1 EXERCICES

Exercice 1.1 Soient $p \geqslant 3$ premier et $r \in \mathbb{N}$. Montrer que $(1+p)^{p^r} = 1 + p^{r+1} \bmod p^{r+2}$.

Exercice 1.2

1. Montrer que le polynôme $P(X) = 1 + X + \cdots + X^{p-1}$ ne peut être le produit de deux polynômes non constants de $\mathbb{Z}[X]$
   (on étudiera le polynôme $\bmod(p)$)
2. Montrer que le polynôme P est irréductible sur $\mathbb{Q}[X]$.

Exercice 1.3 On suppose que n est un nombre premier.

1. Que peut-on dire de l'application $(k,q) \mapsto (k+q, k-q)$ de $(\mathbb{Z}/n\mathbb{Z})^2$ dans lui-même ?
2. Evaluer le module du complexe $S = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \exp\left[\frac{2\pi i k^2}{n}\right]$
3. On suppose que n est un nombre premier de la forme $n = 4k+1$.
   (a) Montrer l'existence d'une solution à l'équation $x^2 = -1 \bmod(n)$.
   (b) Calculer alors S^2.
   (c) Qu'en est-il si n est toujours un nombre premier mais de la forme $n = 4k+3$?

Exercice 1.4 Soit $N_k(X) = \dfrac{X(X-1)..(X-k+1)}{k!}$.
Montrer que, pour tout $m \in \mathbb{Z}$, on a $N_k(m) \in \mathbb{Z}$.
En déduire que, pour tout $(a_1, .., a_k) \in \mathbb{Z}^k$, le produit $\prod_{1 \leqslant i < j \leqslant k} (a_j - a_i)$ est divisible par $1!2!..(k-1)!$.

Exercice 1.5 Soit p un nombre premier, k un entier naturel. Calculer la somme $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$.

Exercice 1.6 Soit p un nombre premier.

1. Montrer que $(p-1)! = -1 \bmod p$.
2. On suppose que $p \geqslant 3$ et on considère le rationnel $S = \sum_{k=1}^{p-1} \frac{1}{k}$.
   Soit A l'entier naturel tel que $S = \dfrac{A}{(p-1)!}$.
   Montrer que $A = 0 \bmod(p)$.
3. On suppose $p \geqslant 5$. Montrer que $A = 0 \bmod p^2$.

2 Indications

Indication pour l'exercice : Procéder par récurrence sur r.

Indication pour l'exercice :

1. A l'aide de la somme d'une suite géométrique et du binôme de Newton, on donne une autre forme à P et en justifiant que $\binom{p}{k} = 0$ si $k \in [\![1, p-1]\!]$, en déduire que $\overline{P(X)} = \overline{X^p} \bmod p$. Si on a $P = RS$, en déduire la forme de $\overline{R}$ et $\overline{S}$ puis celle de R et de S.
2. Montrer que l'on peut toujours se ramener au cas où R et S sont dans $\mathbb{Z}[X]$.

Indication pour l'exercice : On suppose que n est un nombre premier.

1. C'est un morphisme de groupe additif dont le noyau est ... si $n \neq 2$ donc c'est un .... si $n \neq 2$. Le cas $n = 2$ est simple.
2. Utiliser $S\overline{S}$ pour obtenir une double somme et effectuer le changement de variable $(u, v) = (k - m, k + m)$.
3. (a) Utiliser le théorème de Lagrange pour montrer que $x^{n-1} = 1 \bmod n$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ puis, par des considérations sur le nombre de racines d'un polynôme, montrer qu'il existe un x tel que $x^{2k} \neq 1 \bmod n$ et conclure.
   (b) Soit ε une solution de $\varepsilon^2 = -1 \bmod n$, effectuer le changement de variable $(u, v) = (k - \varepsilon m, k + \varepsilon m)$ dans la double somme S^2.
   (c) Montrer pour commencer que tout élément de $(\mathbb{Z}/n\mathbb{Z})$ est de la forme $x^2 \bmod n$ ou $-x^2 \bmod n$. En utilisant que la somme des racines de l'unité vaut 0, en déduit que $S = -\sum_{k \in \mathbb{Z}/n\mathbb{Z}} \exp\left[-\dfrac{2\pi i k^2}{n}\right]$ puis que

$$S^2 = -\sum_{(k,m) \in (\mathbb{Z}/n\mathbb{Z})^2} \exp\left[\frac{2\pi i(k^2 - m^2)}{n}\right]$$

   et c'est reparti pour le changement de variable.

Indication pour l'exercice : Pour la première question, rien à dire.
Pour la seconde, introduire le déterminant de Vandermonde puis faire des opérations sur les lignes et les colonnes pour faire apparaitre les polynômes N_k sur tous les coefficients.

Indication pour l'exercice : Que peut-on dire de l'application $x \mapsto x^k$? (morphisme ? injectif ? surjectif ?). Ah le beau changement de variable.

Indication pour l'exercice :

1. Hormis 1 et -1, tous les éléments de $(\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ ont des inverses distincts d'eux même ($x \neq \dfrac{1}{x}$ car $x^2 \neq 1$), regrouper deux à deux ces éléments dans la factorielle.
2. Multipler par $(p-1)!$ dans l'égalité et vérifier que $\dfrac{(p-1)!}{k}$ est bien un entier et que l'on a $\overline{\left[\dfrac{(p-1)!}{k}\right]} = \overline{(p-1)!} \times \overline{k}^{-1}$. Uitliser alors que l'application $\overline{k} \mapsto \overline{k}^{-1}$ est une bijection pour faire un changement de variable dans la somme $\bmod p$.
3. Raisonner $\bmod p^2$ en remarquant que tous les éléments entre 1 et $p-1$ sont premiers à p^2.

3 Corrections

Correction de l'exercice : Indisponible actuellement (mais cela va venir)

Correction de l'exercice : Indisponible actuellement (mais cela va venir)

Correction de l'exercice : Indisponible actuellement (mais cela va venir)

Correction de l'exercice : Indisponible actuellement (mais cela va venir)

Correction de l'exercice : Indisponible actuellement (mais cela va venir)

Correction de l'exercice : Indisponible actuellement (mais cela va venir)