a quadratic residue in $F_p$ then $w^{(p+1)/4}$ is a square root of $w$. We prove that $s$ must be 1 if $k < a-1$, and $-1$ if $k = a-1$.

**Case 1** $k < a-1$. Then $k+1 \leq a-1$ and $k+3 \leq a+1$. Suppose $s = -1$ in (8) and (9). Then, from (4), $x^2 - 2rx - 1$ is irreducible and its roots are primitive $2^{k+2}$th roots of unity. Hence the roots of $x^4 - 2rx^2 - 1$ are primitive $2^{k+3}$th roots of unity. As $k+3 \leq a+1$, $x^4 - 2rx^2 - 1$ has two irreducible factors of degree 2, and assume $x^2 - 2\bar{r}x + \bar{s}$ is one of them. Then, by a similar argument leading to (8) and (9), we find that

$$\bar{s}^2 = -1 \tag{10}$$

and

$$4\bar{r}^2 - 2\bar{s} = 2r \tag{11}$$

have at least one solution $(\bar{r}, \bar{s}) \in F_p \times F_p$. This is impossible , as $-1$ is a quadratic nonresidue in $F_p$.

Therefore $s = 1$ in (8) and (9). Since (3) has irreducible factors of degree 2, for every $u \in H_k$, $(u+1)/2$ must be a quadratic residue in $F_p$. Let $u_1 = ((u+1)/2)^{(p+1)/4}$. Then

$$x^4 - 2ux^2 + 1 = (x^2 - 2u_1x + 1)(x^2 - 2(-u_1)x + 1).$$

So (1) is true for $k+1$.

**Case 2** $k = a-1$. In this case, $k+2 = a+1, k+3 = a+2 > a+1$. Suppose $s = 1$ in (8) and (9). Then both $x^2 - 2rx + 1$ and $x^2 + 2rx + 1$ are irreducible and have roots being primitive $2^{a+1}$th roots of unity. Thus the roots of

$$x^4 - 2rx^2 + 1 \tag{12}$$

and

$$x^4 + 2rx^2 + 1 \tag{13}$$

are primitive $2^{a+2}$th roots of unity. Since $p$ has order 4 modulo $2^{a+2}$, a primitive $2^{a+2}$th root of unity is of degree 4 over $F_p$. So (12) and (13) must be irreducible over $F_p$.

It is easy to see that if $(r+1)/2 = \bar{r}^2$ for some $\bar{r} \in F_p$, then $x^2 - 2\bar{r}x + 1$ divides (12); if $(r-1)/2 = \tilde{r}^2$ for some $\tilde{r} \in F_p$, then $x^2 - 2\tilde{r}x - 1$ divides (12). So for (12) to be irreducible, both $(r+1)/2$ and $(r-1)/2$ must be quadratic nonresidues. Similarly, for (13) to be irreducible, both of $(-r+1)/2$ and $(-r-1)/2$ must also be quadratic nonresidues. This is impossible, since $-1$ is a quadratic nonresidue in $F_p$ and one of $(r+1)/2$ and $-(r+1)/2$ is a quadratic nonresidue in $F_p$.

Therefore $s = -1$ in (8) and (9). Hence, for each $u \in H_k$, $(u-1)/2$ is a quadratic residue in $F_p$. Let $u_1 = ((u-1)/2)^{(p+1)/4}$. Then

$$x^4 - 2ux^2 + 1 = (x^2 - 2u_1x - 1)(x^2 - 2(-u_1)x - 1).$$

So (2) is true for $e = 0$.

