USING THE THEORY OF CYCLOTOMY
TO FACTOR CYCLOTOMIC POLYNOMIALS
OVER FINITE FIELDS

GREG STEIN

Abstract. We examine the problem of factoring the \( r \)th cyclotomic polynomial, \( \Phi_r(x) \), over \( \mathbb{F}_p \), \( r \) and \( p \) distinct primes. Given the traces of the roots of \( \Phi_r(x) \) we construct the coefficients of \( \Phi_r(x) \) in time \( O(r^4) \). We demonstrate a deterministic algorithm for factoring \( \Phi_r(x) \) in time \( O((r^{1/2+\epsilon}\log p)^9) \) when \( \Phi_r(x) \) has precisely two irreducible factors. Finally, we present a deterministic algorithm for computing the sum of the irreducible factors of \( \Phi_r(x) \) in time \( O(r^6) \).

1. Introduction

In 1990, V. Shoup [19] related the problem of deterministically constructing arbitrary extensions of finite fields to that of factoring cyclotomic polynomials. We concern ourselves here with the problem of factoring the \( r \)th cyclotomic polynomial, \( r \) prime, over prime fields. The case where these two primes are the same is covered very effectively by Artin-Schreier theory (see, for example, [12, p. 325, Theorem 6.4] or [19, Lemma 2.3]), so we will only be concerned with the case where the primes are distinct.

In this text the term operation refers to an addition or multiplication of binary digits. By \( O(a) \) operations we mean that the number of operations is bounded by some fixed multiple of \( a \).

Please note that many polynomial time algorithms exist for factoring polynomials over finite fields which are probabilistic or depend upon unproven hypotheses (see, for example, [4], [7], [9], [17], or [5, section 3.4.4]). The techniques presented here are not intended to compete with these in running time. For this reason, analyses of running times are not as accurate as possible. For more precise running times for various operations the reader is referred to [3] and [11].

Sections 1 and 2 are an introduction and a brief review of the theory of cyclotomy. In Sections 3 and 4 we show how to derive the factors of \( \Phi_r(x) \) from the traces of the roots of \( \Phi_r(x) \) over \( \mathbb{F}_p \) in time \( O(r^4) \). In Section 5 we demonstrate a deterministic algorithm which does not depend on ERH for finding these factors in time \( O((r^{1/2+\epsilon}\log p)^9) \) in the case where \( \Phi_r(x) \) has precisely two irreducible
factors over $\mathbb{F}_p$. Section 6 gives a deterministic algorithm which does not depend upon ERH, for computing the sum of the irreducible factors of $\Phi_r$ in time $O(r^6)$.

2. A Review of Cyclotomy

Throughout this text we shall apply the results of the theory of cyclotomy, originally developed by Gauss, to explore the relationship between the traces of the $r$th roots of unity and the irreducible factors of the $r$th cyclotomic polynomial. To this end we begin with a brief review of the theory of cyclotomy. More thorough treatments can be found in Storer [22], Berndt, Evans and Williams [2], Dickson [6], Myerson [16], or Baumert and Mills [11].

In the classical treatment of cyclotomy the following definitions and observations are made over $\mathbb{Q}$. Given a prime number, $r$, positive integers $d$ and $m$ with $dm = r - 1$, and a primitive element, $\alpha$, of $\mathbb{F}_r$ (that is, an element of $\mathbb{F}_r$ which multiplicatively generates $\mathbb{F}_r^*$), we define the cyclotomy classes

\[
H_0 = \{1, \alpha^m, \alpha^{2m}, \ldots, \alpha^{(d-1)m}\},
\]

\[
H_1 = \{\alpha, \alpha^{m+1}, \alpha^{2m+1}, \ldots, \alpha^{(d-1)m+1}\},
\]

\[\vdots\]

\[
H_i = \{\alpha^i, \alpha^{m+i}, \alpha^{2m+i}, \ldots, \alpha^{(d-1)m+i}\},
\]

\[\vdots\]

\[
H_{m-1} = \{\alpha^{m-1}, \alpha^{m+(m-1)}, \alpha^{2m+(m-1)}, \ldots, \alpha^{(d-1)m+(m-1)}\}.
\]

Noting that $\alpha^{m+i}H_0 = \alpha^iH_0$, we see that we may index the $H_i$ with $\mathbb{Z}/m\mathbb{Z}$. We then define the *cyclotomic numbers*, $(i, j), i, j \in \mathbb{Z}/m\mathbb{Z}$, by

\[
(i, j) = \#(H_i^+ \cap H_j),
\]

where $H_i^+ = \{x + 1 \mid x \in H_i\} \subseteq \mathbb{F}_r$.

We should remark at this point that one may find primitive elements of $\mathbb{F}_r^*$ in time $r^{O(1)}$ (for each $b \in \mathbb{F}_r^*$ check whether $b^{\frac{r-1}{m}} = 1$, for all primes $l$ dividing $r - 1$, roughly $O(r \log^2 r)$ operations). Note also that $H_i$ can be computed by performing $d$ multiplications in $\mathbb{F}_r$, that $H_i^+$ can be computed by performing $d < r$ additions in $\mathbb{F}_r$, that $H_i^+ \cap H_j$ can be found in $O(d \log d)$ operations (by sorting and looking for matches) and then $(i, j)$ can be computed by counting to at most $d$. Therefore, all of the cyclotomy classes and cyclotomic numbers can be deterministically computed in time $O(r \log^2 r)$.

If we now think of working over some field, $\mathbb{F}$, and let $\zeta$ represent a primitive $r$th root of unity in an appropriate extension field, $\mathbb{K}$, then one defines the *periods*, $t_i$, by

\[
t_i = \sum_{j=0}^{d-1} \zeta^{\alpha^{m+j+i}} = \sum_{a \in H_i} \zeta^a.
\]

Noting that $t_i = t_{m+i}$, we consider the $t_i$ to be indexed by $\mathbb{Z}/m\mathbb{Z}$.

Although the classical theory of cyclotomy is used to study roots of unity over the rationals, all of the basic definitions and theorems make sense and are true over any field. In particular, we wish to look at a special application of this theory with the intention of factoring the $r$th cyclotomic polynomial, $\Phi_r = x^{\frac{r-1}{p}} - 1 + x + x^2 + \cdots + x^{r-1}$, over $\mathbb{F}_p$, $r$ and $p$ distinct primes. The elementary theory of finite
fields (see, for example, [10], [13] or [14]) tells us that \( \Phi_r \) will factor into \( m \) distinct irreducible polynomials, each of degree \( d \), where \( d = \text{ord}(p, r) \), the order of \( p \) in \( \mathbb{F}_r^* \) (that is, the least positive integer \( d \) so that \( p^d \equiv 1 \mod r \)) and \( m = \frac{r - 1}{d} \). We now compute the cyclotomy classes using this choice of \( d \) and \( m \).

