Matrices Over Modular Arithmetic

Consider matrices from the set $M_{k\times k}(\mathbb{Z}_m)$, where $\mathbb{Z}_m$ denotes the field of integers modulo m. We wish to explore the properties of such matrices, especially when taken to integer powers. For shorthand, we call such a matrix a *modular matrix*.

Example. One such matrix is

$$\begin{bmatrix} 1 & 3 & 2 \\ 0 & 6 & 5 \\ 4 & 4 & 2 \end{bmatrix} \in M_{3\times 3}(\mathbb{Z}_7).$$

Theorem. Let A be any modular matrix of dimension k and modulus m. The sequence $A, A^2, A^3, \ldots$ is eventually periodic.

Proof. The sequence being periodic is equivalent to any matrix appearing more than once in the sequence. Since the sequence is infinite and there are m^{k^2} modular matrices of same dimension and modulus, we can always choose a sequence index greater than m^{k^2} and argue by the Pigeonhole Principle that there must exist a duplicate matrix. Thus, the sequence must repeat at some point (not necessarily with the starting matrix). ■

With this in mind, we now begin discussing invertibility.

Definition. The *determinant* of a modular matrix with modulus m is simplify defined to be the regular determinant taken modulo m.

Theorem. A modular matrix $A \in M_{k\times k}(\mathbb{Z}_m)$ is invertible iff $\det A$ is invertible in $\mathbb{Z}_m$. That is to say, iff $\gcd(\det A, m) = 1$.

Proof. Since the properties of determinants still apply, $\det A^{-1} = (\det A)^{-1}$, so clearly if $\gcd(\det A, m) > 1$, this cannot exist. Thus, it suffices to show that all matrices with $\det A$ such that $\gcd(\det A, m) = 1$ are invertible.

TODO. ■

Notation. We denote the set of invertible modular matrices with size $k\times k$ and modulo m by $N_{k\times k}(\mathbb{Z}_m)$.

With this, we can now see some sets of modular matrices have a structure to them.

Theorem. $N_{k\times k}(\mathbb{Z}_m)$ forms a group under multiplication.

Proof. Most of the necessary properties follow readily from matrix algebra, so we may quickly verify the conditions:

- **Associativity**: We have trivially that $A(BC) = (AB)C$.
- **Identity Element**: The unique identity element for $M_{k\times k}(\mathbb{Z}_m)$ is I_k.
- **Inverse Element**: It is already stated that each element has a (two-sided) inverse. Since this inverse is also invertible, it is included the group.

■

Because this group is of finite order, we have that for any invertible modular matrix A, there exists some smallest non-zero exponent r, the order of the element, such that $A^r = I_k$. We wish to the order, or some multiple of it, which shall give us a tool to reduce the exponent of a modular matrix power.

This motivates us to take a look at the cyclic group generated by the element A. Note that for any group G where $|G| = n$ we have that $g^n = e$ for all $g \in G$, so we are motivated to find the order of this cyclic group, or some multiple of it.

Observe that the cyclic group generated by some invertible modular matrix A is a subgroup of all invertible modular matrices of same size and modulus. By Lagrange's theorem, we can find that the order of all such invertible matrices is a multiple of the order of A. Thus, our focus now shifts to the entire group of invertible matrices and finding its order.

Remark. It should be noted that there is also a well-behaved closed form for the number of invertible modular matrices for *prime* m. Consider an argument where we choose k linearly independent vectors of size k one-by-one. For the first vector, we have $m^k - 1$ choices (all but the zero vector). For the second vector, we have $m^k - m$ choices since there are m vectors that can be formed as a linear combination of the first chosen vector. The third has $m^k - m^2$ choices by a similar reasoning. In general, the number of invertible matrices for a prime modulus m is given by

$$(m^k - 1)(m^k - m)(m^k - m^2)\cdots(m^k - m^{k-1}) = \prod_{i=0}^{k-1}(m^k - m^i).$$

The reason this fails to count all invertible matrices for composite m is because not all matrices with nonzero determinant are invertible in such instances.

Since this doesn't generalize well for prime powers, we'll have to find some other approach. It suffices to find a multiple of the order for prime powers, since for any composite number, we may simply take the LCM of the orders of its pure prime power components. This motivates a new approach.

Definition. Let the *determinant frequency* of some congruency class a with respect to the set $N_{k\times k}(\mathbb{Z}_m)$ be the number of matrices $A \in N_{k\times k}(\mathbb{Z}_m)$ such that $\det A = a$. We shall denote this frequency by $\mathfrak{q}(a)$.

With this, we can decompose the invertible matrices into a sum of over all determinants that give inverses. In particular, we want to calculate

$$\sum_{\gcd(a,m)=1} \mathfrak{q}(a).$$

While this doesn't do much for us, there's one really nice simplification that we can make.

Theorem. For all a such that $\gcd(a, m) = 1$, $\mathfrak{q}(a)$ are all equal.

Proof. Consider the mapping $x \mapsto qx$, where $\gcd(a, m) = 1$. Since q^{-1} exists, this mapping is invertible, and is thus a bijection over $\mathbb{Z}_m$. We observe that applying such a mapping elementwise to a modular matrix also forms a bijection. Since the properties of determinants apply, this mapping transforms $\det A$ to be $q^k \det A$. Since $\gcd(\det A, m) = \gcd(a, m) = 1$ and $\gcd(q, m) = 1$, we can always choose a q such that $q^k = a^{-1}$. This means that we can always construct a bijection between modular matrices of determinant a and modular matrices of determinant 1, which suffices to show that each of the specified congruency classes for determinants contains the same number of elements. ■

This allows us to simplify our sum a bit further, transforming into

$$\sum_{\gcd(a,m)=1} \mathfrak{q}(a) = \varphi(m)\mathfrak{q}(1).$$

Unfortunately, I'm not so sure how hard it is to determine $\mathfrak{q}(1)$ in general. Of course the set of modular matrices of determinant 1 forms a group in of itself, so there's something to work with, but I'm not sure how far one can get in terms of counting. Perhaps we should aim for a general asymptotic, although this isn't really applicable to reducing matrix powers.

Perhaps I'll come back to this later if I have any ideas.