SORBONNE UNIVERSITÉ

Bases de l'Arithmétique et Cryptologie Romantique

Version du 15 janvier 2021

TD

Exercice 1 – Questions introductives de Cryptologie

1. Rappeler la définition de la cryptologie.
2. Quelle est la différence entre cryptographie et cryptanalyse ?
3. Quelle est la différence entre la cryptographie et la stéganographie ?
4. Quel mathématicien célèbre s'est illustré en participant à la cryptanalyse de la machine à chiffrer utilisée par l'armée allemande pendant la seconde guerre mondiale ?
5. Donner le nom de la machine dont on parle dans la question précédente ?
6. L'utilisation des moyens cryptographiques est-elle libre en France ? Qu'en est-il du transfert de moyens de cryptanalyse ?

1 Quelques bases

Exercice 2 – Rappels d'arithmétique de base

1. Que représente l'expression $31 \mod 26$? Quelle est son représentant canonique ?
2. Que vaut $-3 \mod 26$?
3. Rappeler la définition d'un nombre premier. Du pgcd de deux entiers.
4. Donner la table de multiplication modulo 12.
5. Donner l'ensemble des couples $(a.b) \in \{0, \ldots, 11\}^2$ tels que b soit l'inverse de a pour l'addition modulo 12
6. Donner l'ensemble des couples $(a.b) \in \{0, \ldots, 11\}^2$ tels que b soit l'inverse de a pour la multiplication modulo 12
7. Exhiber un élément a dans $\{0, \ldots, 11\}$ différent de 0 tel qu'il existe un $b \neq 0$ et vérifiant $a \times b = 0 \mod 12$.
8. Résoudre l'équation $7x + 5 = 4 \mod 12$. Qu'en est-il de l'équation $3x + 5 = 7 \mod 12$?

Exercice 3 – Structures algébriques

1. Rappeler la définition d'un groupe.
2. Vérifier que l'ensemble des classes modulo un entier n muni de l'addition forme bien un groupe (on le note généralement $\mathbb{Z}/n\mathbb{Z}$).
3. Rappeler la définition d'un groupe cyclique. Montrer que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique.
4. Montrer que tout groupe fini cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Ce dernier est donc le groupe cyclique de cardinal n canonique.
5. Rappeler la définition d'un groupe commutatif (dit aussi abélien). Donner un groupe de permutation qui n'est pas commutatif.

Exercice 4 – Python, les listes et les statistiques

1. Étant donnée une liste d'éléments numériques (des entiers ou des flottants) donner un fonction Python permettant d'en calculer la moyenne.
2. Étant donnée une variable aléatoire discrète X représentée à l'aide de deux listes de même longueur (la première représentant les valeurs prises par X et la seconde les probabilités correspondant à chacune de ces valeurs) donner une fonction Python permettant de calculer l'espérance de X.
3. Avec les mêmes notations que la question précédente, donner une fonction Python permettant de calculer la variance et l'écart type de X.
4. Soit ℓ une liste Python. Rappeler comment construire toutes les sous-listes de ℓ que l'on peut extraire à l'aide de la syntaxe $\ell[a : b : c]$ où a, b, c sont des entiers (pas forcément positifs).

2 Chiffrement et déchiffrement

Exercice 5 – Mono-alphabétique

1. Rappeler le principe de base de la cryptographie mono-alphabétique. Avec quelle opération mathématique cela peut-il se définir ? Quelle est la clé secrète ?
2. (**Chiffrement de César**) Quelle est la particularité du chiffrement de César dans l'ensemble des chiffrements mono-alphabétiques ? En déduire que la clé secrète peut être définie par le symbole dans l'alphabet d'arrivée correspondant à une lettre fixée dans l'alphabet de départ (le A par exemple). Rappeler avec quelle opération mathématique le chiffrement et le déchiffrement de César peut se définir.
3. (**Chiffrer, déchiffrer des messages pour César**) L'alphabet de départ et d'arrivée est le même : les caractères majuscules non accentués.
   — Chiffrer le message `ATTAQUESURLUTECEDEMAIN` avec la clé `R`.
   — déchiffrer le message `IVIRYNPELCGBYBTVR` avec la clé `N`.
4. En supposant que les alphabets d'entrée et de sortie soient celui des 26 lettres majuscules, estimer la difficulté de retrouver un texte clair à partir d'un chiffré sans connaître la clé pour un chiffrement par décalage ou plus généralement un chiffrement mono-alphabétique.
5. Sur quel principe mathématique se base la cryptanalyse d'un chiffrement mono-alphabétique ?

