CHINESE REMAINDER THEOREM FOR CYCLOTOMIC POLYNOMIALS IN $\mathbb{Z}[X]$

KAMALAKSHYA MAHATAB AND KANNAPPAN SAMPATH

Abstract. By the Chinese remainder theorem, the canonical map
$$\Psi_n : \mathbb{R}[X]/(X^n - 1) \to \bigoplus_{d|n} \mathbb{R}[X]/\Phi_d(X)$$
is an isomorphism when $R$ is a field whose characteristic does not divide $n$ and $\Phi_d$ is the $d$th cyclotomic polynomial. When $R$ is the ring $\mathbb{Z}$ of rational integers, this map is injective but not surjective. In this paper, we give an explicit formula for the elementary divisors of the cokernel of $\Psi_n$ using the prime factorisation of $n$. We also give a pictorial algorithm using Young Tableaux that takes $O(n^3 + \epsilon)$ bit operations for any $\epsilon > 0$ to determine a basis of Smith vectors (see Definition 3.1) for the codomain of $\Psi_n$. In general when $R$ is a unique factorisation domain, we prove that the determinant of $\Psi : \mathbb{R}[X]/(\prod f_j) \to \bigoplus \mathbb{R}[X]/(f_j)$ written with respect to the standard basis is $\prod_{1 \leq i < j \leq n} R(f_j, f_i)$, where $f_i$’s are pairwise relatively prime monic polynomials and $R(f_j, f_i)$ is the resultant of $f_j$ and $f_i$.

1. Introduction

Motivation. Let $m_1, \ldots, m_r$ be pairwise coprime elements in a principal ideal domain (PID) $R$, that is, for $i \neq j$, if $a | m_i$ and $a | m_j$, then, $a$ is a unit in $R$. The Chinese remainder theorem (CRT) states that, for $a_1, \ldots, a_r \in R$, the system (in $X$)
\begin{align*}
X &\equiv a_1 \mod m_1 \\
X &\equiv a_2 \mod m_2 \\
& \quad \vdots \\
X &\equiv a_r \mod m_r
\end{align*}
(1.1)
has a solution and any two solutions are congruent modulo $\prod_i m_i$. In terms of ideals, the natural map from the ring $R/(\prod_i m_i)$ to the ring $\prod_i R/(m_i)$ is an isomorphism. The surjectivity of the natural map encapsulates the fact that the system (1.1) has a solution and the injectivity encapsulates the fact that any two solutions are congruent modulo $\prod_i m_i$.

However, such a theorem does not hold true over rings which are not PID’s. For example, consider the system (in $h(X)$ over $\mathbb{Z}[X]$):
\begin{align*}
h(X) &\equiv 1 \mod (X - 1) \\
h(X) &\equiv 0 \mod (X + 1).
\end{align*}
This system does not have a solution over \( \mathbb{Z}[X] \): to wit, if \( f_1(X), f_2(X) \in \mathbb{Z}[X] \) are such that
\[
\begin{align*}
h(X) &= f_1(X)(X - 1) + 1 \\
h(X) &= f_2(X)(X + 1),
\end{align*}
\]
then, we are led to the absurdity \( 2f_2(1) = 1 \). This phenomenon serves as a motivation for the questions we study in this article.

**Setup.** Let \( R \) be an integral domain which is not a field, so that \( R[X] \) is not a PID. Suppose that \( f \) is a monic polynomial and
\[
f = \prod_{i=1}^{n} f_i,
\]
where \( \{f_i\}_{i=1}^{n} \) are pairwise coprime polynomials in \( R[X] \). Consider the natural map:
\[
\Psi_f : R[X]/(f) \to \bigoplus_i R[X]/(f_i) \quad \text{where } h(X) \mapsto \bigoplus_i h(X) \mod f_i.
\]
The map becomes injective if \( R \) is replaced by its field of fractions; therefore, \( \Psi_f \) is injective. However, as we have already remarked in general, \( \Psi_f \) is not surjective. As a measure of the failure of surjectivity, we would like to determine the cokernel \( G_1(f) \) of the map \( \Psi_f \):
\[
0 \to R[X]/(f) \xrightarrow{\Psi_f} \bigoplus_i R[X]/(f_i) \xrightarrow{\Psi_f} G_1(f) \to 0.
\]
We would also like to understand when a given element \( \alpha \in \bigoplus_i R[X]/(f_i) \) lies in the image of \( \Psi_f \). To the best of our knowledge, it seems to us that problems of this nature have not been explicitly studied elsewhere in the literature.

Specialising ourselves to \( R = \mathbb{Z} \) and the polynomial \( f(X) = X^n - 1 \) with its factorisation \( \prod_{d|n} \Phi_d(X) \) into cyclotomic polynomials, we shall solve the above problems.

**Results.** Let us consider the map \( \Psi_n \) defined by:
\[
\Psi_n : \mathbb{Z}[X]/(X^n - 1) \to \bigoplus_{d|n} \mathbb{Z}[X]/(\Phi_d(X)) \quad \text{where } X^i \mapsto \bigoplus_{d|n} X^i \mod \Phi_d(X)
\]
and extended \( \mathbb{Z} \)-linearly. The associated exact sequence is:
\[
0 \to \mathbb{Z}[X]/(X^n - 1) \xrightarrow{\Psi_n} \bigoplus_{d|n} \mathbb{Z}[X]/(\Phi_d(X)) \xrightarrow{\Psi_n} G_1(n) \to 0.
\]
The domain and codomain of \( \Psi_n \) are free \( \mathbb{Z} \)-modules of the same rank and therefore, the cokernel \( G_1(n) \) is a finite abelian group. We endow \( \mathbb{Z}[X]/(X^n - 1) \) with the basis
(1, X, ..., X^{n-1}) and \( \mathbb{Z}[X]/(\Phi_d(X)) \) with the basis \( (1, X, ..., X^{(d-1)}) \). Denote the matrix of \( \Psi_n \) with respect to this basis by \( A_n \). For example, we have
\[
A_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.
\]
The structure of the abelian group \( G_1(n) \) is completely determined by the elementary divisors of \( A_n \) (see for instance, [10, Theorem 7.7]). For example, the elementary divisors of \( A_6 \) are \( \{1, 1, 1, 2, 6, 6\} \) and the group \( G_1(6) \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \). We first reduce the problem of determining the elementary divisors of \( A_n \) to that of \( A_{pe} \) for a prime \( p \) (Theorem 2.4). For a prime \( p \), the matrix \( A_{pe} \) has the following structure (Lemma 2.5):
\[
(1.2) \quad A_{pe} = \begin{pmatrix}
A_{pe-1} & A_{pe-1} & \cdots & A_{pe-1} & A_{pe-1} \\
I_{pe-1} & 0 & \cdots & 0 & -I_{pe-1} \\
0 & I_{pe-1} & \cdots & 0 & -I_{pe-1} \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \cdots & I_{pe-1} & -I_{pe-1}
\end{pmatrix}
\]
with \( A_{pe} = A_1 = (1) \); we exploit this recursive structure in determining the elementary divisors of the matrix \( A_{pe} \).

From this approach, we deduce that (Proposition 2.18), if \( (e_1, \ldots, e_n) \) is the tuple of elementary divisors of \( A_n \) with \( e_i \mid e_{i+1} \), then the tuple \( Q_n = (e_1, \frac{e_1}{e_2}, \ldots, \frac{e_1}{e_{n-1}}) \) of quotients is a rearrangement of the tuple
\[
(\underbrace{p_1 \ldots p_1}_{a_1 \text{ times}}, \underbrace{p_2 \ldots p_2}_{a_2 \text{ times}}, \ldots, \underbrace{p_r \ldots p_r}_{a_r \text{ times}}, \underbrace{1 \ldots 1}_{n - \sum a_i \text{ times}})
\]
where \( n = p_1^{a_1} \cdots p_r^{a_r} \) and \( p_i \)'s are distinct primes. Moreover, the \( s \)th \( p_i \) appears at the index \( n - \frac{s}{p_i} + 1 \) in \( Q_n \). Since \( |G_1(n)| = |\det(A_n)| \), we have that (Corollary 2.10):
\[
|G_1(n)| = \prod_{i=1}^{r} p_i^{n(1-p_i^{-\alpha_i})} = \prod_{k=1}^{n} \gcd(k, n).
\]
In Appendix A, we prove:
\[
(1.3) \quad \det(A_n) = \prod_{\substack{d_1, d_2 | n \\ 1 \leq d_1 < d_2 \leq n}} \mathcal{R}(\Phi_{d_1}, \Phi_{d_2}) = (-1)^{n-1} \prod_{i=1}^{r} p_i^{n(1-p_i^{-\alpha_i})},
\]
where \( \mathcal{R}(g_1, g_2) \) is the resultant of the polynomials \( g_1 \) and \( g_2 \). More generally, if \( f \) is a monic polynomial over a unique factorisation domain and if \( f = \prod_{k=1}^{n} f_k \) is a factorisation of \( f \) into pairwise relatively prime polynomials, then (Theorem A.3),
\[
(1.4) \quad \det(\Psi_f) = \prod_{1 \leq i < j \leq n} \mathcal{R}(f_j, f_i).
\]
We notice that the group algebra \( \mathbb{Z}[G] \) over \( \mathbb{Z} \) of a group \( G \) isomorphic to the cyclic group \( \mathbb{Z}/n\mathbb{Z} \) is \( \mathbb{Z}[X]/(X^n - 1) \). From this perspective, the absolute value of the determinant of \( \Psi_n \) is the index of the group algebra \( \mathbb{Z}[G] \) in \( \bigoplus_{p=0}^{n} \mathbb{Z}[X]/\Phi_{p^n}(X) \). Raymond Ayoub and Christine Ayoub determine this index [23, Theorem 7(C)].
They also determine a basis for this quotient \( \mathbb{Z} \)-module, which is then used to determine a basis of Smith vectors (Definition 3.1) for the group algebra \( \mathbb{Z}[G] \), in the case \( n = p^e \) for a prime \( p \).

In this paper, we carry out the program of determining a basis of Smith vectors for a general \( n \) (Section 4) by a pictorial algorithm involving Young diagrams. A basis of Smith vectors for a general \( n \) can be realised as the columns of the matrix \( U_n^{-1} \) for some \( U_n \in \text{GL}_n(\mathbb{Z}) \) for which there exists a \( V_n \in \text{GL}_n(\mathbb{Z}) \) such that \( U_n A_n V_n \) is the Smith normal form of \( A_n \) (Lemma 3.2). The best known algorithm [15, Proposition 7.20] for computing the Smith normal form and the unimodular transformations takes \( O(n^{3.373+\epsilon}) \) for any \( \epsilon > 0 \) while the algorithm we present determines a basis of Smith vectors for a general \( n \) in \( O(n^{3+\epsilon}) \) for any \( \epsilon > 0 \) without actually computing these transformation matrices (Theorem 4.9).

**Framework.** In Section 2 we compute the elementary divisors of \( A_n \). In Section 3 we prove some basic facts required in the algorithm for determining a basis of Smith vectors for \( n \) which is followed by a presentation of the algorithm in Section 4. In the appendix that follows, we compute the determinant of \( A_n \) in a way that generalises to any factorisation of a monic polynomial over a unique factorisation domain into pairwise relatively prime polynomials.

2. Smith Normal Form of \( A_n \)

We begin with the following observation:

**Lemma 2.1.** Given relatively prime positive integers \( n \) and \( m \), the ring homomorphism \( P_{m,n} : \mathbb{Z}[X]/(X^m - 1) \otimes \mathbb{Z}[Y]/(Y^n - 1) \to \mathbb{Z}[t]/(t^{mn} - 1) \) defined by:

\[
P_{m,n}(X \otimes 1) = t^n \text{ and } P_{m,n}(1 \otimes Y) = t^m
\]

is an isomorphism. Furthermore, with respect to the standard basis, the matrix of \( P_{m,n} \) as a \( \mathbb{Z} \)-module homomorphism is a permutation matrix.

