CSci 4554 Assignment 4

Due Friday, February 26th in class

Problem 1 (20 points). Consider a procedure of recognizing whether a given integer p appears among the first $k = \log_2 p$ numbers generated by a pseudo-random number generator with an unknown seed $x \in_U [1, m]$, where m is a known constant. The function used by the generator is deterministic and runs in time polynomial in k. The recognition procedure works by generating a random seed and testing whether p is among the first k numbers generated starting at this seed.

Question 1 (5 points). Give a step-by-step algorithm for recognizing p using the procedure given above.

Question 2 (8 points). Let R_k denote the set of numbers that are generated in at most k steps by the pseudo-random number generator with any seed x, as described above. Let single-quoted string denote the result of the recognition algorithm in question 1. Compute the probabilities $\epsilon = \text{Prob}['p \in R'_k \mid p \in R_k]$ and $\delta = \text{Prob}['p \in R'_k \mid p \notin R_k]$. Show all your work.

Question 3 (2 points). Is the algorithm Monte Carlo, Las Vegas, or Atlantic City? Please explain using your answer to question 2.

Question 4 (5 points). Prove that the algorithm is in *PP* (Probabilistic Polynomial) class. Would is still be in *PP* if we change k to be equal to p? Please explain your answer.

Problem 2 (15 points). Suppose that in the Quantum Key Distribution algorithm (as given in the book) Alice and Bob use the rectilinear polarizer (and, consequently, observer) $\frac{1}{3}$ of the time, and diagonal polarizer (observer) $\frac{2}{3}$ of the time. This is known to Eve. How does this affect the completeness and soundness probabilities (ϵ and δ)? Show all your work.

Will the modified algorithm still be in the *BPP* class? Please explain your answer using the computed probabilities.

Problem 3 (9 points). Find inverses of elements in a given group with a given operation. Recall that the inverse of a is defined as a^{-1} such that $a \circ a^{-1} = e$, where e is the group identity.

1. Find inverses of $3, -1/5, -1$ in $(\mathbb{R}/\{0\}, \times)$ ($\times$ stands for multiplication).
2. Find inverses of $0, 1, 7$ in the "clock group" $(\mathbb{Z}_{12}, +(mod\ 12))$
3. Find inverses of $7, 8, 11$ in $\mathbb{Z}^*_{15}$ (see p. 141 for the definition of $\mathbb{Z}^*_n$).

Problem 4 (4 points). Find all subgroups of $(\mathbb{Z}_{15}, +(mod\ 15))$ and of $\mathbb{Z}_{15}^*$.

Problem 5 (8 points). Find the order of the following elements in the given groups:

1. $3, 4, 5$ is $\mathbb{Z}_8$.
2. $3, 7$ in $\mathbb{Z}_8^*$.
3. $2, 4, 5$ in $\mathbb{Z}_7^*$.

Problem 6 (8 points). Which of the following groups are cyclic? If a group is cyclic, show at least one of its generators and show how each element is generated. If it is not cyclic, please briefly explain why none of its elements are a generator. It would help to write out all group elements first.

1. $\mathbb{Z}_8$
2. $\mathbb{Z}_4^*$
3. $\mathbb{Z}_2^*$ (how many elements does the group have?)
4. $\mathbb{Z}_5^*$