Exercice 6 – Poly-alphabétique

1. Le chiffrement de Vigenère peut être vu comme une généralisation du chiffrement de César : au lieu de décaler chacune des lettres du message clair selon une lettre (la clé secrète), on va décaler des blocs de lettres selon un mot. Donner un schéma expliquant le chiffrement de Vigenère.
2. — À l'aide de la clé `CESAR`, déchiffrer le message `XSMSRXIRDVLEIUVNUMEJRSANKU` obtenu en utilisant le chiffrement de Vigenère.
   — Avec la clé `CIPHER` chiffrer le message `LATTAQUEESTPREVUEPOURDEMAIN`.
3. Expliquer quel principe mathématique permet de modéliser le chiffrement de Vigenère.

3 Indice de coïncidence et de coïncidence mutuelle

Exercice 7 – Indice de Coïncidence

1. (**Définition**) Rappelez la définition de l'indice de coïncidence d'un texte.
2. (**Calcul**) D'après le tableau suivant, calculer l'indice de coïncidence d'un texte écrit en anglais.

Langue	A	B	C	D	E	F	G	H	I	J	K	L	M
Français	9,42	1,02	2,64	3,39	15,87	0,95	1,04	0,77	8,41	0,89	0,00	5,34	3,24
Anglais	8.08	1.67	3.18	3.99	12.56	2.17	1.80	5.27	7.24	0.14	0.63	4.04	2.60

Langue	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Français	7,15	5,14	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32
Anglais	7.38	7.47	1.91	0.09	6.42	6.59	9.15	2.79	1.00	1.89	0.21	1,65	0.07

3. (**Propriétés**) Montrez que l'indice de coïncidence est invariant par chiffrement par substitution. Qu'en déduisez-vous sur le principe de distinction ?

Exercice 8 – Test de Kasiski vs Indice de Coïncidence

1. (**Cours**) Rappelez le principe du test de Kasiski.
2. (**Utilisation**) Le texte suivant est issu d'un chiffrement par Vigenère d'un texte en anglais. Utilisez le test de Kasiski pour retrouver la longueur de la clé. Peut-on conclure directement à l'aide des indications données dans le texte ? Si non, pour quelle raison ? Si oui expliquer comment.

```
GSRLCVXYEJ TBZKEIPAGP BEAVTBEAVH RCFTGVSSTB PKFQNNNTVJ GUOIWTEHAO
HPWVPVGBEX UQBRYEARRU ENZERYTHUE BKWPAFLFZX LYYEAZWUEU CMNEFWCEAK
LRRIXTEGRR MLGUXUECCH IMRNNLEFVT ONSBTISFYN MJLVSCYOVR GIIYLFVVCB
TGKLRPLZLV XNLYDLVIZE XEHUIFELEA ZQJHYYAVAE ONPOVVFEUY WYMFJOOZDI
ATNZEULVMN STKPBNACHD EATCNIFIZS XPIVRQMICX LTBNCYVZHR NNEARRVNMA
BIEGIIYTEH GHUEMFYGTY CMYICOYEKP SSRIXTEGRL SCBTWJOOWW JYSFCNXYIA
CYSBJXUEIC RTPRALWRWM GTYOMFLVSI HGCMZINLMZ SASNSTKEYO HRIFIZIMLY
CEGCIYMIEQ IWEBFRVNNP KDWGHYNHDT BNYYMJSSTB PKRZRNUCXW IJAHOLZQCL
YLFRRNBCCW RRQTBPIYEA TUDFRPZEGZ KPEGAQZFRR
```

3. (**IC et longueur de clé**) Expliquer comment l'indice de coïncidence permet de retrouver la longueur de la clé lors d'une cryptanalyse de Vigenère.
4. (**Application**) Le tableau suivant est le résultat pour $k = 3, \ldots, 20$, du calcul de l'indice de coïncidence moyen des sous-chaînes $S_i = s_i s_{i+k} s_{i+2k} \cdots$ pour $i \in [0, k-1]$.

k	IC moyen	k	IC moyen
3	0.0431208310349463	12	0.0423336353568912
4	0.0429338103756708	13	0.0396449704142012
5	0.0412621359223301	14	0.0701810833389781
6	0.0428238229266580	15	0.0410287751464222
7	0.0683182595511363	16	0.0429611131476051
8	0.0426682692307692	17	0.0427533861152915
9	0.0450287596385600	18	0.0436051815362160
10	0.0414027149321267	19	0.0445558340295182
11	0.0405418663975556	20	0.0412307692307692

   En déduire la longueur de la clé du chiffrement de Vigenère utilisé pour chiffrer ce texte en anglais.
5. (**Bonus**) Vous finirez la cryptanalyse de ce texte chez vous.

