Transposition as a permutation: a tale of group actions and modular arithmetic

Jeff Hooper
Franklin Mendivil
Department of Mathematics and Statistics
Acadia University

Abstract

Converting a matrix from row-order storage to column-order storage involves permuting the entries of the matrix. How can we determine this permutation given only the size of the matrix? Unexpectedly, the solution to this question involves the use of elementary group theory and number theory. This includes the Chinese Remainder Theorem, finding multiplicative generators modulo p^n for prime p and using these to find orbit generators for a group action, a subgroup of $\mathbb{Z}_N^*$ acting on all of $\mathbb{Z}_N$.

1 Introduction

Suppose we have the following matrix stored in row order in computer memory:

$$A = \begin{pmatrix} 1 & 10 & 3 & 5 & 8 & 9 & 20 \\ 3 & -3 & 19 & -5 & 10 & 9 & 100 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

This means that the matrix is stored (row-by-row) as

`value`	1	10	3	5	8	9	20	3	-3	19	-5
`location`	0	1	2	3	4	5	6	7	8	9	10
`value`	10	9	100	1	1	1	1	0	0	0	
`location`	11	12	13	14	15	16	17	18	19	20	

On the other hand, the transpose of A,

$$A^T = \begin{pmatrix} 1 & 3 & 1 \\ 10 & -3 & 1 \\ 3 & 19 & 1 \\ 5 & -5 & 1 \\ 8 & 10 & 0 \\ 9 & 9 & 0 \\ 20 & 100 & 0 \end{pmatrix},$$

is stored (also row-wise) in memory as

value	1	3	1	10	-3	1	3	19	1	5	-5
location	0	1	2	3	4	5	6	7	8	9	10
value	1	8	10	0	9	9	0	20	100	0	
location	11	12	13	14	15	16	17	18	19	20	

In going from A to A^T we have simply permuted the matrix values around among the memory locations used to store the matrix. In describing this permutation, the actual matrix entries are not particularly relevant; only the locations are important. Thus, in our example above, we can write the resulting permutation as

$$\begin{array}{cccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 1 & 4 & 7 & 10 & 13 & 16 & 19 & 2 & 5 & 8 & 11 & 14 & 17 & 20 \end{array}$$

[This is to be read as: 'the value in location 0 remains in location 0,' 'the value in location 1 moves to location 3,' and so on.]

The most convenient way (for us) of representing this permutation turns out to be as a product of disjoint cycles. Doing this we obtain the representation

$$(0)(1\ 3\ 9\ 7)(2\ 6\ 18\ 14)(4\ 12\ 16\ 8)(5\ 15)(10)(11\ 13\ 19\ 17)(20).$$

A similar permutation can be found to describe this transposition for any $m \times n$ matrix. The question that naturally arises is: Can we predict the structure of this permutation based only on the size of the matrix (i.e. using only the knowledge of m and n)?

Because of its dynamical origins, this permutation arises in other contexts. An example of this is the study of perfect shuffles, as described in [21].

A perfect shuffle of a deck of $2n$ cards comprises the following process. The original deck is 'cut' into two piles of size n: Pile A consists of cards $1-n$ while Pile B consists of cards $(n+1)-2n$. These piles are then interleaved into a new pile of size $2n$ by alternately taking one card from each pile. Since the cards are moved to new locations depending only on their original position, these shuffles give rise to similar permutations.

If, during the interweaving, the top card for the new $2n$ pile is chosen from Pile A (and hence the bottom card from Pile B) then the result of the shuffle will leave the top and bottom cards of the original deck in place, and this type of shuffle (called an 'out shuffle' in [21]) corresponds to transposing a $2 \times n$ matrix.

The main theme of this paper is an analysis of these permutations in terms of a fusion of group theory and number theory, which allows us a complete description of the permutation, and in fact gives rise to an algorithm for finding the permutation explicitly and hence for performing the transposition "in-place". The key idea is that the process of permuting the elements may be related to the action of the subgroup $\langle m \rangle$ of $\mathbb{Z}^*_{mn-1}$ acting on the full set $\mathbb{Z}_{mn-1}$. Because our

original motivating factor for this work was the problem of matrix transposition, the discussion is based around the problem of using group theory and number theory to design an algorithm to solve the in-place matrix transposition problem. In particular, we shall use matrix terminology and intuition throughout, to help ground the discussion in a particular application.

The paper is organized as follows. Section 2 introduces the appropriate group action and shows that the orbits under the action are precisely the cycles of our permutation. In Section 3 we examine the key problems of determining the number of orbits and of finding representatives for each. An essential result is Proposition 3, which allows us to decompose the problem by factoring $mn-1$ into prime powers, solve these simpler cases, and reconstruct the general solution. We completely describe answers to both when our modulus $mn-1$ is either prime or a product of distinct primes. This leaves us with the cases in which the modulus is a prime power, and Sections 4 and 5 are devoted to these. The prime $p=2$ quite often behaves differently than other primes (it has been called the 'oddest prime'!) and this is the case here, which is why the analysis of modulus 2^k must be separated from the rest. Section 6 is devoted to examples which pull together the results of the previous sections to see how the complete permutation is constructed. We close with a final discussion section which includes some suggestions for further explorations of the ideas used in the paper.

2 Modular arithmetic and group actions enter the scene

Returning to our example of a 3×7 matrix, we recall that the permutation is

$$(0)(1\ 3\ 9\ 7)(2\ 6\ 18\ 14)(4\ 12\ 16\ 8)(5\ 15)(10)(11\ 13\ 19\ 17)(20).$$

The values in the first and last memory locations (locations 0 and 20) do not move, which is an obvious property of the transpose. In this particular case, the value in memory location 10 also remains stationary.

Looking at the orbit (1 3 9 7) we see that it seems that for the first two elements, we are multiplying by 3 to get to the next element in the cycle. Considering these numbers mod 20, this is true for all of them: $9 \cdot 3 \equiv 7 \bmod 20$ and $7 \cdot 3 \equiv 1 \bmod 20$. In fact, as the reader will quickly verify, this is true for each of the orbits.

This is a general feature of this permutation.

Proposition 1. *Let A be a* `M` *by* `N` *matrix stored in row order. Then the value in memory location $n <$* `N*M`-1 *(starting with location 0) is moved to location $n *$* `M` $\bmod$ `N*M`-1 *when you perform a transpose on A and store A^T in row order.*

Proof. This is clear since if we write

$$n = j + i * \texttt{N} \quad \text{with } i = 0, 1, \ldots, (M-1) \text{ and } j = 0, 1, \ldots, (N-1),$$

so that n is in the ith row and jth column, we see that

$$n * \mathtt{M} = j * \mathtt{M} + i * \mathtt{N} * \mathtt{M} = j * \mathtt{M} + i * (\mathtt{M} * \mathtt{N1}) + i = j * \mathtt{M} + i \bmod \mathtt{N} * \mathtt{M} - 1$$

is in the jth row and ith column of A^T. □

As the value $\mathtt{M} * \mathtt{N} - 1$ *is important and will recur many times, for simplicity we will denote it by* D*.*

According to the proposition, if we work with the locations mod D, then the value in location a is sent to location $a\mathtt{M} \bmod \mathtt{D}$, the value in $a\mathtt{M} \bmod \mathtt{D}$ is sent to location $a\mathtt{M}^2 \bmod \mathtt{D}$, the value in location $a\mathtt{M}^2 \bmod \mathtt{D}$ to location $a\mathtt{M}^3 \bmod \mathtt{D}$, and so on. Eventually $\mathtt{M}^r \equiv 1 \bmod \mathtt{D}$ for some power r and so we have the cycle $(a\ a\mathtt{M} \bmod \mathtt{D}, a\mathtt{M}^2 \bmod \mathtt{D}, a\mathtt{M}^3 \bmod \mathtt{D}, \ldots, a\mathtt{M}^{r-1} \bmod \mathtt{D})$ in this decomposition.

