COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Intro to Modern Algebra I
Math GU4041
New York, 2021/01/27

Exercise Sheet 3

Modular Arithmetics

Exercise 1. Prove the following statements.

(a) Every odd natural number is either of the form $4n+1$ or of the form $4n+3$, for some $n \in \mathbb{N}$.

(b) Every odd number of the form $4n+3$ has at least a prime factor of the form $4n+3$.

(c) There is an infinite number of primes of the form $4n+3$.

Exercise 2. Given a fixed $n \in \mathbb{N}$, $n > 1$, the relation

$$a \equiv b \pmod{n}$$

defined as

$$n \mid (a-b)$$

is an equivalence relation.

Exercise 3. 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 4. 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 5. Given a fixed $n \in \mathbb{N}$, $n > 1$, prove that $[a] \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $(a, n) = 1$. (Hint: use Bézout's identity).

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

Exercise 7. Find two permutations $\sigma, \tau \in \mathfrak{S}_4$ that don't commute, i.e. such that

$$\sigma\tau \neq \tau\sigma \,.$$

Then compute the four permutations $(\sigma\tau)^2, \sigma^2\tau^2, (\sigma\tau)^{-1}, \sigma^{-1}\tau^{-1}$.