Exercice 9 – Indice de Coïncidence Mutuelle

1. Sachant que le texte suivant

```
WWWVJRKYTB XFDZHTXAXT PHPACUVABO RFXQTATAWP TDIZSASDTI TACWROXRIZ
IHLMCWREEW VMIWSZPBHF WOXFDIXFTF XTTDSQIFCA UFSYPBGQAM VURGAAJZHE
JTJURSLQCQ ITXGXTTCVK RZIMGZCRXH XQSHSTXGSI CZMYXHEFXC REIVEFPZSZ
VDSQBWWMUZ EFRCRFGOHU RHMACWRFTF QEIVIODATA CSRFHCJFWS VMKSRMGSJQ
LORPHWQBAS EYPBENXFHM CRXTTDLMCH EEBOPYTASD NOXMLCQMC
```

a été chiffré en utilisant une clé de taille 4 et le cryptosystème de Vigenère, retrouvez le texte clair en utilisant la table des indices de coïncidence mutuelle suivante

i	j	Indice de coïncidence mutuelle entre s_i et Dec(s_j, d) avec $d = 0, \ldots, 25$												
0	1	0.034	0.064	0.038	0.042	0.027	0.041	0.040	0.031	0.031	0.034	0.039	0.029	0.045
		0.028	0.041	0.033	0.047	0.035	0.037	0.034	0.044	0.046	0.032	0.052	0.031	0.031
0	2	0.053	0.043	0.044	0.025	0.035	0.050	0.042	0.035	0.027	0.033	0.044	0.063	0.041
		0.033	0.027	0.042	0.037	0.033	0.033	0.035	0.036	0.029	0.040	0.032	0.043	0.034
0	3	0.024	0.029	0.039	0.063	0.045	0.028	0.026	0.047	0.034	0.035	0.036	0.038	0.032
		0.029	0.045	0.043	0.041	0.034	0.047	0.040	0.031	0.029	0.037	0.054	0.042	0.037
1	2	0.036	0.034	0.028	0.040	0.041	0.041	0.034	0.038	0.044	0.040	0.063	0.043	0.032
		0.030	0.044	0.039	0.034	0.038	0.035	0.027	0.027	0.042	0.039	0.037	0.033	0.049
1	3	0.036	0.040	0.065	0.042	0.024	0.029	0.046	0.037	0.029	0.046	0.040	0.021	0.033
		0.050	0.046	0.031	0.033	0.049	0.031	0.030	0.037	0.048	0.038	0.034	0.040	0.030
2	3	0.023	0.024	0.043	0.044	0.050	0.039	0.043	0.040	0.025	0.034	0.027	0.045	0.035
		0.045	0.041	0.023	0.034	0.043	0.076	0.040	0.025	0.031	0.032	0.045	0.034	0.048

4 Chiffrements polygrammiques

Exercice 10 – Chiffrement ADFGVX

On utilise le carré de Polybe suivant :

	A	D	F	G	V	X
A	c	l	o	f	w	j
D	y	m	t	5	b	4
F	i	7	a	2	8	s
G	p	3	0	q	h	x
V	k	e	u	ℓ	6	d
X	v	r	g	z	n	9

et une transposition de longueur ℓ.

1. Quel est le taux d'expansion de ce chiffrement pour une clef de longueur ℓ ?
2. Chiffrer le texte `attaquesurparisle12janvier` avec la transposition $[2, 1, 4, 6, 3, 5]$.
3. Déchiffrer le texte `GFFFV FFDFF DDFXG FVDVV XFVVF GXGAD AXDGV FGVFX FFVAF FVV` à l'aide du même tableau et de la permutation $[3, 1, 6, 2, 5, 4]$.