This proves by induction that (1) and (2) with $e = 0$ hold. As the factors in (1) and (2) (with $e = 0$) are minimal polynomials of roots of unity, they are all irreducible over $F_p$. For $e > 0$, (2) obviously holds as it is true for $e = 0$. We just need to prove that every factor in (2) is irreducible over $F_p$. For any $u \in H_a$, we have proved that $x^2 - 2ux - 1$ is irreducible over $F_p$. Let $\alpha_1, \alpha_2$ be its two roots. We know that $\alpha_1, \alpha_2 \in F_{p^2}$ and have order $2^{a+1}$. By Theorem 3.75 [5, page 124], $x^{2^e} - \alpha_1$ and $x^{2^e} - \alpha_2$ are irreducible over $F_{p^2}$ for any integer $e \geq 1$. Hence

$$(x^{2^e} - \alpha_1)(x^{2^e} - \alpha_2) = x^{2^{e+1}} - 2ux^{2^e} - 1$$

is irreducible over $F_p$.

This completes the whole proof. □

Note that when $p \equiv -1 \bmod 8$ (so $a > 2$), $1/2$ is a quadratic residue in $F_p$. From the above proof we see that if $k < a-1$ then, for every $u \in H_k$, $(u+1)/2$ is a quadratic residue in $F_p$,thus $u+1$ is a quadratic residue. Observe that the irreducibility of $x^2 - 2ux + 1 = (x-u)^2 - (u^2-1)$ implies that $u^2 - 1 = (u-1)(u+1)$ is a quadratic nonresidue. So $u-1$ is a quadratic nonresidue. Similarly, for $u \in H_{a-1}$, $u-1$ is a quadratic residue and $u+1$ is a quadratic nonresidue. For $u \in H_a$, we can only say that $u^2+1$ is a quadratic nonresidue due to the irreducibility of $x^2 - 2ux - 1$. In summary, we have

**Corollary 2** *If $p \equiv -1 \bmod 8$ (hence $a > 2$), then*

**(a)** *for each $1 \le k < a-1$ and $u \in H_k$, $u+1$ is a quadratic residue in $F_p$ and $u-1$ is a quadratic nonresidue in $F_p$;*

**(b)** *for each $u \in H_{a-1}$, $u-1$ is a quadratic residue in $F_p$ and $u+1$ is a quadratic nonresidue in $F_p$;*

**(c)** *for each $u \in H_a$, $u^2+1$ is a quadratic nonresidue in $F_p$.*

This solves, in a theoretical sense, a problem arising from primality testing [3, (11.6)(a)] and [2, section 5], as remarked by Lenstra [4, page 344].

**Corollary 3** *For $1 \le k \le a$, let $u \in H_k$. Define*

$$v = \begin{cases} (1-u^2)^{(p+1)/4}, & \text{if } k < a, \\ (-1-u^2)^{(p+1)/4}, & \text{if } k = a. \end{cases}$$

*Then $u + iv \in F_{p^2} = F_p(i)$ is a $2^{k+1}$th primitive root of unity where $i = \sqrt{-1}$.*

*Proof.* For $u \in H_k$ with $k < a$, we know from Corollary 2 that $1-u^2$ is a quadratic residue in $F_p$. So $v = (1-u^2)^{(p+1)/4}$ is a square root of $1-u^2$, that is, $v^2 = 1-u^2$. Hence $u+iv$ is a root of $x^2 - 2ux + 1$. By Theorem 1, $u+iv$ is a $2^{k+1}$th primitive root of unity. For $u \in H_a$, the proof is similar. □

As $x^{2^t}-1=(x-1)\prod_{i=0}^{t-1}(x^{2^i}+1)$, the following corollary is an immediate consequence of Theorem 1.

**Corollary 4** *For any integer $t \geq 1$, the following factorization over $F_p$ is complete:*

**(a)** *if $t < a+1$, then*

$$x^{2^t}-1=(x-1)(x+1)\prod_{i=1}^{t-1}\prod_{u\in H_i}(x^2-2ux+1);$$

**(b)** *if $t \geq a+1$, then*

$$x^{2^t}-1=(x-1)(x+1)\prod_{\substack{u\in H_i\\ 1\leq i\leq a-1}}(x^2-2ux+1)\prod_{\substack{u\in H_a\\ 0\leq r\leq t-a-1}}(x^{2^{r+1}}-2ux^{2^r}-1).$$

