

# 10861 Security By Ambiguity

Many of you have probably had some contact with cryptography (don't worry if you haven't, though, no deep knowledge of cryptography is needed here). In this problem, we will concern ourselves with an encryption scheme consisting of a composition of two different ciphers, a so called *permutation cipher*, and a so called *substitution cipher*.

In a permutation cipher of block length n, we choose as a secret key a permutation  $\pi = \pi_1 \ \pi_2 \dots \pi_n$  of the integers 1 to n. We then encrypt a block of n symbols by permuting them according to  $\pi$ , i.e. the encryption of  $a = a_1 a_2 \dots a_n$  would be  $a_{\pi_1} \ a_{\pi_2} \dots a_{\pi_n}$ .

The substitution cipher, on the other hand, concerns itself with the alphabet of the symbols we use to encode a message. Let the size of the alphabet be m, and assume without loss of generality that the m symbols of the alphabet are the integers 1 to m. We then choose a permutation  $\tau = \tau_1 \ \tau_2 \dots \tau_m$  of the alphabet, and simply encrypt a symbol  $a_i$  by  $\tau_{a_i}$ , i.e. we substitute each symbol according to the permutation  $\tau$ .

Composing these two ciphers is straight-forward; simply do both the permutation of the symbols according to  $\pi$ , and the substitution of the symbols according to  $\tau$ . Breaking this combined cipher is usually (slightly) more difficult than breaking either one of the two simpler ciphers.

Peter is a clever kid with a very limited memory, and he would like to have the combined strength of these two ciphers while only having to remember one permutation as his secret key, rather than two. He has realised that the two different steps are (in some vague sense) independent, and has thus gotten the idea to consider the special case of the above scheme where n=m, and  $\tau=\pi^{-1}$  (the inverse of  $\pi$ ; simply choosing  $\tau=\pi$  seems too risky, even for Peter). This way, he only has one permutation to remember, while still getting both the permutation step and the substitution step.

As an example, consider using n=m=5, and the permutation  $\pi=4\ 2\ 1\ 3\ 5$ . The inverse  $\tau$  of  $\pi$  is 3 2 4 1 5. Take the message block 2 5 3 4 2. Applying the permutation cipher (with secret key  $\pi$ ) transforms the message to 4 5 2 3 2, and applying the substitution cipher (with secret key  $\tau$ ) gives 1 5 2 4 2, which is the encryption of the message 2 5 3 4 2 using Peter's scheme (with secret key  $\pi=4\ 2\ 1\ 3\ 5$ ).

However, you, being an even more clever kid than Peter, doubt the security of Peter's new scheme, and as a step in investigating this, you should write a program which, given an encrypted block, determines the number of possible inputs which could have been encrypted to that block (assuming that any key is possible).

## Input

Input consists of several test cases. Each test case begins with an integer  $1 \le n \le 50$ , denoting both the length of an input block and the size of the alphabet. Then follows a line containing n integers between 1 and n, representing the encryption of some input block.

Input is terminated by a case where n = 0.

#### Output

For each test case, output a line containing the number of different inputs that could have been used. You may assume that the answer will fit in a 64-bit signed integer.

### Sample Input

## **Sample Output**

1 5 120