MATHEMATICS OF COMPUTATION
Volume 70, Number 235, Pages 1237–1251
S 0025-5718(00)01233-3
Article electronically published on March 24, 2000

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

GREG STEIN

ABSTRACT. We examine the problem of factoring the rth 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 rth 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 $O\left((r^{1/2+\epsilon}\log p)^9\right)$ in the case where $\Phi_r(x)$ has precisely two irreducible

Received by the editor December 1, 1998 and, in revised form, June 22, 1999.
2000 *Mathematics Subject Classification.* Primary 11T06, 11T24, 11T22; Secondary 12Y05, 13P05.
Key words and phrases. Finite field, factorization, cyclotomic, polynomial.
Supported in part by PSC-CUNY Research Foundation Grant 69666-00 29.

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 Φ_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 rth roots of unity and the irreducible factors of the rth 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 [1].

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, α, of $\mathbb{F}_r$ (that is, an element of $\mathbb{F}_r$ which multiplicatively generates $\mathbb{F}_r^*$), we define the *cyclotomy classes*

$$\begin{aligned}
H_0 &= \{1, \alpha^m, \alpha^{2m}, \ldots, \alpha^{(d-1)m}\},\\
H_1 &= \{\alpha, \alpha^{m+1}, \alpha^{2m+1}, \ldots, \alpha^{(d-1)m+1}\},\\
&\vdots\\
H_i &= \{\alpha^i, \alpha^{m+i}, \alpha^{2m+i}, \ldots, \alpha^{(d-1)m+i}\},\\
&\vdots\\
H_{m-1} &= \{\alpha^{m-1}, \alpha^{m+(m-1)}, \alpha^{2m+(m-1)}, \ldots, \alpha^{(d-1)m+(m-1)}\}.
\end{aligned}$$

Noting that $\alpha^{m+i}H_0 = \alpha^i H_0$, 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 $b^{\frac{r-1}{l}} = 1$, 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 ζ represent a primitive rth root of unity in an appropriate extension field, $\mathbb{K}$, then one defines the *periods*, t_i, by

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

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 rth cyclotomic polynomial, $\Phi_r = \frac{x^r-1}{x-1} = 1 + x + x^2 + \cdots + x^{r-1}$, 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 Φ_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 $p^d \equiv 1 \bmod r$) 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 ζ be a primitive rth root of unity in some extension field of $\mathbb{F}_p$ so that the irreducible factors of $\Phi_r(x)$ over $\mathbb{F}_p$ are

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

and note that $t_i = \text{trace}_{\mathbb{F}_p}(\zeta^{\alpha^i})$, 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. $(i, j) = \begin{cases} (j, i) & d \text{ even}, \\ (j + \frac{m}{2}, i + \frac{m}{2}) & d \text{ odd}. \end{cases}$

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. $\sum_{i=0}^{m-1} (i, j) = d - \eta_j$ *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 α 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

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

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

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

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

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

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

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 $(r-1)^{st}$ degree polynomials in Y over $\mathbb{Z}$.

Let $\mathcal{S}$ 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

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

and note that there is a one-to-one correspondence with the $\binom{d}{l}$ terms in (3.2) with the elements of $\mathcal{S}$. We then define an equivalence relation on $\mathcal{S}$ 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 $\mathcal{S}_1 \subseteq \mathcal{S}$ be the union of all partitions containing precisely d elements of $\mathcal{S}$ and let $\mathcal{S}_2 \subseteq \mathcal{S}$ be the union of all partitions containing fewer than d elements of $\mathcal{S}$. In addition, let $\mathcal{T}_1 = \{\{i_1, \ldots, i_l\} \in \mathcal{S}_1 \mid p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod d\}$ and $\mathcal{T}_2 = \mathcal{S}_1 - \mathcal{T}_1$.

