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

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

c) The number of A in $\mathbf{T}_p$ such that det(A) is not divisible by p is
Solution:

$$det(\mathbf{A}) = \begin{vmatrix} a & b \\ c & a \end{vmatrix} \tag{2}$$

$$= a^2 - bc \tag{3}$$

$$\tag{4}$$

Total number of possible matrices

$$= p \times p \times p = p^3 \tag{5}$$

We can find number of matrices whose determinant is divisible by p
Required number = Total - number of matrices whose determinant is divisible by p

$$a^2 - bc \equiv 0 \mod p \tag{6}$$

$$a^2 \equiv bc \mod p \tag{7}$$

Case 1: a=0

$$bc \equiv 0 \mod p \tag{8}$$

i) b=0, c as p-1 choices

$$\text{number of cases} = 1 \times p = p \tag{9}$$

ii) c=0, b as p-1 choices

$$\text{number of cases} = 1 \times p = p \tag{10}$$

$$\text{total in this case} = 2(p) - 1 \tag{11}$$

-1 for extra case of overlap at 'b' and 'c' both zero
Case 2: $a \neq 0$
let $a^2 = k$

$$\text{'a' has p-1 choices} \tag{12}$$

$$bc \equiv k \mod p \tag{13}$$

$$c \equiv k.b^{-1} \mod p \ (b^{-1}\text{multiplicative inverse of b modulo p}) \tag{14}$$

For every 'b' we have a fixed 'c' for their are p-1 pairs of (b,c)

$$\text{number of cases} = (p-1) \times (p-1) = (p-1)^2 \tag{15}$$

Finally adding total number cases from (11) and (15)

$$= 2p - 1 + (p^2 - 2p + 1) = p^2 \tag{16}$$

Finally required value is

$$\text{required ans} = total - (16) \tag{17}$$

$$= p^3 - p^2 \tag{18}$$

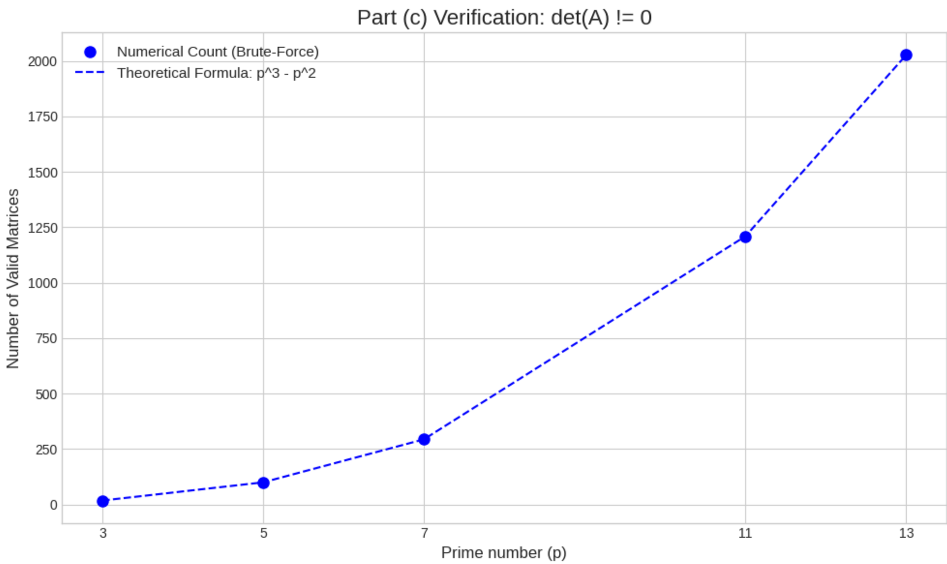

Fig. 1