11. Интерактивные доказательства, 0-knowledge протоколы

1. Придумайте 0-knowledge протокол для доказательства того, что Мерлин знает решение некоторого судоку $n^2 \times n^2$.
Правила такие: доска $n^2 \times n^2$ разбивается на непересекающиеся блоки $n \times n$. В каждой ячейке может быть число от 1 до n. Изначально доска заполнена некоторым количеством чисел, которые в процессе заполнения менять нельзя. В каждом столбце, строке и блоке все числа должны быть разные.
2. Докажите, что $\mathbf{AM} = BP \cdot \mathcal{NP}$.
3. Докажите, что $\#3SAT_D \in IP$. Для этого:

- Превратите булевы формулы в многочлены, значение которых совпадает с булевой формулой на одинаковом наборе. Такая операция называется арифметизацией.
- Определите, как с помощью арифметизации получить число выполняющих наборов.
- Постройте интерактивное доказательство того, что число выполняющих наборов действительное такое. Для этого понадобятся вычисления по модулю p.
- Оцените вероятность принятия для верификатора.

4 (Доп). Все Доп+ задачи.