**Proof.** We note that \( t^{ni+ mj} \equiv t^\alpha \text{ mod } (t^{mn} - 1) \) if and only if \( ni + mj \equiv \alpha \text{ mod } mn \). Now, by the Chinese Remainder Theorem for \( \mathbb{Z} \), the set

\[
\{ ni + mj : 0 \leq i < m - 1, 0 \leq j < n - 1 \}
\]

consists all the residues mod \( mn \), exactly once. Thus, \( P_{m,n} \) is a bijection between the standard bases. This proves the lemma. \( \square \)

**Lemma 2.2.** Suppose that \( m \) and \( n \) are relatively prime positive integers. Then, the map \( T_{m,n} : \mathbb{Z}[X]/\Phi_m(X) \otimes \mathbb{Z}[Y]/\Phi_n(Y) \to \mathbb{Z}[t]/\Phi_{mn}(t) \) defined by

\[
\overline{X} \otimes \overline{Y} \mapsto \overline{t}^{ni+ mj}
\]

and extending \( \mathbb{Z} \)-linearly is a ring isomorphism.

**Proof.** Consider the maps:

\[
\phi : \mathbb{Z}[X]/(\Phi_m(X)) \to \mathbb{Z}[t]/(\Phi_{mn}(t)) \quad \text{and} \quad \psi : \mathbb{Z}[Y]/(\Phi_n(Y)) \to \mathbb{Z}[t]/(\Phi_{mn}(t))
\]

\[
\overline{X} \mapsto \overline{t}^n \quad \overline{Y} \mapsto \overline{t}^m
\]

Now, \( T_{m,n} \) is composition of the canonical map \( \phi \circ \psi \) with the identification map \( \overline{t} \otimes \overline{y} \mapsto \overline{t} \otimes \overline{y} : \mathbb{Z}[t]/(\Phi_{mn}(t)) \otimes \mathbb{Z}[t]/(\Phi_{mn}(t)) \to \mathbb{Z}[t]/(\Phi_{mn}(t)) \). Thus, \( T_{m,n} \) is a ring homomorphism.
To prove surjectivity, we show that $\mathfrak{T} \in \mathbb{Z}[t]/\Phi_{mn}(t)$. Indeed, since $\mathfrak{T}$ is invertible in $\mathbb{Z}[t]/\Phi_{mn}(t)$ and that $\gcd(m, n) = 1$, there are integers $i, j \in \mathbb{Z}$ such that $t^{ni + mj} \equiv t \pmod{\Phi_{mn}(t)}$.

We claim that, this map is also injective: letting $K$ be the kernel of the map $T_{m,n}$, the exact sequence:

$$0 \rightarrow K \rightarrow \mathbb{Z}[X]/\Phi_m(X) \otimes \mathbb{Z}[Y]/\Phi_n(Y) \rightarrow T_{m,n} \rightarrow \mathbb{Z}[t]/\Phi_{mn}(t) \rightarrow 0$$

splits since $\mathbb{Z}[t]/\Phi_{mn}(t)$ is a free $\mathbb{Z}$-module showing:

$$\mathbb{Z}[X]/\Phi_m(X) \otimes \mathbb{Z}[Y]/\Phi_n(Y) \simeq K \oplus \mathbb{Z}[t]/\Phi_{mn}(t)$$

Being a submodule of a free module over the PID $\mathbb{Z}$, $K$ is a free $\mathbb{Z}$-module. A comparison of the rank tells us that $K$ is of rank 0. Thus, $K = \{0\}$, equivalently, $T_{m,n}$ is injective. □

Remark 2.3. Along the lines of the proof of Lemma 2.2, it may be shown that, for relatively prime positive integers $m$ and $n$, the $\mathbb{Z}$-linear extension of the map

$$(2.2) \quad X^i \otimes Y^j \mapsto T_{m,n}(X^i Y^j) : \mathbb{Z}[X]/\Phi_m(X) \otimes \mathbb{Z}[Y]/\Phi_n(Y) \rightarrow \mathbb{Z}[t]/\Phi_{mn}(t), \quad 0 \leq i \leq \phi(m) - 1, \quad 0 \leq j \leq n - 1$$

is a ring isomorphism.

2.1. **Smith Equivalence of** $A_m \otimes A_n$ **and** $A_{mn}$. For a matrix $A$ over the integers, let $S(A)$ denote the Smith normal form of $A$ in which all the elementary divisors are non-negative. We now state and prove one of the main results of this section:

**Theorem 2.4.** $S(A_m \otimes A_n) = S(A_{mn})$.

**Proof.** Consider the following diagram:

$$\begin{array}{c}
\mathbb{Z}[X]/(X^m - 1) \otimes \mathbb{Z}[Y]/(Y^n - 1) \overset{\Psi_m \otimes \Psi_n}{\longrightarrow} \bigoplus_{d_1 \mid m} \bigoplus_{d_2 \mid n} \mathbb{Z}[X]/\Phi_{d_1}(X) \otimes \mathbb{Z}[Y]/\Phi_{d_2}(Y) \\
\mathbb{Z}[t]/(t^{mn} - 1) \overset{\Psi_{mn}}{\longrightarrow} \bigoplus_{d \mid mn} \mathbb{Z}[t]/(\Phi_d(t)) \end{array}$$

The map $\Psi_m \otimes \Psi_n$ is the canonical map, defined by:

$$(\Psi_m \otimes \Psi_n)(X^i \otimes Y^j) = \Psi_m(X^i) \otimes \Psi_n(Y^j)$$

and extended $\mathbb{Z}$-linearly. We shall prove that there is an isomorphism $T(m, n)$ that renders the diagram commutative.

Indeed, define $T(m, n)$ by

$$T(m, n) = \bigoplus_{d_1 \mid m \atop d_2 \mid n} T_{d_1, d_2}$$

For later purposes, we note that $\det(S(A)) = |\det(A)|$ is non-negative.
Clearly, \( T(m, n) \) is an isomorphism. As is seen by the following computation, \( T(m, n) \) also renders the above diagram commutative:

\[
\begin{align*}
(\Psi_{mn} \circ P_{m,n})(\overline{X}^i \otimes \overline{Y}^j) &= \Psi_{mn}(t^{ni+mj}) \\
&= (t^{ni+mj} \mod \Phi_d(t))d_{mn}
\end{align*}
\]

\[
\begin{align*}
(T(m, n) \circ (\Psi_m \otimes \Psi_n))(\overline{X}^i \otimes \overline{Y}^j) &= T(m, n)(\Psi_m(\overline{X}^i) \otimes \Psi_n(\overline{Y}^j)) \\
&= T(m, n)(X^{ni} \mod \Phi_m(X) \otimes Y^{mj} \mod \Phi_n(Y)) \\
&= (t^{ni+mj} \mod \Phi_d(t))d_{mn}.
\end{align*}
\]

This completes the proof.

Motivated by Theorem 2.4, we present our strategy to determine \( S(A_n) \): first determine \( S(A_{p^n}) \) for \( p \nmid n \); since Kronecker product of diagonal matrices is a diagonal matrix, describe the smith form of a diagonal matrix; finally, use this to determine the elementary divisors of \( A_n \).

### 2.2. Smith Normal Form of \( A_{p^n} \) for a prime \( p \)

Let \( p \) be a prime. We begin by noting that, we have an explicit formula for \( \Phi_{p^n}(X) \):

\[
(2.3) \quad \Phi_{p^n}(X) = \sum_{i=0}^{p-1} X^{ip^{n-1}}.
\]

Using this information, the following lemma determines \( A_{p^n} \) recursively:

**Lemma 2.5.** \( A_{p^n} \) is a block matrix given by (1.2).

**Proof.** Let \( A_{p^n} = (B_{ij})_{1 \leq i,j \leq p} \) where \( B_{ij} \) are matrices of size \( p^{i-1} \times p^{j-1} \). Since \( X^{(k-1)p^{i-1}+i} \equiv X^i \mod \Phi_{p^n}(X) \) when \( 0 \leq j \leq e-1, 0 \leq i \leq p^{j-1} \) and \( 1 \leq k \leq p \), it follows that \( B_{1k} = A_{p^{k-1}} \). Also, \( X^i \) is itself the remainder on division by \( \Phi_{p^n}(X) \) when \( 0 \leq i \leq \phi(p^n) - 1 = p^e - p^{e-1} - 1 \). This shows that \( (B_{ij})_{2 \leq i,j \leq p} \) is an identity matrix. Finally, using

\[
X^{p^{i-1}(p-1)+i} \equiv -X^{p^{i-1}(p-2)+i} - X^{p^{i-1}(p-3)+i} - \ldots - X^{p^{i-1}+i} - X^i \mod \Phi_{p^n}(X),
\]

we see that, \( B_{ip} = -I \) for \( 2 \leq i \leq p \). This completes the proof.

**Theorem 2.6.** For \( e > 0 \), the distinct elementary divisors of \( A_{p^n} \) are \( \{p^i : 0 \leq i \leq e\} \). The multiplicity of \( p^i \) is \( \phi(p^{e-1}) \).

For \( n \times n \) matrices \( L \) and \( M \), let us write \( L \sim M \) to mean that \( L \) and \( M \) are Smith equivalent: that is, \( L \sim M \) if and only if there are matrices \( P, Q \in \text{GL}_n(\mathbb{Z}) \) such that \( M = PLQ \).

**Proof.** We prove this by induction on \( e \).
The case $e = 1$. $A_p$ is a $p \times p$ matrix of the form:

$$
A_p = \begin{pmatrix}
1 & 1 & \ldots & 1 & 1 \\
1 & 0 & \ldots & 0 & -1 \\
0 & 1 & \ldots & 0 & -1 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & 1 & -1 \\
\end{pmatrix}
$$

Adding all the columns to the rightmost column, we get the matrix:

$$
A_p \sim B_p := \begin{pmatrix}
1 & 1 & \ldots & 1 & p \\
1 & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & 1 & 0 \\
\end{pmatrix}
$$

Therefore, we have, $|\det(A_p)| = p$, from which the theorem follows.

The Induction Step. Consider the matrix (1.2). Proceeding analogous to the $e = 1$ case, we note that, $A_{p^e}$ is Smith equivalent to the matrix

$$
A_{p^e} \sim B_{p^e} := \begin{pmatrix}
A_{p^{e-1}} & A_{p^{e-1}} & \ldots & A_{p^{e-1}} & pA_{p^{e-1}} \\
I_{p^{e-1}} & 0 & \ldots & 0 & 0 \\
0 & I_{p^{e-1}} & \ldots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & I_{p^{e-1}} & 0 \\
\end{pmatrix}
$$

Now, performing row operations, we may obtain the following equivalent to $A_{p^e}$:

$$
\begin{pmatrix}
0 & 0 & \ldots & 0 & pA_{p^{e-1}} \\
I_{p^{e-1}} & 0 & \ldots & 0 & 0 \\
0 & I_{p^{e-1}} & \ldots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & I_{p^{e-1}} & 0 \\
\end{pmatrix}
$$

We now interchange rows to obtain the following form:

$$
\begin{pmatrix}
I_{p^{e-1}} & 0 & \ldots & 0 & 0 \\
0 & I_{p^{e-1}} & \ldots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & I_{p^{e-1}} & 0 \\
0 & 0 & \ldots & 0 & pA_{p^{e-1}} \\
\end{pmatrix} \sim \begin{pmatrix}
I_{p^{e-1}} & 0 & \ldots & 0 & 0 \\
0 & I_{p^{e-1}} & \ldots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & I_{p^{e-1}} & 0 \\
0 & 0 & \ldots & 0 & pS(A_{p^{e-1}}) \\
\end{pmatrix}
$$

Since this matrix is in Smith normal form, it must be the Smith normal form of the matrix $A_{p^e}$. Now, we verify the assertions of the theorem: indeed, the elementary divisors of $A_{p^e}$ are \{ $p^i : 0 \leq i \leq e$ \}; the multiplicity of $p^{i+1}$ is $\phi(p^{e-1-i})$ for $0 \leq i \leq e - 1$ (from the induction hypothesis) and $1$ appears $p^{e-1}(p - 1) = \phi(p^e)$ times. This completes the proof. □
Remark 2.7. We may actually calculate the determinant of $A_{pe}$ for $e > 0$ from the proof of Theorem 2.6. Let $I(p, k)$ be the column block matrix

$$I(p, k) = \begin{pmatrix} I_{p^{k-1}} \\ \vdots \\ I_{p^k} \end{pmatrix}$$

of $p - 1$ blocks. Consider the matrix $T_{pe}$ defined as follows:

$$T_{pe} = \begin{pmatrix} I_{p^e - p^{e-1}} & I(p, e) \\ 0 & I_{p^{e-1}} \end{pmatrix}.$$

Then, it is an easy computation to see that $A_{pe} T_{pe} = B_{pe}$ (see (2.5)). Since $\det(T_{pe}) = 1$ for all $p$ and $e$, we see that

$$\det(A_{pe}) = \det(B_{pe}) = (-1)^{\phi(p^e)} p^{\phi(p^e)} \det(A_{p^e-1}).$$

This gives us a recursive formula for the determinant of $A_{pe}$ (indeed, we know $\det(A_1) = \det((1)) = 1$). It now follows that

$$\det(A_{pe}) = (-1)^{p^e - 1} p^{\sum_{k=0}^{e-1} \phi(p^k)}.$$

Thus, for $e > 0$, we have that $\det(A_{pe})$ is positive for all odd primes $p$ and negative for $p = 2$.

