

## Problem 2: Hilbert's Hotel Solution

We want to determine whether  $n + 1$  is prime. To just calculate whether  $n + 1$  is prime with the usual calculations, will become very time expensive when  $n$  becomes large. We are also given the number of ways we can order the  $n$  guests over the  $n$  rooms. First let us reason what this number is.

If  $n = 1$ , then we have only one guest and one room, so there is one way to order them.

If  $n = 2$ , then there are 2 guest and 2 rooms. For the first guest, we have 2 rooms to chose from. Once we have appointed the first guest to their room, the second guest automatically gets the other room. Thus we have 2 ways of appointing guests to the room.

If  $n = 3$ , then there are 3 guests and 3 rooms. For the first guest, we have 3 rooms to chose from. Once we have appointed the first guest to their room, we have still 2 rooms to choose from to appoint the second guest to. Once appointed the first two guests, we cannot choose anymore for the third guest and we have to appoint him/her to the only room left. Thus we have  $3 \cdot 2 = 6$  ways of appointing the guests to the room.

This same method we can use for  $n$  guests and  $n$  rooms. For the first guest, we can choose  $n$  rooms for appointing. After appointing the first guest, for the second guest, we have  $n - 1$  rooms we can appoint the guest to. When we go on like this, we see that there are  $n \cdot (n - 1) \cdot \dots \cdot 2 \cdot 1 = n!$  ways of appointing the  $n$  guests to the room.

We are given thus  $n! \bmod (n + 1)$ . Now we can note that if  $n + 1$  is not prime, we can write it as a product  $n + 1 = a \cdot b$  with  $a, b < (n + 1)$ . Now as  $a, b < (n + 1)$ , these numbers occur in  $(n + 1)$ . Now, as long as we have  $a \neq b$ , this will result in  $n! \bmod (n + 1) \equiv 0$ . Now see that for every  $n > 2$  not prime, except for  $n = 4$ , we can find such  $a, b$ . Note that when  $n + 1$  is prime, there do not exist such factors, so  $n! \bmod (n + 1)$  is not equal to 0 (in fact,  $n! \bmod (n + 1) \equiv n$ , see [https://en.wikipedia.org/wiki/Wilson's\\_theorem](https://en.wikipedia.org/wiki/Wilson's_theorem)).