L'ancien major de l'école polytechnique Georges-Jean Painvin entré en tant que réserviste au service du chiffre français, réussit à cryptanalyser entre avril et mai 1918, le cryptosystème ADFGVX mis en place par les allemands au début mars de la même année. En particulier, cette analyse lui permit de déchiffrer un message allemand sur l'organisation d'une attaque au nord de Compiègne. Cette attaque déjouée fût un des tournants pour la victoire des français. Le secret sur cette attaque fût classé pendant 50 ans (classique concernant le secret militaire) et le colonel allemand Nebel fût fort désappointé lorsqu'en 1967 il apprit que son cryptosystème était cassé depuis fort longtemps !

Exercice 11 – Inversion modulaire et Chiffrement de Hill

1. (**Préliminaires**) Rappeler la définition de l'anneau $A = \mathbb{Z}/7\mathbb{Z}$. Donner la table d'addition et de multiplication de A. L'anneau A possède-t-il des diviseurs de zéro ? Est-il intègre ? Est-il un corps ? Quelle est la différence majeure entre $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/26\mathbb{Z}$?
2. (**Chiffrement affine**) Donner la définition d'un cryptosystème par chiffrement affine avec $\mathcal{P} = \mathcal{C} = A$. Quelle est la différence principale avec le cas où $\mathcal{P} = \mathcal{C} = \mathbb{Z}/26\mathbb{Z}$?
3. (**Chiffrement de Hill**) Le cryptosystème poly-alphabétique de Hill que nous allons étudier ici permet de chiffrer des données de deux caractères de l'alphabet $\mathbb{Z}/7\mathbb{Z}$. Une clé K sera représentée par une matrice 2×2 à coefficients dans $\mathbb{Z}/7\mathbb{Z}$ et la fonction de chiffrement correspondante sera l'application de K sur un vecteur de deux caractères. Donner la représentation formelle de ce cryptosystème comme nous l'avons vu en cours. Quelle caractéristique doit avoir la matrice K pour que le cryptosystème soit valide ?
4. Montrer que l'ensemble des matrices 2×2 sur un anneau A forme lui-même un anneau et que le sous-ensemble des matrices inversibles est un groupe pour la multiplication.
5. Montrer que, lorsqu'elle existe, l'inverse d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ peut être calculée par la formule suivante (matrice complémentaire) :
$$B = (\det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
où det est le déterminant de A et est égal à $ad - cb$.
6. Déduire de la question précédente un moyen de reconnaître une matrice inversible. Donner alors une nouvelle spécification du chiffrement de Hill, exhiber un exemple de chiffrement et déchiffrement pour une clé bien choisie.

Exercice 12 – Cryptanalyse du Chiffrement de Hill

1. (**Cours**) Rappelez quelles sont les hypothèses faites lors d'une cryptanalyse à clair/chiffré connu.
2. (**Attaque du chiffrement de Hill**) Supposons la taille $m \times m$ de la matrice clé connue. Montrer comment le chiffrement de Hill peut être cryptanalysé à l'aide d'un texte (succession de blocs) clair/chiffré bien choisi.
3. (**Application**) Supposons que le texte `FRIDAY` est chiffré en utilisant le cryptosystème de Hill (modulo 26) avec une taille de blocs $m = 2$ en le texte `PQCFKU`.

5 Exercices des annales

Exercice 13 – Cryptanalyse de Vigenère par mot probable

On s'intéresse ici à une méthode de cryptanalyse générale, celle du *mot probable*, appliquée au chiffrement de Vigenère. Dans tout cet exercice on part donc de l'hypothèse que nous connaissons un mot probable dans le texte clair et que le cryptosystème utilisé est de type Vigenère.

1. Expliquez comment vous pourrez utiliser cette hypothèse pour cryptanalyser un texte chiffré. Vous décrirez bien toutes les hypothèses nécessaires pour mener à bien votre cryptanalyse.
2. Votre bataillon a intercepté un message hier à destination d'un sous-marin ennemi (francophone). Sachant que ces messages commencent toujours par un bulletin météo de la forme *lundi ciel bleu etc.* ou encore *vendredi orage venant de l'ouest etc.* et que le mot clé est rarement de longueur plus grande que 5. On vous demande de cryptanalyser cette interception

```
YURGQ ZOAJM EYTDD QLSHA MNTDY GYSXZ XCLHX MLLHA F
```