As \( H_0 \) is the unique subgroup of \( \mathbb{F}_r^* \) with order \( d \) and, since \( \text{ord}(p, r) = d \), it follows that

\[
H_0 = \langle p \rangle = \{1, p, p^2, \ldots, p^{d-1}\} \subseteq \mathbb{F}_r^*.
\]

Now let \( \zeta \) be a primitive \( r \)th root of unity in some extension field of \( \mathbb{F}_p \) so that the irreducible factors of \( r(x) \) over \( \mathbb{F}_p \) are

\[
g_i(x) = \prod_{j=0}^{d-1} (x - \zeta^{a^j p^i}) = \prod_{a \in H_i} (x - \zeta^a), \quad i \in \mathbb{Z}/m\mathbb{Z},
\]

and note that \( t_i = \text{trace} g_i(\zeta^{a^j}) \), the sum of the roots of \( g_i(x) \) or, equivalently, that \( -t_i \) is the coefficient of \( x^{d-1} \) in \( g_i(x) \).

It will also be of use to include here some of the basic identities concerning the cyclotomic numbers. A proof of the following may be found in [22, Lemma 3, p. 25] or in [2, Theorem 2.2.1, p. 69].

**Lemma 2.1.**

1. \((i, j) = (m - i, j - i)\).
2. \((i, j) = \begin{cases} (j, i) & \text{if } d \text{ even}, \\ (j + \frac{m}{2}, i + \frac{m}{2}) & \text{if } d \text{ odd.} \end{cases} \)
3. \(\sum_{j=0}^{m-1} (i, j) = d - \theta_i \) where \( \theta_i = \begin{cases} 1 & d \text{ even, } i = 0, \\ 1 & d \text{ odd, } i = \frac{m}{2}, \\ 0 & \text{otherwise.} \end{cases} \)
4. \(\sum_{j=0}^{m-1} (i, j) = d - \eta_j \) where \( \eta_j = \begin{cases} 1 & j = 0, \\ 0 & \text{otherwise.} \end{cases} \)

A simple observation we will need later on, but not proved in any of the citations above, is the following lemma.

**Lemma 2.2.** For \( d \neq 1 \), in \( \mathbb{F}_r \)

\[
\sum_{\gamma \in H_i} \gamma = 0.
\]

**Proof.** Note that, in \( \mathbb{F}_r \)

\[
\sum_{\gamma \in H_i} \gamma = \alpha^i + \alpha^i p + \alpha^i p^2 + \cdots + \alpha^i p^{d-2} + \alpha^i p^{d-1};
\]

therefore,

\[
p \sum_{\gamma \in H_i} \gamma = \alpha^i p + \alpha^i p^2 + \alpha^i p^3 + \cdots + \alpha^i p^{d-1} + \alpha^i p^d
\]

and, since \( p^d = 1 \), we have

\[
p \sum_{\gamma \in H_i} \gamma = \sum_{\gamma \in H_i} \gamma.
\]

But \( d \neq 1 \) implies that \( p \neq 1 \) and, since \( p \) and \( r \) are distinct primes, it follows that \( p \neq 0 \). Hence \( \sum_{\gamma \in H_i} \gamma = 0. \)
3. Determining the Coefficients of the $g_i(x)$ from the $t_i$

The primary technique used here, delineated in Lemma 3.1, was actually first alluded to in the characteristic zero case by Gauss in [8, Section VII]. In this section we explicitly describe this technique, apply it to the characteristic $p$ case, and make a running time analysis. In particular, we show that we may compute, in time $O(r^4)$, each of the coefficients of the $g_i(x)$ in a specific way as $\mathbb{Z}$-linear combinations of the $t_i$. To accomplish this we first make a combinatorial observation.

Given $p$ and $r$, distinct primes, let $\alpha$ be a primitive element of $\mathbb{Z}/r\mathbb{Z}$ and let $d$, $m$ and the $H_i$ be as defined as in the previous section. Rather than work over $\mathbb{F}_p$ we shall work in $\mathcal{R}$, where $\mathcal{R} = \mathbb{Z}[Y]/(Y^r - 1)$. In $\mathcal{R}$ define the counterpart of $t_i$ to be

$$v_i = \sum_{k=0}^{d-1} Y^{\alpha_i} p^k, \quad i \in \mathbb{Z}/m\mathbb{Z},$$

and the counterpart of $g_i(x)$ to be

$$(3.1) \quad f_i(x) = \prod_{k=0}^{d-1} (x - Y^{\alpha_i} p^k), \quad i \in \mathbb{Z}/m\mathbb{Z},$$

in $\mathcal{R}[x]$.

Lemma 3.1. There exist two unique sets of integers, $\{\alpha^{(u)}_{st}\}_{u,t \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}}$ and $\{\beta^{(s)}_{t}\}_{u \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}}$, which can be computed deterministically in time $O(r^4)$, so that the coefficient of $x^i$ in $f_u(x)$ is

$$(-1)^{d-s} \left( \beta^{(s)}_{t} + \sum_{i=0}^{m-1} \alpha^{(u)}_{st} v_i \right).$$

We postpone the proof until we have made some observations.

Since $Y^r = 1$ in $\mathcal{R}$, we may view the exponents of $Y$ as elements of $\mathbb{Z}/r\mathbb{Z}$. Therefore each $f_u \in \mathcal{R}$ has a unique coset representative which is a polynomial in $x$ of degree $d$ whose coefficients are $(r-1)^m$ degree polynomials in $Y$ over $\mathbb{Z}$.

Let $S$ be the collection of all cardinality $l$ subsets of $\mathbb{Z}/d\mathbb{Z}$. Expanding (3.1) formally, we can write the coefficient of $x^{d-l}$ in $f_u(x)$ as

$$(3.2) \quad (-1)^l \sum_{\{i_1, \ldots, i_l\} \in S} Y^{\alpha^{(u)}(p^{i_1} + \cdots + p^{i_l})}$$

and note that there is a one-to-one correspondence with the $\binom{d}{l}$ terms in (3.2) with the elements of $S$. We then define an equivalence relation on $S$ by $\{i_1, \ldots, i_l\} \sim \{i_1 + k, \ldots, i_l + k\}$ for every $k \in \mathbb{Z}/d\mathbb{Z}$ and note that under this relation no partition contains more than $d$ elements. Now let $S_1 \subseteq S$ be the union of all partitions containing precisely $d$ elements of $S$ and let $S_2 \subseteq S$ be the union of all partitions containing fewer than $d$ elements of $S$. In addition, let $T_1 = \{\{i_1, \ldots, i_l\} \in S_1 \mid p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod d\}$ and $T_2 = S_1 - T_1$.