Once we have the permutation written as a product of disjoint cycles, it is easy to perform the transpose with only one additional memory location. We simply store the value from one entry, shift all the others in the cycle, and then restore the value into its proper place. For example, for the cycle (1 3 9 7), if we store the value in memory location 1 (in our example from the beginning, this is a 10), then we copy the value from memory location 7 into memory location 1, copy the value from memory location 9 into memory location 7, copy the value from memory location 3 into memory location 9 and then, finally, take our stored value (the number 10 in this case) and place it into memory location 3.

Since we can do this for each cycle in the permutation, once we have the cyclic decomposition of the permutation, we only need ONE additional memory location in order to perform the matrix transpose. Furthermore, it is easy (as we see by Proposition 1) to see where any given memory location moves. This means that we only need to find a representative from each cycle in the cyclic decomposition in order to know this decomposition. That is, for our example above, as long as we know that there are 8 cycles in the decomposition and that the elements $0, 5, 10, 16, 1, 13, 6$ and 20 are all in distinct cycles, we can reconstruct the entire cyclic decomposition.

In fact, Proposition 1 indicates that we can view the cycle decomposition as the collection of orbits of a group action. The group is $\langle \mathtt{M} \rangle$, the cyclic group generated by M under multiplication modulo D and this group is acting on $\mathbb{Z}_{\mathtt{D}}$, the full set of integers mod D. The orbit starting at 1 (or the cycle starting with 1) is just the subgroup $\langle \mathtt{M} \rangle$ itself, and is particularly important, so we call it the *primary orbit*. Note also that by the orbit-stabilizer theorem on group actions (see for instance [9]), the lengths of all orbits are divisors of the group order, and hence of the length of the primary orbit.

For the remainder of this paper we will ignore the orbit (D), as it is always there and thus easy to predict. It turns out that we must consider the zero orbit (0), even though it is also always present.

3 Finding orbit representatives

In light of Proposition 1 and the subsequent discussion, the crux of the algorithm we design here involves first determining the number of orbits and then finding a representative from each orbits.

The first clue to finding a complete set of orbit representatives lies in looking at the case where D is a prime number. In this case, the set $\{1, 2, \ldots, \mathtt{D}-1\} = \mathbb{Z}_{\mathtt{D}}^*$ is a cyclic group under multiplication (see [17], Theorem 4-3). Furthermore, if we look at the orbit starting with 1 we see that we have a subgroup of $\mathbb{Z}_{\mathtt{D}}^*$, the subgroup generated by the element M. This means that the other non-zero orbits are precisely the cosets of this subgroup and therefore finding all the orbits means finding all the cosets. However, by Lagrange's Theorem, we know that the length of the primary orbit is a divisor of the order of $\mathbb{Z}_{\mathtt{D}}^*$ (which is equal to $\mathtt{D}-1$ in this case) and all the other non-zero orbits have this same length. So we have $(\mathtt{D}-1)/(\textit{length of primary orbit})$ non-zero orbits.

Suppose that L is the length of the primary orbit modulo the prime D. Suppose further that g is a primitive root modulo D (that is, the powers of g generate $\mathbb{Z}_{\mathtt{D}}^*$). Since L is the length of the primary orbit, the element M has order L in $\mathbb{Z}_{\mathtt{D}}^*$. In fact because $\mathbb{Z}_{\mathtt{D}}^*$ is cyclic, the primary orbit contains all $x \in \mathbb{Z}_{\mathtt{D}}^*$ with $x^L = 1$ (see, for example, [12, Theorem 4.3]). Let $(\mathtt{D}-1)/L = N$ be the number of cosets (non-zero orbits). Then g^N is also a generator of the primary orbit: it is in the primary orbit since $g^{NL} = g^{\mathtt{D}-1} = 1$ and is a generator since $(g^N)^i \neq 1$ for $i < L$. However, this then means that the elements $g, g^2, g^3, \ldots, g^{N-1}$ will be representatives of the other cosets, so of the other orbits. This results in a very simple method of obtaining all the orbit representatives when D is prime. We summarize this discussion in the following result.

Proposition 2. *Let D be a prime. Then all nonzero orbits are cosets of* $\langle \mathtt{M} \rangle$*, the primary orbit, in* $\mathbb{Z}_{\mathtt{D}}^*$*. With* L *the length of the primary orbit and* g *a primitive element modulo D, the generators for the nonzero orbits are* g^i*,* $i = 0, 1, \ldots, \frac{\mathtt{D}-1}{L} - 1$*.*

As an example, consider the case of a 3×4 matrix (so that $\mathtt{D} = 11$). In this case the cyclic decomposition of the transposition permutation is

$$(0)(1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8)$$

and we see that $\mathbb{Z}_{11}^*$ is decomposed into the subgroup (1 3 9 5 4) and its coset (2 6 7 10 8).

We have seen that $L = 5$ is the length of the primary orbit. It is not too hard to see that $g = 2$ is a primitive root. Thus there are two cosets which are represented by the elements $g^0 = 1$ and $g^1 = 2$. From this we obtain the three orbits, including the zero orbit.

Notice that the length of the primary orbit is the same as the multiplicative order of the element M modulo D. In general, this order is very difficult to predict in advance. For our purposes we must generate the primary orbit and so it is simple enough to compute its length (and hence the order of M) as we generate the primary orbit.

What if D is not a prime number? Well, the Chinese Remainder Theorem (see for example [19]) tells us that $\mathbb{Z}_{\mathtt{D}}$ is isomorphic to a product of commutative rings of the form $\mathbb{Z}_k$, with the individual rings in this product being given by the prime factorization of D. But how does this help in finding the orbits of the group action?

To motivate our discussion, we look at the example of a 4 by 9 matrix (where $\mathtt{D} = 35$) with orbit structure (recall that we ignore the orbit (35))

(0)
(1 4 16 29 11 9)
(22 18 2 8 32 23)
(31 19 6 24 26 34)
(17 33 27 3 12 13)
(15 25 30)
(10 5 20)
(21 14)
(7 28).

If we look at the orbits generated modulo 5 and 7 by multiplication by 4 we see that modulo 5 we have

(0)
(1 4)
(2 3)

while for modulo 7 we have

(0)
(1 4 2)
(3 5 6)

The first thing to notice is that there are 9 orbits modulo 35 and three each modulo 5 and 7. This is highly suggestive. In fact, if we reduce each of the original orbits modulo 5 and modulo 7, we get a pair of modulo 5 and modulo 7 orbits. For example, taking the principal orbit (1 4 16 29 11 9), and reducing modulo 5 we obtain the orbit (1 4) . Modulo 7 we obtain the orbit (1 4 2). This suggests that if we can understand the orbit structure modulo 5 and modulo 7, we should somehow be able to combine them to get the orbits modulo 35. In fact, this is exactly the case and is a consequence of the Chinese Remainder Theorem.

To illustrate this, consider the modulo 5 orbit (1 4) and the modulo 7 orbit (3 5 6). If we repeat the first orbit three times and the second two times and place them side-by-side we get the array:

$$\begin{array}{cccccc} 1 & 4 & 1 & 4 & 1 & 4 \\ 3 & 5 & 6 & 3 & 5 & 6 \end{array}$$

Now, using the Chinese Remainder Theorem we find the unique element x in $\mathbb{Z}_{35}$ which satisfies $x = 1 \bmod 5$ and $x = 3 \bmod 7$. In this case, the element x is 31. Next we find that $19 = 4 \bmod 5$ and $19 = 5 \bmod 7$. Continuing in this fashion, we build up the modulo 35 orbit (31 19 6 24 26 34).

Performing this same procedure with all combinations of modulo 5 and modulo 7 orbits will give all the modulo 35 orbits (the interested reader is encouraged to try this).

There is a possible problem, however. Consider the case of a 2 by 8 matrix. The orbit structure modulo 15 is

(0)
(6 12 9 3)
(1 2 4 8)
(11 7 14 13)
(10 5).

