

FEUILLE DE TRAVAUX DIRIGÉS 7

ARITHMÉTIQUE DES ENTIERS

Exercice 1.

Déterminer les triplets $(a, b, c) \in (\mathbb{N}^*)^3$ tels que

$$\text{ppcm}(a, b) = 42 \quad , \quad \text{pgcd}(a, c) = 3 \quad \text{et} \quad a + b + c = 29.$$

Exercice 2 (Algorithme d'Euclide et Théorème de Bézout).

- (1) Quel est le pgcd de 47 et 111 ?
- (2) Déterminer deux entiers u et v vérifiant $47u + 111v = 1$.

Exercice 3 (Congruences).

- (1) Montrer que pour tout entier naturel n , 5 divise $2^{3n+5} + 3^{n+1}$.
- (2) Montrer que pour tout entier n , 30 divise $n^5 - n$.
- (3) Quel est le reste de la division euclidienne de $16^{(2^{1000})}$ par 7 ?

Exercice 4 (Nombres de Mersenne, nombres de Fermat).

- (1) Soient $a \geq 2$ et $n \geq 2$ deux entiers. Si $a^n - 1$ est un nombre premier, montrer que $a = 2$ et que n est premier. Les nombres premiers de cette forme sont appelés *nombres de Mersenne*.
- (2) Soit $n \in \mathbb{N}^*$. Si $2^n + 1$ est premier, montrer que n est une puissance de 2. Les nombres de la forme $F_k = 2^{2^k} + 1$ sont appelés *nombres de Fermat*.
- (3) Montrer que les nombres de Fermat $\{F_k\}_{k \in \mathbb{N}}$ sont premiers entre eux deux à deux.
- (4) En déduire une autre démonstration du fait qu'il y a une infinité de nombres premiers.

Exercice 5.

Soit A la somme des chiffres de 4444^{4444} , écrit dans le système décimal, et soit B la somme des chiffres de A . Que vaut C , la somme des chiffres de B ?

Exercice 6 (Cas particuliers du théorème de la progression arithmétique de Dirichlet).

- (1) Montrer qu'il existe une infinité de nombres premiers de la forme $6n - 1$, $n \in \mathbb{N}^*$.
- (2) Soit $p > 5$ un nombre premier. Montrer que 5 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv \pm 1_{[10]}$
Indication : Utiliser la loi de réciprocité quadratique.
- (3) En déduire qu'il existe une infinité de nombres premiers de la forme $10n - 1$, $n \in \mathbb{N}^*$.

Problème 1 (Nombres pseudo-premiers et nombres de Carmichael).

Le théorème de Fermat affirme que si n est premier et si $a \wedge n = 1$, alors $a^{n-1} \equiv 1_{[n]}$. Le but de ce problème est de montrer que la réciproque est fautive.

Soit un entier $a \geq 2$. Un entier n est dit *pseudo-premier* en base a si n n'est pas premier et si $a^{n-1} \equiv 1_{[n]}$.

- (1) Si $p > 2$ est un nombre premier ne divisant pas $a(a^2-1)$, montrer que $n = (a^{2p}-1)/(a^2-1)$ est un nombre pseudo-premier en base a .
- (2) En déduire que pour tout entier $a \geq 2$, il existe un infinié de nombres pseudo-premiers en base a .

Un entier $n \geq 2$ est appelé *nombre de Carmichael* si n n'est pas premier et si pour tout entier a premier avec n , $a^{n-1} \equiv 1_{[n]}$.

- (3) Si $n = p_1 p_2 \dots p_k$, où les p_i sont des nombres premiers distincts, et si $p_i - 1 | n - 1$ pour tout i , montrer que n est un nombre de Carmichael.
- (4) Réciproquement, montrer que tout nombre de Carmichael peut se mettre sous la forme $n = p_1 p_2 \dots p_k$ où les p_i sont des nombres premiers distincts et où $p_i - 1 | n - 1$ pour tout i
Indication : on pourra utiliser le fait que pour un groupe commutatif fini G , si p premier divise le cardinal de G , alors il existe dans G au moins un élément d'ordre p .
- (5) Montrer qu'un nombre de Carmichael a au moins 3 facteurs premiers.
- (6) Soit $n = pqr$ un nombre de Carmichael à trois facteurs premiers $p < q < r$. Si p est fixé, montrer que q et r sont bornés.