Now observe that if $p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod r$, then $p^{i_1+k} + \cdots + p^{i_l+k} = p^k(p^{i_1} + \cdots + p^{i_l}) \equiv 0 \bmod r$ and conversely, since $p^k \neq 0 \bmod r$ and $r$ is prime. That is, if $\{i_1, \ldots, i_l\} \sim \{j_1, \ldots, j_l\}$ then $\{i_1, \ldots, i_l\} \in T_1$ (or $T_2$) if, and only if, $\{j_1, \ldots, j_l\} \in T_1$ (or $T_2$, respectively). Therefore we may write $T_1 = P_1 \cup \cdots \cup P_{n_1}$
and $T_2 = Q_1 \cup \cdots \cup Q_{n_2}$, disjoint unions, where the $P_i$ and the $Q_i$ are partitions under the equivalence relation. Further note that $S = T_1 \cup T_2 \cup S_2$, where $T_1$, $T_2$ and $S_2$ are pairwise disjoint. We may now rewrite (3.2) as

$$(-1)^l \left( \sum_{k=1}^{n_1} \sum_{(i_1,\ldots,i_l) \in P_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{k=1}^{n_2} \sum_{(i_1,\ldots,i_l) \in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{(j_1,\ldots,j_l) \in S_2} Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} \right).$$

(3.3)

**Lemma 3.2.** If $P_k$, $Q_k$ and $S_2$ are as above, then

1. $\sum_{(i_1,\ldots,i_l) \in P_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = d$;
2. $\sum_{(i_1,\ldots,i_l) \in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = v_s$, where $p^{i_1} + \cdots + p^{i_l} \in H_{s-u}$; and
3. $\sum_{(j_1,\ldots,j_l) \in S_2} Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} = \#(S_2)$.

**Proof of Lemma 3.2 1.**

$$\{i_1,\ldots,i_l\} \in P_k \Rightarrow p^{i_1} + \cdots + p^{i_l} \equiv 0 \mod r \Rightarrow Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = 1.$$ Since $\#(P_k) = d$, the result follows.

**Proof of Lemma 3.2 2.** Say

$$Q_k = \{\{i_1,\ldots,i_l\},\ldots,\{i_1+(d-1),\ldots,i_l+(d-1)\}\},$$

then $\{i_1,\ldots,i_l\} \in Q_k \Rightarrow p^{i_1} + \cdots + p^{i_l} \not\equiv 0 \mod r \Rightarrow \alpha^u(p^{j_1} + \cdots + p^{j_l}) \not\equiv 0 \mod r$. Therefore there exist $e_k$, $1 \leq e_k \leq m-1$, such that $p^{i_1} + \cdots + p^{i_l} = \alpha^{e_k} p^j \in H_{e_k}$, hence $p^{i_1+n} + \cdots + p^{i_l+n} = \alpha^{e_k} p^{j+n} \in H_{e_k}$ and

$$\sum_{(i_1,\ldots,i_l) \in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = d \sum_{n=0}^{d-1} Y^{\alpha^u p^{j+n}} = \sum_{n=0}^{d-1} Y^{\alpha^u p^{n+j}} = v_{e_k+n}.$$ 

**Proof of Lemma 3.2 3.** If $\{j_1,\ldots,j_l\} \in S_2$, then there exist $n \in \mathbb{Z}/d\mathbb{Z} - \{0\}$ so that $\{j_1,\ldots,j_l\} = \{j_1+n,\ldots,j_l+n\} \in S_2$, hence $p^{j_1} + \cdots + p^{j_l} = (p^{j_1} + \cdots + p^{j_l}) p^n \in F_r$, but $p^n \not\equiv 1 \mod r$, so $p^{j_1} + \cdots + p^{j_l} \equiv 0 \mod r$, hence $\alpha^u(p^{j_1} + \cdots + p^{j_l}) \equiv 0 \mod r$, and therefore $Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} = 1 \in R$, and the lemma is proved.

We are now in a position to prove Lemma 3.1

**Proof of Lemma 3.1.** If we now let $e_{d-l}^{(u)}$ be the number of the $Q_1,\ldots,Q_{n_2}$ from Lemma 3.2 so that $\sum_{(i_1,\ldots,i_l) \in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = v_t$ and let $\beta_{d-l}^{(u)}$ equal $\#(S_2) + d n_2$, then, referring to Lemma 3.2 and (3.3), we have that the coefficient of $x^{d-l}$
Recall from the paragraph following Lemma 3.1 that the are therefore linearly independent in \(Q\), having degree no more than \(r\); unique coset representatives in \(R\) for.

The results of Lemma 3.2 show that \(Y\) as suggested in (3.6), we see that computing \(f_i(x)\) by \(\#(S) = \binom{d}{2} < 2^d\). Computing \(W_{i+1}(x)\) from \(W_i(x)\) as suggested in (3.3), we see that computing \(xW_i(x)\) involves increasing each exponent of \(x\) in \(W_i(x)\) by 1, \(O(r)\) operations. We then compute \(Y^{\alpha^np^{i+1}}W_i(x)\) by multiplying each of the polynomial coefficients of \(W_i(x)\) by \(Y^{\alpha^np^{i+1}}\) which involves at most \(d\cdot r\) additions modulo \(r\), or \(O(r^2\log r)\) operations. Finally, computing \(xW_i(x) - Y^{\alpha^np^{i+1}}W_i(x)\) involves at most \(d\cdot r\) additions of integers bounded by \(2^d\), or \(O(r^3)\) operations. As this process is repeated \(d\) times, we see that an upper bound for the computation is \(O(r^4)\) operations. This completes the proof of Lemma 3.1.
Before specializing to finite fields, we make the following observation.

**Lemma 3.3.** For \( i, t \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z} \), \( \beta_s^{(i)} = \beta_s^{(0)} \) and \( \alpha_{s,t}^{(i)} = \alpha_{s,t}^{(0)} \).

