GROUPES ET ARITHMETIQUE, I

(1) Donner tous les sous-groupes de $\mathbb{Z}, +$; de $Z/n\mathbb{Z}, +$ $(n \in \mathbb{N}^*)$

(2) Soit $n \in \mathbb{N}$, $n \geq 2$ et soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ordre de dans $\mathbb{Z}/n\mathbb{Z}$, $+$ est donné par

$$ord_{\mathbb{Z}/n\mathbb{Z}}(\overline{a}) = ppcm(a,n)/a = n/pgcd(a,n).$$

Trouver tous les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.

(3) Calculer $Aut(\mathbb{Z}, +)$ et $Aut(\mathbb{Z}/n\mathbb{Z}, +)$.

(4) On considère $\mathbb{Z}/n\mathbb{Z}$

On pose $U(\mathbb{Z}/n\mathbb{Z}) = \{x \in \mathbb{Z}/n\mathbb{Z} \mid \exists y \in \mathbb{Z}/n\mathbb{Z} \ : \ xy = 1\}$

a) Calculer $U(\mathbb{Z}/6\mathbb{Z})$ $U(\mathbb{Z}/8\mathbb{Z})$; Montrer que $U(\mathbb{Z}/n\mathbb{Z})$ est un sous ensemble de $\mathbb{Z}/n\mathbb{Z}$ qui forme un groupe pour la multiplication et que $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid (x,n) = 1\}$

b) On définit $\varphi : \mathbb{N}^* \to \mathbb{N} : n \longmapsto |U(\mathbb{Z}/n\mathbb{Z})|$ (φ est appelée l'indicatrice d'Euler) Montrer que $(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$

c) Calculer $\varphi(p^r)$ pour p un premier et $r \in \mathbb{N}^*$.

d) Montrer que si $n = p_1^{r_1} \cdots p_s^{r_s}$ alors $\varphi(n) = n(1 - p_1^{-1})(1 - p_2^{-1}) \cdots (1 - p_s^{-1})$.

(5) Soit $d, n \in \mathbb{N}$, tel que d divise n. Soit g un générateur d'un groupe cyclique G d'ordre n.

a) Montrer que l'ensemble

$$\{g^{kn/d} \mid k \leq d \text{ et } (k,d) = 1\}$$

est l'ensemble des éléments d'ordre d dans G.

b) Montrer que le nombre d'éléments d'ordre d dans G est $\varphi(d)$

c) Montrer que $\sum_{d/n} \varphi(d) = n$

(6) a) Montrer que

$$\sum_{d/n} (-1)^{n/d}.\varphi(d) = \begin{cases} 0 \text{ si } n \text{ pair} \\ -n \text{ si } n \text{ impair} \end{cases}$$

b) Montrer que si $(x,n) = 1$ alors n divise $x^{\varphi(n)} - 1$

(7) Calculer le reste de la division euclidienne de 51^{24} par 72.

(8) Soit $n \in \mathbb{N}^*$. On considère D_n le groupe engendré par les éléments a et b vérifiant $a^2 = b^n = (ab)^2 = 1 \quad n \geq 3$

a) Montrer que tout élément de D_n peut se mettre sous la forme $a^i b^j$ où $0 \leq i < 2$ et $0 \leq j < n$

b) Montrer que D_n est isomorphe au groupe des isométries du $n - gone$ régulier.

c) Montrer que D_n est isomorphe au groupe multiplicatif engendré par les matrices $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $y = \begin{pmatrix} e^{2i\pi/n} & 0 \\ 0 & e^{-2i\pi/2n} \end{pmatrix}$

Une application : Le système RSA

Système de cryptage à clé public

Le principe : Une personne R veut pouvoir recevoir des messages de tout autre personne de manière qu'elle soit seule (avec l'expéditeur) à pouvoir comprendre le message. R choisit une clé E d'encryptage et une clé correspondante D de décryptage. E est public (c-à-d) que R fait savoir (dans un annuaire où sur sa page web...) que la clé d'encryptage est E mais D est

secrète et n'est connu que de R. Ces clés se correspondent mais la connaissance de E ne suffit pas à trouver D...

la pratique : R choisit deux nombres premiers très grands distincts p, q et forme $n = pq, m = \varphi(n) = (p-1)(q-1)$. R choisit alors un entier positif $e < m$ et premier avec m. Donc e est inversible dans $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$, soit d tel que $ed \equiv 1(modm)$. Les nombres n, e constituent la clé public mais p, q, m sont conservés secets. Le message à transmettre est d'abord chiffré modulo n et on applique ensuite la fonction

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n : x \mapsto x^e$$

le déchiffrement consiste en la fonction :

$$g : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n : y \mapsto y^d$$

Montrer que $g(f(x)) = x(modn)$ et $f(g(x)) = x(modn)$.

La sécurité du système repose sur la difficulté de factoriser les nombres très grands.

Exemple : $p = 3, q = 11$ Utiliser le système RSA pour crypter la suite $16, 21, 02, 12, 09, 03$. décrypter la suite $28, 26, 27, 24, 26, 14$

$n = 3 \times 11 = 33$ et $m = 2 \times 10 = 20$ Soit $e = 13$ (par exemple) La clé public est donc $(n = 33, e = 13)$. Dans $\mathbb{Z}_{20}$ on a $13^{-1} = 17(mod20)$. Donc la clé privée secrète est 17. Le cryptage utilise la fonction $f(x) = x^{13}(mod33)$ et le décryptage la fonction $g(y) := y^{17}(mod33)$. Le code chiffré correspondant à $16, 21, 02, 12, 09, 03$ est donc $04, 21, 08, 12, 09, 27$. D'autre part la suite cryptée $28, 26, 27, 24, 26, 14$ correspond à $19, 05, 03, 18, 05, 20$.