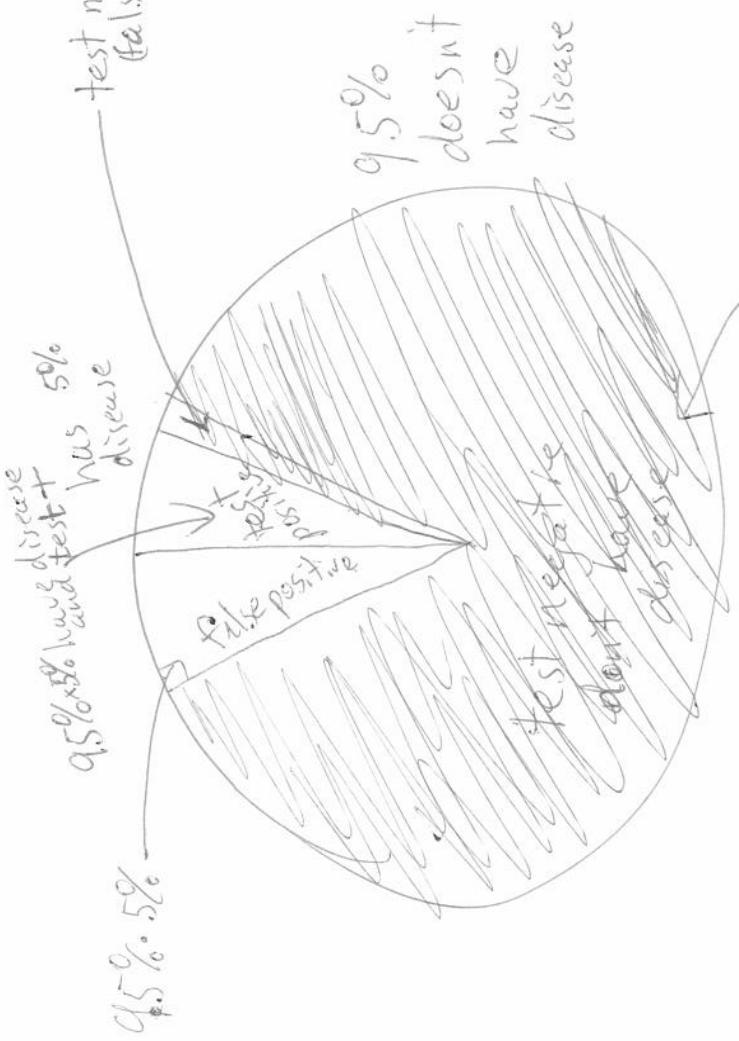


Say that there is a disease which only about 5% of the population has and that there is a test for this disease which is roughly 95% accurate (that is someone who has the disease will test positive 95% of the time and negative 5% of the time, while someone who does not have the disease will test negative 95% of the time and positive 5% of the time).

Given that a patient tests positive for the disease, what is the probability that he or she actually has it?

Is the answer?