**Proof.** Let \( f_i(x) = \prod_{k=0}^{d-1}(x - \sqrt[n]{p^k}) \in \mathbb{R}[x] \) as in (3.1). From (3.3) we get that the coefficient of \( x^d - 1 \) in \( f_i(x) \) is

\[
(3.7) \quad (-1)^t \left( \sum_{k=1}^{n + m} \sum_{\{1, \ldots, u\} \in P_k} Y^{p^1 + \cdots + p^u} + \sum_{\{1, \ldots, j\} \in S_2} Y^{p_1^{i_1} + \cdots + p_1^{i_1}} \right),
\]

where \( S_2 \) is as in Lemma 3.2 and here the \( P_k \) run through all of the partitions of \( S_1 \). If \( e_k \equiv p^1 + \cdots + p^u \) mod \( r \) for some one of the \( \{i_1, \ldots, i_l\} \in P_k \), then we have

\[
(3.8) \quad \sum_{\{i_1, \ldots, j\} \in S_2} Y^{p_1^{i_1} + \cdots + p_1^{i_1}} = \sum_{u=0}^{d-1} Y^{e_k p_1^u} = \sum_{u=0}^{d-1} Y^{p_1^{i_1} + \cdots + p_1^{i_1}}.
\]

If \( e_k = 0 \in \mathbb{F}_r \), then (3.8) is precisely \( ^d \). Otherwise, we have that

\[
\{e_k \alpha^i, e_k \alpha^p, \ldots, e_k \alpha^{d-1}\} = H_{s+i},
\]

where \( e = \alpha^p \in H_s \), some \( i \), hence (3.8) is \( v_s+i \). If \( \{j_1, \ldots, j_l\} \in S_2 \), then, as in Lemma 3.2

\[
(3.9) \quad \sum_{\{j_1, \ldots, j\} \in S_2} Y^{p_1^{j_1} + \cdots + p_1^{j_1}} = \#(S_2).
\]

Now, \( \alpha_{s,t+i}^{(i)} \) is the number of partitions which yield \( v_{s+i} \) and these are the same partitions which yielded \( v_l \) in the coefficient of \( x^d - 1 \) for \( f(x) \). So \( \alpha_{s,t+i}^{(i)} = \alpha_{s,t}^{(i)} \), or \( \alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)} \) if \( \alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)} \).

The following version of the preceding lemma will prove useful later on. It should be noted that this result was noted by Gauss and is usually thought of as a result of Galois theory. This version has been presented in order to express it in our notation and to present a combinatorial proof.

**Lemma 3.4.** If \( i, t, k \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z} \), then

\[
\beta_s^{(i)} = \beta_s^{(k)}, \quad \alpha_{s,t-k}^{(i)} = \alpha_{s,t}^{(i+k)} \quad \text{and} \quad \alpha_{s,t}^{(i)} = \alpha_{s,t}^{(i+k)}.
\]

That is, if the coefficient of \( x^i \) is

\[
\lambda_{0t_0}^{(i)} + \lambda_{1t_1}^{(i)} + \lambda_{2t_2}^{(i)} + \cdots + \lambda_{m_{-2}t_{m-2}}^{(i)} + \lambda_{m_{-1}t_{m-1}}^{(i)} + \beta
\]

in \( g_0 \), then the coefficient of \( x^i \) is

\[
\lambda_{0t_0}^{(i)} + \lambda_{1t_1}^{(i)} + \lambda_{2t_2}^{(i)} + \cdots + \lambda_{m_{-2}t_{m-2}}^{(i)} + \lambda_{m_{-1}t_{m-1}}^{(i)} + \beta, \quad \text{in} \ g_1,
\]

\[
\lambda_{0t_0}^{(i)} + \lambda_{1t_1}^{(i)} + \lambda_{2t_2}^{(i)} + \cdots + \lambda_{m_{-2}t_{m-2}}^{(i)} + \lambda_{m_{-1}t_{m-1}}^{(i)} + \beta, \quad \text{in} \ g_2,
\]

\[
\lambda_{0t_0}^{(i)} + \lambda_{1t_1}^{(i)} + \lambda_{2t_2}^{(i)} + \cdots + \lambda_{m_{-2}t_{m-2}}^{(i)} + \lambda_{m_{-1}t_{m-1}}^{(i)} + \beta, \quad \text{in} \ g_3,
\]

\[
\vdots
\]

\[
\lambda_{0t_0}^{(i)} + \lambda_{1t_1}^{(i)} + \lambda_{2t_2}^{(i)} + \cdots + \lambda_{m_{-2}t_{m-2}}^{(i)} + \lambda_{m_{-1}t_{m-1}}^{(i)} + \beta \quad \text{in} \ g_{m-1}.
\]

**Proof.** That \( \beta_s^{(i)} = \beta_s^{(k)} \) is immediate from Lemma 3.3. To see that \( \alpha_{s,t-k}^{(i)} = \alpha_{s,t}^{(i+k)} \) simply observe that, from Lemma 3.3 and using \( t - k \) in place of \( t \), we have \( \alpha_{s,t-k}^{(i)} = \alpha_{s,t-i-k}^{(0)} \) and, by replacing \( i \) by \( i + k \), \( \alpha_{s,t}^{(i+k)} = \alpha_{s,t-i}^{(0)} \). To see that \( \alpha_{s,t}^{(i)} = \alpha_{s,t+k}^{(i+k)} \) note that \( \alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)} \) and, by replacing \( i \) by \( i + k \) and replacing \( t \) by \( t + k \),

\[
\alpha_{s,t+k}^{(i+k)} = \alpha_{s,t+k-i+k}^{(0)} = \alpha_{s,t-i}^{(0)}.
\]
We now restate Lemma 3.1 over $\mathbb{F}_p$, rather than $\mathbb{R}$.

