COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/02/15

Exercise Sheet 5

Modular Arithmetic

Exercise 1 (7 points)**.** Prove that every positive integer n can be written as a sum of distinct powers of 2, i.e. that for all $n > 0$, there exist integers $0 \leq i_1 < \cdots < i_h$ such that

$$n = 2^{i_1} + \cdots + 2^{i_h} \, .$$

(Hint: use strong induction. In the inductive step, in order to prove the statement for a number n, consider the largest power of 2 that is smaller or equal to n. Don't forget to check that the powers of 2 you construct are all distinct.)

Exercise 2 (7 points)**.** Consider the triple $([-2, 2], \min, \max)$, where $[-2, 2] \subset \mathbb{R}$ is an interval of real numbers, and min and max are operations on two numbers, respectively taking the minimum and the maximum of two given numbers.

Is $([-2, 2], \min, \max)$ a ring? More precisely, show that $([-2, 2], \min, \max)$ respects properties (1), (2), (3), (5) in the definition of a ring, but that it does not respect property (4).

Exercise 3 (7 points)**.** In our definition of a ring, we required that $0 \neq 1$, i.e. that the additive identity and the multiplicative identity are distinct. Why did we make this assumption?

More precisely, consider $(X, +, \cdot)$, a set with two operations that satisfying Property (1), (2), (4), (5) in the definition of a ring, but does not satisfy (3), i.e. in this X we have $0 = 1$. How many elements can X have?

Exercise 4 (6 points)**.** Prove that, in a ring $(R, +, \cdot)$, if $a, b \in R^*$, then $ab \in R^*$.

Exercise 5 (7 points)**.** Prove that, in a ring $(R, +, \cdot)$,

$$\forall a \in R, \ a \cdot 0 = 0 \, .$$

(Hint: use distributivity.)

Exercise 6 (6 points)**.** Given a fixed $n \in \mathbb{N}$, $n > 1$, prove that $a \equiv b \pmod{n}$ if and only if a and b give the same remainder when divided by n.

Exercise 7 (8 points)**.** Given a fixed $n \in \mathbb{N}$, $n > 1$, prove that, if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then

(a) $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.

(b) $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Exercise 8 (6 points)**.** List the elements of $\mathbb{Z}_{16}^*$ and $\mathbb{Z}_{18}^*$.

Exercise 9 (6 points)**.**

(a) Compute the multiplicative inverse of 131 modulo 1979.

(b) Compute the multiplicative inverse of 127 modulo 1091.

(Hint: write the corresponding Diophantine equation, as we did in class, then find a solution computing the Bézout identity.)