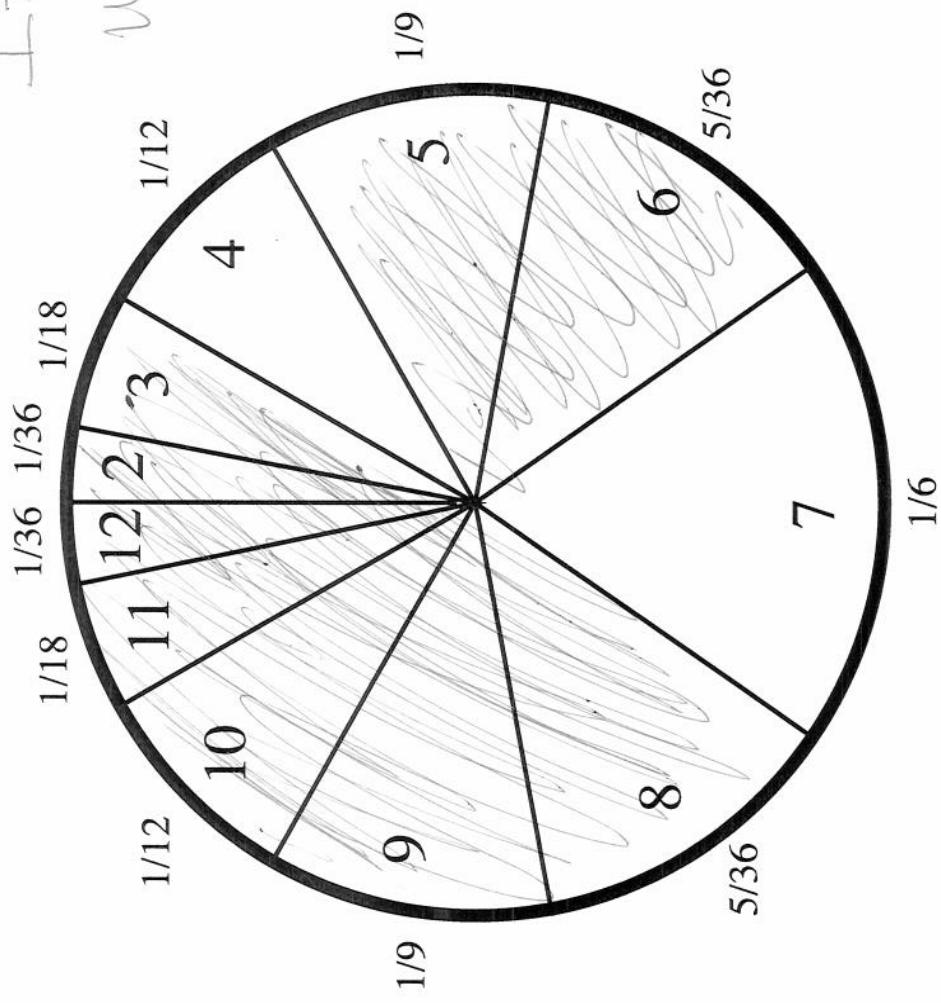
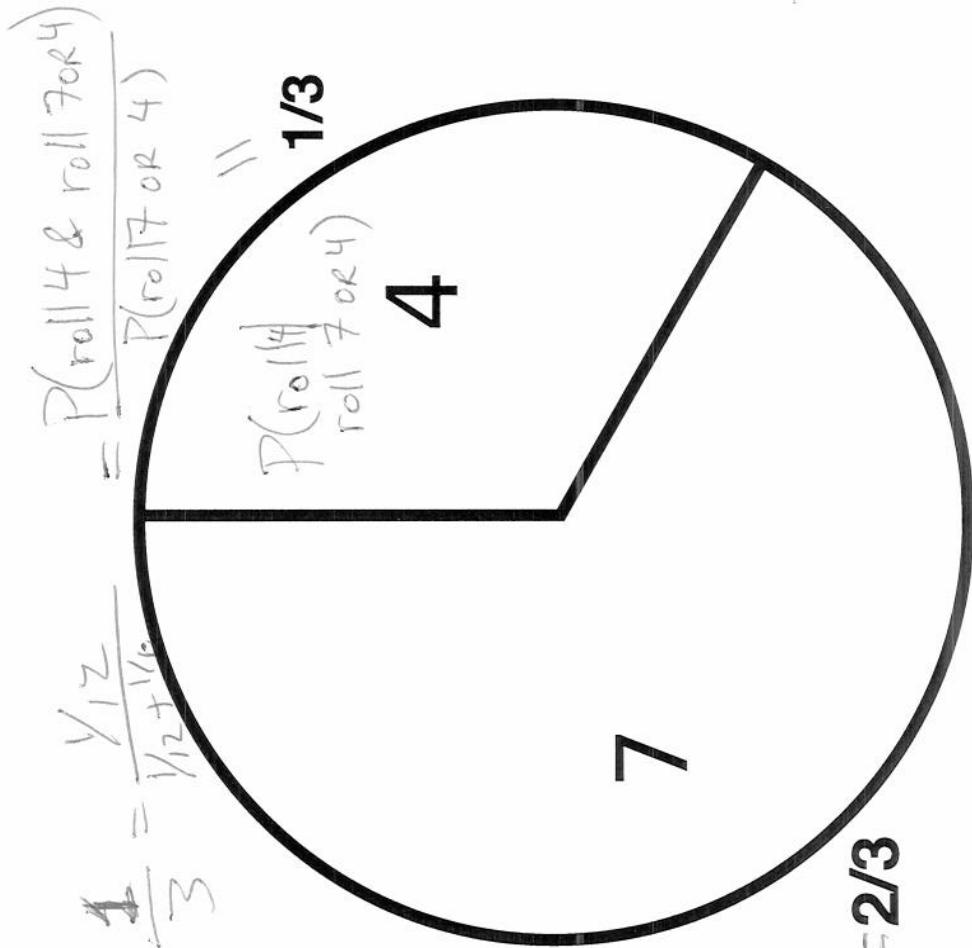
- A) 95%
- B) 90%
- C) 75%
- D) 50%