If we generate orbits using the multiplier 2 modulo 3 we get

(0)
(1 2)

and modulo 5 we get

(0)
(1 2 4 3).

Since there are two orbits modulo 3 and two orbits modulo 5, there are only 4 combinations. However, there are 5 orbits modulo 15.

The situation is best illustrated by laying two orbits side-by-side as follows

1	2	1	2	1	2	1	2
1	2	4	3	1	2	4	3

Since the orbits have length 2 and 4, respectively, we see that the overall pattern repeats every four symbols. However, this means that certain combinations are never found. For example, we are never matching up 1 in the first row with 2 in the second, so the element 7 from $\mathbb{Z}_{15}$ is never represented. In fact, if we perform our procedure with these orbits we get only the orbits (mod 15)

(0)
(6 12 9 3)
(1 2 4 8)
(10 5).

The problem is that $gcd(2, 4) = 2 \neq 1$, so when we place these two orbits side-by-side we do not get all possible pairings and thus miss some elements. Notice that if we shift one of the orbits and then lay them side-by-side we get

2	1	2	1	2	1	2	1
1	2	4	3	1	2	4	3

from which we get the missing orbit (11 7 14 13).

Proposition 3. *Let* $\mathtt{D} = pq$ *where* $gcd(p, q) = 1$ *and suppose that we are using the multiplier* M*. Then for every orbit* $(n_1\ n_2\ n_3\ \ldots\ n_k)$ *modulo* D *we obtain an orbit modulo* p *by reducing this orbit modulo* p *and each orbit modulo* p *arises this way.*

Conversely, suppose that $(n_1\ n_2\ n_3\ \ldots\ n_i)$ *and* $(m_1\ m_2\ m_3\ \ldots\ m_j)$ *are orbits modulo* p *and* q*, respectively. Then we obtain an orbit* $(o_1\ o_2\ o_3\ \ldots\ o_k)$ *by solving the set of* k *equations* $x = m_a \bmod p$ *and* $x = n_b \bmod q$*, where* k *is the least common multiple of* i *and* j*. Furthermore, all orbits modulo* D *arise in this fashion.*

Proof. The first part is clear since if $(n_1\ n_2\ \ldots\ n_k)$ is an orbit modulo $\mathtt{D} = pq$ then $n_i * M = n_{i+1} \bmod \mathtt{D}$ implies that $(n_i \bmod p) * (M \bmod p) = (n_{i+1} \bmod p)$

For the converse, we just notice that since $(n_1\ n_2\ n_3\ \ldots\ n_i)$ is an orbit modulo p and $(m_1\ m_2\ m_3\ \ldots\ m_j)$ is an orbit modulo q then we have $n_a * M = n_{a+1} \bmod p$ and $m_b * M = m_{b+1} \bmod q$. However, these two together imply, by the Chinese Remainder Theorem, the single relation $x * M = y \bmod \mathtt{D}$ where $x = n_a \bmod p$ and $x = m_b \bmod q$ and $y = n_{a+1} \bmod p$ and $y = m_{b+1} \bmod q$.

The fact that we shift the orbits, if necessary, implies that we obtain all possible pairs in $\mathbb{Z}_p \times \mathbb{Z}_q$ so we obtain all possible elements from $\mathbb{Z}_{\mathtt{D}}$. □

This is very nice, as it allows us to decompose the problem one prime at a time. Thus, in order to be able to find orbit representatives modulo a composite D it is sufficient to be able to find orbit representatives modulo all the primes (and prime powers) in the prime decomposition of D.

Calculations with the Chinese Remainder Theorem

It is worth taking a short diversion into the use of the Chinese Remainder Theorem. The Chinese Remainder Theorem states that if $N = m_1 m_2 \cdots m_k$ where $gcd(m_i, m_j) = 1$ for all $i \neq j$ then, as rings,

$$\mathbb{Z}_N \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.$$

Given arbitrary choices of $x_i \in \mathbb{Z}_{m_i}$, the Chinese Remainder Theorem tells us that there is exactly one $x \in \mathbb{Z}_N$ with $x \equiv x_i \bmod m_i$ for each index i. The standard proof of the Chinese Remainder Theorem (see for example [19]) actually shows how to *construct* an element with the required properties; since we will need this, it is worthwhile to comment on how this is done.

Define $P_i = N/m_i$ for $i = 1, 2, \ldots, k$. Then $gcd(P_i, m_i) = 1$, so there exists an element $q_i \in \mathbb{Z}^*_{m_i}$ with the property that $P_i q_i \equiv 1 \bmod m_i$. Once we have these P_i and q_i, we let

$$x = x_1(P_1 q_1) + x_2(P_2 q_2) + \cdots + x_k(P_k q_k).$$

Since $P_i q_i \equiv 1 \bmod m_i$ and $P_i q_i \equiv 0 \bmod m_j$ for $j \neq i$ we see that, as desired, $x \equiv x_i \bmod m_i$.

Example 1 (*Chinese Remainder Theorem computations).* To illustrate the Chinese Remainder Theorem computations, let us take our example of $N = 35$ so that $m_1 = 5$ and $m_2 = 7$. Then $P_1 = 7$ and $P_2 = 5$ and $q_1 = q_2 = 3$. If we want to find an x so that $x \equiv 4 \bmod 5$ and $x \equiv 5 \bmod 7$ then we simply take $x = 4(7)(3) + 5(5)(3) = 84 + 75 = 159 \equiv 19 \bmod 35$. We see that $19 \equiv 4 \bmod 5$ and $19 \equiv 5 \bmod 7$, as desired. $\diamond$

Example 2. As another example, consider a 691×1260 matrix. We see that $\mathtt{D} = 691 \times 1260 - 1 = 79 \times 103 \times 107$ so that $\mathtt{D}$ is *squarefree*. Since we know how to find all the orbits if the modulus is a prime, the Chinese Remainder Theorem will let us put these orbits together to get the full orbit structure.

Lengths of primary orbits: Now, in practice we need to compute the primary orbit modolo $\mathtt{D} = 870659$ (the orbit starting with 1) to move the matrix elements around. During the computation of this primary orbit, it is a simple matter to reduce this orbit modulo 79, modulo 103 and modulo 107 to find the period of the primary orbits for these moduli. For our example, the primary orbit has length 70278 modolo 870659. Reducing this orbit modulo 79 we get an orbit of period 78, reducing it modulo 103 we get an orbit of period 34, and finally reducing it modulo 107 we get an orbit of period 53.

Orbit generators moduli the factors:

For the modulus 79, we see that $\mathbb{Z}_{79}^*$ has 78 elements, so the primary orbit fills out this group and we get only the two orbits starting at 0 and 1 (or any other non-zero element of $\mathbb{Z}_{79}^*$).

For the modulus 103, the reduced primary orbit has period 34 so there are three cosets of this orbit (or, more properly, there are three cosets of the multiplicative subgroup of $\mathbb{Z}_{103}^*$ generated by $691 \equiv 73$). Thus we need three representatives for these cosets. To get these coset representatives, we need a generator of $\mathbb{Z}_{103}^*$. After a few tries, we see that 5 is a generator, so we can take as representatives the elements $1 = 5^0, 5 = 5^1, 25 = 5^2$. So in all we have the orbit representatives $0, 1, 5, 25$.

Finally, for the modulus 107 we see that there are two cosets, since the reduced primary orbit has length 53 and there are 106 elements in $\mathbb{Z}_{107}^*$. In this case we find that 2 is a generator of $\mathbb{Z}_{107}^*$ so we get the orbit representatives $0, 1, 2$.

All this information is summarized in Table 1

Using the Chinese Remainder Theorem: We have two orbit generators for the modulus 79, four orbit generators for the modulus 103 and three orbit generators for the modulus 107. This seems like it should give us only $2 \times 4 \times 3 = 24$ orbits in all. However, we notice that $gcd(78, 34) = 2$ so we will have to do our "shifting" trick to find all the orbits.

