

PROBLEM 3 – Trick

DAY 1 TASK 3
ENGLISH



Student Andrei Heidelbacher
Politehnica University of Timișoara

Solution 1 – 29 points

Let $S = 0 + 1 + \dots + 2N = 2N * (2N + 1) / 2 = N * (2N + 1)$ and $M = 2N + 1$. It is essential to notice that $S \bmod M = 0$. Thus, if we know the sum $S_1 \bmod M$ of all the cards received by the first assistant and the sum $S_2 \bmod M$ of all the cards received by the second assistant, then Dracula's hidden card will be $(0 - S_1 - S_2) \bmod M$. Now, we need to find a protocol through which the assistants can communicate the sum of their cards modulo M .

A protocol is a mapping from every pair of distinct cards (a, b) to a sum $s \bmod M$. A protocol is well-defined if every pair (a, b) is mapped to at most one sum $s \bmod M$. A protocol is admissible if, for any set of N cards with sum $s \bmod M$, there is at least one pair of cards (a, b) contained in this set that is mapped to the sum $s \bmod M$.

We can find well-defined, but not admissible protocols using greedy solutions and improve them using backtracking. Various heuristics to speed-up the process might be needed. Once an admissible protocol is found, we can preprocess it in the program source.

Solution 2 – 78 points

We will present a protocol and then we will prove that it is well-defined and admissible.

Let $(a, b) + s$ denote the pair of cards $(a + s \bmod M, b + s \bmod M)$. We will solve separately two cases.

- N is even

The pairs $(2N, 1) + s, (2N - 1, 2) + s, (2N - 2, 3) + s, \dots, (N + 2, N - 1) + s$ will be mapped to the sum $s \bmod M$. Additionally, the pairs $(0, 2N) + s, (0, 1) + s, (N, 2) + s, (N, 2N - 1) + s, (4, N + 1) + s$ and $(2N - 3, N + 1) + s$ will be mapped to the sum $s \bmod M$. Let's analyze the differences $b - a \bmod M$ for the considered (a, b) pairs: the differences for the first $N - 1$ pairs are $2 \bmod M, 4 \bmod M, 6 \bmod M, \dots, 2N - 2 \bmod M$, and the difference for the pair $(0, 2N)$ is $2N \bmod M$ (all these differences are even and distinct); the differences for the remaining five pairs are $1 \bmod M, N + 3 \bmod M, N - 1 \bmod M, N - 3 \bmod M, N + 5 \bmod M$ (all these differences are odd and distinct, because $N \geq 6$). Thus, for any sum $s \bmod M$, all the pairs (a, b) mapped to this sum have a different $b - a$ difference and can be uniquely identified using this difference and the sum $s \bmod M$.

- N is odd

The pairs $(1, 2N) + s, (2, 2N - 1) + s, (3, 2N - 2) + s, \dots, (N - 1, N + 2) + s$ will be mapped to the sum $s \bmod M$. Additionally, the pairs $(0, 2N) + s, (0, 1) + s, (N, 2) + s, (N, 2N - 1) + s, (4, N + 1) + s$ and $(2N - 3, N + 1) + s$ will be mapped to the sum $s \bmod M$. Let's analyze the differences $b - a \bmod M$ for the considered (a, b) pairs: the differences for the first $N - 1$ pairs are $2N - 1 \bmod M, 2N - 3 \bmod M, 2N - 5 \bmod M, \dots, 3 \bmod M$, and the difference for the pair $(0, 1)$ is $1 \bmod M$ (all these differences are odd and distinct); the differences for the remaining five pairs are $2N \bmod M, N + 3 \bmod M, N - 1 \bmod M, N - 3 \bmod M, N + 5 \bmod M$ (all these differences are even and distinct, because $N \geq 6$). Thus, for any sum $s \bmod M$, all the pairs (a, b) mapped to this sum have a different $b - a \bmod M$ difference and can be uniquely identified using this difference and the sum $s \bmod M$.

PROBLEM 3 – Trick

DAY 1 TASK 3
ENGLISH



Considering the two cases analyzed, we can say the protocol is well-defined.

Let's assume we have a set of N cards with the sum $s \pmod M$ and that there are no pairs $(a, b) + s$ contained in this set. We can have at most one card in this set from each of the triplets $(0, 1, 2N) + s$, $(2, N, 2N - 1) + s$, $(4, N + 1, 2N - 3) + s$. Otherwise, we would have two cards to create a pair from the last six considered in the previous two cases. Thus, we can take at most three cards from these triplets. Also, we can have at most one card from each of the pairs $(3, 2N - 2) + s$, $(5, 2N - 4) + s$, $(6, 2N - 5) + s$, $(7, 2N - 6) + s$, ..., $(N - 1, N + 2) + s$ (in total, $N - 4$). As a consequence, we can have at most $N - 1$ cards from the analyzed pairs and triplets. However, these analyzed cards make a complete partition of the set $\{0, 1, 2, \dots, 2N\}$. Because the initial set contains N cards, we reached a contradiction. Thus, the protocol is admissible.

We can build the matrix that maps the considered (a, b) pairs to a sum $s \pmod M$.

This solution has a time complexity of $O(N^2)$ and a space complexity of $O(N^2)$.

Solution 3 – 100 points

Let the equivalence class $C(a, b) = \{(x, y) \mid y - x \pmod M = b - a \pmod M\}$. For a given sum $s \pmod M$, all pairs mapped to this sum have distinct $b - a$ differences. Thus, a sum can have at most one pair mapped to it in every equivalence class. If we know the sum $s \pmod M$, we can check in time $O(N)$ every equivalence class and find a fit pair. If we know the pair (a, b) , we verify in time $O(N)$ all the pairs from the same equivalence class and find the sum $s \pmod M$.

This solution has a time complexity of $O(N)$ and a space complexity of $O(N)$.