Number Theory and Cryptography
Math UN3020
New York, 2023/01/25

EXERCISE SHEET 2

Euclidean algorithm

Exercise 1 (12 points)**.** Prove the following properties of the divisibility relation.

(a) $\forall n \in \mathbb{Z},\ 1 \mid n$.

(b) $\forall d \in \mathbb{Z} \setminus \{0\},\ d \mid 0$.

(c) If $d \mid n$ and $n \mid q$, then $d \mid q$.

(d) If $d \mid n$ and $d \mid q$, then $\forall s, t \in \mathbb{Z},\ d \mid (sn + tq)$.

(e) $d \mid 1 \Leftrightarrow d = \pm 1$.

(f) If $d \mid n$ and $n \mid d$, then $d = \pm n$.

Definition 1. An **operation** on a set X is a function

$$* : X \times X \ni (a, b) \to a * b \in X, .$$

In other words, an operation on X is a function that takes in input two elements $a, b \in X$, and gives as output one element of X, denoted by $a * b$.

An operation $*$ on X is said to be **associative** if

$$\forall a, b, c \in X, \quad (a * b) * c = a * (b * c)\,.$$

An operation $*$ on X is said to be **commutative** if

$$\forall a, b \in X, \quad a * b = b * a\,.$$

An **identity** for X is an element $\mathrm{id} \in X$ such that

$$\forall a \in X, \quad a * \mathrm{id} = \mathrm{id} * a = a\,.$$

If the operation $*$ has an identity id, an inverse of an element $a \in X$ is an element $b \in X$ such that

$$a * b = b * a = \mathrm{id}\,.$$

Exercise 2 (5 points)**.** Let $(X, *)$ be a set with an operation $* : X \times X \to X$. Assume that the operation is associative. Prove that if an identity element for $*$ exists in X, then it is unique.
(Hint: proceed by contradiction. Assume that there are two distinct identity elements for $*$, give them names. Compute something using $*$, and find a contradiction.)

Exercise 3 (5 points)**.** Let $(X, *)$ be a set with an operation $* : X \times X \to X$. Assume that the operation is associative and admits an identity element $\mathrm{id} \in X$. Consider an element $a \in X$. Prove that if an inverse of a for $*$ exists in X, then it is unique.
(Hint: proceed by contradiction. Assume that there are two distinct inverse elements of a, give them names. Compute something using $*$, and find a contradiction.)

Exercise 4 (8 points)**.** Compute the quotient and remainder of the Euclidean division between the following pairs of numbers:

(a) $25, 4$.

(b) $28, 6$.

(c) $-28, 6$.

(d) $-14, 3$.

Exercise 5 (6 points)**.** Write all the elements of Div_n, the set of divisors of n, where n is one of the following numbers:

(a) 11.

(b) 18.

(c) 24.

Exercise 6 (8 points)**.** Find $\gcd(a, b)$ and express it as a linear combination of a, b (i.e. write $\gcd(a, b) = sa + tb$ with $s, t \in \mathbb{Z}$) for the following pairs of numbers.

(a) $a = 116, b = -84$.

(b) $a = 85, b = 65$.

(c) $a = 72, b = 26$.

(d) $a = 72, b = 25$.

Exercise 7 (8 points)**.** Given two numbers $a, b \in \mathbb{Z}$. Consider the set of their linear combinations:

$$L_{a,b} = \{ \ n \in \mathbb{Z} \ \mid \ \exists s, t \in \mathbb{Z} \text{ s.t. } n = sa + tb \ \} = \{ \ sa + tb \mid s, t \in \mathbb{Z} \ \}$$

Prove that

$$L_{a,b} = \{ \ n \in \mathbb{Z} \ \mid \ \gcd(a, b) \mid n \ \}$$

Exercise 8 (8 points)**.**

(a) You have a 3-gallon and a 5-gallon jug that you can fill multiple times from a tap. The problem is to measure exactly 4 gallons of water. How do you do it?

(b) You have a 9-gallon and a 12-gallon jug that you can fill multiple times from a tap. The problem is to measure exactly 4 gallons of water. Prove that you cannot do it.