First we need the P_i's and q_i's (in the notation above, from the discussion of computations with the Chinese Remainder Theorem). Computing these (by

Table 1: Summary of data for a 691×1260 matrix.

Modulus	length of primary orbit	number of nontrivial orbits	all orbit generators
79	78	1	0, 1
103	34	3	0, 1, 5, 25
107	53	2	0, 1, 2

the Euclidean algorithm), we see that

$$\begin{array}{lll} P_1 = 870659/79 = 11021 & \text{and} & q_1 = 2 \\ P_2 = 870659/103 = 8453 & \text{and} & q_2 = 59 \\ P_3 = 870659/107 = 8137 & \text{and} & q_3 = 43. \end{array}$$

With this data, we get the orbit generators:

0 22042 498727 520769 732094 752317 774359 89666
278949 300991 360162 349891 371933 848618 1 211326
231549 253591 439557 628840 650882 710053 699782 721824
327850 349892 561217 581440 603482 789448 108072 130114
189285.

These generators correspond (in order) to the triples of generators (a, b, c) modulo 79, modulo 103, and modulo 107 given by:

$(0,0,0)$ $(1,0,0)$ $(0,1,0)$ $(1,1,0)$ $(1,73,0)$ $(0,5,0)$ $(1,5,0)$ $(1,56,0)$
$(0,25,0)$ $(1,25,0)$ $(1,74,0)$ $(0,0,1)$ $(1,0,1)$ $(0,1,1)$ $(1,1,1)$ $(1,73,1)$
$(0,5,1)$ $(1,5,1)$ $(1,56,1)$ $(0,25,1)$ $(1,25,1)$ $(1,74,1)$ $(0,0,2)$ $(1,0,2)$
$(0,1,2)$ $(1,1,2)$ $(1,73,2)$ $(0,5,2)$ $(1,5,2)$ $(1.56,2)$ $(0,25,2)$ $(1,25,2)$
$(1,74,2)$.

Notice that we have 9 orbits which correspond to "shifting" the three orbits modulo 103 with generators $1, 5, 25$.

As an example, we will show how to get 520769 and 732094.

Let's start with the generators 1,1 and 0 modulo 79, 103 and 107 respectively. We use the Chinese Remainder Theorem to get an element x of Z_{870659} which reduces to these:

$$x = 1(P_1 q_1) + 1(P_2 q_2) + 0(P_3 q_3) = 22042 + 498727 = 520769.$$

Now since the orbit of 1 modulo 79 has length 78 and the orbit of 1 modulo 103 has length 34 and $gcd(78, 34) = 2$ we will have to do one "shift" to get all the orbits. If we "shift" the second orbit, we want the element of Z_{870659} which reduces to 1 modulo 79, to 73 modulo 103 (since $1 \cdot 691 \equiv 73 \bmod 103$) and to 0 modulo 107. Using the Chinese Remainder Theorem again we get

$$x = 1(P_1 q_1) + 73(P_2 q_2) + 0(P_3 q_3) = 22042 + 36407071 + 0 \equiv 732094.$$

The rest of the orbit generators in the table are computed in a similar fashion.
◇

4 Odd prime powers

As we discussed at the beginning of the previous section, when D is a prime it is easy to find a complete set of orbit representatives because all the non-zero orbits are actually cosets.

When $\mathtt{D} = p^n$ with p an odd prime the situation is very similar to when D is prime. The reason for this is that in this case we also have that $\mathbb{Z}_{\mathtt{D}}^*$ is cyclic. The main difference is that the order of $\mathbb{Z}_{\mathtt{D}}^*$ is not $p^n - 1$ but is $\phi(p^n) = (p-1)p^{n-1}$ (where $\phi(n)$ is the Euler totient function, which counts the number of positive integers $i < n$ which are relatively prime to n). This indicates that not all the orbits will be cosets of the primary orbit since $(p-1)p^{n-1}$ does not divide $p^n - 1$.

A simple example will best illustrate the issues involved.

Example 3. Suppose that we are interested in the orbits of the multiplier 7 modulo 81. These orbits are:

(0)
(1 7 49 19 52 40 37 16 31 55 61 22 73 25 13 10 70 4 28 34 76 46 79 67 64 43 58)
(2 14 17 38 23 80 74 32 62 29 41 44 65 50 26 20 59 8 56 68 71 11 77 53 47 5 35)
(3 21 66 57 75 39 30 48 12)
(6 42 51 33 69 78 60 15 24)
(9 63 36)
(18 45 72)
(27)
(54).

We see that 7 has multiplicative order 27 and that the order of $\mathbb{Z}_{81}^*$ is $(3-1)3^3 = 54$ so there are two cosets of the primary orbit. How do we explain the other orbits? Well, if we look at the orbits of 7 modulo 27 we get:

(0)
(1 7 22 19 25 13 10 16 4)
(2 14 17 11 23 26 20 5 8)
(3 21 12)
(6 15 24)
(9)
(18).

Examining these orbits we see that if we multiply each number by 3, we get the last six orbits modulo 81! This indicates that the orbits of the multiplier m modulo p^n should "nest." That is, there are the orbits arising as cosets modulo p^n, then the orbits arising as cosets modulo p^{n-1}, then those arising as cosets modulo p^{n-2}, and so on.

To see this in this example, we simply have to see that the orbits of the multiplier 7 modulo 9 are

(0)
(1 7 4)
(2 5 8)
(3)
(6)

and the orbits of 7 modulo 3 are:

(0)
(1)
(2).

◇

Proposition 4. *Let p be prime and m be relatively prime to p. If $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n then $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1}. Furthermore, every orbit of m modulo p^{n+1} of the form $(pa_1\ pa_2\ \ldots\ pa_k)$ arises in this fashion.*

Proof. Since $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n, we see that $ma_i \equiv a_{i+1} \bmod p^n$. Thus $mpa_i \equiv pa_{i+1} \bmod p^{n+1}$ so $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1}.

Furthermore, if $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1} we see that $mpa_i \equiv pa_{i+1} \bmod p^{n+1}$ which implies that $ma_i \equiv a_{i+1} \bmod p^n$ so $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n. □

This proposition allows us to find all the orbits of the multiplier m modulo p^n as either cosets of the primary orbit or "lifts" of orbits modulo p^k (for $k < n$). However, these orbits modulo p^k are also either cosets or "lifts."

Going back to our example, we notice that 7 has order 27 modulo 81 and has order 9 modulo 27 and has order 3 modulo 9 and order 1 modulo 3. In fact, this is a general feature modulo odd primes as the next theorem states (see [17], Theorem 4-6).

Theorem 5. *Suppose that p is an odd prime and that m has order t mod p. Let a be the largest exponent such that p^a divides $m^t - 1$ (as integers). Then in $\mathbb{Z}^*_{p^n}$, the order of m is precisely*

$$tp^{\max(0,n-a)}.$$

This theorem tells us that, as we descend through the powers of p, the order of m reduces by a factor of p each time, until no such reduction is possible. This useful fact allows us to count the number of orbits of m that arise as cosets modulo various powers of p. Suppose that the order of m modulo p^n is tp^b. Then there are $(p-1)p^{n-1}/(tp^b)$ orbits arising as cosets modulo p^n. If $b \geq 1$ there

are also this many orbits arising as cosets modulo p^{n-1}. Using this reasoning, we see that there are exactly

$$\begin{aligned}\left(b+\sum_{k=0}^{k=n-b-1}(1/p)^k\right)\frac{(p-1)p^{n-1}}{tp^b} &= \left[b+\frac{p}{p-1}\left(\frac{p^{n-b}-1}{p^{n-b}}\right)\right]\frac{(p-1)p^{n-1}}{tp^b}\\ &= b\frac{(p-1)p^{n-1}}{tp^b}+\frac{p^{n-b}-1}{t}\\ &= b\frac{(p-1)p^{n-1}}{tp^b}+\frac{p^n-p^b}{tp^b}\end{aligned}$$

non-zero orbits.

