Quelques thèmes centraux du cours

1. Décomposition des nombres entiers en produit de nombres premiers,
2. PGCD,PPCM, Théorème de Bézout, lemme de Gauss.
3. Équations diophantiennes.
4. Congruences et $\mathbb{Z}/n\mathbb{Z}$.
5. Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, l'indicatrice d'Euler.
6. Théorème de Fermat, de Wilson, la formule d'Euler.
7. Chiffrement affine, chiffrement de Hill, R.S.A.

Quelques exercices d'arithmétique

Exercice 1

Démontrer que 39 divise $7^{37} + 13^{37} + 19^{37}$

Exercice 2

Ecrire le nombre 1025 en base 2 puis en base 5.

Exercice 3

Démontrer que le produit de cinq entiers consécutifs ne peut-être un carré parfait.

Exercice 4

Calculer $\varphi(225)$

Exercice 5

Si $n \in \mathbb{N}$ est premier avec 2 et avec 3 montrer que 24 divise $n^2 + 47$.

Exercice 6

Si a, b sont deux nombres premiers entre eux quelles sont le valeurs possibles du pgcd de $a^3 + b^3$ et de $a^3 - b^3$?

Exercice 7

Démontrer que si $a > 1$, alors pour chaque couple d'entier positif m, n on a

$$pgcd(a^m - 1, a^n - 1) = a^{pgcd(m,n)} - 1$$

Exercice 8

Est il vrai que si p et $p^2 + 8$ sont des nombres premiers alors $p^3 + 4$ est premier ?

Exercice 9

Montrer que si $a^n - 1$ est premier pour des entiers $a > 1$ et $n > 1$ alors $a = 2$ et n est premier.

Exercice 10

Pour quels entiers positifs n l'xpression $3^n + 1$ est-elle un multiple de 10 ?

Exercice 11

Trouver $u, v \in \mathbb{Z}$, tels que $13u + 15v = 1$.

Exercice 12

Soit a, b des entiers et m, n des entiers positifs. Montrer que le système $x \equiv a \pmod m$ et $x \equiv b \pmod n$ possède des solutions si et seulement si $pgcd(m, n)$ divise $a - b$.

Exercice 13

Soit p un nombre premier montrer que p divise $\binom{p}{2p} - 2$.

Exercice 14

Soit φ l'indicatrice d'Euler. Montrer que $\varphi(n) = \sum_{d|n} \varphi(d)$

Exercice 15

Résoudre en nombre entiers (équations diophantiennes) les équations suivantes :

1. $25x + 10y = 20$
2. $132x + 38y = 3$
3. $17x + 102y = 34$

Exercice 16

Soit $n \in \mathbb{N}$, on pose $M_n = 2^n - 1$. On rappelle qu'un nombre est parfait s'il est égale à la somme de ses diviseurs propres. (par exemple $6 = 1 + 2 + 3$ et $28 = 1 + 2 + 4 + 7 + 14$ sont parfaits).

1. Démontrer que si M_n est premier alors n est premier.
2. Soit $l \in \mathbb{N}$ tel que M_l est premier. Montrer qu'alors $2^{l-1}M_l$ est parfait.

Exercice 17

Trouver le reste de la division par 4 des nombres de la forme $11, 111, 1111, 11111, \ldots$. Montrer qu'aucun de ces nombres n'est un carré parfait.

Exercice 18

1. Calculer les *résidus modulo 10* de 3^n, pour $n \in \{0; 1; 2; 3; 4; 5\}$. Mettre en évidence le *cycle* suivi.
2. Etudier les *résidus modulo 10* de 3^n, pour $n \in \mathbb{N}$.

Exercice 19

Résoudre les systèmes suivants :

$$(A) \quad x \equiv \begin{cases} 3 & \text{mod } 13 \\ 5 & \text{mod } 7. \end{cases} \qquad (B) \quad x \equiv \begin{cases} 6 & \text{mod } 17 \\ 4 & \text{mod } 6. \end{cases}$$

Exercice 20

Dans un codage affine donner par les paramètres (a, b), pourquoi est il important que a soit premier avec 26 (codage des 26 lettres de l'alphabet) ?

On considère le chiffrement affine donné par $(15, 7)$ coder le message "L'examen est très facile".

Exercice 21

1. Soient $a, b \in \mathbb{Z}_0$ et $q, r \in \mathbb{Z}$ tels que : $a = bq + r$. Montrer que $pgcd(a, b) = pgcd(b, r)$.
2. Pour n un entier naturel donné, déterminer $pgcd(4n^3 + 2n^2 + 10n + 1, 2n^2 + n + 4)$.
3. Soit n un entier naturel. Montrer que $pgcd(2n + 4, 3n + 3)$ ne peut etre que $1, 2, 3$ ou 6.

Exercice 22

Soit $n \in \mathbb{N}$ un entier positif non nul.

1. Montrer que si $n \in \mathbb{N}$ un entier positif non nul alors 2 divise $3^n + 1$.
2. Montrer que pour $k \in \mathbb{N}$, $3^{4k} \equiv 1\ mod(5)$.
3. Trouver tous les entiers positifs n tels que 10 divise $3^n + 1$.

Exercice 23

Montrer que 105 est inversible dans $\mathbb{Z}/143\mathbb{Z}$ et calculer son inverse.

Exercice 24

Montrer que, pour n un entier positif, on a $n^{13} \equiv n \pmod 2$ et que $n^{13} \equiv n \pmod 5$; en déduire que le dernier chiffre de n^{13} est le même que le dernier chiffre de n.

Exercice 25

1. Soit p_1 et p_2 des nombres premiers. En utilsant le théorème chinois, montrer qu'il existe un entier x tel que x est divisible par p_1^2 et $x + 1$ est divisible par p_2^2.
2. Montrer que pour tout $k \in \mathbb{N}$ on peut trouver un entier x tel que $x, x+1, x+2, \ldots, x+k$ sont divisibles par des carrés parfaits (i.e. montrer que pour $1 \leq j \leq k$, il existe $a_j \in \mathbb{Z}$ tel que a_j^2 divise $x + j$).

Exercice 26

On considère le chiffrement affine de paramètres $(3, 8)$. Coder le message "PUBLIC". Trouver l'inverse de trois modula 26 et donner le décodage de la lettre reçue "M" qui a été envoyée en utilisant le chiffrement affine ci-dessus de paramètres $(3, 8)$.