

CIMPA research school on Group Actions in Arithmetic and Geometry

Finite fields – tutorial session

February 26, 2020

1. For each prime $p \leq 13$ and also for $p = 31$, list the values $a \in \mathbb{F}_p^\times$ which are primitive roots modulo p (i.e. generators of the cyclic group \mathbb{F}_p^\times). Next, for each a and for $n = 1, 2, \dots, p - 1$, compute a^n . Deduce a table of the discrete logarithm modulo p with respect to the primitive root a .
2. Let $n \in \{1, 2, 3, 4\}$. Among 2^n playing cards, you select one without telling me which one it is. I display some of them and I ask you whether the card you selected is one of them. You answer yes or no.
 - (a) How many questions should I ask in order to know which card you selected?
 - (b) Same problem, but now you are allowed to give me at most one wrong answer, and I want to decide whether or not all your answers were right. If you gave always the right answer, I want to know which card you selected (*error detecting code*).
 - (c) Same problem, again you are allowed to give me at most one wrong answer, but now, I want to know which card you selected, even if one of your answers was wrong (*error correcting code*).
3. Three people are in a room, each has a hat on his head, the colour of which is black or white. Hat colours are chosen randomly. Everybody sees the colour of the hat of everyone else, but not on one's own. People do not communicate with each other. Everyone tries to guess (by writing on a piece of paper) the colour of their hat. They may write: Black/White/Abstain.
The people in the room win together or lose together as a team. The team wins if at least one of the three persons does not abstain, and everyone who did not abstain guessed the colour of their hat correctly.
 - (a) What could be the strategy of the team to get the highest probability of winning? What is this probability?
 - (b) Same questions with seven people.