For our example, we see that 7 has order $27 = 3^3$ modulo 81 and order 1 modulo 3. Thus $n = 4$, $t = 1$, and $b = 3$ and so we see that there are

$$3\frac{(3-1)3^3}{27}+\frac{3^4-3^3}{27} = 6+2 = 8$$

non-zero orbits.

Generating Orbits for Example 3 So, how do we put all this information together to actually generate the orbits of the multiplier 7 modulo 81?

First, we compute the primary orbit and see that it has length 27. Since $\phi(81) = 54$, we see that there must be two cosets – the primary orbit and one coset. Since $\mathbb{Z}_{81}^*$ is cyclic, if we find a cyclic generator we can find coset representatives. It turns out that 2 is a primitive root modulo 81 (and, in fact, modulo 3^n for all n). Thus, we use the two orbit representatives $2^0 = 1$ and $2^1 = 2$.

Consider next the orbits of the multiplier 7 modulo $3^3 = 27$. We know that 7 has order 9 modulo 27 (by Theorem 5) and $\phi(27) = 18$. Thus there are also two cosets of this primary orbit. Again, we can use the generator 2, so we have the two orbit representatives $3(2^0) = 3$ and $3(2^1) = 6$.

Next we consider the orbits of 7 modulo $3^2 = 9$. Since 7 has order 3 modulo 9 and $\phi(9) = 6$, we again have two cosets. Again using 2 as a primitive root we get the two orbit representatives $9(2^0) = 9$ and $9(2^1) = 18$.

Finally, we consider the orbits of 7 modulo 3. Here 7 has order 1 modulo 3 and $\phi(3) = 2$ so we again have two cosets with orbit representatives $27(2^0) = 27$ and $27(2^1) = 54$.

These orbits, along with the zero orbit (0), form all the orbits of the multiplier 7 modulo 81. $\diamond$

This example highlights a potential problem. We must find a primitive root g modulo p^k for each $k \leq n$. How do we do this?

Theorem 6. *Let p be an odd prime. If g is a primitive root modulo p and modulo p^2, then g is a primitive root modulo p^n for all n. If g is a primitive root modulo p but not a primitive root modulo p^2, then $g+p$ is a primitive root modulo p^n for all n.*

Proof. The first part is a consequence of Theorem 5 since if g is a primitive root modulo p and p^2 then it has order $(p-1)$ modulo p and order $(p-1)p$ modulo p^2 and thus must have order $(p-1)p^{n-1}$ modulo p^n.

For the second part, suppose that g is primitive mod p but not mod p^2. Then g necessarily has order $p-1$ mod p^2, so

$$g^{p-1} = 1 + bp^2$$

for some b. Let $h = g + p$ and consider powers of h. The element h is clearly a primitive root mod p, and so satisfies $h^{p-1} = 1 + ap$ for some $0 \leq a < p$. We have

$$\begin{aligned} h^p &= (g+p)^p \\ &= g^p + up^2 \\ &= g + vp^2 \end{aligned}$$

so that $h^p \equiv g \bmod p^2$. Hence h has exactly order $\phi(p^2) = p(p-1)$ in $\mathbb{Z}_{p^2}$, and the result now follows from Theorem 5. □

Empirically, the smallest positive primitive root modulo p is usually also a primitive element modulo p^2. In fact, by a computer search the only prime less than 11 000 000 for which this fails is 40487 for which 5 is a primitive root but is not a primitive element modulo $(40487)^2$.

It is certainly possible for the primary orbit to have maximal length modulo p^n, in which case all the "images" of the primary orbit modulo p^k will also have maximal length. An example of this is for the multiplier 10 and the modulus $7^3 = 343$ where the primary orbit has length 294. The opposite extreme is also possible where all orbits have length 1, but this only happens when the multiplier is 1.

5 Powers of two

The prime 2 is special since the group $\mathbb{Z}_{2^n}^*$ is not cyclic. In fact, writing C_m for the cyclic group of order m, we have that $\mathbb{Z}_{2^n}^* \cong C_{2^{n-2}} \times C_2$ for $n \geq 3$ (while $\mathbb{Z}_2^* = \{1\}$ and $\mathbb{Z}_4^* \cong C_2$). It turns out that (see for example [19], Theorem 2.43) the elements 5 and $-1 = 2^n - 1$ always generate $\mathbb{Z}_{2^n}^*$ for $n \geq 3$. In other words, every element of $\mathbb{Z}_{2^n}^*$ may be expressed as either 5^k or -5^k for $0 \leq k \leq 2^{n-2}$.

Since the structure of $\mathbb{Z}_{2^n}^*$ is so simple, it is not difficult to modify our procedure to find orbit representatives. The only differences result from the fact that $\mathbb{Z}_{2^n}^*$ is not cyclic.

Again, to illustrate the procedure in this case, we will look at an example.

Example 4. We consider the multiplier 7 and the modulus 32 with orbits

(0)
(1 7 17 23)
(31 25 15 9)
(3 21 19 5)
(29 11 13 27)
(2 14)
(30 18)
(6 10)
(26 22)
(4 28)
(12 20)
(8 24)
(16).

We see that 7 has multiplicative order 4 modulo 32. Since $\phi(32) = 16$, there are four orbits which arise as cosets. Since $7 \neq -1 \bmod 32$, we see that 7 must either equal 5^k for some k or equal -5^k for some k. Further, because 7 has order 4 and 5 has order 8, it must be the case that k is even. This means that we can use $1 = 5^0$, $31 \equiv -1 = -5^0$, 5 and $27 \equiv -5$ as representatives for these cosets.

Now when we move to considering those orbits which arise as cosets modulo 16, we see that 7 has order 2 modulo 16. This means that again there are four orbits which arise as cosets (modulo 16). By the same reasoning as before, we see that we can use $2 = 2(1)$ and $30 = 2(15) = 2(-1) \bmod 16$ and $10 = 2(5)$ and $22 = 2(11) = 2(-5) \bmod 16$ as orbit representatives for these orbits.

Moving on to orbits modulo 8, we see that $7 = -1 \bmod 8$. This means that 7 is not a power of 5 and the orbit starting with g will be $(g \quad -g)$. Since $\phi(8) = 4$, we obtain two orbits at this stage with corresponding orbit representatives $4 = 4(1) = 4(5^0)$ and $20 = 4(5)$. Notice that since $7 \equiv -1$ all the orbit generators are powers of 5 which we "lift" from modulo 8 to modulo 32 by multiplying by 4.

Next we consider modulo 4 orbits. Here again $7 = -1 \bmod 4$. Since $\phi(4) = 2$ and 7 has order two, there is only one orbit for which we get the orbit representative $8 = 8(1)$.

Finally, considering orbits modulo 2 we get the orbit representative 16(1). This takes care of all the non-zero orbits. $\diamond$

One interesting thing to notice in this example is that 7 had order 4 modulo 32 and order 2 modulo $16, 8, 4$ and 2. Knowing how the order of the multiplier changes as we descend through the various powers of two is important in order to be able to find an algorithm for the general case. The next result establishes this for us.

In the next Proposition and the succeeding discussion, we shall make use of the following representation of an odd positive integer $b \geq 3$. Since b is an odd integer, it is congruent to either 1 or 3 mod 4. Set $d = b - 1$ if $b \equiv 1 \bmod 4$,

and $d = b+1$ otherwise. Then d is a multiple of 4, and we can write d uniquely in the form $d = 2^r\ a$ with a odd and $r \geq 2$. This is our representation.