Remark 2.8. Denote the totality of column (resp. row) operations needed to bring $A_{pe}$ to its Smith normal form by $V_{pe}$ (resp. $U_{pe}$) so that, $U_{pe}$ and $V_{pe}$ satisfy the following:

$$U_{pe} A_{pe} V_{pe} = S(A_{pe}).$$

The matrix $V_{pe}$ can be read off from the proof of the last proposition to be:

$$V_{pe} = \begin{pmatrix} I_{p^e - p^{e-1}} & I(p, e) V_{p^{e-1}} \\ 0 & V_{p^{e-1}} \end{pmatrix} = \begin{pmatrix} I_{p^{e-1}} & V_{p^{e-1}} \\ I_{p^{e-1}} & V_{p^{e-1}} \\ \vdots & \vdots \\ I_{p^{e-1}} & V_{p^{e-1}} \end{pmatrix}.$$

For later purposes, we note that the following equation sets up a recursion for the matrix $W_{pe} := A_{pe} V_{pe}$ with $W_1 = (1)$:

$$W_{pe} = \begin{pmatrix} A_{p^{e-1}} & \cdots & A_{p^{e-1}} & pW_{p^{e-1}} \\ I_{p^{e-1}} & \cdots & I_{p^{e-1}} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ I_{p^{e-1}} & \cdots & I_{p^{e-1}} & 0 \end{pmatrix}.$$

See Lemma 3.2 for an interpretation of the columns of $W_{pe}$.

Corollary 2.9. Suppose that

$$n = p_1^{a_1} \cdots p_r^{a_r}.$$
is the factorisation of a positive integer $n$. The Smith normal form $S(A_n)$ of the matrix $A_n$ is the Kronecker product

\[ S(A_n) = S \left( \bigotimes_{i=1}^{r} S(A_{p_i^{\alpha_i}}) \right). \]

Let $A$ be an $n \times n$ matrix and $B$ be an $m \times m$ matrix, then, we have:

\[ \det(A \otimes B) = (\det(A))^m(\det(B))^n. \]

Since $\det(S(A)) = |\det(A)|$, we get the following:

**Corollary 2.10.** In the notations of Corollary 2.7, we have,

\[ |\det(A_n)| = \prod_{i=1}^{r} p_i^{(n_1-\alpha_i)} \]

**Remark 2.11.** One may cast the expression for $|\det(A_n)|$ in many different forms. For example, by comparing the exponent of primes in both sides, one may prove:

\[ |\det(A_n)| = \prod_{k=1}^{n} \gcd(k,n). \]

In turn, this yields several nice expressions for the determinant:

\[ g(n) := \prod_{k=1}^{n} \gcd(k,n) = \prod_{d|n} d^{\phi(d)} = n^n \prod_{d|n} \frac{1}{d^{\phi(d)}}. \]

The arithmetic properties of the function $g$ have been studied in [11]. The author begins by observing that, for a multiplicative function $h$, the function

\[ g(n; h) := \prod_{k=1}^{n} h(\gcd(k,n)) \]

satisfies a curious relationship for relatively prime positive integers $m$ and $n:

\[ g(mn; h) = g(m; h)^n g(n; h)^m. \]

and concludes that $g(n; h)^{1/n}$ is multiplicative. However, it is now clear that, underlying this curiosity is the Kronecker product (Corollary 2.10). It is shown that the Dirichlet series

\[ \sum_{n=1}^{\infty} \frac{\log(g(n))}{n^s} \]

converges absolutely for $\Re(s) > 2$ and equals $-\frac{\zeta'(s)}{\zeta(s)}$ where $\zeta(s)$ is the Riemann’s zeta function. More intricate connections between the function $g(n)$ and the Riemann’s zeta function are established (see Corollary 4, loc. cit.). It is also shown that,

\[ g(n) \leq 27 \left( \frac{\log(n)}{\omega(n)} \right)^{n \omega(n)} \]

where $\omega(n)$ is the number of distinct prime divisors of $n$. 
Calculating the sign of this determinant turns out to be quite tricky. We will take a different approach (see Appendix A) to calculate the determinant which will also tell us the sign of \( \det(A_n) \).

### 2.3. Smith Normal Form of a Diagonal Matrix

The next order of business is to work out the Smith normal form of a diagonal matrix, \( D \):

\[
D = \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix}
\]

Notice that, we may first permute the rows of \( D \) so that the zero rows of the matrix are the last few rows of \( D \). If \( D^o \) denotes the maximum principal submatrix of \( D \) whose rows are all non-zero, the Smith normal form of \( D \) is, simply:

\[
S(D) = \begin{pmatrix}
S(D^o) \\
0
\end{pmatrix}
\]

Thus, we may assume that \( \{a_1, \ldots, a_n\} \) are all non-zero.

**The Algorithm.** Given a diagonal matrix

\[
D = \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix}
\]

where \( a_i \neq 0 \) for all \( i \), let \( \mathcal{P} \) be the set of primes that appear in at least one of the \( a_i \)'s. The algorithm proceeds in two steps:

1. Corresponding to a prime \( p_j \in \mathcal{P} \), we may associate that partition \( \lambda^{(j)} \) obtained by rearranging the sequence of numbers \( (\gamma_1, \ldots, \gamma_i, \ldots, \gamma_n) \) in weakly decreasing order, where \( p_j^{\gamma_i} \parallel a_i \). Indeed, a partition associated to a prime this way has at most \( n \) non-zero parts.
2. The elementary divisors of the matrix \( D \) are now given by the formulae:

\[
e_k = \prod_{j=1}^{r} p_j^{\lambda^{(j)}_n - k + 1}
\]

The fact that \( \lambda^{(j)} \) is a sequence of weakly decreasing non-negative integers shows that,

\[
e_1 \mid \cdots \mid e_n.
\]

We shall find it convenient to develop a pictorial language for the algorithm. The partitions naturally suggest Young diagrams:

**Definition 2.12 (Young Diagram).** The Young diagram associated to a partition \( \lambda = (\lambda_1, \ldots, \lambda_l) \) is a left-aligned array of boxes with the \( i \)th row of the array containing \( \lambda_i \) boxes.

For example, the Young diagram of the partition \( \nu = (2, 2, 1) \) is Figure 1. Notice, that, by definition, Young diagram of a partition \( \nu \), that of \( (\nu, 0) \), \( (\nu, 0, 0) \) etc. are
CHINESE REMAINDER THEOREM FOR CYCLOTOMIC POLYNOMIALS IN $\mathbb{Z}[X]$

all the same. Now, in terms of Young diagrams, we may visualise the algorithm as:

**Examples 2.13.**

(1) Consider the diagonal matrix

$$D = \begin{pmatrix} 6 & 4 & \vdots \\ 4 & 7 & \vdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

The set $P$ is therefore $\{2, 3, 7\}$. A simple calculation shows that, the associated partitions are

- $2 \leftrightarrow (2, 2, 1, 0)$
- $3 \leftrightarrow (1, 1, 0, 0)$
- $7 \leftrightarrow (1, 0, 0, 0)$

Therefore, the elementary divisors are:

- $e_1 = 2^03^07^0 = 1$
- $e_2 = 2^13^07^0 = 2$
- $e_3 = 2^23^17^0 = 12$
- $e_4 = 2^23^17^1 = 84$

As indicated towards the end of the algorithm, it may be helpful to draw the Young diagrams (and this will play a crucial role as we proceed!) on a ruled sheet of paper, see Figure 3.

(2) Let $S$ be a matrix in Smith normal form, with none of its elementary divisors 0. We show that the result of our algorithm and the elementary divisors coincide. Let $S = \text{diag}(e'_1, \ldots, e'_n)$ with $e'_1 \mid \cdots \mid e'_n \neq 0$. The set $P$ in this case is the set of prime divisors of $e'_n$. Suppose that the prime factorisation of the $e'_i$’s is:

- $e'_1 = p_1^{\alpha_{i1}} \cdots p_j^{\alpha_{i j}} \cdots p_r^{\alpha_{ir}}$
- $\vdots$
- $e'_k = p_1^{\alpha_{k1}} \cdots p_j^{\alpha_{kj}} \cdots p_r^{\alpha_{kr}}$
- $\vdots$
- $e'_n = p_1^{\alpha_{n1}} \cdots p_j^{\alpha_{nj}} \cdots p_r^{\alpha_{nr}}$. 

Figure 1. Young Diagram of $(2, 2, 1)$
Figure 2. Algorithm seen through Young Diagrams
Notice that, since $e'_1 | \cdots | e'_n$, it follows that,

$$\alpha_{n_j} \geq \cdots \geq \alpha_{k_j} \geq \cdots \geq \alpha_{1_j} \geq 0 \text{ for all } j.$$  

We see that, the partition associated to a prime $p_j \in \mathcal{P}$ is $(\alpha_{n_j}, \ldots, \alpha_{1_j})$. Now, computing the elementary divisors from our formulae,

$$e_k = \prod_{j=1}^{r} p_j^{\lambda_j^{(j)}} = \prod_{j=1}^{r} p_j^{\alpha_{(n - (n - k + 1) + 1)}j} = \prod_{j=1}^{r} p_j^{\alpha_{kj}} = e'_k$$

This tells us that, our algorithm is correct at least in the case where the diagonal matrix is already in Smith normal form. But, since the elementary divisors of any diagonal matrix is, by definition, the elementary divisors of its Smith normal form, we have actually, proven that, our algorithm, indeed gives us the elementary divisors of the diagonal matrix.

(3) Let $G$ be a finite abelian group. The elementary divisors are easily computed from the primary decomposition by step 2 of the algorithm. Conversely, given its elementary divisors, the primary decomposition is the set of pairs $(p_j, \lambda_j)$ obtained from step 1 of the algorithm, with these elementary divisors as the entries of a diagonal matrix.

**Theorem 2.14.** The above algorithm indeed gives the Smith normal form of the matrix $D$.

**Proof.** See Example 2.13(2). □

Before we can compute the elementary divisors of $A_n$, we need to compute the partitions and primes in the Kronecker product. To do this, we recall that, for the matrix $S(A_{\alpha})$, the set $\mathcal{P}$ is singleton $\{p\}$ and the partition associated to $p$ is,

$$p \leftrightarrow (\ldots, \alpha - i, \ldots, \alpha - i, \ldots), \quad 0 \leq i \leq \alpha$$

where $\alpha - i$ appears $\phi(p^i)$ times, $0 \leq i \leq \alpha$ (see Theorem 2.6).
Now, in the Kronecker Product, $S(A_p^{n_1}) \otimes S(A_p^{n_2})$, the set $P$ of primes is $\{p_1, p_2\}$ and the associated partitions are,

\[
p_1 \leftrightarrow (\ldots, n_1 - i, \ldots, n_1 - i, \ldots) \quad \phi(p_1)^{n_1} \text{ times}, \quad 0 \leq i \leq n_1
\]

\[
p_2 \leftrightarrow (\ldots, n_2 - j, \ldots, n_2 - j, \ldots) \quad \phi(p_2)^{n_2} \text{ times}, \quad 0 \leq j \leq n_2
\]

The following is easily seen by induction:

**Theorem 2.15.** Suppose that

\[
n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}
\]

is the factorisation of a positive integer $n$. Then, the set $P$ of primes for the diagonal matrix

\[
\bigotimes_j S(A_{p_j^{\alpha_j}})
\]

is the set $\{p_1, \ldots, p_r\}$ and the associated partitions are

\[
p_j \leftrightarrow (\ldots, \alpha_j - i, \ldots, \alpha_j - i, \ldots) \quad \phi(p_j)^{n/p_j} \text{ times}, \quad 0 \leq i \leq \alpha_j.
\]

for $j = 1, \ldots, r$.

