

1. Recall the Euclid-GCD( $a, b$ ) algorithm discussed in the lectures for finding the gcd of two integers  $a$  and  $b$ . Prove the following theorem:

**Theorem (Lame's theorem):** *For any integer  $k \geq 1$ , if  $a > b \geq 1$  and  $b < F_{k+1}$ , then the call Euclid-GCD( $a, b$ ) makes fewer than  $k$  recursive calls.*

Here  $F_k$  denotes the  $k^{\text{th}}$  number in the Fibonacci sequence  $(0, 1, 1, 2, 3, 5, 8, 13, \dots)$

2. You must have seen the following puzzle: You are given two jugs, one of capacity 5 liters and the other of capacity 3 liters, and an unlimited source of water. Using only these two jugs, can you make sure the larger jug contains exactly 4 liters of water?

1. Solve the above puzzle.

2. Now, suppose you are given two jugs with capacities  $S$  and  $L$ , where  $S$  and  $L$  are positive integers. Design an algorithm that takes as input a positive integer  $B$  and outputs "Not Possible" if it is not possible to leave  $B$  liters of water in any of the two jugs, and otherwise it outputs the precise way to make sure that one of the jugs has exactly  $B$  liters of water.

3. Discuss the closure property of multiplication modulo  $m$  with respect to  $\mathbb{Z}_m^*$ .

4. Let  $N = p \cdot q$  for primes  $p$  and  $q$ . Let  $e, d \in \mathbb{Z}_{\phi(N)}^*$  such that  $e \cdot d \equiv 1 \pmod{\phi(N)}$ , where  $\phi(N) = (p-1) \cdot (q-1)$ . In the lectures, we have seen that  $\forall M \in \mathbb{Z}_N^*, (M^e)^d \equiv M \pmod{N}$ . Show that this holds for all  $M \in \mathbb{Z}_N$ .

5. Show that we can easily factor  $N$  when we know that  $N$  is the product of two primes,  $p$  and  $q$ , and we know the value of  $(p-1)(q-1)$ .

6. We will use the following definition of cyclic groups.

**Definition (Cyclic group):** *Let  $G$  be a group and let  $a$  be any element of this group. Let  $\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbb{Z}\}$ . The group  $G$  is called a cyclic group if there exists an element  $a \in G$  such that  $G = \langle a \rangle$ . In this case,  $a$  is called the generator of  $G$ .*

Show that for small primes  $p = 2, 3, 5, 7, 11$ ,  $\mathbb{Z}_p^*$  is a cyclic group.