$$P(\text{has disease} \mid \text{test positive}) = \frac{P(\text{have disease} \& \text{test positive})}{P(\text{test positive})}$$

$$= \frac{0.95 \times 0.95}{0.95 \times 0.05 + 0.95 \times 0.05} = \frac{1}{2} = 0.5 = 50\%$$

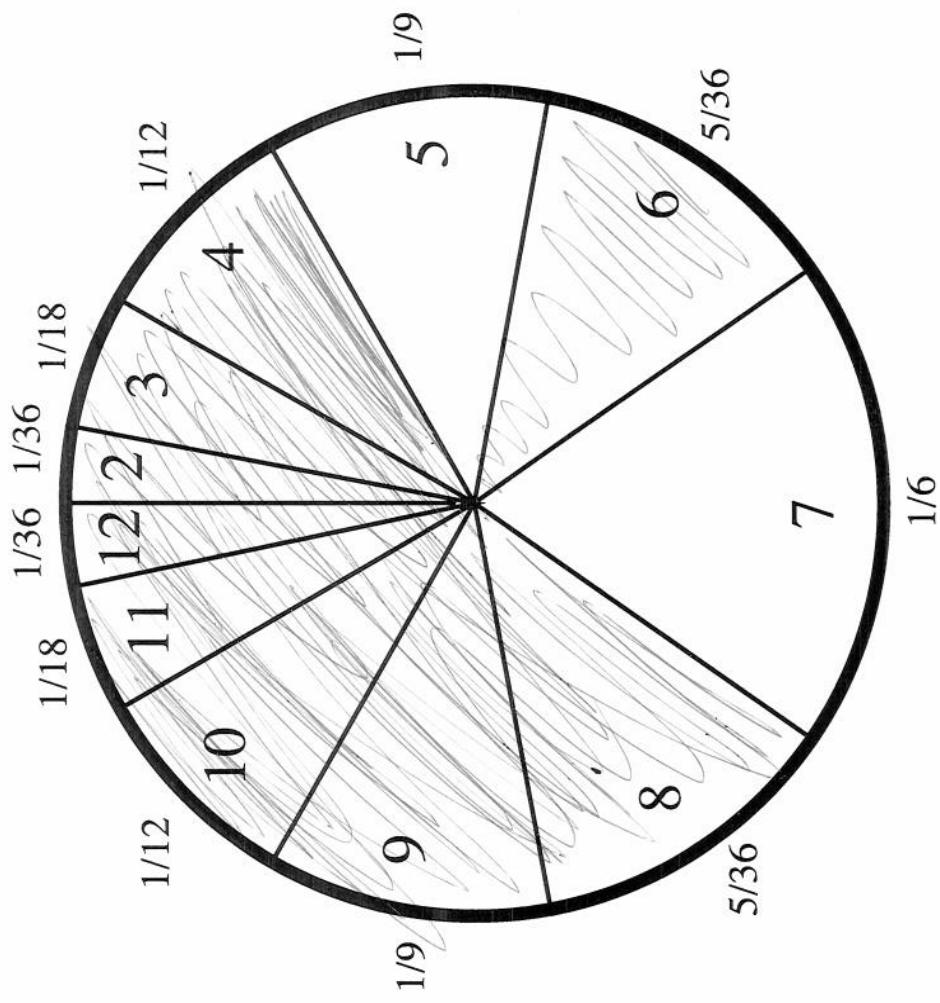
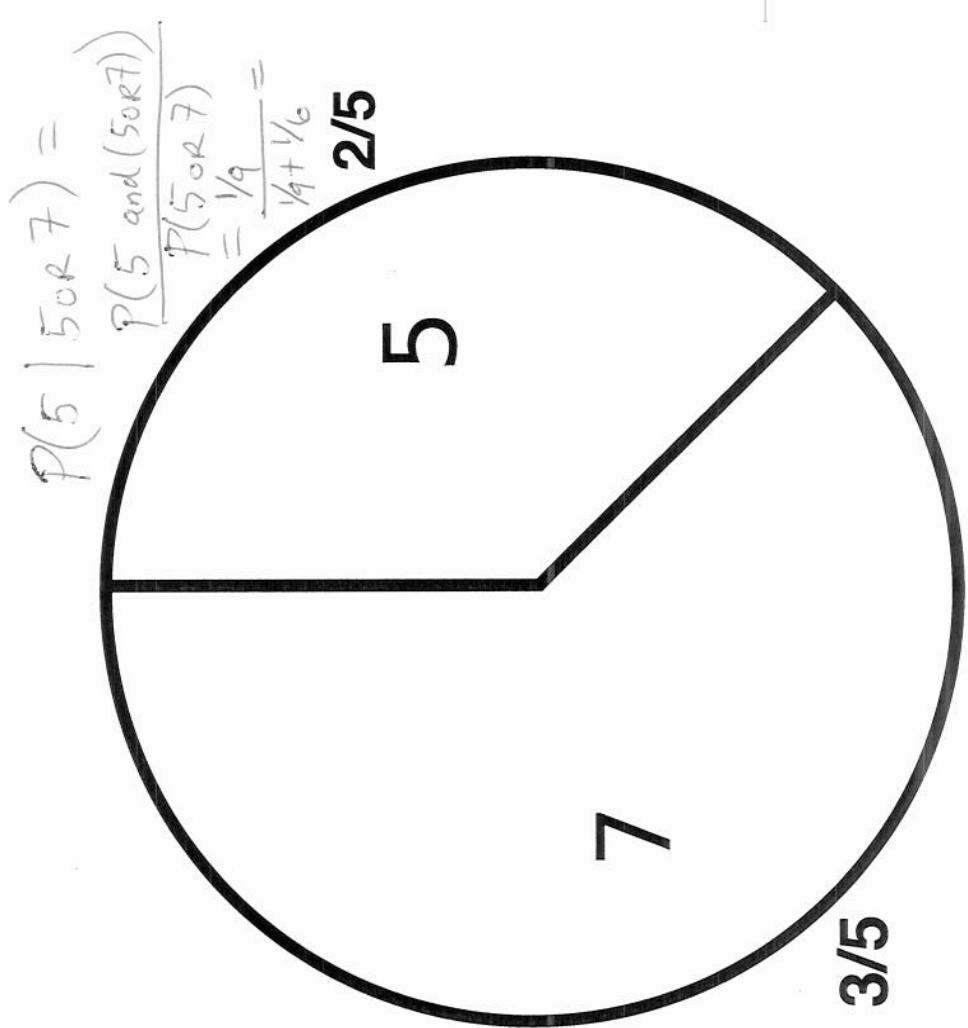
$$\text{If first roll } 4 \\ W_{in} = \text{roll 4 before a 7} \\ = P(\text{roll 4} | \text{roll 7 or 4})$$