The last proposition together with the algorithm completely solves the problem of determining the elementary factors of the matrix $A_n$. We illustrate this in an example:

**Example 2.16.** Let $n = 12 = 2^23^1$. Then, the set $P$ of primes for the diagonal matrix $S(A_4) \otimes S(A_3)$ is $\{2, 3\}$. Associated partitions are:

\[
2 \leftrightarrow (2, 2, 2, 1, 1, 1)
\]

\[
3 \leftrightarrow (1, 1, 1, 1)
\]

Now, the formulae for the elementary divisors show that, the elementary divisors of $A_{18}$ are $\{1, 1, 1, 1, 1, 1, 2, 2, 6, 12, 12, 12\}$. Pictorially, we have:

\[
\begin{array}{ccc}
2 & 2 & 3 \\
2 & 2 & 3 \\
2 & 2 & 3 \\
2 & 3 & 6 \\
2 & 2 & 2 \\
2 & 2 & 1 \\
\vdots & \vdots & \vdots \\
1 & 1 & 1
\end{array}
\]

**Figure 4.** The Elementary Divisors of $A_{12}$
2.4. Consequences. To proceed further, we need some more notions related to a Young Diagram. The height of a Young diagram $Y$ is the number of rows in $Y$. A cell in $Y$ is called a corner if it is the last cell in its row and there is no other cell below it.

Suppose that a positive integer $n$ has the factorisation

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

with $\alpha_i > 0$ and $p_1 < \cdots < p_r$. Let $E(A_n)$ denote the multiset of elementary divisors of $A_n$.

**Proposition 2.17.** With notations as above, we have:

1. the multiplicity of 1 in $E(A_n)$ is $n - \frac{n}{p_1}$.
2. the least integer $d > 1$ in $E(A_n)$ is $p_1$ and its multiplicity in $E(A_n)$ is

$$\begin{cases} \frac{n}{p_1} - \frac{n}{p_2}, & \text{if } p_2 < p_1^2 \\ \frac{n}{p_2} - \frac{n}{p_1}, & \text{if } p_2 > p_1^2 \end{cases}$$

3. The largest integer $m \in E(A_n)$ is $n$ and its multiplicity in $E(A_n)$ is

$$n \max \{ \frac{n}{p_i^{\alpha_i}} : 1 \leq i \leq r \}.$$

**Proof.**

1. The multiplicity of 1 in $E(A_n)$ is

$$n - \max \left\{ \text{height of } p_i \text{ tableau} \mid 1 \leq i \leq r \right\}$$

$$= n - \frac{n}{p_1}$$

2. Let $d > 1$ be the least elementary divisor of $A_n$. Then, $d$ is the product of the lowest non-empty rows of $p_i$ tableaux. Since the $p_1$-tableau is the tallest having one box in the last row, this $d$ must be $p_1$. The multiplicity of $p_1$ is

$$\frac{n}{p_1} - \text{Index of the row containing the second last corner}$$

$$= \begin{cases} \frac{n}{p_1} - \frac{n}{p_2}, & \text{if } \frac{n}{p_2} > \frac{n}{p_1^2} \\ \frac{n}{p_1} - \frac{n}{p_1^2}, & \text{if } \frac{n}{p_2} < \frac{n}{p_1^2} \end{cases}$$

which proves the claim.

3. The largest elementary divisor is the product of the numbers in the first row of Figure 2. This number is clearly $n$. The multiplicity of $n$ in $E(A_n)$ is the index of the row containing the first corner. We see that this multiplicity is

$$\min \left\{ \frac{n}{p_i^{\alpha_i}} : 1 \leq i \leq r \right\}$$

$$= \frac{n}{\max \{ \frac{n}{p_i^{\alpha_i}} : 1 \leq i \leq r \}}$$

This completes the proof. \qed
This proposition and its proof suggests that, Figure 2 in principle, gives a “formula” for the elementary divisors and their multiplicities, equivalently, the multiset \( E(A_n) \). We leave it to the reader to prove Proposition 2.17 using the following:

**Proposition 2.18.**

1. The \( n \)-tuple \( \left( e_1, \frac{e_2}{e_1}, \ldots, \frac{e_n}{e_{n-1}} \right) \) is a permutation of the \( n \)-tuple 
   \[
   \left( p_1, \ldots, p_1, p_2, \ldots, p_2, \ldots, p_r, \ldots, p_r, \frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_r}, \ldots, \frac{1}{\alpha_r}, \frac{1}{n - \sum \alpha_i} \right)
   \]

2. The ratio \( \frac{e_j}{e_{j-1}} \) is \( p_i \) if and only if \( j = n - \frac{n}{p_i} + 1 \) for some \( t \) satisfying \( 1 \leq t \leq \alpha_i \).

**Proof.**

1. We need to prove that \( \frac{e_j}{e_{j-1}} \) is a prime divisor of \( n \). Note that this claim is equivalent to proving that every row in Figure 2 has at most one corner. That is, exactly one of the \( p_i \) tableaux has a corner. Towards a contradiction, assume that there are two distinct primes \( p_{i_1} \) and \( p_{i_2} \) whose tableaux for \( n \) have a corner each in the same row \( R \):

   \[
   R = \frac{\sum_{j=0}^{l_2} n}{\phi(p_{i_2}^{l_2})} = \frac{\sum_{j=0}^{l_2} n}{\phi(p_{i_2}^{l_2})}
   \]

   This equality implies that

   \[
   \frac{n}{p_{i_1}^{\alpha_{i_1}-l_1}} = \frac{n}{p_{i_2}^{\alpha_{i_2}-l_2}}
   \]

   which is a contradiction, since \( p_{i_1} \) and \( p_{i_2} \) are distinct primes.

2. Notice that index \( k \) of the \( n \)-tuple contains \( p_i \) if the row \( k \) contains a corner of the \( p_i \)-tableau. These indices are therefore given by

   \[
   \left\{ \frac{n}{p_i^{r_j}} \sum_{j=0}^{r_j} \phi(p_i^{r_j-j}) + 1 \bigg| r = 0, 1, \ldots, \alpha_i - 1 \right\}
   \]

   Thus, we get, the indices which contain \( p_i \) are

   \[
   \left\{ \frac{n}{p_i} + 1 \bigg| r = 1, \ldots, \alpha_i \right\}
   \]

   which completes the proof. \( \square \)

**Corollary 2.19.** If \( n \) is square-free, that is, \( \alpha_i = 1 \) for all \( i = 1, \ldots, r \), then

\[
\left( e_1, \frac{e_2}{e_1}, \ldots, \frac{e_n}{e_{n-1}} \right) = (p_r, \ldots, p_1, 1, \ldots, 1)
\]
Corollary 2.20. Consider the $n$-tuple \((e_1, \frac{e_2}{\alpha_2}, \ldots, \frac{e_n}{\alpha_n})\). The number of times \(p_i\) appears before \(p_j\) appears the \(r\)th time (\(1 \leq r \leq \alpha_j\)) is the integer \(t\) such that \(p_i^t < p_j^t < p_i^{t+1}\).

Proof. If \(p_i\) appears exactly \(t\) times before \(p_j\) appears the \(r\)th time, then, by (2) of Proposition 2.18, we have:
\[
\frac{n}{p_i^t} + 1 < \frac{n}{p_j^r} + 1 < \frac{n}{p_i^{t+1}} + 1
\]
which immediately proves the proposition. \(\square\)

In the following sections, we shall describe a basis for \(G_1(n)\) through a pictorial algorithm: by a basis for \(G_1(n)\) is meant a set of generators
\[
\{0 \oplus 0 \oplus \cdots \oplus \bigoplus_{i=1}^{n} 1 \oplus 0 \oplus \cdots \oplus 0 : 0 \leq i \leq n-1\}
\]
for the abelian group \(\bigoplus \mathbb{Z}/e_i\mathbb{Z}\) where \((e_0, \ldots, e_{n-1})\) is the tuple of elementary divisors for \(A_n\).

3. Setup for the Algorithm

In this section, we will state the definitions and prove some basic lemmas that are instrumental to the algorithm in the next section.

To determine a basis for \(G_1(n)\), it suffices to find a basis \(\{p^{(j)} : 0 \leq j \leq n-1\}\) for \(\bigoplus_{\Phi|n} \mathbb{Z}[X]/\Phi_d(X)\) so that
\[
(3.1) \quad \{\overline{v}_n(p^{(j)}) : e_j > 1\}
\]
is a set of generators for the abelian group \(G_1(n)\) with respect to which the relations are the simplest possible:
\[
(3.2) \quad e_j \overline{v}_n(p^{(j)}) = 0.
\]
This idea is captured by the following definition:

Definition 3.1. Given a positive integer \(n\), let \((e_0, \ldots, e_{n-1})\) be the tuple of elementary divisors of \(A_n\). We say that \((p^{(j)} : 0 \leq j \leq n-1)\) is a Smith vector for \(n\) if:
1. \(\{p^{(j)} : 0 \leq j \leq n-1\}\) is a \(\mathbb{Z}\)-basis of \(\bigoplus_{\Phi|n} \mathbb{Z}[X]/\Phi_d(X)\) and
2. \(a_jp^{(j)} \in \text{Im}(\Psi_n)\) if and only if \(e_j \mid a_j\).

The following lemma will tell us how to compute Smith vector for \(n\):

Lemma 3.2. If \((p^{(j)})\) is a Smith vector for \(n\), then, there exists \(U_n, V_n \in GL_n(\mathbb{Z})\) such that \(S(A_n) = U_nA_nV_n\) and \(A_nV_n(\overline{V}) = e_jp^{(j)}\) where \((e_0, \ldots, e_{n-1})\) is the tuple of elementary divisors of \(A_n\).

Proof. We introduce a notation for the standard basis of the direct sum \(\bigoplus_{\Phi|n} \mathbb{Z}[X]/\Phi_d(X)\); for a divisor \(d\) of \(n\), and for every \(i\) such that \(0 \leq i \leq \phi(d) - 1\), put:
\[
g_i,d(X) := 0 \oplus \cdots \oplus 0 \oplus X^i \mod (\Phi_d(X)) \oplus 0 \oplus \cdots \oplus 0.
\]
Let $U_n$ be the endomorphism of $\oplus_{d|n} \mathbb{Z}[X]/\langle \Phi_d(X) \rangle$ that exchanges the basis underlying the given Smith vector with the standard basis:

$$p^{(j)} \mapsto g_{i,d} \text{ where } j = \sum_{d'^{'}<d, d'|n} \phi(d') + i.$$ 

Thus, $U_n$ is invertible. Since $e_j p^{(j)}$ is in the image of $A_n$, it follows that there are vectors $h^{(j)} \in \mathbb{Z}[X]/(X^n - 1)$ such that

$$A_n(h^{(j)}) = e_j p^{(j)}.$$ 

Define the map $V_n : \mathbb{Z}[X]/(X^n - 1) \rightarrow \mathbb{Z}[X]/(X^n - 1)$ as follows:

$$\overline{X}^j \mapsto h^{(j)}, \quad 0 \leq j \leq n - 1$$

Clearly, $U_n A_n V_n = S(A_n)$. It suffices to check that $V_n$ is an isomorphism, that is, $\det(V_n) = \pm 1$:

$$U_n A_n V_n = S(A_n) \Rightarrow \det(U_n) \det(A_n) \det(V_n) = \det(S(A_n))$$

$$\Rightarrow \det(A_n) \det(V_n) = \pm |\det(A_n)| \quad \text{(since } \det(U_n) = \pm 1)$$

$$\Rightarrow \det(V_n) = \pm 1 \quad \text{(since } \det(A_n) \neq 0 \text{ and } \mathbb{Z} \text{ is an integral domain}).$$

This completes the proof. \hfill \Box

From Lemma 2.4 we see that $\{e_n(j)p^{(j)} : 0 \leq j \leq n - 1\}$ is a basis for the image of $\Psi_n$ and we have the following isomorphism of $\mathbb{Z}$-modules:

$$G_1(n) \simeq \bigoplus_{e_j > 1} (\overline{\Psi}_n(p^{(j)})) \simeq \bigoplus_{e_j > 1} \mathbb{Z}/e_j \mathbb{Z}. \quad (3.3)$$

In Lemma 2.4, for relatively prime positive integers $m$ and $n$, we have shown that $S(A_{mn}) = S(A_m \otimes A_n)$. It is now natural to ask if, Smith vectors for $m$ and $n$ can be coaxed to produce a Smith vector for $mn$. In the commutative diagram of maps in Figure 5 since both the rows are exact and $P_{m,n}$ and $T(m,n)$ are isomorphisms, a straightforward diagram chasing proves that $f_{m,n}$ is an isomorphism (see also [10, Lemma 7.1]). In the next lemma, we consider the tensor product of Smith vectors

$$\begin{array}{cccccccc}
0 & \rightarrow & \mathbb{Z}[X]/(X^n - 1) & \otimes & \mathbb{Z}[Y]/(Y^m - 1) & \otimes & \mathbb{Z}_d[m \langle \Phi_d(X) \rangle] & \otimes & \mathbb{Z}[X]/(X^n - 1) & \otimes & \mathbb{Z}[Y]/(Y^m - 1) & \otimes & \mathbb{Z}_d[n \langle \Phi_d(Y) \rangle] & \rightarrow & G_1(m,n) & \rightarrow & 0 \\
& & \downarrow{P_{m,n}} & & \downarrow{\Psi_{m,n}} & & \downarrow{T(m,n)} & & \downarrow{f_{m,n}} & & \downarrow{\Psi_{m,n}} & & \downarrow{f_{m,n}} & & & \\
0 & \rightarrow & \mathbb{Z}[t]/(t^{mn} - 1) & \rightarrow & \bigoplus_{d|mn} \mathbb{Z}[t]/(\Phi_d(t)) & \rightarrow & \bigoplus_{d|mn} \mathbb{Z}[t]/(\Phi_d(t)) & \rightarrow & G_1(mn) & \rightarrow & 0 \\
\end{array}$$

**Figure 5. Tensor Product of Smith Vectors**

in the top row of Figure 5 and study its properties in the bottom row.

