Licence de Math-Info.
Université d'Artois.
03/03/09.
Durée 3h

Examen
ARITHMÉTIQUE
Session 2

Les calculatrices et les documents sont interdits.

La rédaction sera prise en compte dans la notation.

Cours. (4 points=1+(1+2))

1) Démontrer qu'il y a une infinité de nombres premiers.

2)a) Enoncer le (petit) théorème de Fermat.

b) Le démontrer.

Exercice 1. (3 points)

Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $49x + 153y = 5$.

Exercice 2. (5 points=1+(1+0,5+1,5)+1)

1) Enoncer le théorème de Wilson.

On souhaite le démontrer.

2)a) On suppose que p est premier.

i) Déterminer les $x \in \{1, \dots, p\}$ dont la classe $\dot{x} \in \mathbb{Z}/p\mathbb{Z}$ vérifie $\dot{x}^2 = \dot{1}$.

ii) Quels sont les $x \in \{1, \dots, p\}$ dont la classe $\dot{x}$ est son propre inverse pour le produit dans $\mathbb{Z}/p\mathbb{Z}$?

iii) En déduire la classe de $(p-1)!$ dans $\mathbb{Z}/p\mathbb{Z}$ et conclure.

b) Montrer la réciproque.

Exercice 3. (3 points=0,5+1+1,5)

Soit $n \in \mathbb{N}$ avec $n \geq 2$. On note $s \in \mathbb{N}$ tel que $s \geq 1$ et $2^s \leq n < 2^{s+1}$.

1) Justifier qu'un tel entier s existe.

2) Pour $j \in \{0, \ldots, s-1\}$, minorer $\displaystyle\sum_{k=2^j}^{2^{j+1}-1} \frac{1}{k}$ par une constante strictement positive (indépendante de j et s).

3) Montrer que $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \geq \frac{s}{2}$. En déduire que $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \geq c \ln(n)$, où $c > 0$ est une constante (indépendante de n).

Exercice 4. (9 points=1,5+(2,5+1)+(1+1)+2)

1) On fixe un entier $n \geq 2$. Soient a, b et $c \in \mathbb{N}$, non nuls, avec $a^b \equiv 1\,[n]$ et $a^c \equiv 1\,[n]$. Enfin, on désigne par d le pgcd de b et c.

Montrer que $a^d \equiv 1\,[n]$.

Soit p un nombre premier tel que $p \equiv 3\,[4]$.

2) Supposons qu'il existe un entier a tel que $a^2 \equiv -1\,[p]$.

a) En justifiant que l'on peut appliquer le 1. avec $b = 4$ et $c = p - 1$, montrer que $a^2 \equiv 1\,[p]$.

b) Quel est l'ensemble des solutions de $a^2 \equiv -1\,[p]$?

3) Soient x et y des entiers tels que p divise $x^2 + y^2$.

a) On suppose que p ne divise pas x. Justifier qu'il existe $z \in \mathbb{N}$ tel que $\bar{x}.\bar{z} = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. En déduire qu'alors $y^2.z^2 \equiv -1\,[p]$.

b) Montrer que p divise x et y.

4) En déduire que si un entier N est somme de deux carrés d'entiers alors les nombres premiers congrus à 3 modulo 4 intervenant dans la décomposition N apparaissent avec un exposant pair.