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 $p^k \not\equiv 0 \bmod r$ and r is prime. That is, if $\{i_1, \ldots, i_l\} \sim \{j_1, \ldots, j_l\}$ then $\{i_1, \ldots, i_l\} \in \mathcal{T}_1$ (or $\mathcal{T}_2$) if, and only if, $\{j_1, \ldots, j_l\} \in \mathcal{T}_1$ (or $\mathcal{T}_2$, respectively). Therefore we may write $\mathcal{T}_1 = P_1 \cup \cdots \cup P_{n_1}$

and $\mathcal{T}_2 = Q_1 \cup \cdots \cup Q_{n_2}$, disjoint unions, where the P_i and the Q_i are partitions under the equivalence relation. Further note that $\mathcal{S} = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{S}_2$, where $\mathcal{T}_1$, $\mathcal{T}_2$ and $\mathcal{S}_2$ are pairwise disjoint. We may now rewrite (3.2) as

$$(-1)^l \left(\sum_{k=1}^{n_1} \sum_{\{i_1,\ldots,i_l\}\in P_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{k=1}^{n_2} \sum_{\{i_1,\ldots,i_l\}\in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{\{j_1,\ldots,j_l\}\in \mathcal{S}_2} Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} \right). \tag{3.3}$$

Lemma 3.2. *If P_k, Q_k and $\mathcal{S}_2$ 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. $\sum_{\{j_1,\ldots,j_l\}\in \mathcal{S}_2} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = \#(\mathcal{S}_2)$.

Proof of Lemma 3.2 1.

$$\{i_1,\ldots,i_l\} \in P_k \Rightarrow p^{i_1}+\cdots+p^{i_l} \equiv 0 \bmod r \Rightarrow Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = 1.$$

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 $\{i_1,\ldots,i_l\} \in Q_k \Rightarrow p^{i_1}+\cdots+p^{i_l} \neq 0 \in \mathbb{F}_r \Rightarrow \alpha^u(p^{j_1}+\cdots+p^{j_l}) \neq 0 \in \mathbb{F}_r$. Therefore there exists e_k, $1 \leq e_k \leq m-1$, so that $p^{i_1}+\cdots+p^{i_l} = \alpha^{e_k}p^l \in H_{e_k}$, hence $p^{i_1+n}+\cdots+p^{i_l+n} = \alpha^{e_k}p^{n+l} \in H_{e_k}$ and

$$\sum_{\{i_1,\ldots,i_l\}\in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} = \sum_{n=0}^{d-1} Y^{\alpha^{u+e_k}p^{n+l}} = \sum_{n=0}^{d-1} Y^{\alpha^{u+e_k}p^n} = v_{u+e_k}. \tag{3.4}$$

□

Proof of Lemma 3.2 3. If $\{j_1,\ldots,j_l\} \in \mathcal{S}_2$, then there exists $n \in \mathbb{Z}/d\mathbb{Z} - \{0\}$ so that $\{j_1,\ldots,j_l\} = \{j_1+n,\ldots,j_l+n\} \in \mathcal{S}_2$, hence $p^{j_1}+\cdots+p^{j_l} = \left(p^{j_1}+\cdots+p^{j_l}\right)p^n \in \mathbb{F}_r$, but $p^n \not\equiv 1$ or $0 \bmod r$, so $p^{j_1}+\cdots+p^{j_l} \equiv 0 \bmod r$, hence $\alpha^u(p^{j_1}+\cdots+p^{j_l}) \equiv 0 \bmod r$, 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 $\alpha_{d-l,t}^{(u)}$ 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 $\#(S_2) + dn_2$, then, referring to Lemma 3.2 and (3.3), we have that the coefficient of x^{d-l}

in $f_u(x)$ is

(3.5)

$$(-1)^l \left(\sum_{k=1}^{n_1} \sum_{\{i_1,\ldots,i_l\}\in P_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{k=1}^{n_2} \sum_{\{i_1,\ldots,i_l\}\in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{\{j_1,\ldots,j_l\}\in \mathcal{S}_2} Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} \right)$$

$$= (-1)^l \left(\sum_{k=1}^{n_1} d + \sum_{\{i_1,\ldots,i_l\}\in Q_k} v_s + \#(\mathcal{S}_2) \right)$$

$$= (-1)^l \left(\beta_{d-l}^{(u)} + \sum_{i=0}^{m-1} \alpha_{d-l,i}^{(u)} v_i \right),$$

where the s in the next to last expression is the s such that $p^{i_1}+\cdots+p^{i_l} \in H_{s-u}$.

