Written test n.1 (A)

1. Solve for x. $3x + 7 \equiv 11 \pmod{14}$.
2. Given the Bézout identity $3 \cdot 4 + 11 \cdot (-1) = 1$ find $3^{-1} \in \mathbb{Z}_{11}$.
3. Which integers are invertible under multiplication modulo 12 and why?
4. Explain why $6x \equiv 5 \pmod{10}$ has no solutions.
5. There are two events A and B with probability $\frac{1}{2}$. The probability that both A and B happen is $\frac{1}{100}$. What is the probability that none of these two events happen?
6. There are two events A and B with probability $\frac{1}{3}$. The probability that both A and B happen is $\frac{1}{12}$. What is the conditional probability $\mathsf{P}[A \mid B]$?
7. Explain how you calculate the index of coincidence for input `ABABBC`?
8. Find the mutual index of coincidence for the strings `AABBC` and `FFAEE`

Written test n.1 (B)

1. Solve for x. $6x \equiv 3 \pmod{9}$.
2. Write out the Bézout identity for integers 9 and 39.
3. How many elements are invertible under multiplication in $\mathbb{Z}_{99}$?
4. Explain why $\varphi(p) = p - 1$ holds for any prime p.
5. There are two events A and B with probability $\frac{1}{3}$. The probability that both A and B happen is $\frac{1}{6}$. What is the probability that none of these two events happen?
6. There are two events A and B with probability $\frac{1}{2}$. The probability that both A and B happen is $\frac{1}{3}$. What is the conditional probability $\mathsf{P}[A \mid B]$?
7. Find the index of coincidence **IC** for the string `CBCCCBAD`
8. Find the mutual index of coincidence for the strings `CBCC` and `AGCC`

Solutions (A)

1. If $3x+7 \equiv 11 \pmod{14}$, then $3x \equiv 4 \pmod{14}$ and hence $x = 4 \cdot 3^{-1} \mod 14$. As from the Bezout identity $(-9)\cdot 3 + 2 \cdot 14 = 1$ we imply $3^{-1} \equiv -9 \equiv 5 \pmod{14}$, we have $x = 5 \cdot 4 \mod 14 = 20 \mod 14 = \mathbf{6}$.

2. From $3 \cdot 4 + 11 \cdot (-1) = 1$, it follows that $3^{-1} \mod 11 = \mathbf{4}$.

3. The integers $1, 5, 7, 11$ from $\mathbb{Z}_{12}$ are invertible modulo 12 because they are relatively prime to 12. Thereby, any integer n is invertible modulo 12, if and only if it is expressible in the form $n = 1 + 12k$, $n = 5 + 12k$, $n = 7 + 12k$, or $n = 11 + 12k$, for any $k \in \mathbb{Z}$.

4. The equation $6x \equiv 5 \pmod{10}$ has no solutions because $\gcd(6, 10) = 2$ does not divide 5.

5. $\mathsf{P}[\overline{A \cup B}] = 1 - \mathsf{P}[A \cup B] = 1 - \mathsf{P}[A] - \mathsf{P}[B] + \mathsf{P}[A \cap B] = 1 - \frac{1}{2} - \frac{1}{2} + \frac{1}{100} = \mathbf{\frac{1}{100}}$.

6. $\mathsf{P}[A \mid B] = \frac{\mathsf{P}[A \cap B]}{\mathsf{P}[B]} = \frac{1/12}{1/3} = \frac{3}{12} = \mathbf{\frac{1}{4}}$.

7. $\mathrm{IC}(\texttt{ABABBC}) = \frac{n_A(n_A-1)}{n(n-1)} + \frac{n_B(n_B-1)}{n(n-1)} + \frac{n_C(n_C-1)}{n(n-1)} = \frac{2}{30} + \frac{6}{30} + \frac{0}{30} = \frac{8}{30} = \mathbf{\frac{4}{15}} \approx \mathbf{0.267}$, where n_A, n_B, n_C are the numbers of A, B, and C, respectively, and $n = 6$ is the length of the string.

8. The mutual index of coincidence for the strings AABBC and FFAEE is

$$\mathrm{IC}(\texttt{AABBC}, \texttt{FFAEE}) = \frac{n_A \cdot n'_A}{n \cdot n'} = \frac{2 \cdot 1}{5 \cdot 5} = \mathbf{\frac{2}{25}} = \mathbf{0.08} \ .$$

Solutions (B)

1. As $\gcd(6, 9) = 3$ divides 3 the equation is solvable and the solutions are exactly the solutions of $2x \equiv 1 \pmod{3}$, which implies $x = \mathbf{2}$.

2. We compute $\gcd(9, 39)$ using the extended Euclidean algorithm:

9	39	a	b
9	3	a	$b - 4a$
0	3	$a - 3(b - 4a)$	$b - 4a$

Hence, $\gcd(9, 39) = 3$ and the Bezout identity is $(-\mathbf{4}) \cdot \mathbf{9} + \mathbf{1} \cdot \mathbf{39} = \mathbf{3}$.

3. The number of invertible elements in $\mathbb{Z}_{99}$ is $\varphi(99) = \varphi(3^2 \cdot 11) = (3^2 - 3^1) \cdot (11 - 1) = \mathbf{60}$.

4. If p is prime, then all non-zero elements $x \in \mathbb{Z}_p$ are invertible because $\gcd(x, p) = 1$. Hence, $\varphi(p) = p - 1$.

5. $\mathsf{P}[\overline{A \cup B}] = 1 - \mathsf{P}[A \cup B] = 1 - \mathsf{P}[A] - \mathsf{P}[B] + \mathsf{P}[A \cap B] = 1 - \frac{1}{3} - \frac{1}{3} + \frac{1}{6} = \mathbf{\frac{1}{2}}$.

6. $\mathsf{P}[A \mid B] = \frac{\mathsf{P}[A \cap B]}{\mathsf{P}[B]} = \frac{1/3}{1/2} = \mathbf{\frac{2}{3}}$.

7. $\mathbf{IC}(\texttt{CBCCCBAD}) = \frac{n_A(n_A-1)}{n(n-1)} + \frac{n_B(n_B-1)}{n(n-1)} + \frac{n_C(n_C-1)}{n(n-1)} + \frac{n_D(n_D-1)}{n(n-1)} = \frac{0}{56} + \frac{2}{56} + \frac{12}{56} + \frac{0}{56} = \frac{14}{56} = \mathbf{\frac{1}{4}} = \mathbf{0.25}$, where n_A, n_B, n_C, n_D are the numbers of A, B, C, and D, respectively, and $n = n' = 4$ is the length of both strings.

8. The mutual index of coincidence for the strings CBCC and AGCC is:

$$\mathrm{IC}(\texttt{CBCC}, \texttt{AGCC}) = \frac{n_C \cdot n'_C}{n \cdot n'} = \frac{3 \cdot 2}{4 \cdot 4} = \frac{6}{16} = \mathbf{\frac{3}{8}} = \mathbf{0.375} \ .$$