M1-Math : Algèbre 1 - Introduction à l'Arithmétique

Contrôle continu 1

Exercice 1. Résoudre le système de congruence suivant

$$\begin{cases} x = 4\ [7] \\ x = 2\ [3] \\ x = 3\ [5] \end{cases}$$

Exercice 2. Pour $n \geq 1$ on définit le n-ième nombre de Mersenne par $M_n = 2^n - 1$.

1) Montrer que si M_n est premier alors n est premier.
2) Soit $p \geq 3$ un nombre premier et q un facteur premier de M_p.
   a) Pourquoi q est-il différent de 2 ? En déduire que $\bar{2}$ est inversible dans $\mathbb{Z}/q\mathbb{Z}$ et que l'ensemble $A = \{n \in \mathbb{Z} \mid \bar{2}^n = \bar{1}\}$ est bien défini.
   b) Montrer que A est un idéal de $\mathbb{Z}$.
   c) Montrer que $p \in A$ et $q - 1 \in A$.
   d) En déduire que $q - 1$ est un multiple de p puis que $q - 1$ est un multiple de $2p$.

Exercice 3. Nous allons étudier l'infinité des nombres premiers congrus à 1 modulo 4. Considérons $m \in \mathbb{N}$ tel que $m \geq 2$ et $a = (m!)^2 + 1$. On note p un diviseur premier de a.

1) Montrer que $p \neq 2$ et p ne divise pas $m!$.
2) Montrer que $(m!)^{p-1} = (-1)^{\frac{p-1}{2}}[p]$.
3) Montrer que $(m!)^{p-1} = 1[p]$ et en déduire que $p = 1[4]$.
4) En appliquant le raisonnement ci-dessus avec m premier satisfaisant $m = 1\ [4]$, montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Problème

On appelle fonction arithmétique toute application $f : \mathbb{N}^* \to \mathbb{C}$. En voici quelques exemples intéressants

— $\tau(n)$: le nombre de diviseurs de n
— $\sigma(n)$: la somme des diviseurs de n, $\sigma(n) = \sum_{d|n} d$
— $\omega(n)$: le nombre de diviseurs premiers de n
— $\varphi(n)$: la fonction d'Euler
— $\mu(n)$: la fonction de Möbius définie par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré non trivial (différent de 1)} \\ (-1)^{\omega(n)} & \text{sinon} \end{cases}$$

Nous dirons qu'une fonction arithmétique f est multiplicative si $f(1) = 1$ et $f(mn) = f(m)f(n)$ lorsque m et n sont premiers entre eux.

1) Déterminer la valeur de ces cinq fonctions arithmétiques pour $n = 12$.

2) Que vaut $j!$ modulo 4 pour $j > 3$? Déterminer alors $\sum_{j=1}^{n} \mu(j!)$ si $n \geq 3$.

La fonction τ

3) Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Montrer que

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

4) Montrer que la fonction τ est multiplicative.
5) Déterminer le plus petit entier positif n tel que $\tau(n) = 6$.
6) Montrer que $\tau(n)$ est impair si et seulement si n est un carré parfait.

La fonction σ

Si $n \in \mathbb{N}^*$, on note D_n l'ensemble des diviseurs de n

7) Soit m et $n \in \mathbb{N}^*$. On pose $F : D_m \times D_n \to D_{mn}; (a, b) \mapsto ab$. Montrer que, si m et n sont premiers entre eux, F est une bijection.
8) Montrer que la fonction σ est multiplicative.
9) Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Montrer que

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

La fonction de Möbius

10) Montrer que la fonction μ est multiplicative.
11) Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Écrire les diviseurs d de n vérifiant $\mu(d) \neq 0$ en fonction des p_i. Parmi ces diviseurs combien ont exactement k facteurs premiers distincts ?
12) Montrer que pour $n \geq 2$

$$\sum_{d|n} \mu(d) = 0$$

Que vaut cette somme pour $n = 1$?

La fonction d'Euler

Pour $n \in \mathbb{N}^*$, nous allons calculer $\Phi(n) = \sum_{d|n} \varphi(d)$.

13) Calculer $\Phi(6)$.
14) Soit p un nombre premier et $\alpha \in \mathbb{N}$. Rappeler l'expression $\varphi(p^\alpha)$ et calculer $\sum_{d|p^\alpha} \varphi(d)$.
15) On utilise les notations de la question 7). Soit m et n des entiers premiers entre eux et $a \in D_m$ et $b \in D_n$. Montrer que $a \wedge b = 1$.
16) Déduire des questions 7) et 15) que Φ est multiplicative.
17) Montrer que $\Phi(n) = n$ pour tout $n \in \mathbb{N}^*$.

Formule d'inversion de Möbius

Soit $f : \mathbb{N}^* \to \mathbb{C}$ une fonction arithmétique. On pose $F(n) = \sum_{d|n} f(d)$ pour $n \in \mathbb{N}^*$.

18) Démontrer la formule d'inversion de Möbius :

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$$

19) Déduire de la question précédente que

a) μ est la seule fonction $f : \mathbb{N}^* \to \mathbb{C}$ vérifiant $\alpha(1) = 1$ et $\sum_{d|n} f(d) = 0$ pour $n > 1$.

b) on a la formule $\varphi(n) = \sum_{d|n} \mu(\frac{n}{d}) d$.