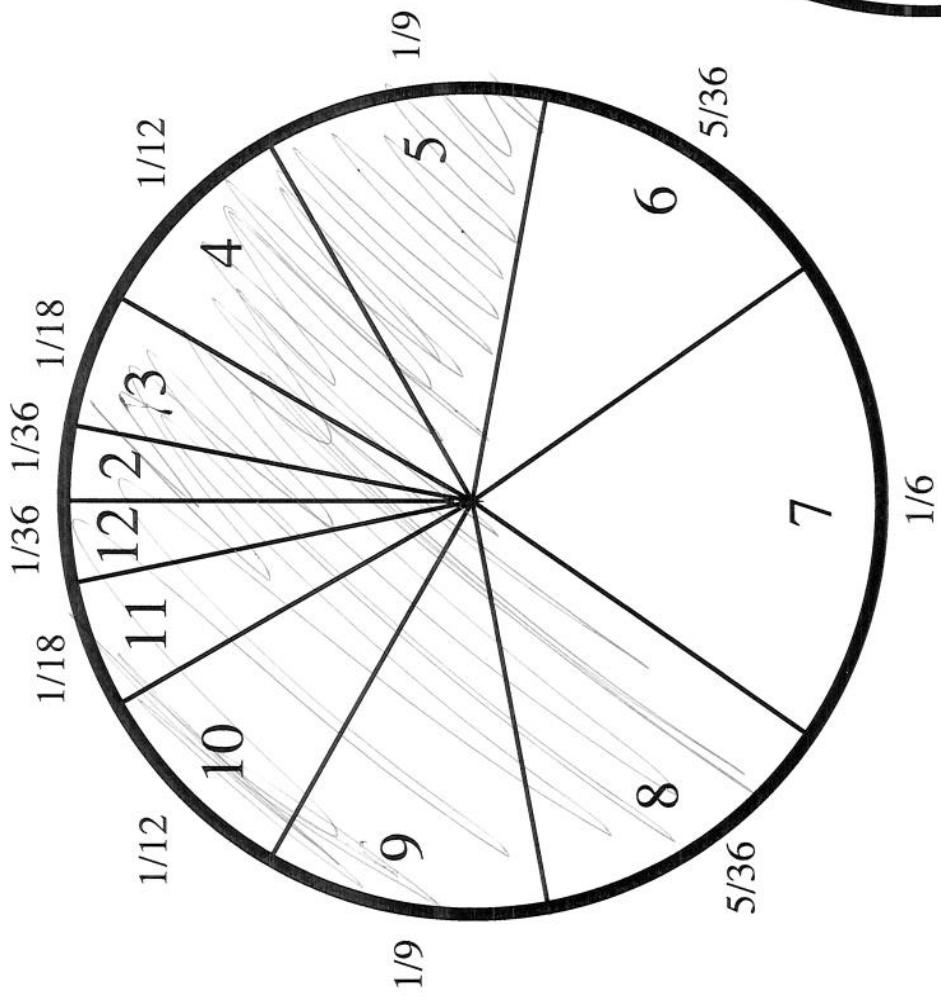