**Theorem 3.5.** We can deterministically compute two subsets of $\mathbb{F}_p$,

$$\left\{ \alpha_{si}^{(u)} \right\}_{u,t \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}} \text{ and } \left\{ \beta_{si}^{(u)} \right\}_{u \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}},$$

in time $O(r^4)$, so that the coefficient of $x^s$ in $g_u(x)$ is

$$\tag{3.9} (-1)^{d-s} \left( \beta_{si}^{(u)} + \sum_{i=0}^{m-1} \alpha_{si}^{(u)} t_i \right).$$

Furthermore, we have that, for $i, t, k \in \mathbb{Z}/m\mathbb{Z}$, and $s \in \mathbb{Z}/d\mathbb{Z},$

$$\begin{align*}
\beta_{si}^{(i)} &= \beta_{si}^{(0)}, \\
\alpha_{s,t}^{(i)} &= \alpha_{s,t-i}^{(0)}, \\
\beta_{si}^{(i)} &= \beta_{si}^{(k)}, \\
\alpha_{s,t-k}^{(i)} &= \alpha_{s,t}^{(i+k)}, \\
\alpha_{s,t}^{(i)} &= \alpha_{s,t+k}^{(i)}.
\end{align*}$$

**Proof.** To prove existence and to compute the $\alpha_{si}^{(u)}$ and $\beta_{si}^{(u)}$ we simply reduce, modulo $p$, those integers discussed in Lemmas 3.2 and 3.4. When replacing $\mathbb{R}$ by $\mathbb{C}$ and computing over $\mathbb{F}_p$, we need only compute some of the additions modulo $p$, thereby replacing one factor of $r$ in the time bound by a factor of log $p$, thus giving us a time bounded by a polynomial in $r^3$ and log $p$. Please note that if $p \gg r$, in particular, if $p > 2^d$, then, since these coefficients never exceed $2^d$, we may perform the additions as before without reduction modulo $p$. Hence, the number of operations needed to compute the $\alpha_{si}^{(u)}$ and $\beta_{si}^{(u)}$ is $O(r^4)$. \qed

It should be noted that since $1 = -t_0 - t_1 - \cdots - t_{m-1}$ we may rewrite (3.9) as

$$\tag{3.10} (-1)^{d-s} \left[ \sum_{i=0}^{m-1} \delta_{si}^{(u)} t_i \right],$$

where $\delta_{si}^{(u)} = \alpha_{si}^{(u)} - \beta_{si}^{(u)}$, allowing us to write the coefficients of the $g_i(x)$ as homogeneous linear polynomials in the $t_i$. We may further observe that, as a result of Lemmas 3.2 and 3.4, we have, for $i, t, k \in \mathbb{Z}/m\mathbb{Z}$ and $s \in \mathbb{Z}/d\mathbb{Z},$

$$\begin{align*}
\delta_{si}^{(i)} &= \delta_{s,t-i}^{(0)}, \\
\delta_{s,t-k}^{(i)} &= \delta_{s,t}^{(i+k)}, \\
\delta_{s,t}^{(i)} &= \delta_{s,t+k}^{(i)}.
\end{align*}$$

Please note that in the statement of Theorem 3.5, we have lost the uniqueness portion of Lemma 3.1 and that, as $t_0 + \cdots + t_{m-1} = -1$, the $\alpha_{si}^{(u)}$ and $\beta_{si}^{(u)}$ will not be unique.

One remark that should be made at this point is that in the computation of the $\alpha_{si}^{(u)}$ and the $\beta_{si}^{(u)}$, $p$ itself has only been used to determine the cyclotomy classes $H_0, \ldots, H_{m-1}$ in $\mathbb{Z}/r\mathbb{Z}$. Therefore, if $p_1$ and $p_2$ are primes with $\operatorname{ord}(p_1, r) = \operatorname{ord}(p_2, r)$ (in particular, if $p_1 \equiv p_2 \bmod r$) they will generate the same cyclotomy classes and in the same order (assuming that the same primitive element, $\alpha$, for $\mathbb{F}_p^*$ was used). Hence, aside from the reduction mod $p_1$ or $p_2$, the $\alpha_{si}^{(u)}$, $\beta_{si}^{(u)}$ and $\delta_{si}^{(u)}$...
will be the same for both \( p_1 \) and \( p_2 \), and that, if both of these primes are \( > 2^d \), we need not even concern ourselves about this reduction.

**Example 3.6.** Let \( p = 31 \) and \( r = 19 \). We find that \( d = 6 \), \( m = 3 \), choose \( \alpha = 2 \) and let \( \zeta \) represent a primitive 19th root of unity over \( \mathbb{F}_{31} \). From this we compute the cyclotomy classes

\[
H_0 = \{1, 12, 11, 18, 7, 8\}, \\
H_1 = \{2, 5, 3, 17, 14, 16\}, \\
H_2 = \{4, 10, 6, 15, 9, 13\},
\]

and the cyclotomy periods

\[
t_0 &= \zeta + \zeta^{12} + \zeta^{11} + \zeta^{18} + \zeta^7 + \zeta^8, \\
t_1 &= \zeta^2 + \zeta^5 + \zeta^3 + \zeta^{17} + \zeta^{14} + \zeta^{16}, \\
t_2 &= \zeta^4 + \zeta^{10} + \zeta^6 + \zeta^{15} + \zeta^9 + \zeta^{13}.
\]

Using formula (3.5) from Lemma 3.1, we arrive at Table 1 which describes the coefficients of the powers of \( \zeta \) for each power of \( x \). The number in row \( x^n \) and column \( \zeta^i \) is \( g_{si}^{(n)} \). The number in column 1 and row \( x^n \) is \( g_{s0}^{(n)} \). Hence

\[
g_0 &= x^6 - t_0 x^5 + (3 + t_0 + t_2) x^4 - (2 + 2t_0 + t_1) x^3 \\
    & \quad + (3 + t_0 + t_2) x^2 - t_0 x + 1,
\]

and by Lemma 3.3 we have

\[
g_1(x) &= x^6 - t_1 x^5 + (3 + t_1 + t_0) x^4 - (2 + t_1 + 2t_2) x^3 \\
    & \quad + (3 + t_1 + t_0) x^2 - t_1 x + 1, \\
g_2(x) &= x^6 - t_2 x^5 + (3 + t_2 + t_1) x^4 - (2 + t_2 + 2t_0) x^3 \\
    & \quad + (3 + t_2 + t_1) x^2 - t_2 x + 1.
\]

Alternatively, using the characterization in (3.10), we get

\[
g_0(x) &= x^6 - t_0 x^5 - (2t_0 + 3t_1 + 2t_2) x^4 + (t_1 + 2t_2) x^3 \\
    & \quad - (2t_0 + 3t_1 + 2t_2) x^2 - t_0 x + 1, \\
g_1(x) &= x^6 - t_1 x^5 - (2t_0 + 2t_1 + 3t_2) x^4 + (2t_0 + t_2) x^3 \\
    & \quad - (2t_0 + 2t_1 + 3t_2) x^2 - t_1 x + 1, \\
g_2(x) &= x^6 - t_2 x^5 - (3t_0 + 2t_1 + 2t_2) x^4 + (t_0 + 2t_1) x^3 \\
    & \quad - (3t_0 + 2t_1 + 2t_2) x^2 - t_2 x + 1.
\]

<table>
<thead>
<tr>
<th></th>
<th>( H_0 )</th>
<th>( H_1 )</th>
<th>( H_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \zeta^{12} )</td>
<td>( \zeta^{11} )</td>
<td>( \zeta^8 )</td>
</tr>
<tr>
<td>( x )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( x^2 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x^3 )</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x^4 )</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x^5 )</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x^6 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Recalling the remarks immediately preceding this example, we see that we may replace \( p = 31 \) with any prime \( p \) with \( \text{ord}(p, 19) = 6 \), and we will get precisely the same results.

