5.4.35

EE25BTECH11041 - Naman Kumar

Question:
Let p be an odd prime number and $\mathbf{T_p}$ be the following set of 2×2 matrices

$$\mathbf{T_p} = \left\{ \mathbf{A} = \begin{pmatrix} a & b \\ c & a \end{pmatrix} : a, b, c \in \{0, 1, 2, \ldots, p-1\} \right\} \tag{1}$$

b) The number of $\mathbf{A}$ in $\mathbf{T}_p$ such that the trace of $\mathbf{A}$ is not divisible by p but det($\mathbf{A}$) is divisible by p is

Solution:
Step 1: Trace of $\mathbf{A}$

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \tag{2}$$

$$tr(\mathbf{A}) = a + a = 2a \tag{3}$$

$$2a \mod p \not\equiv 0 \tag{4}$$

p is a odd prime , the number 2 is not a multiple of p, so 'a' must also be non-zero, Therefore the condition simplifies to:

$$a \mod p \not\equiv 0 \tag{5}$$

so for a their are p-1 chooses.
Step 2: $det(\mathbf{A}) \mod p \equiv 0$

$$det(\mathbf{A}) = \begin{vmatrix} a & b \\ c & a \end{vmatrix} \tag{6}$$

$$= a^2 - bc \tag{7}$$

$$a^2 - bc \mod p \equiv 0 \implies bc \equiv a^2 \pmod p \tag{8}$$

'a' as p-1 choices leaving a=0,let $a^2 = k$

$$bc = k (k \neq 0) \tag{9}$$

neither of 'b' and 'c' be zero
for 'b' we have p-1 choices leaving zero

$$bc \equiv k \tag{10}$$

$$c \equiv k.b^{-1} \ (b^{-1}\text{multiplicative inverse of b modulo p}) \tag{11}$$

so for every 'b' we have 'c'
Therefore their are p-1 pairs of (b,c)
Finally, total number matrix $\mathbf{A}$

$$= (p-1)(p-1) = (p-1)^2 \tag{12}$$

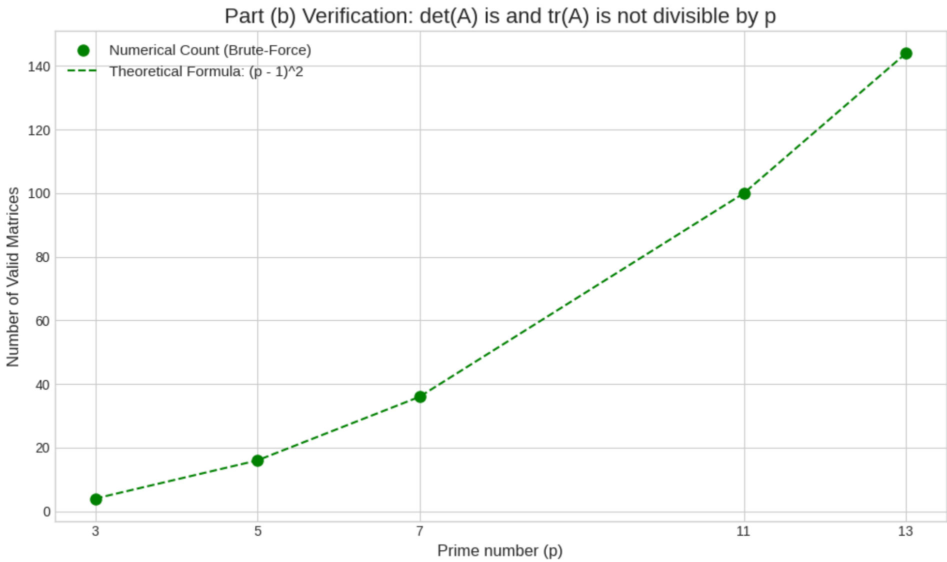
Part (b) Verification: det(A) is and tr(A) is not divisible by p
Numerical Count (Brute-Force)
Theoretical Formula: (p - 1)^2
Number of Valid Matrices
0
20
40
60
80
100
120
140
3
5
7
11
13
Prime number (p)

Fig. 1