

Durée : 1 heure.

Aucun document ni calculatrice n'est autorisé.

Veillez répondre sur le sujet.

NOM .....

PRÉNOM .....

**Sans indiquer votre raisonnement, compléter ci-dessous.**Pour toutes les questions  $a, b, c \in \mathbb{Z}$  et  $n \in \mathbb{N}$ .

1.  $b|a$  si il existe  $q \in \mathbb{Z}$  tel que  $a = qb$ .
2.  $7\mathbb{Z} = \{7q, q \in \mathbb{Z}\} = \{\dots, -14, -7, 0, 7, 14, 21, \dots\}$
3.  $\mathcal{D}(0) = \mathbb{Z}$
4. Une relation binaire  $R$  est d'ordre si elle est réflexive, antisymétrique et transitive.
5. Combien de solutions admet l'équation  $15x + 6y = 4$  dans  $\mathbb{Z} \times \mathbb{Z}$ ? 0
6.  $a \equiv_n b$  si  $n|(b - a)$ , c'est-à-dire s'il existe  $k \in \mathbb{Z}$  tel que  $b = a + nk$ .
7.  $\mathbb{Z}/4\mathbb{Z} = \{C(0), C(1), C(2), C(3)\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$
8.  $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$
9. Dans  $\mathbb{Z}/6\mathbb{Z}$ ,  $\bar{3} = \{x \in \mathbb{Z}, xR3\} = \{x \in \mathbb{Z}, 6|x - 3\} = \{x \in \mathbb{Z}, x \equiv_6 3\} = \{x \in \mathbb{Z}, \exists k \in \mathbb{Z} : x = 3 + 6k\}$
10.  $\varphi(n)$  s'appelle fonction indicatrice d'Euler.
11. Soit  $\bar{x} \neq \bar{0} \in \mathbb{Z}/n\mathbb{Z}$ . S'il existe  $\bar{y} \neq \bar{0} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\bar{x} \cdot \bar{y} = \bar{0}$ ,  $\bar{x}$  est appelé diviseur de zéro.
12. Écrire en langage mathématiques l'équation qui nous permet de calculer l'inverse de 5 modulo 7 :  
 $5x \equiv_7 1$
13. L'inverse de 5 modulo 7 vaut 3
14. Soient  $1960 = 2^3 \cdot 5 \cdot 7^2$  et  $2016 = 2^5 \cdot 3^2 \cdot 7$ .  $1960 \wedge 2016 = 2^3 \cdot 7 = 56$  et  $1960 \vee 2016 = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2 = 70560$
15.  $(2023)^4 \equiv_5 1$
16. Relation de Bézout entre  $a$  et  $b$  : Il existe  $u, v \in \mathbb{Z}$ ,  $au + bv = \text{pgcd}(a, b)$
17. Théorème de Gauss : Si  $a \wedge b = 1$  et  $a|bc \Rightarrow a|c$
18. Un nombre qui n'est pas premier est appelé composé.
19. Aujourd'hui c'est vendredi. Quel jour de la semaine serons-nous dans  $3^{2023}$  jours? Lundi
20. RSA est un système de chiffrement à clé publique (et privée).