4. Further identities among the \( \alpha^{(u)}_d \) and \( \beta^{(u)}_d \)

We now wish to demonstrate some symmetries which occur among the \( \alpha^{(u)}_d \) and the \( \beta^{(u)}_d \). We begin by comparing the coefficients of \( x^t \) and \( x^{d-t} \). It should be noted that versions of the following results are alluded to without proof in [8, p. 423] for the characteristic zero case.

Let \( S \) be the collection of all \( l \) element subsets of \( \mathbb{Z}/d\mathbb{Z} \) and \( S' \) the collection of all \( d-l \) element subsets of \( \mathbb{Z}/d\mathbb{Z} \). Let \( \varphi : S \to S' \) be the bijection \( \varphi(I) = I^C \) (the complement of \( I \) in \( \mathbb{Z}/d\mathbb{Z} \)). Define an equivalence relation, \( \sim \), on both \( S \) and \( S' \) as in the proof of Lemma 3.1, that is, \( \{i_1, \ldots, i_t\} \sim \{i_1 + k, \ldots, i_t + k\} \), for each \( k \in \mathbb{Z}/m\mathbb{Z} \), and note that for \( I_1, I_2 \in S \) we have

\[
I_1 \sim I_2 \Leftrightarrow \varphi(I_1) \sim \varphi(I_2).
\]

Let \( S_1 \) be the subset of \( S \) consisting of all elements belonging to equivalence classes with \( d \) elements, and let \( S_2 \) be the set of all elements of \( S \) belonging to equivalence classes with fewer than \( d \) elements. Similarly define \( S'_1 \) and \( S'_2 \), subsets of \( S' \). Let \( P_1, \ldots, P_l \) and \( P'_1, \ldots, P'_w \) be the equivalence classes contained in \( S_1 \) and \( S'_1 \), respectively. By (4.1) we see that \( \varphi(S_1) = S'_1 \), and \( \varphi(S_2) = S'_2 \), that \( w = t \), and that, with the appropriate ordering, \( \varphi(P_k) = \varphi(P'_k), 1 \leq k \leq t \). Recalling (3.7) we note that in \( f_i(x) \) the coefficient of \( x^{d-t} \) is

\[
(-1)^d \sum_{\{i_1, \ldots, i_t\} \in P_k} \sum_{\{j_1, \ldots, j_t\} \in S_2} y^{\alpha^i_j (p^{i_1} + \cdots + p^{i_t})} + \sum_{\{j_1, \ldots, j_t\} \in S_2} y^{\alpha^i_j (p^{j_1} + \cdots + p^{j_t})},
\]

and that the coefficient of \( x^t \) is

\[
(-1)^{d-t} \sum_{k=1}^l \sum_{t} (P_k) \sum_{j_1, \ldots, j_t} y^{\alpha^i_j (p^{j_1} + \cdots + p^{j_t})}.
\]

Recall that \( \alpha^{(0)}_d \) is the number of \( P_k \) in (4.2) that yield \( v_t \), that \( \alpha^{(0)}_{d-t} \) is the number of \( P'_k \) in (4.3) that yield \( v_t \), and that \( \beta^{(0)}_l = \#(S_2) + d \) (the number of equivalence classes from (4.2) which do not yield any \( v_t \)) and that \( \beta^{(0)}_{d-t} = \#(S'_2) + d \) (the number of equivalence classes from (4.3) which do not yield any \( v_t \)).

**Lemma 4.1.** If \( d \) is even, then, for \( s \in \mathbb{Z}/d\mathbb{Z} \), \( i, k \in \mathbb{Z}/m\mathbb{Z} \), we have

\[
\beta^{(i)}_l = \beta^{(i)}_{d-l},
\]

\[
\alpha^{(i)}_k = \alpha^{(i)}_{d-k}.
\]

**Proof.** Note that \( (p^{d/2})^2 = 1 \in \mathbb{F}_r \). Since \( \text{ord}(p, r) = d \), it follows that \( p^{d/2} \neq 1 \), hence \( p^{d/2} = -1 \in \mathbb{F}_r \). Now, if \( d \) is even, then \( d/2 \in \{0, 1, \ldots, d\} \subset \mathbb{F}_r \). More generally, for \( k = 0, 1, \ldots, \frac{d}{2} - 1 \), we have

\[
\alpha^{i} p^k = -\alpha^{i} p^{d/2 + k} \in \mathbb{F}_r.
\]

That is, in \( H_i = \{\alpha^{i}, \alpha^{i} p^2, \ldots, \alpha^{i} p^d\} \subset \mathbb{F}_r^+ \) we have

\[
\alpha^{i} = -\alpha^{i} p^{d/2}, \alpha^{i} p = -\alpha^{i} p^{d/2+1}, \ldots, \alpha^{i} p^{d/2-1} = -\alpha^{i} p^{d-1}.
\]
Therefore

(4.5) \[ \gamma \in H_i \iff -\gamma \in H_i, \]

and, recalling Lemma 2.2

(4.6) \[ \sum_{\gamma \in H_i} \gamma = 0. \]

Let \( I = \{i_1, \ldots, i_l\} \in S \) and \( I^C = \{i_{l+1}, \ldots, i_d\} \in S'. \) From (4.6) we have that, since \( H_0 = \{p^0, p^1, p^2, \ldots, p^{d-1}\} \) and \( \{i_1, \ldots, i_d\} = \{0, 1, \ldots, d-1\}, \)

\[ p^{i_1} + \cdots + p^{i_l} = -(p^{i_{l+1}} + \cdots + p^{i_d}) \in \mathbb{F}_r. \]

Now, if \( I = \{i_1, \ldots, i_l\} \in S_2, \) hence \( I^C = \{i_{l+1}, \ldots, i_d\}, \) and \( p^{i_1} + \cdots + p^{i_l} = 0, \) then \( p^{i_{l+1}} + \cdots + p^{i_d} = 0, \) so \( Y^{p^{i_1} + \cdots + p^{i_l}} = Y^{p^{i_{l+1}} + \cdots + p^{i_d}} = 1 \in \mathbb{R}. \) Therefore