To see that these integers are unique, we note that $1, v_0, v_1, \ldots, v_{m-1}$ each have unique coset representatives in $\mathcal{R}$ which are polynomials in Y with coefficients in $\mathbb{Z}$ having degree no more than r, no two of them sharing terms of like degree. They are therefore linearly independent in $\mathbb{Q}[Y]/(Y^r-1)$, viewed as an r-dimensional $\mathbb{Q}$ vector space, hence unique in $\mathcal{R} = \mathbb{Z}[Y]/(Y^r-1)$, which can be thought of as sitting inside of $\mathbb{Q}[Y]/(Y^r-1)$.

All that remains is to show that these integers can be computed in time $O(r^4)$. Recall from the paragraph following Lemma 3.1 that the $f_i(x)$ can be viewed as dth degree polynomials in x whose coefficients are $(r-1)^{st}$ degree polynomials in Y. The results of Lemma 3.2 show that $\alpha_{st}^{(u)}$ is the coefficient for v_t in the coefficient for Y^u in the coefficient of x^s. We now demonstrate a technique for expanding (3.1) which differs from the one in Lemma 3.2.

Let

$$W_i^{(u)}(x) = \prod_{k=0}^{i} \left(x - Y^{\alpha^u p^k} \right) \in \mathcal{R}[x],$$

and note that $f_u(x) = W_{d-1}^{(u)}(x)$ and that

$$W_{i+1}^{(u)}(x) = W_i^{(u)}(x) \left(x - Y^{\alpha^u p^{i+1}} \right) = x W_i^{(u)}(x) - Y^{\alpha^u p^{i+1}} W_i^{(u)}(x). \tag{3.6}$$

For any $i \in \mathbb{Z}/d\mathbb{Z}$, $W_i^{(u)}(x)$ is a polynomial in x of degree at most $d < r$ with coefficients which are polynomials in Y of degree at most r. The coefficients of these polynomials in Y are integers bounded above by the $\alpha_{st}^{(u)}$, which are in turn bounded by $\#(S) = \binom{d}{l} < 2^d$. Computing $W_{i+1}^{(u)}(x)$ from $W_i^{(u)}(x)$ as suggested in (3.6), we see that computing $xW_i^{(u)}(x)$ involves increasing each exponent of x in $W_i^{(u)}(x)$ by 1, $O(r)$ operations. We then compute $Y^{\alpha^u p^{i+1}} W_i^{(u)}(x)$ by multiplying each of the polynomial coefficients of $W_i^{(u)}(x)$ by $Y^{\alpha^u p^{i+1}}$ which involves at most $d \cdot r$ additions modulo r, or $O(r^2 \log r)$ operations. Finally, computing $xW_i^{(u)}(x) - Y^{\alpha^u p^{i+1}} W_i^{(u)}(x)$ 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 $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)}$.*

Proof. Let $f_i(x) = \prod_{k=0}^{d-1}(x - Y^{\alpha^i p^k}) \in \mathcal{R}[x]$ as in (3.1). From (3.3) we get that the coefficient of x^{d-l} in $f_i(x)$ is

$$(3.7)\quad (-1)^l \left(\sum_{k=1}^{n_1+n_2} \sum_{\{i_1,\ldots,i_l\}\in P_k} Y^{\alpha^i p^{i_1}+\cdots+\alpha^i p^{i_l}} + \sum_{\{j_1,\ldots,j_l\}\in S_2} Y^{\alpha^i p^{j_1}+\cdots+\alpha^i p^{j_l}} \right),$$

where $\mathcal{S}_2$ is as in Lemma 3.2, and here the P_k run through all of the partitions of $\mathcal{S}_1$. If $e_k \equiv p^{i_1} + \cdots + p^{i_l} \bmod r$ for some one of the $\{i_1, \ldots, i_l\} \in P_k$, then we have

$$(3.8)\qquad \sum_{\{i_1,\ldots,i_l\}\in P_k} Y^{\alpha^i p^{i_1}+\cdots+\alpha^i p^{i_l}} = \sum_{u=0}^{d-1} Y^{e_k \alpha^i p^u} = \sum_{u=0}^{d-1} Y^{\alpha^u (p^{i_1+u}+\cdots+p^{i_l+u})}.$$

