Arithmétique Contrôle (terminal) du 10/05/2021 | Numéro étudiant :

NOM : Prénom :

Durée : 2h.
Les documents (cours, TD, ...) et les appareils (calculatrice, téléphones, ...) ne sont ***pas*** *autorisés.* ***Le sujet comporte 8 pages réparties en deux feuilles pliées.***

ATTENTION, chaque réponse devra être soigneusement justifiée (ne pas se contenter d'une suite de calculs sans explications).

Exercice 1. *3 points.* Questions de cours

1. Soient a, b des entiers relatifs. Définir de façon précise le fait que « a divise b ».

2. Soient a, b des entiers relatifs, et $n \geq 2$ un entier naturel. Définir de façon précise le fait que « a est congru à b modulo n ».

3. Soient $a, b \in \mathbb{Z}$ et $n \geq 2$. On suppose que $a \equiv 5 \pmod{n}$ et $b \equiv 6 \pmod{n}$. Montrer en utilisant les opérations arithmétiques usuelles et la définition de la question 2 que $ab \equiv 30 \pmod{n}$.

4. Définir de façon précise le fait qu'un entier $n \in \mathbb{N}$ soit un nombre premier.

Tournez la page

Exercice 2. *3 points.*

1. Donner la décomposition en facteurs premiers de 2020. (Rappel, ici comme dans les autres questions, tout calcul doit être expliqué).

2. Quel est l'ensemble des diviseurs premiers de 2020 ?

3. Donner l'ensemble des entiers relatifs qui divisent 2020.

4. Sachant que 43 divise 2021, donner l'ensemble des entiers naturels qui divisent 2021.

Tournez la page

Exercice 3. *4 points.*

1. Écrire en Python (ou en pseudo-code) une fonction **pgcd** qui retourne le pgcd de deux entiers naturels a et b au moyen de l'algorithme d'Euclide.

2. En utilisant les étapes de votre algorithme, calculer $\text{pgcd}(123, 963)$.

3. Sachant que 1789 est un nombre premier, quelles sont les valeurs possibles pour $\text{pgcd}(n, 1789)$ lorsque $n \in \mathbb{Z}$? (À justifier, bien sûr.)

Tournez la page

4. Pourquoi est-on sûr qu'il existe des entiers relatifs u, v tels que $3000u + 1789v = 1$?

5. En utilisant l'algorithme d'Euclide étendu, calculer des entiers relatifs u, v tels que

$$3000u + 1789v = 1.$$

Passez à la deuxième feuille de sujet

Numéro étudiant :

NOM : Prénom :

Exercice 4. *4 points.*

1. Calculer $2^k \pmod{13}$ pour $k = 1, 2, \ldots, 12$.

2. Pourquoi pouvait-on prédire la valeur de $2^{12} \pmod{13}$?

3. Déduire de 1. la valeur du plus petit entier strictement positif k tel que $4^k \equiv 1 \pmod{13}$

4. Déduire de 1. la valeur de $2^{145} \pmod{13}$

5. Déduire de 1. la valeur de $145^{145} \pmod{13}$

Tournez la page

Exercice 5. *3 points.*

Montrer par récurrence que pour tout entier naturel n, on a

$$\sum_{k=0}^{n}(2k+1) = (n+1)^2$$

Tournez la page

Exercice 6. *4 points.*

1. Expliquer comment fonctionne le principe général de la « cryptographie à clef publique ».

2. Alice et Bob utilisent le chiffrement RSA. Alice veut envoyer le message $m = 2019$ à Bob. La clef publique de Bob est $(n = 2021, e = 5)$. Indiquer quel calcul doit effectuer Alice pour chiffrer son message avant de l'envoyer, et faire ce calcul.

Tournez la page

3. Trouver des entiers relatifs (u, v) tels que

$$1932u + 5v = 1$$

4. Bob sait que $\phi(n) = 1932$. Quelle est sa clef privée d ?

5. On note x le message chiffré envoyé par Alice. Quel calcul doit faire Bob pour déchiffrer ce message ? (On ne demande pas d'effectuer ce calcul.)

Fin de l'énoncé