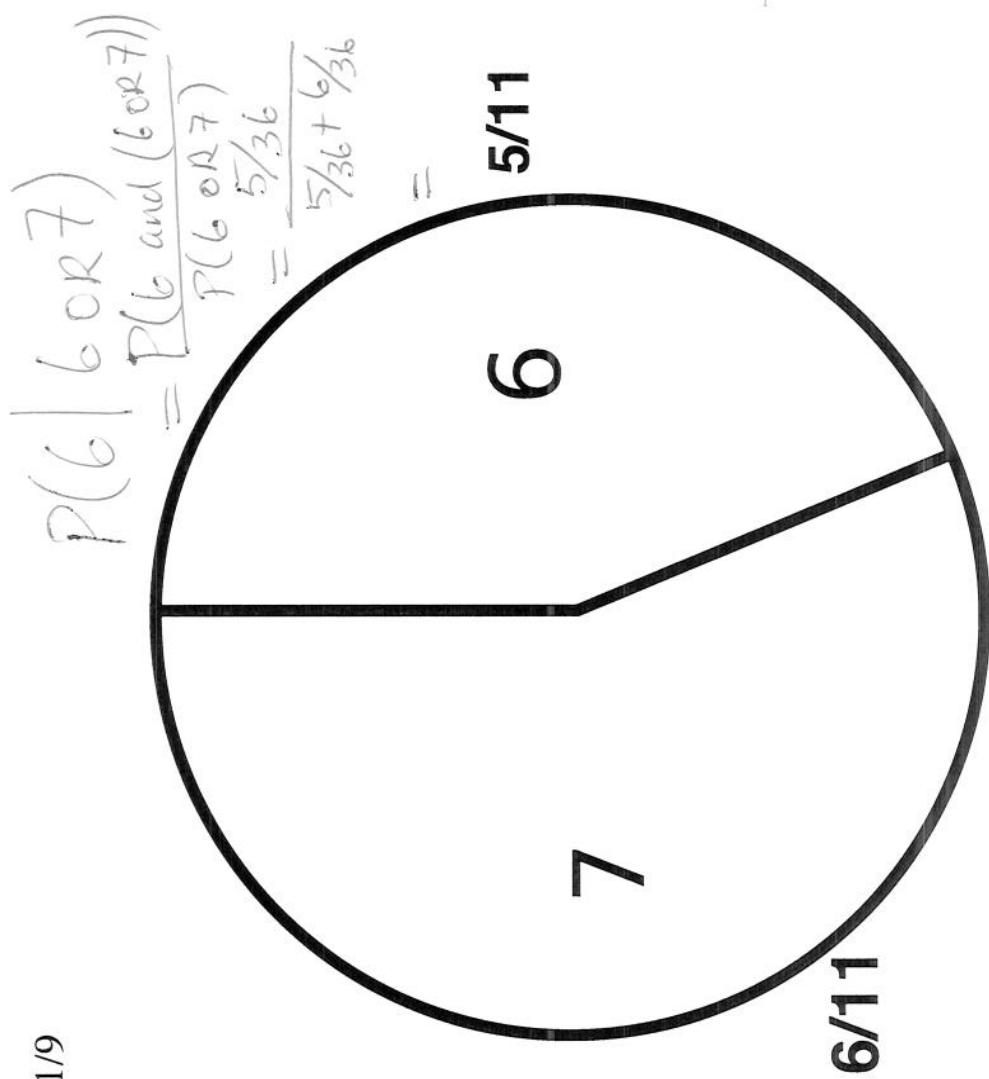