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

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

where $e = \alpha^s p^i \in H_s$, some i, hence (3.8) is v_{s+i}. If $\{j_1, \ldots, j_l\} \in \mathcal{S}_2$, then, as in Lemma 3.2, $\sum_{\{j_1,\ldots,j_l\}\in\mathcal{S}_2} Y^{\alpha^i p^{j_1}+\cdots+\alpha^i p^{j_l}} = \#(\mathcal{S}_2)$. So certainly $\beta_s^{(i)} = \beta_s^{(0)}$. Now, $\alpha_{s,t+i}^{(i)}$ is the number of partitions which yield v_{t+i} and these are the same partitions which yielded v_t in the coefficient of x^{d-l} for $f(x)$. So $\alpha_{s,t+i}^{(i)} = \alpha_{s,t}^{(0)}$, or $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)}$. □

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*

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

That is, if the coefficient of x^s is

$$\lambda_0 t_0 + \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_{m-2} t_{m-2} + \lambda_{m-1} t_{m-1} + \beta$$

in g_0, then the coefficient of x^s is

$$\begin{aligned}
&\lambda_{m-1} t_0 + \lambda_0 t_1 + \lambda_1 t_2 + \cdots + \lambda_{m-3} t_{m-2} + \lambda_{m-2} t_{m-1} + \beta, \quad \text{in } g_1,\\
&\lambda_{m-2} t_0 + \lambda_{m-1} t_1 + \lambda_0 t_2 + \cdots + \lambda_{m-4} t_{m-2} + \lambda_{m-3} t_{m-1} + \beta, \quad \text{in } g_2,\\
&\lambda_{m-3} t_0 + \lambda_{m-2} t_1 + \lambda_{m-1} t_2 + \cdots + \lambda_{m-5} t_{m-2} + \lambda_{m-4} t_{m-1} + \beta, \quad \text{in } g_3,\\
&\qquad\qquad\vdots\\
&\lambda_1 t_0 + \lambda_2 t_1 + \lambda_2 t_2 + \cdots + \lambda_{m-1} t_{m-2} + \lambda_0 t_{m-1} + \beta \quad \text{in } g_{m-1}.
\end{aligned}$$

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 $i+k$, $\alpha_{s,t}^{(i+k)} = \alpha_{s,t-i-k}^{(0)}$. To see that $\alpha_{s,t}^{(i)} = \alpha_{s,t+k}^{(i+k)}$ note that $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)} = \alpha_{s,t}^{(0)}$ 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 $\mathcal{R}$.

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

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

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

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

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

$$\begin{aligned}
\beta_s^{(i)} &= \beta_s^{(0)},\\
\alpha_{s,t}^{(i)} &= \alpha_{s,t-i}^{(0)},\\
\beta_s^{(i)} &= \beta_s^{(k)},\\
\alpha_{s,t-k}^{(i)} &= \alpha_{s,t}^{(i+k)},\\
\alpha_{s,t}^{(i)} &= \alpha_{s,t+k}^{(i+k)}.
\end{aligned}$$

Proof. To prove existence and to compute the $\alpha_{st}^{(u)}$ and $\beta_s^{(u)}$ we simply reduce, modulo p, those integers discussed in Lemmas 3.1, 3.2, and 3.4. When replacing Y by ζ 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 $\alpha_{st}^{(u)}$ and $\beta_s^{(u)}$ is $O(r^4)$. □

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

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

where $\delta_{si}^{(u)} = \alpha_{si}^{(u)} - \beta_s^{(u)}$, 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 3.3 and 3.4, we have, for i, t, $k \in \mathbb{Z}/m\mathbb{Z}$ and $s \in \mathbb{Z}/d\mathbb{Z}$,

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

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 $\beta_s^{(u)}$ 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 $\beta_s^{(u)}$, 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, α, for F_r^* was used). Hence, aside from the reduction mod p_1 or p_2, the $\alpha_{si}^{(u)}$, $\beta_s^{(u)}$ 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 ζ represent a primitive 19th root of unity over $\mathbb{F}_{31}$. From this we compute the cyclotomy classes

$$\begin{aligned} H_0 &= \{1, 12, 11, 18, 7, 8\}, \\ H_1 &= \{2, 5, 3, 17, 14, 16\}, \\ H_2 &= \{4, 10, 6, 15, 9, 13\}, \end{aligned}$$

and the cyclotomy periods

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

Using formula (3.5) from Lemma 3.1, we arrive at Table 1 which describes the coefficients of the powers of ζ for each power of x. The number in row x^s and column ζ^i is $\alpha_{si}^{(0)}$. The number in column 1 and row x^s is $\beta_s^{(0)}$. Hence

