# Information Systems Security
# Exercices Series 1 Correction - Modular Arithmetics Reminders

September 22nd, 2021

1. Compute :
   - $4 + 3 \mod 7 = 0$
   - $4 - 3 \mod 7 = 1$
   - $4 * 3 \mod 7 = 12 \mod 7 = 5$
   - $5 * 3 * 1 \mod 8 = 7$
   - $-44 \equiv -2 \equiv 5 \mod 7$

2. In $\mathbb{Z}_7$, compute :
   - 

| + | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| **1** | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| **2** | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| **3** | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| **4** | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| **5** | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| **6** | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

   - 

| $*$ | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| **2** | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| **3** | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| **4** | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| **5** | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| **6** | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

   - 

| **number** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **additive inverse** | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

   - 

| **number** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **multiplicative inverse** | none | 1 | 4 | 5 | 2 | 3 | 6 |

3. ($\mathbb{Z}_7$,+) is a group : addition is associative, neutral element is 0, closure is respected (see exercise 2, additive table), and they all have an inverse (see exercise 2, additive inverse)).

4. ($\mathbb{Z}_8$,$*$) is not a group, as some numbers do not have a multiplicative inverse : 0, 2, 4 and 6.

5. ($\mathbb{Z}_8^*$,$*$) is a group : multiplication is associative, neutral element is 1, closure is respected, and they all have a multiplicative inverse.

6. ($\mathbb{Z}_n^*$,$*$) is a group : multiplication is associative, neutral element is 1, closure is respected (as the product of two elements that do not divide n cannot produce an element that divides n).
   The only tricky part is the inverse. But we know it exists : As $\mathbb{Z}_n^*$ is the set of $a \in \mathbb{Z}$ such that $pgdc(a,n) = 1$, then by Euler's theorem, $a^{\Phi(n)} \equiv 1 \mod n$, which can be written as $a \cdot a^{\Phi(n)-1} \equiv 1 \mod n$.
   So "a" does indeed have an inverse : $a^{-1} = a^{\Phi(n)-1} \mod n$ (and since closure is respected, $a^{Phi(n)-1}$ is in this set as it is just the product of "a" many times).

7. Give the order of :

   - $2^1 = 2 \mod 7$
     $2^2 = 4 \mod 7$
     $2^3 = 8 \mod 7 = 1$
     So $ord_7(2) = 3$.
   - With the successive powers of 3, we have : 3, then $3^2 \mod 7 = 2$, then 6, then 4, then 5, and finally $3^6 \mod 7 = 1$. So the order of 3 mod 7 is : $ord_7(3) = 6$.
   - Same reasoning : We have 3, then 9, then 7, then 1, which gives us $ord_{10}(3) = 4$.

8. Thanks to the previous exercise, we know that 3 is a primitive root modulo 7 (generator of $\mathbb{Z}_7^*$).

9. 1 is not (obviously). 2 is a primitive root modulo 11 (as its successive powers modulo 11 are : 2-4-8-5-10-9-7-3-6-1). 3 is not (3-9-5-4-1). 4 is not (4-5-9-3-1). 5 is not (5-3-4-9-1). 6 is a primitive root (6-3-7-9-10-5-8-4-2-1). 7 is also one (7-5-2-3-10-4-6-9-8-1), as well as 8 (8-9-6-4-10-3-2-5-7-1). Finally, 9 is not a primitive root (9-4-3-5-1), and 10 is not one either (10-1).
   The primitive roots modulo 11 (generators of $\mathbb{Z}_{11}^*$) are 2, 6, 7 and 8.

10. First, we need to find the elements that are co-prime with 12. These elements are 1, 5, 7 and 11 (as 2,3,4,6,8,9,10 all divide 12).
    Then 1 is obviously not a primitive root. Neither is 5 (successive powers are 5-1). Idem for 7 (7-1) and 11 (11-1).
    So there is no primitive root modulo 12.