(4.7) \[ \sum_{\{i_1, \ldots, i_l\} \in S_2} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in S_2} Y^{p^{i_{l+1}} + \cdots + p^{i_d}} = \#(S_2). \]

Similarly, if \( \{i_1, \ldots, i_l\} \in P_k \) and \( p^{i_1} + \cdots + p^{i_l} = 0 \in \mathbb{F}_r, \) then

(4.8) \[ \sum_{\{i_1, \ldots, i_l\} \in P_k} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in P_k} Y^{p^{i_{l+1}} + \cdots + p^{i_d}} = \#(P_k). \]

Lastly, suppose \( \{i_1, \ldots, i_l\} \in P_w \) and \( p^{i_1} + \cdots + p^{i_l} = e_w \neq 0 \in \mathbb{F}_r, \) then \( e_w \in H_x, \) where \( e_w = \alpha^p \in \mathbb{F}_r, \) some \( l. \) Further note that \( e_w = p^{i_1} + \cdots + p^{i_l} \) implies \( e_w p^u = p^{i_1+u} + \cdots + p^{i_l+u} \) and that, by (4.5), we have \( H_x = \{e_w p^u\}_{u=0}^{d-1} = \{-e_w p^u\}_{u=0}^{d-1}. \)

Referring now to (4.6) and (4.7),

\[
\sum_{\{i_1, \ldots, i_l\} \in P_w} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{u=0}^{d-1} Y^{p^{i_1+u} + \cdots + p^{i_l+u}} = \sum_{u=0}^{d-1} Y^{e_w p^u} = \sum_{u=0}^{d-1} Y^{-p^{i_1+u} + \cdots + p^{i_d}} = \sum_{u=0}^{d-1} Y^{p^{i_1+u} + \cdots + p^{i_d+u}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in P_w} Y^{p^{i_{l+1}} + \cdots + p^{i_d}}
\]

and, noting that \( \sum_{u=0}^{d-1} Y^{e_w p^u} = v_x, \) we see that \( P_w \) yields \( v_x \) if, and only if, \( P'_w \) yields \( v_x. \)

Since \( \alpha_{lk}^{(0)} \) is the number of the \( P_w \) which yield \( v_k \) and \( \alpha_{d-l,k}^{(0)} \) is the number of \( P'_w \) which yield \( v_k, \) it follows that \( \alpha_{lk}^{(0)} = \alpha_{d-l,k}^{(0)}. \) Further, (4.7) and (4.8) show that \( \beta_1^{(0)} = \beta_{d-1}^{(0)}. \) Combining this result with Lemma 3.3, we have

\[
\beta_1^{(i)} = \beta_1^{(0)} = \beta_{d-1}^{(0)} = \beta_{d-i}^{(i)}
\]

and

\[
\alpha_{lk}^{(i)} = \alpha_{l,k-i}^{(0)} = \alpha_{d-l,k-i}^{(0)} = \alpha_{d-l,k}^{(i)},
\]

which completes the proof of the lemma.
hence

If

and, for \( s \in \mathbb{Z}/d\mathbb{Z} \), \( i, k \in \mathbb{Z}/m\mathbb{Z} \), there exists \( a \in \mathbb{Z}/m\mathbb{Z} \) so that

\[
\beta^{(i)}_l = \beta^{(i+a)}_d, \quad \alpha^{(i)}_l = \alpha^{(i+a)}_d.
\]

Proof. First note that, unlike the case for \( d \) even, if \( p^s \equiv -1 \mod r, 1 < s \leq d - 1 \), then \( d \) divides \( 2s \). But \( d \) is odd, so \( d \) divides \( s \), but \( 0 < s < d \), a contradiction. Therefore there exists an \( a \in \mathbb{Z}/m\mathbb{Z} - \{0\} \) such that \(-1 \in H_a\); that is, \(-1 \equiv \alpha^a p^h \mod r \) for some \( 0 \leq h \leq d - 1 \). So we have

\[
H_0 = \{1, p, p^2, \ldots, p^{d-1}\} \subseteq \mathbb{F}_r^*
\]

and

\[
H_a = \{\alpha^a p^s, \alpha^a p^{h+1}, \alpha^a p^{s+1}, \ldots, \alpha^a p^{h+d-1}\} \subseteq \mathbb{F}_r^*,
\]

and, for \( 0 \leq k \leq d - 1 \),

\[(4.9) \quad p^k = -\alpha^a p^{h+k} \in \mathbb{F}_r^*,
\]

In particular,

\[
\gamma \in H_0 \iff -\gamma \in H_a.
\]

Let \( I = \{i_1, \ldots, i_l\} \in S \) and \( I' = \{i_{l+1}, \ldots, i_d\} \in S' \). Working in \( \mathbb{F}_r \), from \((4.9)\) we have

\[
p^{i_1} + \cdots + p^{i_l} = -\left(\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l}\right),
\]

and from Lemma 2.2 we have, since \( H_a = \{\alpha^a, \alpha^a p, \ldots, \alpha^a p^{d-1}\} \) and

\[
\{h+i_1, \ldots, h+i_d\} = \{0, 1, \ldots, d-1\}
\]

that

\[
\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l} = \left(\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l}\right),
\]

hence

\[
p^{i_1} + \cdots + p^{i_l} = \alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l}.
\]

If \( \{i_1, \ldots, i_l\} \in S_2 \), then \( p^{i_1} + \cdots + p^{i_l} = 0 \), so \( \alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l} = 0 \), hence \( \alpha^a p^h \left(\alpha^a p^{i_1} + \cdots + \alpha^a p^{i_l}\right) = 0 \), and finally since \( \alpha^a p^h \neq 0 \), \( \alpha^a p^{i_1} + \cdots + \alpha^a p^{i_l} = 0 \). So we have

\[
(4.10) \quad \sum_{\{i_1, \ldots, i_l\} \in S_2} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in S_2'} Y^{\alpha^a \left(p^{i_{l+1}} + \cdots + p^{i_d}\right)} = \#(S_2).
\]