$$\begin{aligned} g_0 &= x^6 - t_0 x^5 + (3 + t_0 + t_2)x^4 - (2 + 2t_0 + t_1)x^3 \\ &\quad + (3 + t_0 + t_2)x^2 - t_0 x + 1, \end{aligned}$$

and by Lemma 3.3 we have

$$\begin{aligned} g_1(x) &= x^6 - t_1 x^5 + (3 + t_1 + t_0)x^4 - (2 + t_1 + 2t_2)x^3 \\ &\quad + (3 + t_1 + t_0)x^2 - t_1 x + 1, \end{aligned}$$

$$\begin{aligned} g_2(x) &= x^6 - t_2 x^5 + (3 + t_2 + t_1)x^4 - (2 + t_2 + 2t_0)x^3 \\ &\quad + (3 + t_2 + t_1)x^2 - t_2 x + 1. \end{aligned}$$

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

$$\begin{aligned} g_0(x) &= x^6 - t_0 x^5 - (2t_0 + 3t_1 + 2t_2)x^4 + (t_1 + 2t_2)x^3 \\ &\quad - (2t_0 + 3t_1 + 2t_2)x^2 - t_0 x + 1, \\ g_1(x) &= x^6 - t_1 x^5 - (2t_0 + 2t_1 + 3t_2)x^4 + (2t_0 + t_2)x^3 \\ &\quad - (2t_0 + 2t_1 + 3t_2)x^2 - t_1 x + 1, \\ g_2(x) &= x^6 - t_2 x^5 - (3t_0 + 2t_1 + 2t_2)x^4 + (t_0 + 2t_1)x^3 \\ &\quad - (3t_0 + 2t_1 + 2t_2)x^2 - t_2 x + 1. \end{aligned}$$

TABLE 1

		H_0						H_1						H_2					
	1	ζ	ζ^{12}	ζ^{11}	ζ^{18}	ζ^7	ζ^8	ζ^2	ζ^5	ζ^3	ζ^{17}	ζ^{14}	ζ^{16}	ζ^4	ζ^{10}	ζ^6	ζ^{15}	ζ^9	ζ^{13}
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
x^2	3	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
x^3	2	2	2	2	2	2	2	1	1	1	1	1	1	0	0	0	0	0	0
x^4	3	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
x^5	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
x^6	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Recalling the remarks immediately preceding this example, we see that we may replace $p = 31$ with any prime p with $\operatorname{ord}(p, 19) = 6$, and we will get precisely the same results.

4. Further identities among the $\alpha_{st}^{(u)}$ and $\beta_s^{(u)}$

We now wish to demonstrate some symmetries which occur among the $\alpha_{st}^{(u)}$ and the $\beta_s^{(u)}$. We begin by comparing the coefficients of x^l and x^{d-l}. 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 $\mathcal{S}$ be the collection of all l element subsets of $\mathbb{Z}/d\mathbb{Z}$ and $\mathcal{S}'$ the collection of all $d-l$ element subsets of $\mathbb{Z}/d\mathbb{Z}$. Let $\varphi : \mathcal{S} \to \mathcal{S}'$ be the bijection $\varphi(I) = I^C$ (the complement of I in $\mathbb{Z}/d\mathbb{Z}$). Define an equivalence relation, $\sim$, on both $\mathcal{S}$ and $\mathcal{S}'$ as in the proof of Lemma 3.1, that is, $\{i_1, \ldots, i_l\} \sim \{i_1 + k, \ldots, , i_l + k\}$, for each $k \in \mathbb{Z}/m\mathbb{Z}$, and note that for $I_1, I_2 \in \mathcal{S}$ we have

$$I_1 \sim I_2 \Leftrightarrow \varphi(I_1) \sim \varphi(I_2). \tag{4.1}$$

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

$$(-1)^l \left(\sum_{k=1}^{t} \sum_{\{i_1,\ldots,i_l\} \in P_k} Y^{\alpha^i (p^{i_1} + \cdots + p^{i_l})} + \sum_{\{j_1,\ldots,j_l\} \in S_2} Y^{\alpha^i (p^{j_1} + \cdots + p^{j_l})} \right), \tag{4.2}$$

and that the coefficient of x^l is

$$(-1)^{d-l} \left(\begin{array}{c} \sum_{k=1}^{t} \sum_{\{i_{l+1},\ldots,i_d\} \in P_k'} Y^{\alpha^i (p^{i_{l+1}} + \cdots + p^{i_d})} \\ + \sum_{\{j_{l+1},\ldots,j_d\} \in S_2'} Y^{\alpha^i (p^{j_{l+1}} + \cdots + p^{j_d})} \end{array} \right). \tag{4.3}$$