**Lemma 3.3.** Let $m$ and $n$ be relatively prime positive integers. Let $\{p^{(j)} : 0 \leq j \leq m - 1\}$ and $\{q^{(j)} : 0 \leq j \leq n - 1\}$ be Smith vectors for $m$ and $n$ respectively. Then, in the group $G_1(mn)$,

1. the order of the element $\overline{\Psi}_{mn}(p^{(i)}(\overline{X}^i)q^{(j)}(\overline{Y}^j))$ is $e_m(i)e_n(j)$, where $e_k(i)$ denotes the $i$th elementary divisor of $A_k$. 

(2) Suppose that \( \Psi_{mn}(p^{(i)}(T^n)q^{(j)}(T^m)) \) and \( \Psi_{mn}(p^{(i)}(T^n)q^{(j)}(T^m)) \) are non-zero. Then, the intersection

\[
\bigcap_{\alpha} \{ \Psi_{mn}(p^{(i)}(T^n)q^{(j)}(T^m)) \} \cap \{ \Psi_{mn}(p^{(i)}(T^n)q^{(j)}(T^m)) \}
\]

of subgroups is non-trivial if and only if \( i_1 = i_2 \) and \( j_1 = j_2 \).

In this lemma, we interpret \( p^{(j)}(T^n) \) as the element \( \bigoplus_{d|m} p^{(j)}(T^n) \) which belongs to the direct sum \( \bigoplus_{d|m} \mathbb{Z}[t]/\Phi_d(t) \). And, the product \( p^{(i)}q^{(j)} \) is to be interpreted as the element \( \bigoplus_{d|m} p^{(i)}d^{(j)} \) which belongs to \( \bigoplus_{d|m} \mathbb{Z}[t]/\Phi_d(t) \).

**Proof.** By Lemma 3.2 there are isomorphism \( V_m \) and \( V_n \) such that:

\[(3.4) A_mV_m(X^i) = e_m(i)p^{(i)} \quad \text{and} \quad A_nV_n(Y^j) = e_n(j)q^{(j)}\]

for \( 0 \leq i \leq m - 1 \) and \( 0 \leq j \leq n - 1 \). Now, appealing to commutativity of Figure 5 we have:

\[
(\Psi_{mn} \circ P_{m,n})(V_m \otimes V_n)(X^i \otimes Y^j) = (T(m, n) \circ (A_m \otimes A_n))(V_m \otimes V_n)(X^i \otimes Y^j)
\]

\[
= e_m(i)e_n(j)p^{(i)}q^{(j)}(T^m)q^{(j)}(T^m).
\]

Since \( \{ X^i \otimes Y^j : 0 \leq i \leq m - 1, 0 \leq j \leq n - 1 \} \) is a basis for \( \mathbb{Z}[X]/X^{m-1} \otimes \mathbb{Z}[X]/X^{n-1} \), we have that the set \( \{ p^{(i)}(T^n)q^{(j)}(T^m) : 0 \leq i \leq m - 1, 0 \leq j \leq n - 1 \} \) is a \( \mathbb{Z} \)-basis for the codomain of \( \Psi_{mn} \); from the linear independence of these vectors, (2) follows. Now, the set \( \{ e_m(i)e_n(j)p^{(i)}q^{(j)} : 0 \leq i \leq m - 1, 0 \leq j \leq n - 1 \} \) is a basis for the image of \( \Psi_{mn} \) from which (1) follows. \( \Box \)

**Remark 3.4.** More generally, we note that if \( k_1 \) and \( k_2 \) are two relatively prime positive integers, then, we may obtain the young diagram for \( k_1k_2 \) by repeating \( k_2 \) times, the rows of the Young diagram for \( k_1 \) and \( k_1 \) times, the rows of the Young diagram for \( k_2 \). To see this, suppose that

\[ k_1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{and} \quad k_2 = q_1^{\beta_1} \cdots q_s^{\beta_s}, \]

where \( \alpha_i, \beta_j > 0 \) and \( \{ p_i : 1 \leq i \leq r \} \) and \( \{ q_j : 1 \leq j \leq s \} \) are disjoint. Then, in the \( p_j \) tableau for \( k_1 \), the row with \( e \) boxes (where \( 0 \leq e \leq \alpha_j \)) appears \( \phi(p_j^{\alpha_j-e})k_1p_j^{-\alpha_j} \) times, while this row appears \( \phi(p_j^{\alpha_j-e})k_1k_2p_j^{-\alpha_j} \) in the \( p_j \) tableau for \( k_1k_2 \). This proves our claim.

From the lemma, we infer that tensoring Smith vectors does not work, because \( \{ e_m(i)e_n(j) : 0 \leq i \leq m - 1, 0 \leq j \leq n - 1 \} \) is not the set of elementary divisors of \( A_{mn} \). However, we will see how to get over this difficulty in the next section. We conclude this section with the following lemma which we will need in the next section and is interesting in its own right.

**Lemma 3.5.** Let \( P \) be a permutation matrix and \( m \) and \( n \) be relatively prime positive integers. Then, there are diagonal matrices \( D_1 \) and \( D_2 \) satisfying:

\[
\gcd(\det(\Phi_1), m) = 1, \\
\gcd(\det(\Phi_2), n) = 1 \quad \text{and} \quad \\
\det(nD_1 + mD_2P) = 1.
\]
Proof. Let $P$ be a $k \times k$ permutation matrix whose associated permutation is $\pi$. We shall present an algorithm to find integers $\{a_i\}_{i=1}^k$ and $\{b_j\}_{j=1}^k$ such that,

$$D_1 = \text{diag}(a_1, \ldots, a_k) \quad \text{and} \quad D_2 = \text{diag}(b_1, \ldots, b_k)$$

satisfy the requirements of lemma.

**Step 1.** If $\pi$ is a $k$-cycle, then, one may compute $\det(nD_1 + mD_2P)$ by the usual formula:

$$\det(nD_1 + mD_2P) = \sum_{\sigma \in S_k} (-1)^{\text{sgn}(\sigma)} x_{1\sigma(1)} \cdots x_{k\sigma(k)}$$

where $x_{ij}$ are the entries of the matrix $nD_1 + mD_2P$. Now, if $\sigma$ contributes to the sum, then, for all $1 \leq i \leq k$, we have $\sigma(i) = i$ or $\sigma(i) = P(i)$. If $\sigma$ is not the identity permutation, there exists $j$ such that $\sigma(j) = P(j) \neq j$. Setting $S = \{\sigma^j(j) : 1 \leq \ell \leq k\}$, no element of $S$ is fixed by $\sigma$, because if $\sigma(\sigma^j(j)) = \sigma^j(j)$, then $\sigma(j) = j$, a contradiction. Thus, $\sigma|_{\mathcal{S}} = \pi|_{\mathcal{S}}$. But, $\sigma^j(j) = \pi^j(j)$ and therefore, the set $\mathcal{S}$ is all of $\{1, \ldots, k\}$. Thus, $\sigma$ must be identity or $\pi$ whence:

$$\det(nD_1 + mD_2P) = n^k \prod_{l=1}^k a_l + (-1)^{k-1} m^k \prod_{l=1}^k b_l.$$ 

Since $\gcd(m^k,(-1)^{k-1}n^k) = 1$, there exists $u$ and $v$ such that

$$m^ku + (-1)^{k-1}n^kv = 1.$$ 

Then, it is easy to verify that the following choices

$$a_1 = u \quad \quad a_l = 1 \text{ for all } l \neq 1 \quad \quad b_1 = v \quad \quad b_l = 1 \text{ for all } l \neq 1$$

meet the requirements of the lemma.

**Step 2.** If $\pi$ is not a cycle, let the cycle decomposition of $\pi$ be $\pi_1 \ldots \pi_r$. We may now repeat Step 1 on each of the cycles $\pi_i$ and determine the scalars $a_j$ and $b_j$ for those $j$ not fixed by $\pi_i$. \hfill $\Box$

For an alternative proof of this lemma, see [12].

### 4. An Algorithm for determining the Smith Vector for $n$

Given a positive integer $n$ and its prime factorisation

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r},$$

we derived a formula for the elementary divisors of $\Psi_n$ using $r$ Young tableaux, one for each prime $p_i$. Now, we will use the same set of Tableaux diagrams to give an algorithm to find a Smith vector for $n$. The algorithm will use the following three modules:

- **SV($p^e$):** Construct a Smith vector for $p^e$, a prime power.
- **TSV($k_1, k_2, p, q$):** Given Smith vectors $p$ and $q$, respectively, for relatively prime positive integers $k_1$ and $k_2$, construct a Smith vector for $k_1k_2$.
- **SV($n$):** Construct a Smith vectors for $n$ inductively on prime powers.

We will illustrate these modules with the example $n = 6$. We will calculate the bit complexity of each module in Section 4.4.
4.1. $SV(p^e)$. Recall from Lemma 3.2 that, up to scaling by elementary divisors, the columns of the matrix $W_n = A_n V_n$ give a Smith vector for $n$. We have established that $W_{p^e}$ has a simple recursive form (see Remark 2.8). Therefore, a Smith vector $SV(p^e)$ for $p^e$ can be computed from this recursive formula.

**Remark 4.1.** Observe that non-zero coefficients in the Smith vector $SV(p)$ are $\pm 1$. Since the non-zero entries of the matrix $A_{p^e}$ are $\pm 1$, it follows by induction on $e$ that the non-zero coefficients in $SV(p^e)$ are $\pm 1$. We will use this fact on the calculation of bit complexity of the algorithm.

**Examples.**

(4.1) $SV(2) = (\mathbb{T} \oplus 0, \mathbb{T} \oplus \mathbb{T})$

(4.2) $SV(3) = (\mathbb{T} \oplus 0, \mathbb{T} \oplus \mathbb{T}, \mathbb{T} \oplus \mathbb{T})$

4.2. $TSV(k_1, k_2, p, q)$. This module is the most crucial part of our algorithm. Let us first do a pictorial construction and make some observations about it.

**Construction.** To construct the Tableaux diagram for $k_1 k_2$ from the Tableaux diagram for $k_1$ and that of $k_2$, we need to repeat $k_2$ times, the rows of the Tableaux diagram for $k_1$ and $k_1$ times, the rows of the Tableaux diagram for $k_2$ (See Remark 3.3). Throughout this subsection, it will be convenient to assume that the rows of the Tableaux diagram for $n$ are numbered from bottom to top with indices between 0 and $n - 1$. We will also index repetition of a row from the bottom with indices between 0 and $k_1 - 1$. So, the components of the Smith vector attached to the rows of the Tableaux diagram for $k_1$ and $k_2$ must change as follows:

- to the $j_1$th repetition of $i_1$th row of Tableaux diagram of $k_1$, we attach the vector $k_2 p^{(i_1)}(\mathbb{T}^{k_2}) q^{(j_1)}(\mathbb{T}^{k_1})$,
- to the $i_2$th repetition of $j_2$th row of the Tableaux diagram of $k_2$, we attach the vector $k_1 p^{(i_2)}(\mathbb{T}^{k_1}) q^{(j_2)}(\mathbb{T}^{k_1})$.

