



## Mathematical background

### Self-assessment test

---

Select the correct answer.

- Given  $a$ ,  $b$  and  $c$ , which belongs to  $\mathbb{Z}$  number set:
  - If  $\mathbb{Z}$  is a Group, “ $a$ ” value does not have to have inverse.
  - If  $\mathbb{Z}$  is a ring  $(\mathbb{Z}, +, \cdot)$ ,  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  will be met
  - If  $\mathbb{Z}$  is a field, “ $a$ ” value does not have to have inverse.
  - If  $\mathbb{Z}$  is a field, then  $a \cdot b = b \cdot a$  does not have to be met.
- What does it mean that a pair of numbers  $a$  and  $b$  are congruent modulo  $n$ ?
  - Both are divisible by  $n$ .
  - Both are multiples of  $n$ .
  - That  $a-b$  is a multiple of  $n$ .
  - That  $a+b$  and  $a-b$  leave the same remainder after being divided by  $n$ .
- What is the result of  $2343 \bmod 10$ ?
  - 43
  - 23,4
  - 234
  - 3
- Choose a pair of numbers within the congruence  $[9]_{15}$ :
  - 6 y 39
  - 0 y 9
  - 15 y 24
  - 21 y 33
- How many different results could generate a reduction module 7?
  - 7.
  - 6.
  - Endless.
  - It depends on the value of the number to reduce.

- 
6. Assume that  $a \bmod 9 = 3$ , and  $b \bmod 9 = 7$ . Choose the correct result from the following ones, applying modular arithmetic principles:
- $a \cdot b \bmod 9 = 21$ .
  - Given  $c=2$ , then  $a \cdot (b+c) \bmod 9 = 6$ .
  - It depends on the value of the number to reduce.
  - $a+b \bmod 9 = 1$ .
7. The inverse of 3 module 7 is...
- $1/3$ .
  - $-1/3$ .
  - 5.
  - 4
8. According to Fermat and Euler theorems, once applied to equation  $ax=1 \bmod n$ :
- Both demand “ $n$ ” to be a prime number.
  - Fermat is an instance of Euler.
  - Euler needs “ $a$ ” and “ $n-1$ ” to be coprime numbers.
  - If  $n=0$ , both can be applied interchangeably.
9. What of the following Euler totient function is the right one?
- $\Phi(12) = 3$ .
  - $\Phi(35) = 24$ .
  - $\Phi(11) = 11$ .
  - $\Phi(34) = 33$ .
10. The order of 4 regarding 7 is...
- 7, and this is the reason why it is generator.
  - 6, and this is the reason why it is generator.
  - 3, and this is the reason why it is not generator.
  - 6, and this is the reason why it is not generator.