Recall that $\alpha_{lt}^{(0)}$ is the number of P_k in (4.2) that yield v_t, that $\alpha_{d-l,t}^{(0)}$ is the number of P_k' in (4.3) that yield v_t, and that $\beta_l^{(0)} = \#(S_2) + d$(the number of equivalence classes from (4.2) which do not yield any v_t) and that $\beta_{d-l}^{(0)} = \#(S_2') + d$(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*

$$\beta_l^{(i)} = \beta_{d-l}^{(i)},$$
$$\alpha_{lk}^{(i)} = \alpha_{d-l,k}^{(i)}.$$

Proof. Note that $\left(p^{d/2}\right)^2 = 1 \in \mathbb{F}_r$. Since $\operatorname{ord}(p, r) = d$, 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 $k = 0, \ldots, \frac{d}{2} - 1$, we have

$$\alpha^i p^k = -\alpha^i p^{d/2+k} \in \mathbb{F}_r. \tag{4.4}$$

That is, in $H_i = \{\alpha^i, \alpha^i p, \ldots, \alpha^i p^d\} \subseteq \mathbb{F}_r^*$ 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

$$\gamma \in H_i \Leftrightarrow -\gamma \in H_i, \tag{4.5}$$

and, recalling Lemma 2.2,

$$\sum_{\gamma \in H_i} \gamma = 0. \tag{4.6}$$

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 $H_0 = \{p^0, p, p^2, \ldots, p^{d-1}\}$ 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 $Y^{p^{i_1} + \cdots + p^{i_l}} = Y^{p^{i_{l+1}} + \cdots + p^{i_d}} = 1 \in \mathcal{R}$. Therefore

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

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

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

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 $e_w \in H_s$, where $e_w = \alpha^s p^i \in \mathbb{F}_r$, some i. 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 $H_s = \{e_w p^u\}_{u=0}^{d-1} = \{-e_w p^u\}_{u=0}^{d-1}$. Referring now to (3.4) and (4.4),

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

and, noting that $\sum_{u=0}^{d-1} Y^{e_w p^u} = v_s$, we see that P_w yields v_s if, and only if, P_w' yields v_s.

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 $\beta_l^{(0)} = \beta_{d-l}^{(0)}$. Combining this result with Lemma 3.3, we have

$$\beta_l^{(i)} = \beta_l^{(0)} = \beta_{d-l}^{(0)} = \beta_{d-l}^{(i)}$$

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. □

For the case where d is odd we have a similar result with a similar proof.

Lemma 4.2. *If d is odd, $d \neq 1$, then, 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*

$$\beta_l^{(i)} = \beta_{d-l}^{(i+a)},$$
$$\alpha_{lk}^{(i)} = \alpha_{d-l,k}^{(i+a)}.$$

Proof. First note that, unlike the case for d even, if $p^s \equiv -1 \bmod r$, $1 < s \leq d-1$, 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, $-1 \equiv \alpha^a p^h \bmod r$ for some $0 \leq h \leq d-1$. So we have

$$H_0 = \left\{1, p, p^2, \ldots, p^{d-1}\right\} \subseteq \mathbb{F}_r^*$$

and

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

and, for $0 \leq k \leq d-1$,

$$p^k = -\alpha^a p^{h+k} \in \mathbb{F}_r^*. \tag{4.9}$$

In particular,

$$\gamma \in H_0 \Leftrightarrow -\gamma \in H_a.$$

Let $I = \{i_1, \ldots, i_l\} \in \mathcal{S}$ and $I^C = \{i_{l+1}, \ldots, i_d\} \in \mathcal{S}'$. 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 $H_a = \left\{\alpha^a, \alpha^a p, \ldots, \alpha^a p^{d-1}\right\}$ and