Exercice 14 – Sur le chiffrement de Vigenère et le problème d'échange de clé

Dans tout cet exercice on considère des chiffrements de Vigenère à l'aide de clés de longueur identique fixée ℓ. Ces chiffrements s'effectuent comme d'habitude sur l'alphabet standard $\mathcal{A} = \{A, \ldots, Z\}$. Ainsi, les chiffrements qui nous intéressent sont tous des applications de $\mathcal{A}^\ell$ dans $\mathcal{A}^\ell$ et peuvent être rassemblés dans un l'ensemble

$$\mathcal{V}_\ell = \{e_K \,:\, \mathcal{A}^\ell \to \mathcal{A}^\ell \mid e_K \text{ un chiffrement de Vigenère de clé } K \text{ de longueur } \ell\}\,.$$

1. On souhaite munir l'ensemble $\mathcal{V}_\ell$ de l'opération de *composition* dénotée $\circ$ par la suite. On rappelle que la composition $h = f \circ g$ de deux applications f et g (compatibles) est définie par $h(x) = f(g(x))$.
   Montrer que $\mathcal{V}_\ell$ est stable par composition, c'est-à-dire que pour tout couple (e_{K_1}, e_{K_2}) d'éléments de $\mathcal{V}_\ell$, la composition $e_{K_1} \circ e_{K_2}$ est possible et qu'elle résulte en un élément de $\mathcal{V}_\ell$. Vous donnerez explicitement la clé K_3 qui permet de définir la composition $e_{K_1} \circ e_{K_2}$ comme un élément e_{K_3} de $\mathcal{V}_\ell$.
2. Montrer que l'ensemble $\mathcal{V}_\ell$ muni de la composition forme un groupe. Montrer de plus qu'il est commutatif.

On souhaite utiliser uniquement le chiffrement de Vigenère pour réaliser un échange de clé sans rencontre préalable. Plus exactement, nous nous plaçons dans le scénario suivant. Alice et Bob souhaitent communiquer avec un chiffrement symétrique en utilisant la même clé secrète K. C'est Alice qui initialise la démarche et choisit donc la clé K.

Pour réaliser cet échange de clé (en trois passes), Alice et Bob se sont mis d'accord et n'utilisent que des fonctions de chiffrement issues de $\mathcal{V}_\ell$. Ils réalisent alors les étapes suivantes

Étape 1 : Alice choisit une clé K_1 aléatoire de longueur ℓ et envoie $s_1 = e_{K_1}(K)$ à Bob ;
Étape 2 : en retour, Bob choisit une clé K_2 aléatoire de longueur ℓ et envoie $s_2 = e_{K_2}(s_1)$ à Alice ;
Étape 3 : finalement Alice réalise un dernier envoi à Bob

3. Expliquer quel est le dernier envoi réalisé par Alice pour être sûr que Bob ait en sa possession la clé K.
4. Montrer qu'un attaquant peut retrouver la clé K très facilement à partir de s_1, s_2 et le troisième envoi d'Alice.
5. Quelles propriétés doit vérifier un chiffrement symétrique pour que l'on puisse l'utiliser en remplacement du chiffrement de Vigenère dans le cadre d'un échange de clé en trois passes comme expliqué précédemment ?
6. Rappeler l'avantage spécifique au chiffrement One-time Pad de Vernam. Pourraît-il convenir dans le cadre de la question précédente ?

On souhaite maintenant réaliser l'opération suivante : remise anonyme de données chiffrées sans échange de clé. On se place dans le scénario où un indicateur ne voulant pas révéler son identité désire transmettre des informations secrètes à un agent de police. Pour cela on autorise uniquement des chiffrements symétriques comme définis à la question 5.

7. L'indicateur dépose dans un lieu anonyme un message chiffré avec l'explication du procédé de chiffrement utilisé (sans révéler sa clé secrète bien sûr) et prévient le policier de l'endroit où il peut retrouver les données de l'indicateur. Montrer comment ils peuvent procéder pour que l'échange de données se fasse comme l'indicateur le souhaite (i.e. que ce dernier doit rester anonyme).

Exercice 15 – Vigenère Autoclave

On s'intéresse ici à une utilisation du cryptosystème de Vigenère avec une clé de longueur m pour chiffrer un texte de plusieurs blocs de longueur m chacun.