Here, we have multiplied by $k_1$ so that the image of the corresponding element under $\Psi_{mn}$ has order dividing $k_3 - 1$. Finally, we will juxtapose these Tableaux diagrams for $k_1 k_2$ so that the row indices match. This construction is demonstrated in the following figure: In this Tableaux diagram for $k_1 k_2$ we have constructed in Figure , the vectors attached to the $\ell$th row are $k_2 \mathbb{P}_\ell := k_2 p^{(i_1)}(\mathbb{T}^{k_2}) q^{(j_1)}(\mathbb{T}^{k_1})$ and $k_1 \mathbb{Q}_\ell := k_1 p^{(i_2)}(\mathbb{T}^{k_1}) q^{(j_2)}(\mathbb{T}^{k_1})$ where $(i_1, j_1)$ and $(i_2, j_2)$ are uniquely determined by:

(4.3) \[
\begin{cases}
\ell = k_2 i_1 + j_1 = k_1 j_2 + i_2 \\
0 \leq j_s \leq k_{3-s} - 1, \quad s \in \{1, 2\}.
\end{cases}
\]

**Observations.** We now make the following observations about the construction:

1. The diagram in Figure 6 is the Tableaux diagram associated to $k_1 k_2$.

2. For $0 \leq \ell \leq k_1 k_2 - 1$, we have $e_{k_1 k_2}(\ell) = e_{k_1}(i_1) e_{k_2}(j_2)$ where $i_1$ and $j_2$ are determined by (4.3).

**Proof.** Clearly, the Tableaux diagram for $k_1$ contributes $e_{k_1}(i_1)$ and that of $k_2$ contributes $e_{k_2}(j_2)$.

3. With notations as in (2) if we can find $d_{1, \ell}, d_{2, \ell}$ such that $\gcd(d_{1, \ell}, k_1) = \gcd(d_{2, \ell}, k_2) = 1$ and $\{d_{1, \ell} k_2 \mathbb{P}_\ell + d_{2, \ell} k_1 \mathbb{Q}_\ell : 0 \leq \ell \leq k_1 k_2 - 1\}$ is a basis for the codomain of $\Psi_{k_1 k_2}$, then, $(d_{1, \ell} k_2 \mathbb{P}_\ell + d_{2, \ell} k_1 \mathbb{Q}_\ell : 0 \leq \ell \leq k_1 k_2 - 1)$ is a Smith vector for $k_1 k_2$. 


Figure 6. Pictorial Construction for $k_1$ and $k_2$
Proof. From Lemma 3.3, it is clear that the order of \( \Psi_{k_1 k_2}(k_1 \Omega_{\ell}) \) is \( e_{k_1}(i_1) \) and that of \( \Psi_{k_1 k_2}(k_2 \Omega_{\ell}) \) is \( e_{k_2}(j_2) \). Since \( \gcd(d_{x, k}) = 1 \), the order of \( \Psi_{k_1 k_2}(k_{x, \ell}) \) remains unchanged after multiplication by \( d_{x, \ell} \). Therefore, the order of \( \Psi_{k_1 k_2}(d_{1, k_1} \Omega_{\ell} + d_{2, k_2} \Omega_{\ell}) \) equals \( e_{k_1}(i_1) e_{k_2}(j_2) \). This equals \( e_{k_1 k_2}(\ell) \), by (2) and we are done. \( \square \)

(4) Define the following bijections between \([k_1k_2]\) and \([k_1] \times [k_2]\) where \([n] := \{0, 1, \ldots, n - 1\}\):

\[
\iota(\ell) = (i_1, j_1) \quad \iota'(\ell) = (i_2, j_2)
\]

where \((i_1, j_1)\) and \((i_2, j_2)\) are determined from \(\ell\) using (3). Let \(L\) and \(L'\) be total orderings on \([k_1] \times [k_2]\) defined by transferring the order from \([k_1k_2]\) via \(\iota\) and \(\iota'\) respectively. Then, \(L\) is in lexicographic order and \(L'\) is in reverse lexicographic order. Let \(\sigma_{k_1 k_2}\) the permutation \(\iota^{-1} \iota'\) of the set \([k_1k_2]\).

Example 4.2. Take \(k_1 = 2, k_2 = 3\). Then, \(L\) and \(L'\) are increasing along rows in the table below. In cycle notation, \(\sigma_{2, 3} \equiv (1 2 4 3)\).

| \(\ell\) | 0   | 1   | 2   | 3   | 4   | 5   |
|--------|-----|-----|-----|-----|-----|-----|
| \(L\) | (0, 0) | (0, 1) | (0, 2) | (1, 0) | (1, 1) | (1, 2) |
| \(L'\) | (0, 0) | (1, 0) | (0, 1) | (1, 1) | (0, 2) | (1, 2) |

(5) Let \(\Psi = (\Psi_{\ell} : 0 \leq \ell \leq k_1k_2 - 1)\) and \(P\) be the permutation matrix \(\sigma_{k_1 k_2} I\). By Lemma 3.3, there are diagonal matrices \(D_1\) and \(D_2\) such that \(\det(k_2 D_1 + k_1 D_2 P) = 1\). Since \(\{\Psi_{\ell} : 0 \leq \ell \leq k_1k_2 - 1\}\) is a basis for the codomain of \(\Psi_{k_1 k_2}\), we have that the components of \((k_2 D_1 + k_1 D_2 P)\Psi^T\) forms a basis for the codomain of \(\Psi_{k_1 k_2}\). Now, setting \(D_1 = \text{diag}(d_{1, 1}, \ldots, d_{1, k_1k_2 - 1})\) and \(D_2 = \text{diag}(d_{2, 1}, \ldots, d_{2, k_1k_2 - 1})\), by (3) we have that

\[
\text{TSV}(k_1k_2, p, q) := (d_{1, i}k_2 \Omega_{\ell} + d_{2, i}k_1 \Omega_{\ell} : 0 \leq \ell \leq k_1k_2 - 1)
\]

is a Smith vector for \(k_1k_2\).

Algorithm. Given the above observations, we are now ready to present the algorithm for this module.

Step 1: Construct the permutation matrix \(P = \sigma_{k_1 k_2} I\).

Step 2: Construct diagonal matrices \(D_1\) and \(D_2\) as in the proof of Lemma 3.3.

Step 3: Construct the vector \(\Psi = (\Psi_{\ell} : 0 \leq \ell \leq k_1k_2 - 1)\) by the formula:

\[
\Psi_{\ell} = p_{(i_1 k_2)}(\ell k) q_{(j_1 k_1)}(\ell k)
\]

where \(i, j\) and \(\ell\) are related by (4.3).

Step 4: From the entries of the vector \(k_2 D_1 \Psi^T + k_1 D_2 P \Psi^T\), construct the Smith vector \(\text{TSV}(k_1, k_2, p, q)\) as in observation (5).

Example. Let us consider the example \(k_1 = 2, k_2 = 3, p = SV(2)\) and \(q = SV(3)\). The following diagram illustrates the construction we carried out in this subsection.
4.3. $SV(n)$. This algorithm is a recursion using the modules $SV(p^e)$ and $TSV(k_1, k_2, p, q)$.

Algorithm.

Step 1: Factorise $n$ as $p_1^{e_1} \cdots p_r^{e_r}$. For each $p_i^{e_i}$, calculate $SV(p_i^{e_i})$.

Step 2: Having calculated $SV(p_1^{e_1} \cdots p_r^{e_r})$, we calculate $SV(p_1^{e_1} \cdots p_i^{e_i})$ by the formula 

$$SV(p_1^{e_1} \cdots p_i^{e_i}) = TSV(p_i^{e_i}, SV(p_1^{e_1} \cdots p_i^{e_i}), SV(p_1^{e_1} \cdots p_i^{e_i}), SV(p_i^{e_i+1})).$$

4.4. Analysis of Algorithm. To calculate the number of bit operations needed to output $SV(n)$, we need the following definitions and some lemmas.

Recall that, for a polynomial $a(X) = \sum_{i=0}^{n} a_i X^i$ with integer coefficients, its height $ht(a)$ is defined to be $\max\{|a_i| : 0 \leq i \leq n\}$.

Definition 4.3. Given a vector $(p(j) : 0 \leq j \leq n-1)$ having entries in $\bigoplus_{d|n} \mathbb{Z}[X]/\Phi_d(X)$ such that $p(j) = \bigoplus_{d|n} p_d^{(j)}$ mod $\Phi_d(X)$ where $p_d^{(j)}$ is the unique representative of degree at most $\phi(d) - 1$, we define its height to be:

$$ht((p(j) : 0 \leq j \leq n-1)) = \max\{ht(p_d^{(j)}) : d \mid n, 0 \leq j \leq n-1\}.$$

Note 4.4. Given a positive integer $n$, denote the bit length of $n$ by $B(n)$. Let $\mu(n_1, n_2)$ denote the number of bit operations required to multiply a $n_1$-bit number with an $n_2$-bit number. We will also use the same notation $\mu$ to define $\mu(n) := \mu(n, n)$.

(i) We have $\mu(n_1, n_2) \leq \mu(n)$ where $n = \max(n_1, n_2)$. The standard multiplication would suggest $\mu(n) = O(n^2)$ while FFT-method in Schönhage-Strassen algorithm \[14\] indicate that $\mu(n) = O(n \log n \log \log n)$. This bound was later improved by Fürer \[8\].

(ii) Recall that in Step 1 of the proof of Lemma 3.5 we calculate integers $u$ and $v$ such that $um_k + v(-1)^{k-1} n_k = 1$. By extended Euclidean algorithm, this computation takes $O(k^2 \log(n) \log(m))$ bit operations. Also, $B(u)$ and $B(v)$ are $O(k \max(\log(n), \log(m)))$. See \[17\] Section 2.2.

(iii) Let $a(X), b(X) \in \mathbb{Z}[X]$ be polynomials of degree $m$ and $n$ respectively with $m \geq n$ and $b$ monic. Algebraic complexity to calculate remainder of $a(x)$ on division by $b(X)$ is bounded by a constant factor times the algebraic
We begin with some lemmas:

**Lemma 4.5.** Let \(a(X), b(X) \in \mathbb{Z}[X]\) such that \(b(X)\) is monic and \(\deg(a) \geq \deg(b)\). Suppose that \(\text{ht}(a) = M_1\) and \(\text{ht}(b) = M_2\). Let \(a(X) = b(X)q(X) + r(X)\) where \(q(X)\) and \(r(X)\) are quotient and remainder respectively. Then,

\[
\text{ht}(r(X)) \leq M_1(1 + M_2)^\deg(a) - \deg(b) + 1.
\]

**Proof.** In each step of the Standard division algorithm, we subtract a multiple of \(b(X)\) from \(a(X)\) so as to reduce the degree of \(a(X)\). Suppose that, at the \(i\)th stage, we are left with a polynomial of height \(h_i\) where \(0 \leq i \leq \deg(a) - \deg(b) + 1\). Then, \(h_i \leq h_{i-1} + M_2h_{i-1}\) with \(h_0 = M\). So, the height of \(r(X)\) is at most \(M(1 + M_2)^\deg(a) - \deg(b) + 1\). \(\square\)

**Corollary 4.6.** Consider \(a(X), b(X)\) as defined in Lemma 4.5 with \(\deg(a) = m\) and \(\deg(b) = n\). Then the number of bit operations required to compute \(r(X)\) is \(O(m \log m \mu(\log M_2, \log M_1 + m \log M_2))\).

**Proof.** By Note 4.4 (iii), algebraic complexity to compute \(r(X)\) is \(O(m \log m)\). To find an upper bound for bit complexity, we need to multiply the algebraic complexity with \(\mu(B(\text{ht}(b(X))), B(\text{ht}(q(X))))\). From the proof of Lemma 4.5, it is clear that \(\text{ht}(q(X)) = O(M(1 + M_2)^\deg(a) - \deg(b) + 1)\). All these bounds together gives our required result. \(\square\)

We need the following estimate for coefficients of the cyclotomic polynomials due to Bateman.

**Lemma 4.7 (Bateman).** The height of the cyclotomic polynomial \(\Phi_n\) is \(O(\exp(n^{C/\log \log n}))\) for some absolute constant \(C\).

Thus, \(B(\text{ht}(\Phi_n))\) is \(O(n^\epsilon)\) for any \(\epsilon > 0\).