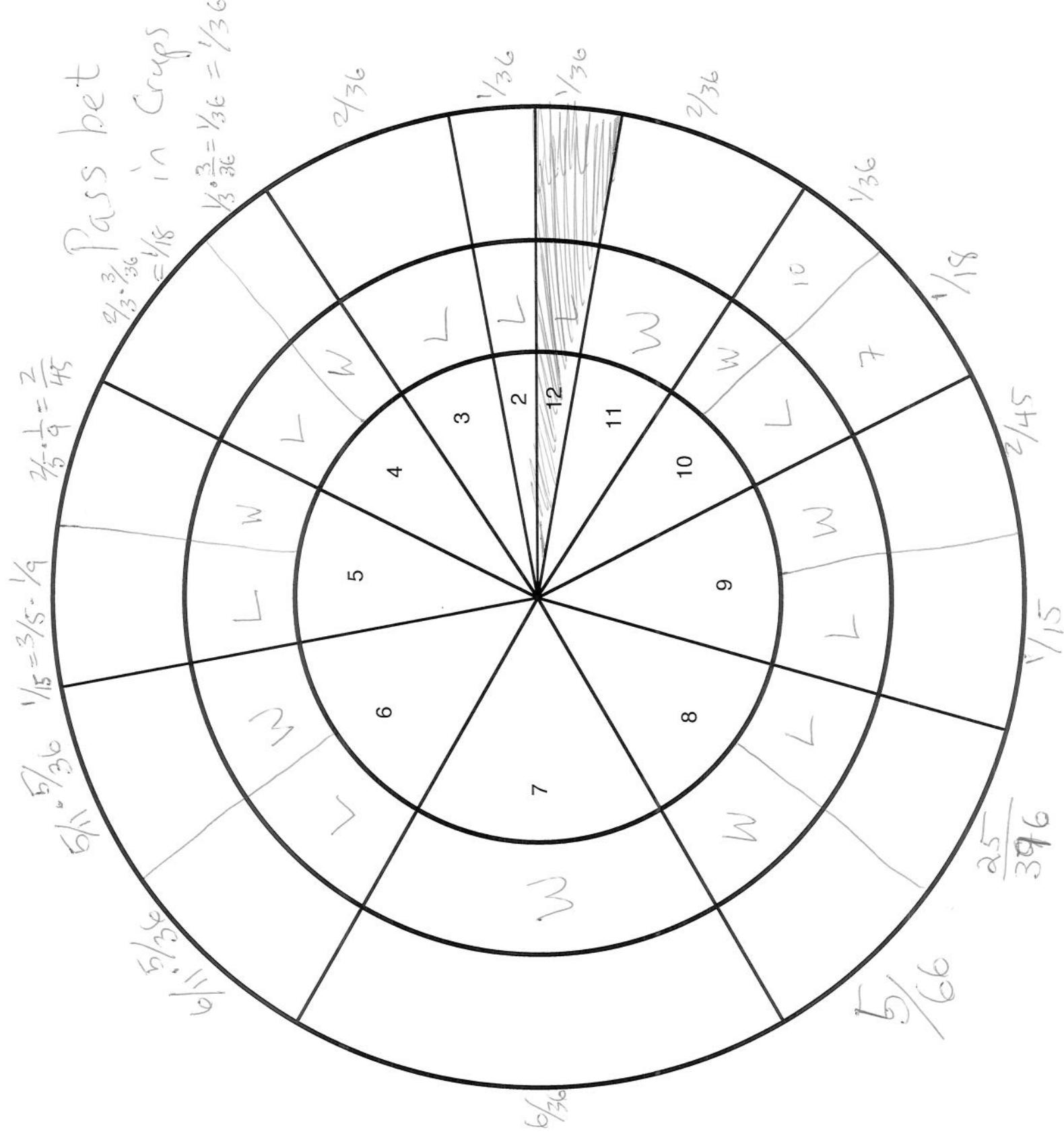
~~$$P\left(\text{roll 7} \& \text{roll 7 or 4}\right) = 2/3$$~~

