

# Homework 1 - Solutions

## 1. Extended Euclidean Algorithm

The Extended Euclidean Algorithm is used to find the greatest common divisor (GCD) of two integers, and it also helps to express the GCD as a linear combination of the two integers. The algorithm not only computes the GCD of two numbers  $a$  and  $b$ , but also finds integers  $x$  and  $y$  such that:

$$ax + by = \gcd(a, b)$$

### Pseudocode:

```
function extendedEuclidean(a, b)
    if b == 0
        return (a, 1, 0) // gcd(a, 0) = a, x = 1, y = 0
    (gcd, x1, y1) = extendedEuclidean(b, a % b)
    x = y1
    y = x1 - (a // b) * y1
    return (gcd, x, y)
```

## 2. Correctness of Euclid's Formula

The correctness of Euclid's formula hinges on two key properties of divisibility:

1. Divisibility Property: If a number  $d$  divides both  $m$  and  $n$ , it also divides the remainder  $r$  when  $m$  is divided by  $n$ .

In other words, if  $d$  divides both  $m$  and  $n$ , then it must also divide  $m - q \cdot n$ , where  $q$  is the quotient when dividing  $m$  by  $n$ .

This means:  $d \mid m$  and  $d \mid n \Rightarrow d \mid (m - q \cdot n)$

And since  $m \% n = m - q \cdot n$ , this means that  $d$  divides  $m \% n$ .

2. Reduction Step: If a number  $d$  divides both  $n$  and  $m \% n$ , then it also divides  $m$ .

This follows from rearranging the division formula:

$$m = n \cdot q + r \quad \text{where } r = m \% n$$

Since  $d$  divides both  $n$  and  $r = m \% n$ , it must divide  $m$ .

Thus, the Euclidean algorithm progressively reduces the problem of finding the GCD of  $m$  and  $n$  to finding the GCD of smaller and smaller pairs, until eventually one of the numbers become 0. At that point, the GCD is the other number.

### 3. Locker Doors Problem

At the start, all the locker doors are closed. A door will be open at the end if it is touched (or toggled) an odd number of times. A door gets touched every time its number is a multiple of the pass number. For example, door 6 gets touched on passes 1, 2, 3, and 6.

Each door gets touched as many times as it has divisors (numbers that divide it evenly). For most numbers, divisors come in pairs, like 1 and 12 for 12, or 2 and 6 for 12. But for perfect squares (like 16), one divisor doesn't have a pair (4 divides 16, but there's no pair for 4).

That means only doors whose numbers are perfect squares (like 1, 4, 9, 16, etc.) will be touched an odd number of times, so those are the doors that stay open.

The number of open doors is the same as the number of perfect squares up to  $n$ , which is the numbers from 1 to  $\sqrt{n}$ . So, if  $n=10$ , only doors 1 and 4 will be open because they are perfect squares.

### 4. Bridge Puzzle

Person 1 (1 minute) and Person 2 (2 minutes) cross (2 minutes total).

Time elapsed: 2 minutes

Person 1 (1 minute) returns with the flashlight (1 minute).

Time elapsed: 3 minutes

Person 5 (5 minutes) and Person 10 (10 minutes) cross (10 minutes total).

Time elapsed: 13 minutes

Person 2 (2 minutes) returns with the flashlight (2 minutes).

Time elapsed: 15 minutes

Person 1 (1 minute) and Person 2 (2 minutes) cross again (2 minutes total).

Time elapsed: 17 minutes

### 5. Complexity Proofs

To show that  $3n + 5 \log n$  is  $\Omega(n)$ , we need to prove that there exists a constant  $c > 0$  and  $n_0$  such that:  $3n + 5 \log n \geq c n$  for all  $n \geq n_0$

Clearly, as  $n$  grows larger, the term  $3n$  dominates over  $5 \log n$ , let  $c=3$ ,  
 $3n + 5 \log n \geq 3n$ . This inequality holds good for  $n \geq 1$ , so  $n_0=1$

Is  $3n+5\log n$  in  $O(n)$ ? Yes,  $3n+5\log n$  is in  $O(n)$ , because the  $n$ -term dominates the logarithmic term as  $n$  grows. Formally, there exists a constant  $c > 0$  and  $n_0$  such that:  
 $3n+5\log n \leq cn$  for all  $n \geq n_0$

for large  $n$ ,  $3n+5\log n$  behaves similarly to  $3n$ , let  $c=4$ ,  $3n+5\log n \leq 4n$ . This inequality holds good for all  $n \geq 1$ , so  $n_0=1$