**Lemma 4.8.** The bit length of the height of \(\text{SV}(n)\) is \(O(n^{1+\epsilon})\) for any \(\epsilon > 0\).

**Proof.** Suppose that the prime factorisation of \(n\) is \(p_1^{e_1} \ldots p_r^{e_r}\). We prove this result by induction on \(r\). By Remark 4.1, we have that

\[
\text{ht}(\text{SV}(p_1^{e_1})) = O(1),
\]

and therefore, the bit length \(B(\text{ht}(\text{SV}(p_1^{e_1})))\) of the height is \(O(1)\).

Let \(p := \text{SV}\left(\frac{n}{p_r^{e_r}}\right)\) and \(q := \text{SV}(p_r^{e_r})\). The bit length of the height of the polynomial \(p^i\text{SV}(p_r^{e_r})q^j\text{SV}(p_r^{e_r})\) (before reducing modulo \(\Phi_{d_1d_2}\)) is

\[
O(\log(\max(\deg(q_j^{(j)})))) + B(\text{ht}(p))
\]

since the coefficients in the product is given by convolution. This equals \(O(\log p r^{e_r} + (np_r^{e_r})^{1+\epsilon})\) for any \(\epsilon > 0\).
Using Lemmas 4.3 and 4.7 after reduction mod $\Phi_{d_1, d_2}$, we get:

$$B(\text{ht}(p_i^{(j_1)} (T^{p_i}_{d_1}) q_j^{(j_2)} (T^{p_j}_{d_2}))) = O(\log p_i^{\varepsilon} + (np_i^{-\varepsilon})^{1+\varepsilon} + n \cdot n^\varepsilon) = O(n^{1+\varepsilon})$$

Now, scaling the coefficients of $p$ and $q$ by $k_2D_1$ and $k_1D_2P$ as in Observation (5) of Section 4.2 contributes to an increase of at most $O(n^{1+\varepsilon})$ bits. This finishes the proof.

Now, we are ready to calculate the bit complexity of each of these modules.

$SV(p^\varepsilon)$. Since $W_{p^\varepsilon}$ is given by a recursive formula, calculation of Smith vector for $p^\varepsilon$ takes $O(p^{2\varepsilon})$ steps.

$TSV(k_1, k_2, p, q)$. We will calculate the bit complexity of this algorithm by going over each step of the algorithm:

- In Step 1, the algorithm needs $O(k_1k_2)$ steps.
- For Step 2, in determining the diagonal matrices $D_1$ and $D_2$ as in Lemma 3.5 we need the cycles of the permutation $\sigma_{k_1, k_2}$. Suppose that the cycle lengths of $\sigma$ are $c_1, \ldots, c_s$ so that $\sum_i c_i = k_1k_2$. By Note 4.4 (ii), the time complexity of this step is

$$O \left( \sum_{i=1}^{s} c_i^2 \log(k_1) \log(k_2) \right) = O \left( (k_1k_2)^2 \log(k_1) \log(k_2) \right).$$

- In Step 3, to construct $\Phi_\ell$, we need to find $p_i^{(j_1)} (T^{p_i}_{d_1}) q_j^{(j_2)} (T^{p_j}_{d_2} (t))$ for every $d_1 \mid k_1$ and $d_2 \mid k_2$. Since $p_i^{(j_1)}$ and $q_j^{(j_2)}$ has $\phi(d_1)$ and $\phi(d_2)$ terms respectively, the standard polynomial multiplication costs $O(\phi(d_1) \phi(d_2))$ bit operations where $\mu_k(p, q) := \mu(B(\text{ht}(p)), B(\text{ht}(q)))$. To reduce modulo $\Phi_{d_1, d_2}(t)$, using Corollary 4.0 and Lemma 4.7 we need

$$O(\mu(\alpha(p, q), (k_1k_2)^\varepsilon)(k_2\phi(d_1) + k_1\phi(d_2)) \log(k_1k_2))$$

bit operations. Here $\alpha(p, q) := B(\text{ht}(pq)) + (k_1k_2)^{2+\varepsilon}$. Setting $\beta(p, q)$ to be the quantity $\mu_k(p, q) + \mu(\alpha(p, q), (k_1k_2)^\varepsilon)$, the total bit complexity for this step is:

$$O \left( \beta(p, q) \sum_{\ell=0}^{k_1k_2-1} \sum_{\substack{d_1|k_1 \cr d_2|k_2}} \phi(d_1d_2) + \log(k_1k_2)(k_2\phi(d_1) + k_1\phi(d_2)) \right)$$

$$= O \left( \beta(p, q) \sum_{\ell=0}^{k_1k_2-1} k_1k_2 + \log(k_1k_2)(k_1k_2\tau(k_2) + k_1k_2\tau(k_1)) \right)$$

where $\tau(n)$ is the number of divisors of $n$.

$$= O(\beta(p, q) \log(k_1k_2)(k_1k_2)^2\tau(k_1k_2))$$

Now, from [b] Theorem 315], we have $\tau(k_1k_2) = (k_1k_2)^\varepsilon$ for any $\varepsilon > 0$. Thus, the bit complexity of Step 3 is $O(\beta(p, q)(k_1k_2)^2\varepsilon)$ for every $\varepsilon > 0$.  

Using the facts in Note 4.4 (ii), one may prove that the bit length of the entries of the matrices $k_2 D_1$ and $k_1 D_2$ are bounded by $O((k_1 k_2)^{1+\epsilon})$. Since there are $(k_1 k_2)^2$ terms in $\mathbf{Q}$, Step 4 needs $O((k_1 k_2)^2 \mu([k_1 k_2]^{1+\epsilon} \epsilon, B(\mathbf{ht}(\mathbf{Q}))))$ bit operations.

Summing the bit complexities of each step, we conclude that the bit complexity of the last step which is given by (4.4) is actually $O(n^2)$. For Step 2, the maximum bit operations are required in the last step of the recursion. We know that, the bit complexity of module $T SV(\frac{n}{p_r^e}, p_r^e, SV(\frac{n}{p_r^e}), SV(p_r^e))$ is:

$$O(n^2 \mu([n^{1+\epsilon}], B(\mathbf{ht}(SV(n)))) + n^{2+\epsilon} \beta(SV(\frac{n}{p_r^e}), SV(p_r^e))).$$

By Lemma 4.8 we have $B(\mathbf{ht}(SV(n)))$ and $\beta(SV(\frac{n}{p_r^e}), SV(p_r^e))$ are both $O(n^{1+\epsilon})$.

Thus, the bit complexity of the last step which is given by (4.4) is actually $O(n^{3+\epsilon})$. Since $r = O(\log(n))$, the bit complexity of the module $SV(n)$ is $O(n^{3+\epsilon})$ for any $\epsilon > 0$.

4.4.1. Space Complexity. Note that the bit length of an integer that appears while executing the module $SV(n)$ is $O(n^{1+\epsilon})$ for any $\epsilon > 0$. The maximum space is needed to store a Smith vector for $n$. Since a Smith vector has $O(n^2)$ terms, the space complexity of $SV(n)$ is $O(n^{3+\epsilon})$ for any $\epsilon > 0$.

We summarise the above discussion in the following theorem:

**Theorem 4.9.** Given a positive integer $n$, the algorithm $SV(n)$ gives a Smith vector for $n$. The bit complexity and space complexity of this algorithm are both $O(n^{3+\epsilon})$ for any $\epsilon > 0$.

We may compare this theorem with the results in the literature in this direction. It appears to us that the best known algorithm for determining Smith normal form $S(A)$ of an integer matrix $A$ and the unimodular transforming matrices $U$ and $V$ are due to Arne Storjohann in his PhD thesis [15]. Let $O(n^\theta)$ be the algebraic complexity involved in multiplying two $n \times n$ matrices with integer entries; best known algorithms give $2 < \theta \leq 3$ (for example, V. Vassilevska Williams gives an algorithm with $\theta = 2.373$ in [10]). He proves:

**Theorem ([15] Proposition 7.20).** For a $n \times m$ matrix $A = (a_{ij})$ of rank $r$ with integer entries, the Smith normal form $S(A)$ and the unimodular transforming matrices $U$ and $V$ may be obtained in $O^*(nrnr^{-1} \log \|A\| + nm(\log \|A\|))$ bit operations where $\|A\| = \max_{i,j} |a_{ij}|$.

Here $O^*(g(n))$ is the soft-Oh notation which drops out polylogarithmic factors: for functions $f, g : \mathbb{R}^n \to \mathbb{R}$, we say that $f = O^*(g)$ if there is a constant $c > 0$ such that $f = O(g \log^c(g))$.

Specialising to our case, it is seen that Storjohann’s algorithm would require $O(n^{1+\theta+\epsilon})$ bit operations. Here we substituted $\log \|A\| = O(n^\epsilon)$ due to Lemma 4.7. Thus, our algorithm is an improvement to this best known algorithm in the special case we are interested in.
Appendix A. Determinant of $A_n$

We now calculate the determinant of the matrix $A_n$ in terms of resultants of cyclotomic polynomials. The advantage of this new approach is the fact that this generalises to any monic polynomial $f$ over a unique factorisation domain (UFD) and any of its factorisations into pairwise relatively prime polynomials. Moreover, this approach determines the sign of $\det(A_n)$ unambiguously.

To calculate the determinant of $A_n$, we propose the following simplification:

A.1. Simplification. Let $\Omega_n$ be the cyclic group of all $n$th roots of unity. The cyclotomic polynomials $\{\Phi_d\}_{d|n}$ factorise over the ring $\mathbb{Z}[\Omega_n]$ of cyclotomic integers. We will see that calculating $\det(A_n)$ becomes very simple when we work over the ring of cyclotomic integers. Now, we shall argue that passing to $\mathbb{Z}[\Omega_n]$ does not affect the computation.

To see this, consider the following diagram of maps and a description of the maps that follows it:

\[\begin{array}{ccc}
\mathbb{Z}[X]/(X^n-1) & \xrightarrow{\iota_1} & \mathbb{Z}[\Omega_n][X]/(X^n-1) \\
\Psi_n & & \Psi_n \\
\bigoplus_{d|n} \mathbb{Z}[X]/\Phi_d(X) & \xrightarrow{\iota_2} & \bigoplus_{d|n} \mathbb{Z}[\Omega_n][X]/\Phi_d(X) \\
\rho_2 & & \rho_2 \\
\bigoplus_{\omega \in \Omega_n} \mathbb{Z}[\Omega_n][X]/(X-\omega) & \rightarrow & \bigoplus_{\omega \in \Omega_n} \mathbb{Z}[\Omega_n][X]/(X-\omega)
\end{array}\]

- The inclusions $\iota_1$ and $\iota_2$ are defined by taking $1 \mapsto 1$ and $X \mapsto X$ between the respective rings.
- The map $\Psi_n$ is the $\mathbb{Z}[\Omega_n]$-linear map, defined by the $\mathbb{Z}[\Omega_n]$ extension of the map:

\[(A.1) \quad \oplus_{\omega \in \Omega_n} X^i \mod \Phi_d(X)\]

- The map $\rho_1$ is the canonical quotient map.
- The map $\rho_2$ is the composition $\rho_1 \circ \Psi_n$.

Note that, the diagram commutes: $\Psi_n \circ \iota_1 = \iota_2 \circ \Psi_n$. Now, we may deduce that the determinant of $\Psi_n$ equals that of $\Psi_n$, when computed with respect to “compatible bases”. In fact, with $(1, X, \ldots, X^{n-1})$ as the basis for the domain of $\Psi_n$ and $(1, X, \ldots, X^{\phi(d)-1})$ as the basis for $\mathbb{Z}[\Omega_n][X]/\Phi_d(X)$, we see that, the determinants are indeed equal. Thus, we are reduced to calculating the determinant of $\Psi_n$. By the multiplicativity of the determinant, we have:

\[(A.2) \quad \det(A_n) = \det(\Psi_n) = \frac{\det(\rho_2)}{\det(\rho_1)}\]

However, to write the matrix of the $\mathbb{Z}[\Omega_n]$-linear maps $\rho_1$ and $\rho_2$, we need an ordered basis for the codomain of $\rho_1$ which is the same as that of $\rho_2$. So, we may fix any total order $\prec$ on $\Omega_n$ so that if $d_1$ and $d_2$ are two divisors of $n$ and $d_1 < d_2$, then, all the primitive $d_1$th roots of unity precede all the primitive $d_2$th roots of unity in the order $\prec$. Say,

\[(A.3) \quad \Omega_n = \prod_{d|n} \{\omega_{d,1}, \ldots, \omega_{d,\phi(d)}\} = \{\omega_{d,j} : d \mid n, 1 \leq j \leq \phi(d)\}\]

where $\omega_{d,j}$ is a primitive $d$th root of unity ($1 \leq j \leq \phi(d)$) and $\Omega_n$ is ordered lexicographically.
Theorem will be used to finish off the computation: also refer to Apostol \[2\] and Dresden \[7\] for alternative proof. The following result

\[
D_{d} = \begin{pmatrix}
1 & \omega_{d,1}^2 & \ldots & \omega_{d,1}^{\phi(d)-1} \\
1 & \omega_{d,2}^2 & \ldots & \omega_{d,2}^{\phi(d)-1} \\
1 & \omega_{d,3}^2 & \ldots & \omega_{d,3}^{\phi(d)-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \omega_{d,\phi(d)}^2 & \ldots & \omega_{d,\phi(d)}^{\phi(d)-1}
\end{pmatrix}
\]

where \(\omega_{d,1} < \cdots < \omega_{d,\phi(d)}\) are primitive \(d\)th roots of unity.