Similarly, if \( \{i_1, \ldots, i_l\} \in P_k \) and \( p^{i_1} + \cdots + p^{i_l} = 0 \in \mathbb{F}_r \), then

\[
(4.11) \quad \sum_{\{i_1, \ldots, i_l\} \in P_k} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in P_k'} Y^{\alpha^a \left(p^{i_{l+1}} + \cdots + p^{i_d}\right)} = \#(P_k).
\]
Lastly, suppose \( \{i_1, \ldots, i_l\} \in P_w \) and \( p^{i_1} + \cdots + p^{i_l} = e_w \neq 0 \in F_r \), then \( e_w \in H_s \) where \( e_w = \alpha^r p^i \in F_r \), some \( i \), and we have

\[
v_s = \sum_{u=0}^{d-1} Y^{e_p^{\nu}} = \sum_{\{i_1, \ldots, i_l\} \in P_w} Y^{p^{i_1} + \cdots + p^{i_l}}
= \sum_{\{i_1, \ldots, i_l\} \in P_w'} Y^{\alpha^{i_1} p^{i_1+1} + \cdots + \alpha^{i_l} p^{i_l+1}}
= \sum_{\{i_1, \ldots, i_l\} \in P_w'} Y^{\alpha^{(i+1)} p^{i+1} + \cdots + \alpha^{(i+a)} p^{i+a}}
\]

So \( P_w \), thinking of \( g_0(x) \), yields \( v_s \) if, and only if, \( P_w' \), thinking of \( g_a(x) \), yields \( v_s \). Since \( \alpha_{ik}^{(0)} \) is the number of the \( P_w \) from \( g_{0}(x) \) which yield \( v_k \), and \( \alpha_{d-l,k}^{(a)} \) is the number of \( P_w' \) from \( g_{a}(x) \) which yield \( v_k \), it follows that \( \alpha_{ik}^{(0)} = \alpha_{d-l,k}^{(a)} \). Further, (4.10) and (4.11) show that \( \beta_i^{(0)} = \beta_i^{(a)} \). Combining this with Lemma 3.3 we have

\[
\beta_i^{(i)} = \beta_i^{(0)} = \beta_i^{(a)} = \beta_i^{(i+a)}
\]

and

\[
\alpha_{ik}^{(i)} = \alpha_{ik}^{(0)} = \alpha_{d-l,k}^{(a)} = \alpha_{d-l,k}^{(i+a)}
\]

which completes the proof of the lemma.

5. The case \( m = 2 \)

In this section we prove a result first presented in [20]. The original work did not contain the explicit description of the algorithms used or as sharp a running time analysis.

**Theorem 5.1.** Given \( p \) and \( r \) odd primes, with \( \text{ord}(p, r) = \frac{r-1}{2} \), then we may factor \( \Phi_r(x) \), the \( r \)th cyclotomic polynomial, over \( F_p \), deterministically in time \( O((r^{1/2+\varepsilon} \log p)^9) \).

**Proof.** As a result of Theorem 3.3 it suffices to compute the traces \( t_0 \) and \( t_1 \). Note that if \( p = 2 \), then since \( t_0 + t_1 = -1 \) we must have that, without loss of generality, \( t_0 = 0 \) and \( t_1 = 1 \). So assume \( p \neq 2 \) and consider the polynomial

\[
(x - t_0)(x - t_1) = x^2 - (t_0 + t_1)x + t_0 t_1 = x^2 + x + t_0 t_1.
\]

Hence

\[
t_0, t_1 = \frac{-1 \pm \sqrt{1 - 4t_0 t_1}}{2}.
\]

From [13] pp. 200–201] we have that \( 1 - 4t_0 t_1 = \pm r \) as \( r \equiv \pm 1 \mod 4 \), respectively, hence

\[
t_0, t_1 = \frac{-1 \pm \sqrt{\pm r}}{2},
\]

where the sign of \( r \) under the radical is determined by whether \( r \equiv \pm 1 \mod 4 \). In 1985 R. Schoof showed in [13] that if \( n \) is a quadratic residue mod \( p \), then \( \sqrt{n} \) can be deterministically computed in \( F_p \) in time \( O((|n|^{1/2+\varepsilon} \log p)^9) \). Since \( t_0 \) and \( t_1 \) exist, it follows that \( 1 - 4t_0 t_1 \) is a quadratic residue mod \( p \) and so can be deterministically computed in time \( O((r^{1/2+\varepsilon} \log p)^9) \). \( \square \)
6. The sum of the $g_i(x)$

In this section we see how to compute the sum of the irreducible factors of the cyclotomic polynomial.

We combine the results of Theorem 3.5 and Lemma 3.3 to prove

**Lemma 6.1.** Given $p$ and $r$, distinct primes, then we may explicitly compute $g_0(x) + \cdots + g_{m-1}(x) \in \mathbb{F}_p[x]$, the sum of the irreducible factors of the $r$th cyclotomic polynomial over $\mathbb{F}_p$, in time $O(r^6)$.

**Proof.** Adding the coefficients for $x^s$ from Theorem 3.5 we have

$$
\sum_{u=0}^{m-1} \left( \beta_s^{(u)} + \sum_{i=0}^{m-1} \alpha_{s,i} t_i \right) = \sum_{u=0}^{m-1} \beta_s^{(u)} + \sum_{i=0}^{m-1} \left( \sum_{u=0}^{m-1} \alpha_{s,i} t_i \right).
$$

Now, using Lemma 3.3 we have that (6.1) equals

$$
m_{\beta_s^{(0)}} + \sum_{u=0}^{m-1} \left[ \sum_{i=0}^{m-1} \alpha_{s,i-u} t_i \right] = m_{\beta_s^{(0)}} + \sum_{i=0}^{m-1} \left[ \sum_{u=0}^{m-1} \alpha_{s,i} t_i \right] = m_{\beta_s^{(0)}} + \sum_{i=0}^{m-1} \left( \sum_{a=0}^{m-1} \alpha_{s,a} \right).
$$

Theorem 3.5 proves that the $\alpha_{s,a}$ and $\beta_{s,a}$ may be computed in time $O(r^4)$. Performing the above computation will therefore cost $O(r^5)$ operations, and then repeating for all values of $s$ takes us to $O(r^6)$ operations.

**Example 6.2.** From Example 3.6 we get that the sum of the factors of $\Phi_{19}(x)$ over $\mathbb{F}_p$ for any prime $p$ with ord$(p, 19) = 6$ is

$$3x^6 - (t_0 + t_1 + t_2)x^5 + (-7t_0 - 7t_1 - 7t_2)x^4 - (-3t_0 - 3t_1 - 3t_2)x^3 + (-7t_0 - 7t_1 - 7t_2)x^2 - (t_0 + t_1 + t_2)x + 3 = 3x^6 + x^5 + 7x^4 - 3x^3 + 7x^2 + x + 3.$$

**References**


The City University of New York, 300 Jay Street, Brooklyn, New York 11201
E-mail address: gregstein@member.ams.org