ABSTRACT

Secret sharing in the Russian cards

A problem in the 2000 Mathematics Olympiad held in Moscow was the following:

Alice, Bob and Cathy each draw cards form a deck of seven cards. Alice and Bob get three cards, Cathy gets only one. The three know which cards were originally in the deck, but each player can see only their own cards. Alice and Bob wish to learn each other's cards without Cathy getting any new information about who has which card, however they are only allowed to make public, truthful announcements which will be heard and understood by Cathy. Can Alice and Bob achieve this? What announcements should they make?

This is the Russian Cards Problem, and it turns out Alice and Bob can, indeed, share the secret of which cards they hold. However, what would happen if there were more cards, or they were distributed differently? Can Alice and Bob still share their secret? Are there cases when they cannot?

In this talk we will give a series of results which give a partial answer to these questions. Some of these results are based on elementary combinatorics and others borrow tools from additive combinatorics. We will also mention some questions that remain open in the field.