In other words, we define a odd and $r \geq 2$ by

$$b = \begin{cases} a\ 2^r + 1 & \text{if } b \equiv 1 \bmod 4; \\ a\ 2^r - 1 & \text{if } b \equiv 3 \bmod 4. \end{cases} \tag{1}$$

Proposition 7. *Consider the group $\mathbb{Z}_{2^n}^*$.*

1. *The elements of order 2 in $\mathbb{Z}_{2^n}^*$ are precisely $2^{n-1} \pm 1$ and $2^n - 1$.*
2. *If $b \in \mathbb{Z}_{2^n}^*$ has order greater than 2, write b in the form given in equation (1), where a is odd and $r \geq 2$. Then b has order 2^{n-r} in $\mathbb{Z}_{2^n}^*$.*

Proof. Because the group $\mathbb{Z}_{2^n}^*$ is isomorphic to $C_{2^{n-2}} \times C_2$, every element has order a power of 2, and there are precisely three elements of order 2. It's easy to see that these are the stated elements.

For the second statement, set $s = n - r$, so that our claim is that b has order 2^s. To see this, we consider $b^{2^{s-1}}$.

$$\begin{aligned} b^{2^{s-1}} &= (\ a\ 2^r \pm 1\ )^{2^{s-1}} \\ &= \sum_{k=0}^{2^{s-1}} \binom{2^{s-1}}{k} (\pm 1)^{2^{s-1}-k} a^k\ 2^{kr} \\ &= 1 \pm 2^{s-1} \cdot a\ 2^r + \tbinom{2^{s-1}}{2}\ a^2\ 2^{2r} \pm \tbinom{2^{s-1}}{3} a^3\ 2^{3r} + \cdots \end{aligned}$$

Writing $a = 1 + 2c$ we see that

$$b^{2^{s-1}} = 1 \pm 2^{r+s-1} \pm 2^{r+s-1}(\ 2c\ ) + \binom{2^{s-1}}{2}\ a^2\ 2^{2r} \pm \binom{2^{s-1}}{3} a^3\ 2^{3r} + \cdots$$

and hence $b^{2^{s-1}} = 1 \pm 2^{r+s-1}$ has order 2. Therefore b has exactly order $2^s = 2^{n-r}$ as required. □

Proposition 8. *1. The elements of order 2 in $\mathbb{Z}_{2^n}^*$ reduce to ± 1 mod 2^{n-1} and so have order either 1 or 2.*

2. Let $s \geq 2$ and suppose that g is an element of order 2^s in $\mathbb{Z}_{2^n}^*$. Then g has order 2^{s-1} mod 2^{n-1}.

Proof. This now follows from the previous lemma. The first statement is clear. For the second, writing g in the form of equation (1):

$$g = a\ 2^r \pm 1$$

where $r = n - s < n - 1$, we see that g reduces mod 2^{n-1} to $a'\ 2^r \pm 1$, with a' odd. Since $r \geq 2$, this representation $a'\ 2^r \pm 1$ is the representation of g given by equation (1), and so g has order $2^{(n-1)-r} = 2^{s-1} \bmod 2^{n-1}$. □

To state this result in another form, set $g_n = g$, and for each k, $1 \leq k \leq n$, set g_k to be the residue of g mod 2^k. Proposition 8 says that if g has order 2^s mod 2^n, then the elements g_n, g_{n-1}, $\ldots g_2$, g_1 have orders either

$$2^s, 2^{s-1}, 2^{s-2}, \ldots 8, 4, 2, 2, 2, 2, \ldots, 2, 1$$

or

$$2^s, 2^{s-1}, 2^{s-2}, \ldots 8, 4, 2, 1, 1, 1, \ldots, 1, 1$$

In particular, if $g = a\ 2^r \pm 1$ is the above representation of g, then g reduces mod 2^{r+2} to either $2^r \pm 1$ or to $2^{r+1} + 2^r \pm 1$, each of which has order 4 mod 2^{r+2}. Reducing mod 2^{r+1} gives $2^r \pm 1$, an element of order 2 in both cases. Then reducing again yields either 1 or -1, so that the order of g stabilizes for the remaining reductions, until the final one.

Using this result, we can count the number of orbits of the multiplier $\mathtt{M}$ modulo 2^n.

Proposition 9. *Let* $\mathtt{M}$ *act by multiplication on* $\mathbb{Z}_{2^n}$*. If* $\mathtt{M} = 1$ *then there are* 2^n *orbits of* $\mathbb{Z}_{2^n}$ *under this action.*

If $\mathtt{M} > 1$ *and* $\mathtt{M} \equiv 1$ *mod* 4*, and if* $\mathtt{M} = a\ 2^r + 1$ *is the representation of* $\mathtt{M}$ *provided by equation (1), then the number of orbits of* $\mathbb{Z}_{2^n}$ *under this action is*

$$(n - r + 2)2^{r-1}\ .$$

If $\mathtt{M} \equiv 3$ *mod* 4*, and if* $\mathtt{M} = a\ 2^r - 1$ *is the representation of* $\mathtt{M}$ *provided by equation (1), then the number of orbits of* $\mathbb{Z}_{2^n}$ *under this action is*

$$1 + (n - r + 1)2^{r-1}\ .$$

Proof. The result for the $\mathtt{M} = 1$ case is clear: every element is left fixed by multiplication by 1.

For the case $\mathtt{M} \equiv 1$ mod 4, we consider the multiplicative action of $\mathtt{M}$ on $\mathbb{Z}^*_{2^k}$ for each k. There are two possibilities. First of all, if $1 \leq k \leq r$, $\mathtt{M} \equiv 1$ mod 2^k, and so $\mathtt{M}$ has order 1 in $\mathbb{Z}^*_{2^k}$. Therefore there are 2^{k-1} orbits (i.e. cosets) of $\mathbb{Z}^*_{2^k}$ under this action, which 'lift' to 2^{k-1} orbits of $\mathbb{Z}^*_{2^n}$. On the other hand, if $r+1 \leq k \leq n$, then $\mathtt{M}$ has order2^{n-r} in $\mathbb{Z}^*_{2^k}$. Since $\mathbb{Z}^*_{2^n}$ is a group of order 2^{n-1}, there are $2^{n-1}/2^{n-r} = 2^{r-1}$ orbits, and again each lifts to an orbit of $\mathbb{Z}^*_{2^n}$.

Taking into account the 0 orbit, we sum up to get a total of

$$\sum_{k=1}^{r} 2^{k-1} + \sum_{k=r+1}^{n} 2^{r-1} + 1 = (2^r - 1) + (n - r)2^{r-1} + 1 = (n - r + 2)2^{r-1}$$

orbits of the action.

A similar argument holds for the case $\mathtt{M} \equiv 3$ mod 4. Again, we consider the multiplicative action of $\mathtt{M}$ on $\mathbb{Z}^*_{2^k}$ for each k. If $r + 1 \leq k \leq n$, the argument is identical to the previous case, and if $k = 1$, we obtain 1 orbit as before. If $2 \leq k \leq r$, however, $\mathtt{M} \equiv -1$ mod 2^k, and so $\mathtt{M}$ has order 2 in $\mathbb{Z}^*_{2^k}$. Hence there are 2^{k-2} orbits of $\mathbb{Z}^*_{2^k}$ under this action, which 'lift' to 2^{k-2} orbits of $\mathbb{Z}^*_{2^n}$.

Taking into account the 0 orbit, we sum up in this case to obtain a total of

$$1+\sum_{k=2}^{r} 2^{k-2}+\sum_{k=r+1}^{n} 2^{r-1}+1 = 1+(2^{r-1}-1)+(n-r)2^{r-1}+1 = 1+(n-r+1)2^{r-1}$$

orbits of the action, as claimed. □

For example, using the multiplier 7 modulo 32 we see that $7 = 2^3 - 1$ so that in the notation of the above proposition, $n = 5$ and $r = 3$. According to the first case of the proposition, the number of orbits is therefore $1 + (5 - 3 + 1)2^{3-1} = 1 + (3)2^2 = 13$, and this is exactly the number we encountered earlier when we wrote the orbits out explicitly.