The matrix \([\rho_2]\) of \(\rho_2\) with respect to the chosen basis is a block column matrix

\[
(R_1, \ldots, R_d, \ldots, R_n)^\ell_d\]

where \(R_d\) is the following matrix:

\[
R_d = \begin{pmatrix}
1 & \omega_{d,1} & \ldots & \omega_{d,1}^{n-1} \\
1 & \omega_{d,j} & \ldots & \omega_{d,j}^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \omega_{d,\phi(d)} & \ldots & \omega_{d,\phi(d)}^{n-1}
\end{pmatrix}
\]

Since the matrices \(D_d\) and \([\rho_2]\) are Vandermonde matrices, we have at once that:

\[
\det(\rho_1) = \prod_{d \mid n} \det(D_d)
\]

\[
= \prod_{d \mid n} \prod_{1 \leq i < j \leq \phi(d)} (\omega_{d,j} - \omega_{d,i})
\]

\[
\det(\rho_2) = \prod_{d_1,d_2 \mid n, 1 \leq i \leq \phi(d_1)} \prod_{1 \leq i \leq \phi(d_2)} (\omega_{d_2,i} - \omega_{d_1,i}) \prod_{d \mid n, 1 \leq i < j \leq \phi(d)} (\omega_{d,j} - \omega_{d,i})
\]

Now, from A.2, we see that:

\[
\det(A_n) = \prod_{d_1,d_2 \mid n, 1 \leq d_1 < d_2 \leq n} \left( \prod_{1 \leq i \leq \phi(d_1)} (\omega_{d_2,i} - \omega_{d_1,i}) \right)
\]

\[
= \prod_{d_1,d_2 \mid n, 1 \leq d_1 < d_2 \leq n} \mathcal{R}(\Phi_{d_2}, \Phi_{d_1})
\]

where \(\mathcal{R}(f, g)\) is the resultant of the polynomials \(f\) and \(g\) (for definition and basic properties of resultants of polynomials, see [13 Chapter 1, Section 3]). The resultant of pairs of cyclotomic polynomials first appears in print in the work of Diederichsen [6], §3, Hilfssatz 2 on integral representations of cyclic groups. We also refer to Apostol [2] and Dresden [7] for alternative proof. The following result will be used to finish off the computation:

THEOREM A.1 (Diederichsen). Let \(m\) and \(n\) be positive integers.
(1) \( R(\Phi_m, \Phi_n) = 0 \) if and only if \( m = n \).

Assume now that \( m > n \).

(2) If \( n = 1 \), then,

\[
R(\Phi_m, \Phi_n) = \begin{cases} 
(-1)^{\phi(m)} & \text{if } m = p^\alpha \text{ for some } \alpha > 0 \\
(-1)^{\phi(m)} & \text{otherwise}
\end{cases}
\]

(3) If \( n > 1 \) and \( \gcd(m, n) = 1 \), then, \( R(\Phi_m, \Phi_n) = 1 \).

(4) If \( n > 1 \) and \( \gcd(m, n) > 1 \), then,

\[
R(\Phi_m, \Phi_n) = \begin{cases} 
p^{\phi(m)} & \text{if } \frac{m}{n} = p^\alpha \text{ for some } \alpha > 0 \\
1 & \text{otherwise}
\end{cases}
\]

We now start from (A.9) and use Theorem A.1 to get a closed form expression for \( \det(A_n) \) in terms of the prime factorisation of \( n \): say, \( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \).

We first rewrite (A.9) as follows:

\[
\prod_{1 \leq d_1 < d_2 \leq n \atop d_1, d_2 \mid n} R(\Phi_{d_2}, \Phi_{d_1}) = \prod_{d \mid n \atop d \neq 1} R(\Phi_d, X - 1) \prod_{1 < d_1 < d_2 \leq n \atop d_1, d_2 \mid n} R(\Phi_{d_2}, \Phi_{d_1})
\]

As a consequence of (A.10), the first product on the right hand side of (A.12) evaluates to:

\[
\prod_{d \mid n \atop d \neq 1} R(\Phi_d, X - 1) = \prod_{d \mid n \atop d \neq 1} (-1)^{\phi(d)} \Phi_d(1) = (-1)^{n-1} n.
\]

For evaluating the second product, by Theorem A.1 note that a pair \((d_1, d_2)\) of divisors of \( n \) contributes to the product if and only if \( d_1 \neq 1 \) and the ratio \( \frac{d_2}{d_1} \) is a prime power, say \( p_1^{e_1} \) for some \( 1 \leq i \leq r \) and \( 1 \leq e_i \leq \alpha_i \); also each such pair contributes \( p_1^{\phi(d_2)} \) to the product. For a fixed prime \( p_i \) \((1 \leq i \leq r)\) and exponent \( e_i \) \((1 \leq e_i \leq \alpha_i)\), every divisor \( d_1 \) of \( \frac{n}{p_i^{e_i}} \) with \( d_1 \neq 1 \) determines a contributing pair \((d_1, d_2)\) of divisors and conversely. Therefore:

\[
\prod_{1 < d_1 < d_2 \leq n \atop d_1, d_2 \mid n} R(\Phi_{d_2}, \Phi_{d_1}) = \prod_{i=1}^{r} \prod_{1 \leq e_i \leq \alpha_i \atop d \mid n p_i^{-e_i} \atop d \neq 1} p_1^{\phi(d)} = \prod_{i=1}^{r} \sum_{e_i=1}^{\alpha_i} p_i^{p_i^{e_i}}
\]

This finishes the computation and we now have:

**Theorem A.2.** For a positive integer \( n \), we have:

\[
\det(A_n) = \prod_{1 \leq d_1 < d_2 \leq n \atop d_1, d_2 \mid n} R(\Phi_{d_2}, \Phi_{d_1}) = (-1)^{n-1} \prod_{i=1}^{r} p_i^{(p_i^{e_i}-1)}
\]
Following the computations done before Theorem A.1 we may prove:

**Theorem A.3.** Suppose that $f$ is a monic polynomial over a UFD and

$$f = \prod_{i=1}^{n} f_i$$

is a factorisation of $f$ into pairwise relatively prime polynomials. Then, the determinant of the canonical map $\Psi_f$ written with respect to the standard basis is:

$$\det(\Psi_f) = \prod_{1 \leq i < j \leq n} R(f_j, f_i). \quad (A.18)$$

**Remark A.4.** From the above theorem, the resultant $R(f_2, f_1)$ is the determinant of the map $\Psi_{f_1f_2}$ written with respect to the standard basis. Specialising to $f_1 = \Phi_m(X)$ and $f_2 = \Phi_n(X)$ with $m > n$, we have the following exact sequence:

$$0 \longrightarrow \mathbb{Z}[X]/\Phi_m(X) \longrightarrow \mathbb{Z}[X]/\Phi_m(X) \oplus \mathbb{Z}[X]/\Phi_n(X) \longrightarrow G_1(\Phi_m(X)\Phi_n(X)) \longrightarrow 0$$

Now, we have $|G_1(f)| = |R(\Phi_m, \Phi_n)|$. Also, the intersection of the ideal generated by $\Phi_m$ and $\Phi_n$ with $\mathbb{Z}$ is given by ([7, Theorem 2]):

$$\langle \Phi_m(X), \Phi_n(X) \rangle \cap \mathbb{Z} = \begin{cases} p\mathbb{Z} & \text{if } \frac{m}{n} = p^\alpha \text{ for some } \alpha > 0 \\ \mathbb{Z} & \text{otherwise} \end{cases} \quad (A.19)$$

Now, setting $r = \phi(m) + \phi(n)$, if $(e_0, \ldots, e_{r-1})$ are elementary divisors of $\Psi_{\Phi_m\Phi_n}$, then, $e_i \mid p$ and $\prod e_i = |R(\Phi_m, \Phi_n)|$. If $\frac{m}{n}$ is not power of a prime, then, $e_i = 1$ for all $i$. If $\frac{m}{n}$ is power of a prime $p$, the elementary divisors are given by $e_i = 1$ for $0 \leq i \leq \phi(n) - 1$ and $e_j = p$ for $\phi(n) \leq j \leq \phi(m) + \phi(n) - 1$.

**Remark A.5.** Let $S$ be a UFD. Then, $R = S[x_1, \ldots, x_n]$ is a UFD and considering the polynomial $f(X) = \prod_i (X - x_i)$ in Theorem A.3 we see that Vandermonde determinant falls out as a special case. The elementary divisors of a Vandermonde matrix over a Dedekind domain has been calculated by M. Bhargava [5, Lemma 2].

**Acknowledgements.** The authors would like to thank the Institute of Mathematical Sciences, Chennai and Indian Statistical Institute, Bangalore, where various parts of this work was carried out, for their hospitality and support. The authors thank Amritanshu Prasad for suggesting numerous improvements. The authors are grateful to Vikram Sharma for guiding them with references for the write-up in Section 4.4.

**References**

[1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullam. *The Design and Analysis of Computer Algorithms*. Pearson Education, eighth edition, 2003.

[2] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proceedings of the American Mathematical Society*, 24(3):457–462, March 1970.

[3] Raymond G. Ayoub and Christine Ayoub. On the group ring of a finite abelian group. *Bull. Austral. Math. Soc.*, 1:245–261, 1969.

[4] P. T. Bateman. Note on the coefficients of the cyclotomic polynomial. *Bull. Amer. Math. Soc.*, 55:1180–1181, 1949.

[5] Manjul Bhargava. Generalized factorials and fixed divisors over subsets of a dedekind domain. *Journal of Number Theory*, 72(1):62–75, 1998.
[6] Fritz-Erdmann Diederichsen. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. *Abh. Math. Sem. Univ. Hamburg*, 13(1):357–412, 1939.

[7] Gregory Dresden. Resultants of cyclotomic polynomials. *Rocky Mountain J. Math.*, 42(5):1461–1469, 2012.

[8] Martin Fürer. Faster integer multiplication. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC ’07, pages 57–66, New York, NY, USA, 2007. ACM.

[9] Godfrey Harold Hardy and Edward Maitland Wright. *An Introduction to the Theory of Numbers*. Oxford science publications, illustrated, reprint edition, 1979.

[10] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, third edition, 2002.

[11] Andrew D. Loveless. The general GCD-product function. *Integers*, 6, July 2006. #A19.

[12] Kamalakshya Mahatab. A problem about determinant of sum of permutation matrices. MathOverflow. URL: http://mathoverflow.net/q/137180 (version: 2013-07-20).

[13] Victor V. Prasolov. *Polynomials*, volume 11 of *Algorithms and Computations in Mathematics*. Springer-Verlag, Berlin, 2004. Translated from the 2001 Russian second edition by Dimitry Leites.

[14] A Schönhage and V Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3 - 4):281 – 292, 1971.

[15] Arne Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology, Zürich, Switzerland, 2000.

[16] Virginia Vassilevska Williams. Multiplying matrices faster than coppersmith-winograd. In *Proceedings of the 44th Symposium on Theory of Computing*, STOC ’12, pages 887–898, New York, NY, USA, 2012. ACM.

[17] Chee-Keng Yap. *Fundamental Problems in Algorithmic Algebra*. Oxford University Press, 2000.

THE INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI
E-mail address: kamalakshya@imsc.res.in

STATISTICS AND MATHEMATICS UNIT, INDIAN STATISTICAL INSTITUTE, BANGALORE-560059.
E-mail address: knsam.name@gmail.com