Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 1
Version 05.04.2019

General remark: Whenever you don't remember definitions or algorithms like the extended Euclidean Algorithm, group, field etc. do a search in literature or the web.

Exercise 1.

Prove by induction that every integer $n \geq 2$ can be written as a product of prime numbers. This product is called the **prime factorization** of the number n and is up to ordering the factors unique. For example $90 = 2 \cdot 3^2 \cdot 5$.

Exercise 2.

The **greatest common divisor** (*gcd*, for short) of $a \in \mathbb{N}$ and $b \in \mathbb{N}$, denoted by $gcd(a, b)$, is the largest positive integer that divides both a and b.
For the pairs of integers a, b given below use the extended Euclidean Algorithm to find the *gcd* g and integers s and t satisfying $g = as + bt$:

i) $a = 13$, $b = 32$,

ii) $a = 40$, $b = 148$ and

iii) $a = 55$, $b = 300$.

Exercise 3.

Show that $(\mathbb{Z}_n, +)$, the integers modulo $n \in \mathbb{N}$ with addition, is an abelian group, where $\mathbb{Z}_n$ is the set $\{0, 1, ..., n - 1\}$ and the rule for addition $+$ is defined as $a + b := (a + b) \ mod \ n$ for $a, b \in \mathbb{Z}_n$.
Recall: A **group** is a 2-tuple $(G, \circ)$ consisting of a nonempty set G together with a binary operation $\circ : G \times G \to G$ that together satisfy the following conditions: Associativity of the group operation $\circ$, existence of the neutral element and existence of an inverse for each $a \in G$.

Exercise 4.

(a) Show that $(\mathbb{Z}_n^*, \cdot)$, the integers modulo $n \in \mathbb{N}$ with multiplication, is an abelian group, where $a \in \mathbb{Z}_n$ is an element of $\mathbb{Z}_n^*$ if and only if a has a multiplicative inverse modulo n and the rule for multiplication $\cdot$ is defined as $a \cdot b := (a \cdot b) \ mod \ n$ for $a, b \in \mathbb{Z}_n$.
How can you use the extended Euclidean Algorithm to find the multiplicative inverse of an element $a \in \mathbb{Z}_n^*$?

(b) Find the multiplicative inverse of 8 modulo 11 using the extended Euclidean Algorithm.

Exercise 5.

Let $n \in \mathbb{N}$, $n > 1$ be fixed.

(a) Suppose every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse modulo n. Show that n is a prime number.

(b) Prove that $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is a prime number.

Recall: For a set F with two binary operations $+ : F \times F \to F$ and $\cdot : F \times F \to F$ we say that $(F, +, \cdot)$ is a **field** if the following holds:

i) $(F, +)$ is an abelian group; its neutral element is denoted by 0,

ii) $(F \setminus \{0\}, .)$ is an abelian group; its neutral element is denoted by 1

iii) the binary operations $+$ and $\cdot$ satisfy the distributive law: $a \cdot (b + c) = ab + ac$ for all $a, b, c \in F$.

Exercise 6.

Let $n \in \mathbb{N}$ be fixed and let $[n] := \{1, ..., n\}$.

(a) Prove that $(S_n, \circ)$ is a group, where S_n is the set of all bijections from $[n]$ to $[n]$ and $\circ$ is the usual function composition.

(b) Is $(S_n, \circ)$ an abelian group?

(c) Give one nontrivial subgroup of $(S_4, \circ)$. How many subgroups does $(S_4, \circ)$ have? Hint: Use Lagrange's theorem.

Recall: $(U, \circ)$ is a subgroup of a group $(G, \circ)$ if $U \subseteq G$ and $(U, \circ)$ is a group.
Lagrange's theorem: If $(G, \circ)$ is a finite group with subgroup $(U, \circ)$, then $|U|$ divides $|G|$.