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

that

$$\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l} = -\left(\alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d}\right),$$

hence

$$p^{i_1} + \cdots + p^{i_l} = \alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d}.$$

If $\{i_1, \ldots, i_l\} \in \mathcal{S}_2$, then $p^{i_1} + \cdots + p^{i_l} = 0$, so $\alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d} = 0$, hence $\alpha^a p^h \left(\alpha^a p^{i_{l+1}} + \cdots + \alpha^a p^{i_d}\right) = 0$, and finally since $\alpha^a p^h \neq 0$, $\alpha^a p^{i_{l+1}} + \cdots + \alpha^a p^{i_d} = 0$. So we have $Y^{p^{i_1} + \cdots + p^{i_l}} = Y^{p^{i_{l+1}} + \cdots + p^{i_d}} = 1 \in \mathcal{R}$ and so

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

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

$$\sum_{\{i_1, \ldots, i_l\} \in P_k} Y^{p^{i_1} + \cdots + p^{i_l}} = \sum_{\{i_{l+1}, \ldots, i_d\} \in P_k'} Y^{\alpha^a \left(p^{i_{l+1}} + \cdots + p^{i_d}\right)} = \#(P_k). \tag{4.11}$$

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 $e_w \in H_s$ where $e_w = \alpha^s p^i \in \mathbb{F}_r$, some i, and we have

$$\begin{aligned} v_s &= \sum_{u=0}^{d-1} Y^{ep^u} = \sum_{\{i_1,\ldots,i_l\}\in P_w} Y^{p^{i_1}+\cdots+p^{i_l}} \\ &= \sum_{\{i_{l+1},\ldots,i_d\}\in P'_w} Y^{\alpha^a p^{h+i_{l+1}}+\cdots+\alpha^a p^{h+i_d}} \\ &= \sum_{\{i_{l+1},\ldots,i_d\}\in P'_w} Y^{\left(\alpha^a p^{i_{l+1}}+\cdots+\alpha^a p^{i_d}\right)} \end{aligned}$$

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 $\alpha_{lk}^{(0)}$ 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 $\alpha_{lk}^{(0)} = \alpha_{d-l,k}^{(a)}$. Further, (4.10) and (4.11) show that $\beta_l^{(0)} = \beta_{d-l}^{(a)}$. Combining this with Lemma 3.3, we have

$$\beta_l^{(i)} = \beta_l^{(0)} = \beta_{d-l}^{(a)} = \beta_{d-l}^{(i+a)}$$

and

$$\alpha_{lk}^{(i)} = \alpha_{l,k-i}^{(0)} = \alpha_{d-l,k-i}^{(a)} = \alpha_{d-l,k}^{(i+a)},$$

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 $\operatorname{ord}(p, r) = \frac{r-1}{2}$, then we may factor $\Phi_r(x)$, the rth cyclotomic polynomial, over $\mathbb{F}_p$, deterministically in time $O\left((r^{1/2+\epsilon}\log p)^9\right)$.*

Proof. As a result of Theorem 3.5, 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 $(x - t_0)(x - t_1) = x^2 - (t_0 + t_1)x + t_0t_1 = x^2 + x + t_0t_1$. Hence

$$t_0, t_1 = \frac{-1 \pm \sqrt{1 - 4t_0t_1}}{2}.$$

From [15, pp. 200–201] we have that $1 - 4t_0t_1 = \pm r$ as $r \equiv \pm 1 \bmod 4$, 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 $r \equiv \pm 1 \bmod 4$. In 1985 R. Schoof showed in [18] that if n is a quadratic residue mod p, then $\sqrt{n}$ can be deterministically computed in $\mathbb{F}_p$ in time $O((|n|^{1/2+\epsilon}\log p)^9)$. Since t_0 and t_1 exist, it follows that $1 - 4t_0t_1$ is a quadratic residue mod p and so can be deterministically computed in time $O\left((r^{1/2+\epsilon}\log p)^9\right)$. □

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 rth cyclotomic polynomial over $\mathbb{F}_p$, in time $O(r^6)$.*

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

$$\sum_{u=0}^{m-1} \left(\beta_s^{(u)} + \sum_{i=0}^{m-1} \alpha_{s,i}^{(u)} t_i \right) = \sum_{u=0}^{m-1} \beta_s^{(u)} + \sum_{u=0}^{m-1} \left(\sum_{i=0}^{m-1} \alpha_{s,i}^{(u)} t_i \right). \tag{6.1}$$