$$= \frac{P\left(\text{roll 7} \& \text{roll 7 or 4}\right)}{P\left(\text{roll 7 or 4}\right)}$$

$$= \frac{1/6}{1/12 + 1/6}$$







Name of Bet	Description	Payoff per \$1	P(Win)	P(Lose)	House Advantange
Pass Bet	2,3,12 -lose 7,11-win 4,5,6,8,9,10- this is the point shooter rolls again until either 7 or the point comes up if point is first then win if 7 is first then lose	\$1	.492929	.507070	1.4% $1.492929 - 1.507070 = -0.0141414 \dots$
Don't Pass Bet	2,3- win 12-roll again 7,11- lose 4,5,6,7,9,10- this is the point shooter rolls again until either 7 or the point comes up if the point is first then lose if 7 is first then win	\$1			1.4%
Field Bet	The next roll is 2,3,4,9,10,11,12-win 5, 6, 7, 8-lose	\$2 for 2 or 12 \$1 otherwise	$\frac{1}{18} \text{win} \2 $\frac{17}{18} \text{lose} \1	$\frac{5}{9}$	5.6% $\frac{2}{18} + \frac{7}{18} - \frac{10}{18} = \frac{1}{18} = 0.055\dots$
Any Craps	The next roll is 2, 3, 12-win 4, 5, 6, 7, 8, 9, 10, 11- lose	\$7			
Any 7	The next roll is a 7- win 2,3,4,5,6,8,9,10,11,12- lose	\$4			
Big 6	If a 6 is rolled before a 7-win If a 7 is rolled before a 6-lose	\$1			
Big 8	If a 8 is rolled before a 7-win If a 7 is rolled before a 8-lose	\$1			
4 Hardway	If a pair of twos is rolled before a 7 or before a 1 and 3- win otherwise lose	\$7			
10 Hardway	If a pair of fives is rolled before a 7 or before a 4 and a 6- win otherwise lose	\$7			
6 Hardway	If a pair of threes is rolled before a 7 or before 2&4 or 1&5-win otherwise lose	\$9			
8 Hardway	If a pair of fours is rolled before a 7 or before 2&6 or 3&5-win otherwise lose	\$9			

$$P(\text{win "don't pass" bet}) = P(\text{losing Pass bet} \mid \text{don't roll } 12)$$

$$\frac{P(\text{losing pass bet \& not roll } 12)}{P(\text{not roll } 12)} = \frac{.50707 \dots - \cancel{.50}}{\cancel{35/36}}$$

$$= .492\cancel{9} \dots$$

$$P(\text{losing "don't pass" bet}) = P(\text{win pass bet} \mid \text{don't roll } 12)$$

$$\frac{P(\text{win pass bet \& don't roll } 12)}{P(\text{don't roll } 12)}$$

$$= \frac{.4929 \dots}{\cancel{35/36}} = .50707 \dots$$

- (4) Find the plaintext corresponding to the ciphertext $PYRA$ given that it was encrypted using the Hill substitution cipher ($\text{mod } 29$) 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

$$\begin{pmatrix} 3 & 5 \\ a & b \end{pmatrix}$$

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**.

- (a) Find the encrypting matrix.
 - (b) Find the decrypting matrix.
 - (c) Find the plaintext if we know the ciphertext **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.

$$\begin{bmatrix} -5 & 3 \\ 5 & 19 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 3b - 5a \equiv 17 \pmod{26} \\ 19b + 5a \equiv 9 \pmod{26} \end{bmatrix}$$

$$\begin{bmatrix} 20 & 0 \\ 0 & 20 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 19 & -3 \\ -5 & -5 \end{bmatrix} \begin{bmatrix} -5 & 3 \\ 5 & 19 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 19 & -3 \\ -5 & -5 \end{bmatrix} \begin{bmatrix} 17 \\ 9 \end{bmatrix} = \begin{bmatrix} 11 & -1 \\ 19 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 9 \end{bmatrix} = \begin{bmatrix} 10 \\ 0 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} f \\ t \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix}$$

$$20a \equiv 10 \pmod{26} \Rightarrow a \equiv 7, 20$$

$$20b \equiv 0 \pmod{26} \Rightarrow b \equiv 13, 0$$

$$\begin{bmatrix} 3 & 5 \\ a & b \end{bmatrix} \begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 6 \\ 9 \end{bmatrix} = 15 + 17 \pmod{26}$$

$$= 5a + 19b \pmod{26}$$

Encrypting matrix: $\begin{bmatrix} 3 & 5 \\ 7 & 13 \end{bmatrix} \left(\begin{bmatrix} 3 & 5 \\ 7 & 0 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 20 & 13 \end{bmatrix} \right) \begin{bmatrix} 3 & 5 \\ 20 & 0 \end{bmatrix}$