

Problem D

Digital Content Protection

Problem ID: content

Time Limit: 2 seconds

Dan is working for a digital content protection company, which is responsible for the content protection of blu-ray discs based on a standard called Anti Content Misuse (ACM).



Picture from Wikimedia Commons

The ACM standard works as follows. Assume there are 2^n blu-ray drives/players. We represent these 2^n drives as the leaves of a complete binary tree of height n , so that each root-to-leaf path consists of n edges. Each node u in this binary tree is assigned an identifier number and contains a random key k_u . The identifier numbers are assigned as follows. The root, r , is assigned 1. In addition, the left and right children of an internal node having number i are assigned numbers $2i$ and $2i + 1$, respectively. This scheme assigns a distinct number to each node in the tree. The keys contained in the nodes are unknown to blu-ray users, but they are available to blu-ray drive manufacturers. Each blu-ray player is assigned the identifier number i ($2^n \leq i \leq 2^{n+1} - 1$) of its corresponding leaf in the tree. A manufacturer of blu-ray drives embeds the keys associated with the nodes in the path from the root to leaf number i in player number i .

To encrypt the content of a blu-ray disc, the company in charge creates a random key k called the master key. First, they encrypt k with the key k_r (recall r is the root node of binary tree) and write it on the disc as a header. Then, they encrypt the content with k , and write the encrypted data on the blu-ray disc. A blu-ray drive first decrypts the header using key k_r embedded in it and recovers the master key k and then, decrypts the content using the key k .

Unfortunately, the keys embedded in a set of blu-ray drives, R , are exposed by hackers and published on the web. As a result, we cannot encrypt the master key k using any of these exposed keys. For example, since all blu-ray drives contain k_r , the encryption scheme above does not work any more. There is a solution oversaw for this situation in the ACM standard. At the cost of a larger header, the industry can safely encrypt the content of a new blu-ray disc. They carefully choose a subset of unexposed keys K in the binary tree such that all blu-ray drives, except for drives in R , have at least one of the keys in K . They encrypt the master key k with each key $k' \in K$ and put the result in the header (i.e., there are $|K|$ ciphertexts in the header). Now, each active blu-ray drive can decrypt at least one of the ciphertexts in the header and can recover the master key k . Dan needs your help to determine a subset of keys K with minimum cardinality (which results in the smallest header) given the identifiers of hacked drives.

Input

The input consists of a single test case. A test case consists of two lines. The first line contains two integers n and $|R|$, where $1 \leq n \leq 62$ and $1 \leq |R| \leq 1000$. $|R|$ is the cardinality of R , the set of exposed drives. The second line contains $|R|$ integers, which are the identifiers of exposed blu-ray drives. You can assume that there is at least one blu-ray drive not hacked.

Output

Display the identifiers of nodes corresponding to the keys in K , satisfying the above requirements and having minimum cardinality, in increasing order and separated with single spaces.

Sample Input	Sample Output
2 1 5	3 4

Sample Input	Sample Output
3 3 10 11 12	4 7 13