Feuille TD 1 - L'anneau $\mathbb{Z}/n\mathbb{Z}$ et le groupe $\mathbb{Z}_n^\star$

Exercice 1. Calcul modulaire et Théorème chinois des restes.

1. Résoudre l'équation $17x = 10[50]$; et $35y = 10[50]$.

2. Trouver tous les x entiers tels que $x \equiv 4 \pmod 5$ et $x \equiv 5 \pmod{11}$. En déduire l'inverse de 49 modulo 55.

   Correction: $x = 4.11.11^{-1[5]} + 5.5.5^{-1[11]}[55] = 44 - 25.2[55] = -6[55] = 49[55]$. *Donc* $y = 49^{-1}[55]$ *a pour modulo* $4^{-1}[5] = 4[5]$ *et* $5^{-1}[11] = 9[11]$. *D'où* $y = 4.11.11^{-1[5]} + 9.5.5^{-1[11]}[55] = 44 - 45.2[55] = 46[55] = 9[55]$.

3. Trouver tous les x entiers dont les restes par 2, 3, 4, 5, et 6 sont respectivement 1, 2, 3, 4, 5.

   Correction: *On ne considère dans un premier temps que le système RNS (3,4,5); on a alors* $x = -1$ *mod 3,4 et 5. Donc* $x = -1[60]$. *On a donc* $x = 60.k - 1$. *On vérifie alors les 2 autres contraintes modulo 2 et 6; on a* $(60k-1)$ *mod*$2 = -1 \mod 2 = 1$ *et* $(60k-1) \mod 6 = -1 \mod 6 = 5$. *Toutes les contraintes sont vérifiées donc* $x = 60k - 1$.

4. Pour le système de résidus [5,7,8,9] expliciter l'isomorphisme du théorème chinois des restes $\Phi : \mathbb{Z}/2520\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ et son inverse Φ^{-1}. Calculer de tête avec ce système $x = (67 \times 28 + (17 \times 121)^{-1})) \mod 2520$.

   Correction: $\Phi(n) = [n \mod 5, n \mod 7, n \mod 8, n \mod 9]$ *et* $\Phi^{-1}([n_5, n_7, n_8, n_9]) = (n_5.504.(504^{-1}[5]) + n_7.360.(360^{-1}[7]) + n_8.315.(315^{-1}[8]) + n_9.280.(280^{-1}[9])) \mod 2520 = -504.n_5 + 1800.n_7 + 945.n_8 + 280.n_9[2520]$.

Exercice 2. Fonction ϕ d'Euler. On étudie ici la fonction $\varphi(n)$, introduite par Euler, d'une importance fondamentale en arithmétique. On pose $\varphi(1) = 1$ et pour $n > 1$, $\varphi(n)$ est le nombre d'entiers $m \in \{1, \ldots, n-1\}$ premiers avec n (i.e. $\gcd(m, n) = 1$).

1 Pour $n = p^k$ où p est premier et $k \in \mathbb{N}^*$, calculer $\varphi(n)$.

   Correction: *Seuls les multiples de p inférieurs à* p_k *sont non premiers avec* p_k*: il y en a* $k-1$. *Donc* $\varphi(p^k) = p^k - k + 1$.

2 Montrer que si n_1 et n_2 sont premiers entre eux : $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$. Indication : utiliser l'isomorphisme entre les anneaux $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ et $(\mathbb{Z}/n_1 n_2\mathbb{Z})$.

   Correction: *En utilisant le TCR, pour tout* $m < n_1 n_2$*, il existe un unique couple* (a, b) *tel que* $m = a \mod n_1$ *et* $m = b \mod n_2$*, et inversement (l'association est bijective). Or m premier avec* $n_1 n_2 \iff m$ *(donc a) premier avec* n_1*) et m (donc b) premier avec* n_2*. D'où* $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$.

3 Dans $\mathbb{Z}/n\mathbb{Z}$, quel est le cardinal du groupe des éléments inversibles?

4 En déduire un algorithme de calcul de l'inverse dans $\mathbb{Z}/n\mathbb{Z}$.
Application : calculer (le plus vite possible) 22^{-1}mod 63 et 5^{2001} mod 24.

Correction: *Soit* $n = \prod_{i=1}^{k} p_i^{\delta_i}$ *la factorisation de* n *en facteurs premiers. D'après 2 et 1, on a :* $\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\delta_i} = \prod_{i=1}^{k}(p_i^{\delta_i} - \delta_i + 1)$.
Algorithme : On fait le TCR sur les entiers: avec $n = n_1 n_2$. *Soit* $m_1 = m[n_1]$ *et* $m_2 = m[n_2]$.
On a $m = m_2 n_1^{-1[n_2]} n_1 + m_1 n_2^{-1[n_1]} n_2[n_1.n_2]$. *D'où :*
$m^{-1[n]} = m_2^{-1[n_2]} n_1^{-1[n_2]} n_1 + m_1^{-1[n_1]} n_2^{-1[n_1]} n_2[n_1.n_2]$.
Application :
63 = 9.7 et $9^{-1/7}.9 = 4.9 = 36$ *et* $7^{-1/9}.7 = 4.7 = 28$. *D'où :* $22 = 1.36 + 4.28[63] \Longrightarrow 22^{-1[63]} = 1.36 + 4^{-1[9]}28[63] = 36 + 7.28[63] = 43[63]$.
ou astuce : 22 = 21+1 et $(21+1)(21-1) = -1[63]$ *d'où* $22^{-1[63]} = -20 = 43[63]$.
$5^2 = 1[24]$ *Donc* $5^{2001} = 5[24]$ *et* $5^{-1[24]} = 5$. *D'où* $5^{-2001} = 5[24]$.

Exercice 3.

1. Soit $N = n_1.n_2.\ldots.n_k$ avec n_1, ... n_k premiers 2 à 2 et f un polynôme. Montrer que le nombre de solutions de l'équation $f(x) \equiv 0[N]$ est le produit du nombre de racines des équations $f(x) \equiv 0[n_i]$.

   Correction:

2. Montrer que n_1, n_2, n_3, n_4 sont premiers 2 à 2 ssi $\gcd(n_1.n_2, n_3.n_4) = \gcd(n_1.n_3, n_2.n_4) = 1$. Généraliser en montrant que $n_1, \ldots, n_k$ sont premiers 2 à 2 ssi $\lceil \log_2 k \rceil$ nombres que l'on explicitera sont premiers 2 à 2.

Exercice 4. Le groupe $\mathbb{Z}_{10}^{\star}$.

1. Que vaut $\Phi(10)$? Expliciter $\mathbb{Z}_{10}^{\star}$ et calculer l'ordre de chaque élément.

   Correction: $\mathbb{Z}_{10}^{\star} = \{1, 3, 7, 9\}$. *Ordres respectifs: 1:1 ; 3:4; 7:4; 9:2.*

2. Soit g la plus petite racine primitive de $\mathbb{Z}_{10}^{\star}$; calculer la table des indices par rapport à g des éléments de $\mathbb{Z}_{10}^{\star}$. A quel groupe additif $\mathbb{Z}_{10}^{\star}$ est-il isomorphe ?

   Correction: $g = 3$. *Ind(1)=0 ; Ind(3)=1; Ind(7)=3; Ind(9)=2.* $\mathbb{Z}_{10}^{\star}$ *est isomorphe au groupe* $(\mathbb{Z}/4\mathbb{Z}, +0)$

3. En utilisant l'élévatuion à la puissance modulo n, donner un algorithme pour calculer x^{-1} dans $\mathbb{Z}_n^{\star}$ connaissant $\Phi(n)$. Préciser le coût.

   Correction: