

5.13.66

Naman Kumar-EE25BTECH11041

26 September,2025

Question c)

Let p be an odd prime number and \mathbf{T}_p be the following set of 2×2 matrices

$$\mathbf{T}_p = \left\{ \mathbf{A} = \begin{pmatrix} a & b \\ c & a \end{pmatrix} : a, b, c \in \{0, 1, 2, \dots, p-1\} \right\} \quad (1)$$

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

Solution

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

$$= a^2 - bc \quad (3)$$

$$(4)$$

Total number of possible matrices

$$= p \times p \times p = p^3 \quad (5)$$

Solution

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

$$a^2 - bc \equiv 0 \pmod{p} \quad (6)$$

$$a^2 \equiv bc \pmod{p} \quad (7)$$

Case 1: $a=0$

$$bc \equiv 0 \pmod{p} \quad (8)$$

Solution

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

$$\text{number of cases} = 1 \times p = p \quad (9)$$

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

$$\text{number of cases} = 1 \times p = p \quad (10)$$

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

Solution

-1 for extra case of overlap at 'b' and 'c' both zero

Case 2: $a \neq 0$

let $a^2 = k$

'a' has $p-1$ choices (12)

$$bc \equiv k \pmod{p} \quad (13)$$

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

Solution

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

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

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

$$= 2p - 1 + (p^2 - 2p + 1) = p^2 \quad (16)$$

Finally required value is

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

$$= p^3 - p^2 \quad (18)$$

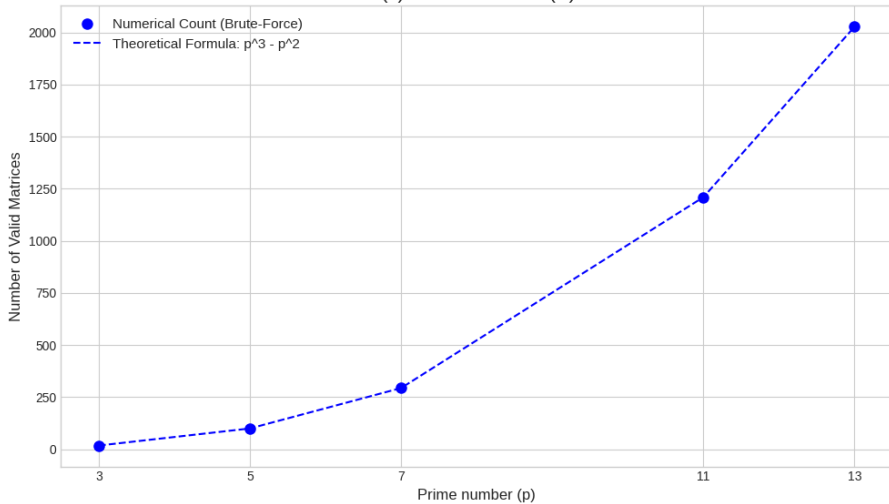
Part (c) Verification: $\det(A) \neq 0$ 

Figure: