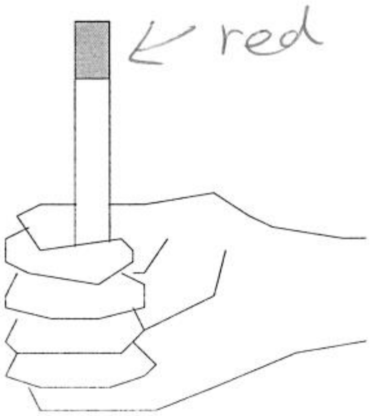
Take three sticks which have their ends colored and place them in a bag. The first stick has two red ends, the second has two black ends and the third stick has a red and a black end.

Now, reach into this bag (no peeking) and grasp one of the sticks by an end so that the other end is showing and pull the stick out. Say that a red end is showing.

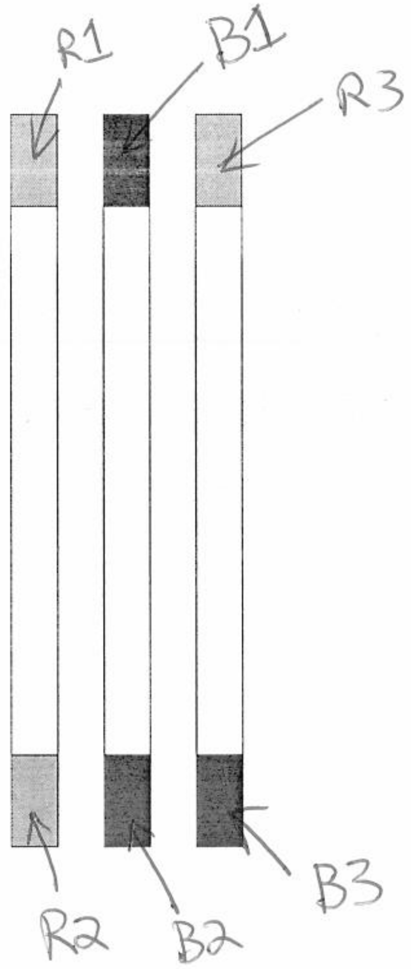
What color is most likely clasped in your fist?

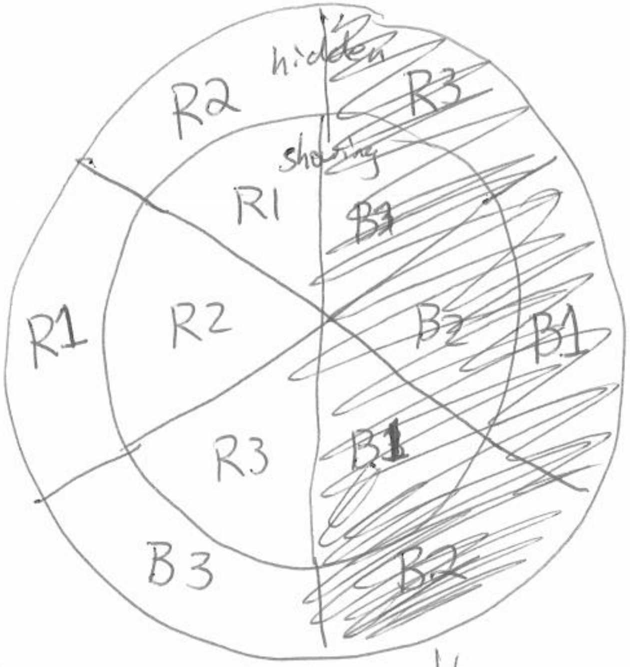


Is the answer?

3 A) red
2 B) black
12 C) red/black are equally likely
3 D) don’t know/care

Let's analyze this problem. Look at the 3 sticks again:





Want to calculate the probability that the hidden is red given that the showing is red

$P(\text{hidden} = \text{red} \mid \text{showing} = \text{red}) = 2/3$

$P(\text{hidden} = \text{black} \mid \text{showing} = \text{red}) = 1/3$

(4) Find the plaintext corresponding to the cyphertext $PYRA$ given that it was encrypted using the Hill substitution cipher (mod 29) with the key

$$\begin{bmatrix} 3 & 3 \\ 28 & 9 \end{bmatrix}$$

(5) Say that we know that the encrypting matrix for a 2×2 Hill transformation mod 26 is of the form

$$\begin{pmatrix} 3 & 5 \\ a & b \end{pmatrix} \qquad 3b - a5 \equiv 17 \pmod{26}$$

but we do not know the last row. We are able to determine that the matrix has determinant 17 and the letters *ft* are sent to the letters **GJ** .

$$\begin{bmatrix} 3 & 5 \\ a & b \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 3\cdot5+5\cdot19 \\ a5+19b \end{bmatrix} = \begin{bmatrix} 6 \\ 9 \end{bmatrix}$$

(a) Find the encrypting matrix.
(b) Find the decrypting matrix.
(c) Find the plaintext if we know the cyphertext **MDCK** was encrypted with this transformation.

