Permanents of 2×2 Matrices Modulo n

A. Bohra and A. Satyanarayana Reddy

Abstract - In this article we compute the number of invertible 2×2 matrices with integer entries modulo n whose permanents are congruent modulo n to a given integer x.

Keywords : modular arithmetic; permanents; determinants

Mathematics Subject Classification (2020) **:** 05B10; 15A15.

1 Introduction and Preliminaries

Let us see why counting the matrices described in the abstract is a natural idea.

Let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ denote the ring of integers modulo n. We will denote GCD(a, b) by (a, b).

Lockhart and Wardlaw compute in [1] the number of square matrices with entries in $\mathbb{Z}_n$ with given determinant x. Trying to do the same after replacing the determinant by the permanent looks like a daunting task, so let us examine the case of 2×2 matrices.

Let $M_2(\mathbb{Z}_n)$ denote the ring of all 2×2 matrices with entries from $\mathbb{Z}_n$.

Definition 1.1 *Let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_n)$. *The* permanent *of* A, *denoted* $perm(A)$, *is defined as*

$$perm(A) = ad + bc \pmod{n}.$$

If $n, x \in \mathbb{N}$, define

$$D_n(x) = \{A \in M_2(\mathbb{Z}_n) | det(A) \equiv x \pmod{n}\}.$$

The number of elements of $D_n(x)$, $|D_n(x)|$, was found in [1]. If we now define

$$F_n(x) = \{A \in M_2(\mathbb{Z}_n) | perm(A) \equiv x \pmod{n}\},$$

and try to find $|F_n(x)|$, there is good news and bad news. The bad news is that it is easy to see that this will be the same number: the sets $F_n(x)$ and $D_n(x)$ are in bijection via the map sending $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & -b \\ c & d \end{bmatrix}$. The good news is that $|F_n(x)|$ shares the properties of $|D_n(x)|$ [1], such as :

1. Multiplicativity in n : If $a, b \in \mathbb{N}$ with $(a,b)=1$, then

$$|F_{ab}(x)| = |F_a(x)| \times |F_b(x)|$$

2. GCD invariance : If $n, x, y \in \mathbb{N}$, then

$$|F_n(x)| = |F_n(y)| \text{ whenever } (n,x) = (n,y)$$

For example, this allows us to conclude that

$$|M_2(\mathbb{Z}_n)| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) |F_n(d)|.$$

Denote by $GL_2(\mathbb{Z}_n)$ the group of units of $M_2(\mathbb{Z}_n)$. If we now set

$$G_n(x) = \{A \in GL_2(\mathbb{Z}_n) | perm(A) \equiv x \pmod{n}\} \text{ and } g_n(x) = |G_n(x)|,$$

we will see that computing the values of $g_n(x)$ for every n and x is an interesting problem.

It is known that $|GL_2(\mathbb{Z}_p)| = (p^2-p)(p^2-1)$. If $\psi : GL_2(\mathbb{Z}_{p^k}) \to GL_2(\mathbb{Z}_p)$ is the group homomorphism induced by the natural ring homomorphism $M_2(\mathbb{Z}_{p^k}) \to M_2(\mathbb{Z}_p)$, then it is easy to check that $|ker\psi| = p^{4(k-1)}$. From the surjectivity of ψ, we have

$$|GL_2(\mathbb{Z}_{p^k})| = p^{4(k-1)}|GL_2(\mathbb{Z}_p)| = p^{4(k-1)}(p^2-p)(p^2-1) \tag{1}$$

(Note that a similar formula holds in arbitrary dimension [1].)

2 The Function $g_n(x)$

We start this section with the following remark related to $G_n(0)$, which we will use frequently.

Remark 2.1 Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_n(0)$. Then $perm(A) \equiv 0 \pmod{n}$ and $(det(A), n) = (ad-bc, n) = 1$. We claim that each of a, b, c, d is relatively prime to n. Suppose it were not true, without loss of generality assume that $(a,n) = r > 1$. Then there is a prime p such that $p|r$. As a consequence $p|a$, now p is prime and $p|ad+bc$ implies $p|b$ or $p|c$ which contradicts the fact that $(ad-bc, n) = 1$.

An immediate consequence of above remark is that for an odd prime p and $k \in \mathbb{N}$ we have

$$g_{p^k}(0) = \phi(p^k)^3 = (p^k - p^{k-1})^3 \tag{2}$$

The following result shows that $g_n(x)$ is multiplicative in n, which is a direct consequence of the proof that $|F_n(x)|$ is multiplicative in n [1]. We are including the proof for the sake of completeness. With Proposition 2.2 and Proposition 2.3 we can compute $g_n(x)$ for every n and x. In the process we show that $g_{p^k}(x)$ assumes only two values. In particular, we show that $g_{p^k}(x) = \begin{cases} g_{p^k}(0) & \text{if } p|x, \\ g_{p^k}(1) & \text{otherwise.} \end{cases}$

Proposition 2.2 *Let $a, b \in \mathbb{N}$ be such that $(a,b) = 1$. Then for every $x \in \mathbb{Z}$*

$$g_{ab}(x) = g_a(x) \times g_b(x).$$

Proof. We make use of the bijection we already have from $F_{ab}(x) \to F_a(x) \times F_b(x)$ in [1] which takes $[c_{ij}] \mapsto ([c_{ij} \pmod a], [c_{ij} \pmod b])$. Consider the same map from $G_{ab}(x) \to G_a(x) \times G_b(x)$. It is injective on the restricted domain since it is injective on the superset $F_{ab}(x)$. The range of the map is clearly contained in $G_a(x) \times G_b(x)$ since a unit (mod ab) is also a unit (mod a) and (mod b) when $(a,b) = 1$. Now given $(R, S) \in G_a(x) \times G_b(x)$ we have a pre-image $T \in F_{ab}(x)$. We claim that this T lies in $G_{ab}(x)$. For if it was not, then $det(T)$ would be a zero divisor in $\mathbb{Z}_{ab}$, that would contradict R and S both being invertible. Thus the map is surjective on the restricted domain as well and hence a bijection from $G_{ab}(x) \to G_a(x) \times G_b(x)$. Thus $g_n(x)$ is multiplicative. □

The next result describes $g_n(x)$ when n is a power of a prime.

Proposition 2.3 *Let $p \in \mathbb{N}$ be a prime number and $k \in \mathbb{N}$. Then:*
(i) for every $x \in \mathbb{Z}$ with $p|x$, $g_{p^k}(x) = g_{p^k}(0)$. Furthermore, if $p = 2$, then $g_{2^k}(0) = 0$.
(ii) if $p \nmid x$, then $g_{p^k}(x) = g_{p^k}(1)$.

Proof. (i) We first construct a bijection from $G_{p^k}(0)$ to $G_{p^k}(p^i)$:

$$\lambda : G_{p^k}(0) \to G_{p^k}(p^i) \text{ by } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b \\ c & d + a^{-1}p^i \end{bmatrix}.$$

It is easy to check that the above map is injective. Given $A \in G_{p^k}(0)$, $\lambda(A) \in G_{p^k}(p^i)$. For $\gcd(ad - bc, p^k) = 1 \implies \gcd\left((ad - bc) + p^i, p^k\right) = \gcd\left(det(\lambda(A)), p^k\right) = 1$. Furthermore, λ is a surjective map as well. This is because given $B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in G_{p^k}(p^i)$, we are guaranteed the existence of the multiplicative inverse $(a')^{-1} \in \mathbb{Z}_{p^k}$ (this can be proved in the same way as Remark 2.1). Now consider $C = \begin{bmatrix} a' & b' \\ c' & d' - (a')^{-1}p^i \end{bmatrix} \in G_{p^k}(0)$. Clearly, $\lambda(C) = B$ and thus

$$|G_{p^k}(0)| = |G_{p^k}(p^i)| \implies g_{p^k}(0) = g_{p^k}(p^i).$$

Now, if $p \nmid m$, define $h_m : G_{p^k}(p^i) \to G_{p^k}(mp^i)$ by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} ma & mb \\ c & d \end{bmatrix}$. This is a bijection, since $(m, p^k) = 1$ there exists $t \in \mathbb{Z}_{p^k}$ such that $mt \equiv 1 \pmod{p^k}$, and the map $h_t : G_{p^k}(mp^i) \to G_{p^k}(p^i)$ defined as $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \mapsto \begin{bmatrix} tp & tq \\ r & s \end{bmatrix}$ is the inverse of h_m. Thus

$$g_{p^k}(0) = g_{p^k}(p^i) = g_{p^k}(mp^i).$$

Now consider the case when $p = 2$ and let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_{2^k}(0)$, so $ad + bc \equiv 0 \pmod{2^k}$ and $2 \nmid det(A) \equiv ad - bc$. Since $2|ad+bc$, both ad and bc have the same parity, so $2|ad-bc$ as well, a contradiction. Thus

$$g_{2^k}(0) = 0.$$

(ii) We prove, more generally, that $g_n(k) = g_n(1)$ if $(k, n) = 1$. There exists $\ell \in \mathbb{Z}_n$ such that $k\ell \equiv 1 \pmod{n}$. The map $h_k : G_n(1) \to G_n(k)$ defined by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} ka & kb \\ c & d \end{bmatrix}$, has inverse $h_\ell : G_n(k) \to G_n(1)$ defined by $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \mapsto \begin{bmatrix} \ell p & \ell q \\ r & s \end{bmatrix}$. □

