COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
*New York, 2023/03/29*

EXERCISE SHEET 10

**Discrete Logarithm**

---

**Exercise 1** (15 points)**.** Prove that for integers $n > 1$ and $k > 1$, we have

$$\varphi(n^k) = n^{k-1}\varphi(n)\,,$$

where $\varphi(n)$ is the Euler's totient function:

$$\varphi(n) := \#\{\ a \in \mathbb{Z}\ \mid\ 1 \leq a \leq n \qquad \text{AND} \qquad \gcd(a,n) = 1\ \}\,.$$

**Exercise 2** (15 points)**.** Notice that, when $n$ is an odd number, $n > 1$, then $[2] \in \mathbb{Z}_n^*$. Let $f$ be a function

$$f : \{\ n \in \mathbb{N}\ \mid\ n \text{ odd} \quad \text{AND} \quad n > 1\} \quad \longrightarrow \quad \mathbb{N}$$

defined as follows: $f(n)$ is the order of $[2]$ modulo $n$.

Prove that, for $h, k$ odd, $h, k > 1$, and $\gcd(h,k) = 1$, we have

$$f(hk) = \operatorname{lcm}(f(h), f(k))\,,$$

where lcm denotes the least common multiple, defined in HW04, Exercise 4.

**Exercise 3** (10 points)**.** Use the baby-steps-giant-steps algorithm to find $h, k$ such that

$$2^h \equiv 7 \pmod{53}\,,$$

$$2^k \equiv 9 \pmod{53}\,.$$

**Exercise 4** (20 points)**.** Solve the following congruences.

(a) $x^5 \equiv 23 \pmod{71}$.

(b) $x^3 \equiv 33 \pmod{61}$.

(c) $x^4 \equiv 11 \pmod{89}$.

(d) $x^8 \equiv 37 \pmod{73}$.

(Hint:) Note that $[7], [2], [3], [5]$ is a primitive element modulo $71, 61, 89, 73$ respectively.