**Remark**

We mention a possible application of the preceding results in applying the Fast Fourier Transform (FFT) over finite fields [6, Chapter IX] and [1, Chapter 7]. The FFT is widely used in many areas including computing the convolution of data, digital signal processing and computing products of polynomials or integers. In [6], to apply the FFT over finite fields one chooses an appropriately large $N=2^e$ and a prime $p$ of the form $Nk+1$. If an $N$th root of unity $\omega$ in $F_p$ is given, then the FFT evaluates a polynomial in $F_p[x]$ of degree at most $N$ at the $N$ points $1,\omega,\omega^2,\ldots,\omega^{N-1}$ in time $O(N\log N)$. The problem here is that, when an integer $e$ and a prime $p=2^ek+1$ are given, there is currently no deterministic polynomial time (in $\log p$ and $e$) algorithm to construct a $2^e$th primitive root of unity in $F_p$. It is suggested in [1] to apply the FFT over the ring $Z_m$ of integers modulo $m$ where $m=2^{N/2}+1$ (which is not necessarily a prime). One advantage of $Z_m$ is that 2 is known to be a primitive $N$th root of unity in $Z_m$. Since the number $m$ is exponential in $N$, the computation in $Z_m$ may be expensive for large $N$. In the following we show that such problems do not exist if one operates the FFT over $F_{p^2}$.

Let $e \geq 1$ be a positive integer and $N = 2^e$. Let $p$ be any prime of the form $2Nk-1$. Define $u = u_e$ inductively: $u_1 = 0$ and

$$u_k = (\frac{1 + u_{k-1}}{2})^{(p+1)/4}, \quad k = 2, 3, \ldots, e.$$

Let

$$v = (1 - u^2)^{(p+1)/4}.$$

Then, by Theorem 1 and Corollary 3, $\omega = u + iv \in F_{p^2} = F_p(i)$ is a $2^e$th primitive root of unity where $i = \sqrt{-1}$. Here the number of $F_p$-operations needed to get $u + iv$ is $O(e \log p)$. So one can compute a $2^e$th primitive root of unity in $F_{p^2}$ quickly for any given integer $e$ and prime $p$ of the form $2Nk - 1$. Also, for fixed $N = 2^e$, the generalized prime number theorem implies that the number of primes $2Nk-1 \leq N^2$ is approximately $N/(2e)$. This means that primes of the required form exist in reasonable abundance and their sizes can be bounded by $N^2$. So the problems encountered in [1] and [6] are avoided when the FFT is applied over $F_{p^2}$.

**Conclusion**

We have given a direct way to compute the coefficients of the irreducible factors of $x^{2^k} + 1$ over $F_p$ for a prime $p \equiv 3 \bmod 4$ and for any given integer $k$. From the coefficients of these irreducible factors, one can produce many quadratic residues and quadratic nonresidues in $F_p$. It was also noticed that our results may be useful in applying the Fast Fourier Transform over finite fields.

# References


[1] Aho, A. V., Hopcroft, J. E., Ullman, J. D.: *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, MA, 1974.

[2] Borho, W., J. Buhl, H. Hoffmann, S. Mertens, E. Nebgen and R. Reckow: Große Primzahlen und Befreundete Zahlen: Über den Lucas-Test und Thabit-Regeln. *Mitt. Math. Ges. Hamburg* **11**, 232–256 (1983).

[3] Cohen, H., Lenstra, H. W., Jr.: Primality testing and Jacobi sums. *Math. Comp.* **42**, 297–330 (1984).

[4] Lenstra, H. W.: Finding isomorphisms between finite fields. *Math. Comp.* **56**, 329–347 (1991).

[5] Lidl, R., Niederreiter H.: *Finite Fields*. Addison-Wesley, Reading, MA, 1983.

[6] Lipson, J. D.: *Elements of Algebra and Algebraic Computing*. Benjamin/Cummings, 1981.

[7] Shoup, V.: New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.* **54**, 435–447 (1990).