(6) What is the house advantage for the '6-hardway' bet? That is, how much is the house expected to win on average per \$1 bet in the game of craps? On this bet, the die is rolled until either a 6 or or a 7 appears and the player wins \$9 if double 3's are showing and loses \$1 otherwise.

$$3\cdot5+5\cdot19 = 15+95 = 110 \equiv 6 \pmod{26}$$

$$\begin{cases} -5a+3b \equiv 17 \\ 5a+19b \equiv 9 \end{cases} \pmod{26} \qquad \text{(eq 1)}$$

$$\begin{bmatrix} -5 & 3 \\ 5 & 19 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 17 \\ 9 \end{bmatrix} \qquad \begin{bmatrix} -5 & 3 \\ 5 & 19 \end{bmatrix}^{-1} = \frac{1}{-6}\begin{bmatrix} 19 & -3 \\ -5 & -5 \end{bmatrix}$$

add these two equations

$$22b \equiv 26 \equiv 0 \pmod{26}$$

$$b \equiv 13, 0 \pmod{26}$$

$b \equiv 0$ $\qquad -5a + 3\cdot0 \equiv 17$ from (eq 1)

$$\Rightarrow a \equiv 6 \pmod{26}$$

$b = 13$ $\qquad -5a + 3\cdot13 \equiv 17 \pmod{26}$ from (eq 1)

$$-5a + 13 \equiv 17 \pmod{26}$$

$$-5a \equiv 4 \pmod{26}$$

$$\Rightarrow a = 20$$

Solution 1

encrypting matrix $\begin{bmatrix} 3 & 5 \\ 6 & 0 \end{bmatrix}$

Solution 2 $\begin{bmatrix} 3 & 5 \\ 20 & 13 \end{bmatrix}$

$$\text{decrypting } \begin{bmatrix} 3 & 5 \\ 6 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & -5 \\ -6 & 3 \end{bmatrix} \cdot 17^{-1} = \begin{bmatrix} 0 & 21 \\ 20 & 3 \end{bmatrix} \cdot 23 = \begin{bmatrix} 0 & 15 \\ 18 & 17 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 5 \\ 20 & 13 \end{bmatrix}^{-1} = \begin{bmatrix} 13 & -5 \\ -20 & 3 \end{bmatrix} \cdot 17^{-1} = \begin{bmatrix} 13 & 15 \\ -18 & 17 \end{bmatrix}$$

wrong matrix to use $\downarrow$

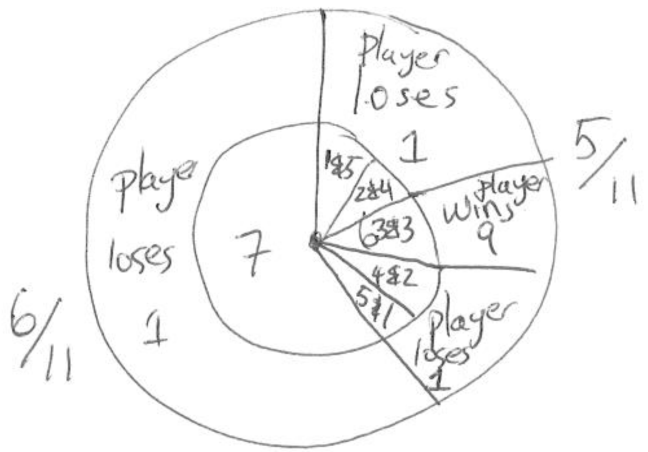
$$\begin{bmatrix} 0 & 15 \\ 18 & 17 \end{bmatrix} \begin{bmatrix} 12 & 2 \\ 3 & 10 \end{bmatrix} = \begin{bmatrix} 19 & 20 \\ 8+25 & 10+14 \end{bmatrix} = \begin{bmatrix} 19 & 20 \\ 7 & 24 \end{bmatrix}$$

M C
D K

T U
H Y

$$\begin{bmatrix} 13 & 15 \\ 8 & 17 \end{bmatrix} \begin{bmatrix} 12 & 2 \\ 3 & 10 \end{bmatrix} = \begin{bmatrix} 19 & 20 \\ 18+25 & 16+14 \end{bmatrix} = \begin{bmatrix} 19 & 20 \\ 17 & 4 \end{bmatrix}$$

T U
R E



1&5
2&4
3&3
4&2
5&1

$$\text{expected value for house} = -\overset{\text{lose \$9}}{9} \cdot \underset{\text{with prob } 1/11}{\frac{1}{11}} + 1 \cdot \frac{10}{11} = +\,{}^{1}\!/_{11}$$

this means that roughly for every $1 bet on the 6 hardway that the house wins 9.1¢ on average.

2. Suppose we have a computer program which generates words from the alphabet A,B,C,D according to the following procedure:

Pick the first letter according to the single frequency table given below then constructs each additional letter using the table of conditional biletter frequencies given below.

a) Calculate the probability that the program produces the word "DACB"

b) Determine the 2 letter word that has the highest probability.

Single letter table

A	10
B	9
C	12
D	9

Biletter table

	A	B	C	D
A	0	3	1	0
B	2	1	4	0
C	0	2	0	3
D	2	1	0	1

$$P(\text{word} = DACB) = P(\text{first letter} = D)P(\text{second} = A \mid \text{first} = D)P(\text{third} = C \mid \text{second} = A) \cdot P(\text{fourth} = B \mid \text{third} = C)$$

$$= \frac{9}{40} \cdot \frac{2}{4} \cdot \frac{1}{4} \cdot \frac{2}{5}$$

AA 0	BA	CA 0	DA
AB $\frac{10}{40} \cdot \frac{3}{4}$	BB	CB $\frac{12}{40} \cdot \frac{2}{5}$	DB
AC	BC $\frac{9}{40} \cdot \frac{4}{7}$	CC 0	DC 0
AD 0	BD 0	CD $\frac{12}{40} \cdot \frac{3}{5}$	DD