Notice that the cases in Proposition 9 can easily be checked by examining the binary representation of M. We simply count the number of 1's (in this binary representation) at the "right end" (the lowest order part) of M. If there is only one 1, then we are in case one. Otherwise we are in case two. We find r by either counting the number of these 1's (case two) or by counting the number of 0's until the next 1 and adding one (case one). For example, 7 in binary is 111 so we are in case two and $r = 3$. As another example, using the multiplier 21 modulo 32 we see that 21 is 10101 in binary so we are in case one with $r = 2$ so there are 10 orbits.

6 Putting it all together

Now that we can find orbit generators modulo all odd prime powers and powers of two, we can try to put all this information together to describe the complete algorithm. We do this for our simple example from Section 2, that of a 3 by 7 matrix.

Example 5. First, we see that $(3)(7) - 1 = 20 = (4)(5)$, so we know that we need to find orbit representatives modulo 4 and modulo 5 for the multiplier 3.

Lengths of primary orbits: We start by explicitly generating the primary orbit modulo 20 (which we will need to do anyway in order to move these matrix elements) and reduce this orbit modulo 4 and modulo 5. We see that this orbit modulo 20 is (1 3 9 7) so we get the primary orbit modulo 4 is (1 3) and modulo 5 is (1 3 4 2). Thus, 3 has order 2 modulo 4 and has order 4 modulo 5.

Orbit generators moduli the factors: Now we will generate the orbit representatives modulo the prime powers 4 and 5. We start with the prime 2.

First, $\phi(4) = 2$ and 3 has order 2 modulo 4, so there is only one orbit modulo 4 with generator 1. When we descend to considering orbits modulo 2 we see that we get a single orbit, which "lifts" (by multiplying by 2) to give the generator 2. Thus, along with the zero orbit, we have the three generators $0, 1, 2$ for the orbits modulo 4 of the multiplier 3.

Now we consider the prime 5. Here we see that 3 has order 4 modulo 5, so there is only one orbit with generator 1. Thus, we get the two orbit generators $0, 1$ for the orbits modulo 5.

Using the Chinese Remainder Theorem: Now we must use the Chinese Remainder Theorem to "lift" these orbit generators to orbit generators modulo 20. We have three orbit generators modulo 4 and two orbit generators modulo 5, so we will have at least 3×2 orbit generators modulo 20. However, we might have to "shift" some orbits as discussed in Section 3.

From the two orbit generators 0 and 0 modulo 4 and 5 respectively, we get the orbit generator 0 modulo 20. We don't have to worry about "shifting" this orbit.

From the two orbit generators 1 and 0, we get the orbit generator 5 modulo 20. The length of the orbit generated by 1 modulo 4 is two while the length of the orbit generated by 0 modulo 5 is one and $gcd(1, 2) = 1$, so we don't need to "shift" this orbit. Thus, we only get the orbit generator 5.

From the two orbit generators 2 and 0, we get the orbit generator 10 modulo 20. The length of the orbit generated by 2 modulo 4 is one and the length of the orbit generated by 0 modulo 5 is one and $gcd(1, 1) = 1$, so there is no need to do any "shifts" of this orbit either. Thus, we only get the orbit generator 10.

Next we consider the two orbit generators 0 and 1, which yield the orbit generator 16 modulo 20. Here the length of the orbit generated by 0 modulo 4 is one which means that we don't need to "shift" this orbit either. So again we only get the one orbit generator 16.

Now we consider the two orbit generators 1 and 1, which yield the orbit generator 1 modulo 20. This time we do need to consider "shifts" of the orbit, since the orbit generated by 1 modulo 4 has length two and the orbit generated by 1 modulo 5 has length four and $gcd(4, 2) = 2 > 1$. This means that we will need two shifts of this orbit – the original orbit plus one "shift." To get this "shift," we simply take the basic orbit generator modulo 5, here this is 1, and multiply it by the multiplier, here 3. This leads to solving the system $x = 1 \bmod 4$ and $x = 3 \bmod 5$ with solution $x = 13$. So we need to use the two orbit generators 1 and 13.

Finally, we consider the two orbit generators 2 and 1, which yield the orbit generator 6 modulo 20.

To perform the matrix transpose, we find that we need to generate orbits using the multiplier 3 modulo 20 starting with the orbit generators $0, 5, 10, 16, 1, 13$ and 6. Clearly we don't need to generate the zero orbit, so we generate the other six orbits and shift the data through each cycle. $\diamond$

Our next example is slightly more complicated but still doable by hand.

Example 6. For a 25 by 185 matrix, we see that $25 \times 185 - 1 = 4624 = (2^4)(17^2)$.
Lengths of primary orbits: The length of the primary orbit modulo `D` is 136. If we reduce this orbit modulo 2^4 we get an orbit of period 2 while reducing it modulo 17^2 we get an orbit of period 136.

Numbers and lengths of orbits modulo the factors: For the modulus $16 = 2^4$ we obtain four orbits of length 2 and one orbit of length 1 (the zero orbit).

Since $\mathtt{M} = 25 \equiv 1 \bmod 8$, all the orbits modulo 8, modulo 4, and modulo 2 are of length one.

For the modulus $289 = 17^2$, we have that $\mathbb{Z}^*_{289}$ contains 272 elements and the primary orbit is of length 136. Thus there are two orbits of length 136 and the zero orbit (of length 1).

For the modulus 17, we obtain two orbits of length 8 along with the zero orbit.

Orbit generators moduli the factors: It turns out that $g = 3$ is a primitive element modulo 17 and also modulo 17^2. Thus we use $1, 3$ as the generators for the nonzero orbits modulo 17^2 and $1, 51$ as the generators for the nonzero orbits modulo 17^2 which arise as "lifts" of orbits modulo 17.

Finally, for the nonzero orbits modulo $16 = 2^4$, we use the orbit generators $1, -1, 5, -5$.

Combining all these orbits (and their "shifts") together with the Chinese Remainder Theorem, we obtain a total of 76 different orbits. $\diamond$

For any reader interested in trying large examples we suggest two in particular. For a 99999 by 1000000 matrix, the above process yields 7, 3, and 7 orbits modulo the prime factors of $\mathtt{D} = 313 \times 1217 \times 262519$ and this results in only 398 distinct non-zero orbits. Notice that the matrix has almost one hundred billion entries. As a second example, for a 105359 by 152615 matrix we obtain only 54 orbit generators modulo the various factors of $\mathtt{D} = 2^3 \times 3^4 \times 11^3 \times 103 \times 181$. However, with the required "shifts," this results in 398628 distinct nonzero orbits.

7 History and Further Directions

The topics explored here initially arose from a quest to find an algorithm to perform an in-place matrix transpose. That is, to rearrange the entries of a matrix in a computer's memory so that what started out stored row-wise ends up being stored column-wise.

The question of an "in-place matrix transform algorithm" appears to have originated as a problem given to students taking the Cambridge University Diploma in Numerical Analysis and Automated Computing in 1957, and several variants of these algorithms have been proposed (see for instance [22], [8], [3], [16], [11], and [4]). This question also appears as an exercise in Knuth's book [14, p. 180]. The algorithms given in these sources can be divided into two classes: one class in which essentially a table of bits is used to keep track of entries which have already been transposed, and the second class in which each cycle of the permutation is first tested to ensure that the cycle is only applied once. Both cases suffer from drawbacks: for the first, one must maintain a fairly substantial table as a database of which entries have already been permuted;

the second saves on storage but requires enormous computational effort as the algorithm proceeds.

In this paper, we describe an alternative algorithm. This algorithm is a variation of the algorithm presented in [20], and differs from the above classes in that it involves a shift in viewpoint to that of group actions. Our group action is the action of a subgroup of $\mathbb{Z}_N^*$ (the multiplicative group modulo N) acting on all of $\mathbb{Z}_N$. We explicitly determine all the orbits of this group action by calculating the number of orbits, the length of each orbit, and also by finding a generator for each orbit. As such, the techniques involved display a wonderful combination of group theory and number theory.

In-place matrix transposition and related problems continue to attract research attention, especially on the technical side (see [5], [7], [10], [15]). To mathematics students this may seem surprising, since mathematically a matrix and its transpose are easily related, and given the current state of computing power; yet there remain numerous technical situations in which such in-place algorithms retain their importance.

The techniques and topics explored here can easily be used to lead students in a number of fruitful directions. We outline here some technical issues that may be explored, as well as lay out some suggestions for several more algebraic/number theoretic ones.

Implementation Issues For students with more of a computer science leaning, there is the entire topic of implementations of algorithms for computer arithmetic, as well as for working with matrices.

There are a few issues which must be taken into account when actually implementing this algorithm for large matrices. The first of these is the implementation of large integer arithmetic. For larger matrices, the modulus `D` may become large enough that computations mod `D` require the use of special arithmetic packages for large integer calculations. Most standard languages (such as C, C++, python) come with additional packages for use in such situations. For the curious reader who wants to implement his or her own arithmetic package, an excellent discussion of specialized algorithms is given in Chapter 14 of [18].

Two further computational issues are number-theoretic. The algorithm must factor `D` in order to examine the orbits prime-by-prime, and must also generate primitive roots mod odd primes. While factoring is a hard problem in general, in practice this is really not a concern, since a current implementation of this algorithm would be on a machine for which `D` would be small enough.

Theorem 6, for instance, made specific use of primitive roots, as did our method of generating orbit representatives. There is no known algorithm which given a prime p, will provide a primitive root mod p, which does not make use of an exhaustive search. In fact, one of the more efficient algorithms for finding such a root is to apply the following test to each possible a:

Lemma 10. *A number $a \in \mathbb{Z}_n^*$ is a primitive root iff for each prime q dividing $\phi(n)$,*

$$a^{\phi(n)/q} \not\equiv 1 \ mod\ n\ .$$

More discussion of these issues can be found, for instance, in [19] or [13].

Since this area remains an active research field on the technical side, another fruitful topic would involve implementation and testing of this algorithm against various algorithms which have been proposed in the literature (as in, for instance, [22], [20], [8], [3], [16], [11],[4], [5], [7], [15], and [10]).

Group Actions The analysis of the algorithm involves the use of group actions in an important way, and so could easily be used to launch a more involved exploration of general ideas on groups acting on sets, and in particular to the connections between transitive actions and cosets. Basic ideas on group actions can be found in, for instance, [9]. For connections with geometry, a beautiful reference is chapter 1 in the classic pair of texts [2], although in later chapters these get very technical very quickly.

Applications of Group Actions Aside from general notions related to group actions, the material included here leads quickly and easily into applications. An important one is the notion of applying group actions to combinatorial problems. Fraleigh [9] is a standard reference and covers most of the key ideas, though the symmetry is brought into play more extensively in the beautiful text [1].

A second beautiful application is to frieze groups and periodic tilings of the plane. The books [2] and [12] contain excellent discussions of these.

Primitive Roots An extremely fruitful direction for exploration involves primitive roots. As noted in the discussion preceding and following Theorem 6, there are many unresolved questions concerning primitive roots. If we choose a prime p, how can we find a primitive root g modulo p^k? If instead we fix a positive integer g and consider moduli p^k for $p \geq g$, for how many p is g actually a primitive root? The famous Artin conjecture states that there should be infinitely many such p.

In addition, the statement of Theorem 2 itself can be used to explore the general structure of primitive roots mod p^k where the prime p is fixed and the exponent k is allowed to vary. In the form presented here, the theorem actually asserts much less than the entire picture. For instance, there are $\phi(\phi(p))$ primitive roots modulo p, and for each one g, exactly one of the p integers modulo p^2 which reduce to g mod p fails to be a primitive root mod p^2. Similar patterns arise as we look at higher powers of p. A good discussion of these ideas may be found in [13].

The *p*-adic numbers In the previous paragraph, we suggested examining the connections between primitive roots mod p^k and primitive roots mod p^{k+1}. One may also generalize this a little and consider these reduction maps all at once, piecing these together to yield a sequence of surjective homomorphisms:

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \mathbb{Z}/p^2\mathbb{Z} \longleftarrow \mathbb{Z}/p^3\mathbb{Z} \longleftarrow \cdots \longleftarrow \mathbb{Z}/p^k\mathbb{Z} \longleftarrow \mathbb{Z}/p^{k+1}\mathbb{Z} \longleftarrow \cdots$$

Looking at 'compatible' strings of elements mod p leads one directly to a standard definition of the p-adic numbers, and the fact that this new set of numbers somehow combines all of the rings $\mathbb{Z}/p^k\mathbb{Z}$ and the way in which they are connected by the reduction homomorphisms. An excellent introduction to these ideas can be found in Neukirch's article, Chapter 6 of [6].

Acknowledgments. The second author was partially supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] M.A. Armstrong, *Group Theory and Symmetry*, Springer-Verlag, New York, 1988.

[2] M. Berger, *Géometrie*, Springer-Verlag, New York, 1989.

[3] J. Boothrotd, *Algorithm 302: Transpose Vector Storage Array*, Communications of the ACM **10**, No. 5 (1967), 292–3.

[4] E.G. Cate and D.W. Twigg, *Algorithm 513: Analysis of In-Situ Transposition*, ACM Transactions on Math. Software **3**, No. 1 (1977), 104–110.

[5] M. Dow, *Practical aspects and experiences : Transposing a matrix on a vector computer*, Parallel Computing **21** (1995) 1997–2005.

[6] H.-D. Ebbinghaus et.al., *Numbers*, Springer-Verlag, New York, 1991.

[7] F.E. Fich, J.I. Munro, and P.V. Poblete, *Permuting In Place*, SIAM. J. Comp. **24** No. 2 (1995), 266–278.

[8] W. Fletcher and R. Silver, *Algorithm 284: Interchange of Two Blocks of Data*, Communications of the ACM **9**, No. 5 (1966), 326.

[9] J.B. Fraleigh, *A First Course in Abstract Algebra*, 7th ed., Addison-Wesley, 2003.

[10] F. Gustavson, L. Karlsson, and B. Kågström, *Parallel and Cache-Efficient In-Place Matrix Storage Format Conversion*, ACM Transactions on Mathematical Software **38** No. 3 (2012), 17:1–17:32.

[11] M.R. Ito, *Remark on Algorithm 284: Interchange of Two Blocks of Data*, ACM Transactions on Math. Software **2**, No. 4 (1976), 392–3.

[12] J.A. Gallian, *Contemporary Abstract Algebra*, 6th ed., Houghton-Mifflin, 2006.

[13] G. A. Jones and J. Mary Jones, *Elementary Number Theory*, Springer-Verlag, New York, 1998.

[14] D.E. Knuth, *The Art of Computer Programming, Vol. I*, Addison-Wesley, Reading, Mass., 1969.

[15] S. Krishnamoorthy, G. Baumgartner, et. al., *Efficient Parallel Out-of-core Matrix Transposition*, Int. J. High Perf. Comp. and Netw. **2** Vol 2-4 (2004), 110–119.

[16] S. Laflin and M.A. Brebner, *Algorithm 380: In-Situ Transposition of a Rectangular Matrix*, Communications of the ACM **13**, No. 5 (1970), 324–6.

[17] W.J. Leveque, *Topics in Number Theory, Volumes 1 and 2*, Dover reprint, 2002.

[18] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *The Handbook of Applied Cryptography*, CRC Press, 1996. [Full text is available at `http://www.cacr.math.uwaterloo.ca/hac/`.]

[19] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed, Wiley, 1991.

[20] G. Pall and E. Seiden, *A problem in Abelian Groups, with application to the transposition of a matrix on an electronic computer*, Math. Comp. **14** (1960) 189–192.

[21] D.J. Scully, *Perfect shuffles through dynamical systems*, Math. Magazine **77**, No. 2 (2004) 101–117.

[22] P.F. Windley, *Transposing Matrices in a Digital Computer*, Comput. J. **2** (1959), 47–8.