The following result follows immediately from Propositions 2.2 and 2.3

Corollary 2.4 *Let $p_1, p_2, \ldots, p_r$ be distinct odd primes.*
(i) Let $n = p_1^{a_1} \cdots p_r^{a_r} \in \mathbb{N}$. Then $g_n(x)$ takes 2^r possible values.
(ii) Let $n = 2^a p_1^{a_1} \cdots p_r^{a_r} \in \mathbb{N}$, where $a > 0$. Then $g_n(x)$ takes $2^{r-1} + 1$ possible values.

Corollary 2.5 *Let $n \in \mathbb{N}$. Then $|GL_2(\mathbb{Z}_n)| = \sum_{d|n} \varphi(\frac{n}{d}) g_n(d)$.*

Proof. We have

$$|GL_2(\mathbb{Z}_n)| = g_n(1) + g_n(2) + \ldots + g_n(n),$$

so it is sufficient to prove that $g_n(a) = g_n(b)$ whenever $(a, n) = (b, n)$. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $(k, n) = d > 1$, then $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where $0 \le b_i \le a_i$, and from Proposition 2.2 we have

$$g_n(d) = \prod_{p_i|d} g_{p_i^{a_i}}(d) \prod_{p_j \nmid d} g_{p_j^{a_j}}(d).$$

Now from Proposition 2.3 we have

$$g_n(d) = \prod_{p_i|d} g_{p_i^{a_i}}(0) \prod_{p_j \nmid d} g_{p_j^{a_j}}(1) = g_n(k).$$

□

Corollary 2.6 *Let p be an odd prime and $k \in \mathbb{N}$. Then:*
(i) $g_{p^k}(0) = (p^k - p^{k-1})^3$
(ii) $g_{p^k}(1) = p^{3(k-1)}(p-1)(p^2+1)$
(iii) $g_{2^k}(0) = 0$
(iv) $g_{2^k}(1) = 6 \times 8^{k-1}$.

Proof. (i) is (2).
(ii) follows from (i), (1), Proposition 2.3, and Corollary 2.5.
(iii) is in Proposition 2.3 (i).
(iv) follows from (iii), (1), Proposition 2.3, and Corollary 2.5. □

We can now use the fact that $g_n(x)$ is multiplicative in n and the previous corollary to find values of $g_n(x)$ for all $n, x \in \mathbb{N}$. We illustrate this process with a couple of examples.

For the first example, $g_{75}(x)$ can take four values:

1. $g_{75}(0) = g_3(0)g_{25}(0) = 64,000$
2. $g_{75}(1) = g_3(1)g_{25}(1) = 260,000$
3. $g_{75}(3) = g_3(0)g_{25}(1) = 104,000$
4. $g_{75}(5) = g_3(1)g_{25}(0) = 160,000.$

Any other $g_{75}(x)$ is equal to one of these four, e.g.

$$g_{75}(14) = g_3(14)g_{25}(14) = g_3(1)g_{25}(1) = 260,000$$

and

$$g_{75}(35) = g_3(35)g_{25}(35) = g_3(1)g_{25}(0) = 160,000.$$

For the second example, the three possible values of $g_{24}(x)$ are :

1. $g_{24}(0) = g_8(0)g_3(0) = 0$
2. $g_{24}(1) = g_8(1)g_3(1) = 7,680$
3. $g_{24}(3) = g_8(1)g_3(0) = 3,072.$

Any other $g_{24}(x)$ is equal to one of these three, e.g.

$$g_{24}(14) = g_8(14)g_3(14) = g_8(0)g_3(1) = 0 \cdot g_3(1) = 0$$

and

$$g_{24}(35) = g_{24}(11) = g_8(11)g_3(11) = g_8(1)g_3(1) = 7,680.$$

References

[1] J.M. Lockhart, W.P. Wardlaw, Determinants of Matrices over the Integers Modulo m, *Math. Mag.*, **80** (2007), 207–214. Also available at the URL:http://www.jstor.org/stable/27643029

Ayush Bohra
Department of Mathematics,
Shiv Nadar University,
India-201314.
E-mail: ab424@snu.edu.in

Arikatla Satyanarayana Reddy
Department of Mathematics,
Shiv Nadar University,
India-201314.
E-mail: satya.a@snu.edu.in

Received: October 28, 2020 **Accepted**: March 8, 2021
Communicated by Declan Quinn