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

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

Theorem 3.5 proves that the $\alpha_{s,a}^{(0)}$ and $\beta_s^{(0)}$ 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 $\operatorname{ord}(p, 19) = 6$ is

$$\begin{aligned} & 3x^6 - (t_0 + t_1 + t_2)x^5 + (-7t_0 - 7t_1 - 7t_2)x^4 - (-3t_0 - 3t_1 - 3t_2)x^3 \\ & \quad +(-7t_0 - 7t_1 - 7t_2)x^2 - (t_0 + t_1 + t_2)x + 3 \\ = \; & 3x^6 + x^5 + 7x^4 - 3x^3 + 7x^2 + x + 3. \end{aligned}$$

References

[1] L.D. Baumert and W.H. Mills, Uniform cyclotomy, *J. Number Theory*, [**14**], (1982), pp. 67-82. MR **83f:**10005

[2] B.C. Berndt, R.J. Evans and K.S. Williams, "Gauss and Jacobi Sums", Wiley, New York, 1998. MR **99d:**11092

[3] D. Bini and V. Pan, "Polynomial and Matrix Computations", Birkhauser, Boston, 1994. MR **95k:**65003

[4] D. Cantor and H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, *Math. Comp.*, [**36**], (1981), pp. 587-592. MR **82e:**12020

[5] H. Cohen, "A Course in Computational Algebraic Number Theory", Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1995. MR **94i:**11105

[6] L.E. Dickson, Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.*, [**57**], (1935), pp. 391-424.

[7] S.A. Evdokimov, Factorization of a solvable polynomial over finite fields and the generalized Riemann Hypothesis, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) [**176**], (1989), pp. 104–117, 153. MR **91a:**11063

[8] C. F. Gauss,"Disquisitiones Arithmeticae", Springer-Verlag, New York, 1986. MR **87f:**01105

[9] M.A. Huang, Generalized Riemann Hypothesis and factoring polynomials over finite fields, *J. Algorithms,* [**12**], (1991), pp. 464-481. MR **92j:**68057
[10] D. Jungnickel, Finite fields. Structure and arithmetics. Bibliographisches Institut, Mannheim, 1993. MR **94g:**11109
[11] D. Knuth,"The Art of Computer Programming", volume 2, *Semi-numerical algorithms,* 3rd ed., Addison-Wesley, Reading, 1998. MR **83i:**68003
[12] S. Lang, "Algebra", Addison-Wesley, Reading, 1965. MR **33:**5416
[13] R. Lidl and H. Niederreiter, "Introduction to Finite Fields and their Applications", revised edition, Cambridge University Press, Cambridge, 1994. MR **95f:**11098
[14] R. Lidl and H. Niederreiter, "Finite Fields", Encyclopedia of Mathematics and its Applications, v.20, Addison-Wesley, Reading, 1983. MR **86c:**11106
[15] G. B. Mathews, "Theory of Numbers", Chelsea, New York, 1961. MR **23:**A3698
[16] G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.*, [**39**], (1981), pp. 251-264. MR **83e:**10058
[17] H. Niederreiter and R. Göttfert, On a new factorization algorithm for polynomials over finite fields, *Math. Comp.*, [**64**], (1995), pp. 347-353. MR **95i:**11145
[18] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* [**44**], (1985), pp. 483-494. MR **86e:**11122
[19] V. Shoup, New algorithms for finding irreducible polynomials over finite fields, *Math. Comp.* [**54**], (1990), pp. 435-447. MR **90j:**11135
[20] G. Stein, Factoring cyclotomic polynomials over large finite fields, in "Finite Fields and Applications", London Mathematical Society Lecture Note Series #233, S. Cohen & H. Niederreiter, eds., Cambridge University Press, pp. 349-354, 1996. MR **98b:**11122
[21] G. Stein, Traces of roots of unity over prime fields, in "Finite Fields: Theory, Applications and Algorithms, *Contemporary Mathematics* #225, R. Mullin and G. Mullen, eds., American Mathematical Society, pp.113-121, 1999. MR **99g:**11145
[22] T. Storer, "Cyclotomy and Difference Sets", Markham, Chicago, 1967. MR **36:**128

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