COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
*New York, 2023/03/08*

EXERCISE SHEET 8

**Lagrange's Theorem**

---

**Exercise 1** (5 points). Solve the following system of congruences.

$$\begin{cases} 2x \equiv 6 & \pmod{15} \\ 4x \equiv 12 & \pmod{50} \\ x \equiv 3 & \pmod{10} \end{cases}$$

**Exercise 2** (6 points). For every one of the rings $\mathbb{Z}_{15}$, $\mathbb{Z}_{14}$, $\mathbb{Z}_{25}$, write an equation of degree 2 that has more than 2 solutions.

**Exercise 3** (5 points). Let $h, k \in \mathbb{Z}$ be coprime integers. Prove that, for every integer $a \in \mathbb{Z}$, we have

$$\gcd(a, hk) = 1 \quad \Leftrightarrow \quad [\ \gcd(a, h) = 1 \quad \text{AND} \quad \gcd(a, k) = 1\ ]\ .$$

**Exercise 4** (4 points). Compute the following values of the totient function:

$$\varphi(30), \varphi(36), \varphi(100), \varphi(360)\,.$$

**Exercise 5** (4 points). Compute the order of the following elements of $\mathbb{Z}_{21}$: $[2], [4], [5], [8]$.

**Exercise 6** (5 points). Consider the case when $g = [5] \in \mathbb{Z}_{13}^*$. Put the elements of $\mathbb{Z}_{13}^*$ into a rectangle, as we did in class during the proof of Lagrange's Theorem.

**Exercise 7** (8 points)**.**

(a) Let $g \in \mathbb{Z}_n^*$ be an element of order 9. What is the order of $g^3$? What is the order of $g^2$?

(b) Let $g \in \mathbb{Z}_n^*$ be an element of order 12. What is the order of $g^3$? What is the order of $g^8$?

**Exercise 8** (5 points)**.** Let $g \in \mathbb{Z}_n^*$ be an element such that $g^9 = [1]$ and $g^{16} = [1]$. Show that $g = [1]$.

**Exercise 9** (6 points)**.**

(a) Find the last two digits of $3^{125}$.

(b) Find the last two digits of $3^{9999}$.

(c) Find the last three digits of $7^{403}$.

**Exercise 10** (5 points)**.** Find the last two digits of $2^{9999}$.
(Hint:) Note that 2 is NOT coprime with 100. Compute $2^{9999}$ modulo 25 and $2^{9999}$ modulo 4.

**Exercise 11** (7 points)**.** Show that there exist 2023 consecutive integers, each of which is divisible by a perfect square greater than one.

(Hint:) use the Chinese Remainder Theorem.