Pour chiffrer le premier bloc B_0 du texte on utilise le chiffrement de Vigenère avec la clé privée K. Pour un bloc B_i arrivant à la position $i > 0$ dans le texte, on utilise le chiffrement de Vigenère en prenant comme clé le chiffré du bloc B_{i-1}.

1. Représenter le chiffrement d'un texte de n blocs de longueur m à l'aide d'un schéma. Expliquer comment déchiffrer ce texte.
2. À l'aide de ce cryptosystème, chiffrer le texte `ATTAQUEPARIS` avec la clé $K =$`UP`. Déchiffrer le texte `URIRDDWJ` avec la clé `DN`.
3. Supposons que la longueur de la clé soit connue. Est-ce que l'utilisation du cryptosystème de Vigenère de cette manière peut être cryptanalysée avec les techniques vues en cours/TD/TME ? Si non, est-il pour autant plus sûr que l'utilisation classique de Vigenère ? (Argumentez vos réponses.)

Exercice 16 – Cryptanalyse Vigenère

Un texte a été chiffré en utilisant le chiffrement de Vigenère avec une clé de taille ℓ. Le voici ici découpé tous les 5 caractères pour le rendre plus lisible, mais il a été chiffré en ne considérant que des lettres de l'alphabet en majuscules.

```
HIBKA UQFLF SBQSX SKCFB YOAGP ALGTC RTYTL
DGBYO AGPAL OAKYB FBILY OYQTD ISVAI JJNNA
DXNLW NRQPF BVPWN IWAFB YAANR URTZE LYZLF
MEWHI BKAUQ FLALJ GTXRG VNIJP ZREQL KWZA
```

1. Donner les entiers les plus probables pour la longueur de la clé ℓ. Vous expliquerez votre démarche.

6 Groupes, anneaux, pgcd

Exercice 17 – Questions de Cours

1. Dans un anneau A comment sont définis les éléments inversibles et les diviseurs de 0 ? Un diviseur de 0 peut-il être inversible ? Qu'est-ce qu'un anneau intègre ? Donnez un exemple d'un anneau qui l'est et un autre qui ne l'est pas.
2. Rappeler la définition d'irréductibilité pour un élément d'un anneau intègre. Quelle est la définition d'un anneau factoriel ?
3. Quelles caractéristiques (parmi celles citées plus haut) possède l'anneau des entiers $\mathbb{Z}$? Que sont les éléments irréductibles de $\mathbb{Z}$?

Exercice 18 – Sur le PGCD et son calcul

1. Donner la décomposition en produits d'éléments irréductibles des entiers $a = 1170$ et $b = 330$. Donner les listes $D(a)$ et $D(b)$ des diviseurs de a et b et calculer l'intersection $D(a) \cap D(b)$.
2. Déduire de la question précédente le PGCD de a et b.
3. Rappeler la définition du PGCD vue en cours et basée sur les valuations p-adiques. Est-ce que cette définition permet de calculer efficacement le PGCD de deux entiers ?
4. Pour vous convaincre de votre réponse à la question précédente, essayez de calculer le PGCD de 1537 et 1643 à partir des valuations p-adiques de ces deux entiers.
5. En utilisant l'algorithme d'Euclide, calculer le PGCD de la question précédente. Qu'en concluez-vous ?
6. Rappeler la relation de Bachet-Bézout et la définition d'éléments premiers entre eux. Comment repérer une telle propriété sur deux entiers donnés à l'aide de la relation de Bachet-Bézout.
7. Rappeler la définition du ppcm de deux entiers. Quel est la relation entre ab, $\text{pgcd}(a,b)$ et $\text{ppcm}(a,b)$.

Exercice 19 – Lagrange, Bézout et les groupes

Dans tout cet exercice les groupes sont finis et commutatifs. Une notation utilisée ici et par la suite pour éviter les problèmes liés à l'opération du groupe : pour tout entier k strictement positif $[k]g$ représente k opérations de g avec lui-même et $[-1]g$ est l'inverse de g dans le groupe. La notation $[0]g$ représentera donc l'élément neutre du groupe.

1. Rappeler ce qu'est l'ordre d'un élément g d'un groupe fini.
2. Donner l'ordre de chacun des éléments du groupe additif $\mathbb{Z}/30\mathbb{Z}$.
3. En notant $\omega(a)$ l'ordre d'un élément a d'un groupe fini. Montrer que $\omega([k]a) = \dfrac{\omega(a)}{\text{pgcd}(\omega(a),k)}$ pour tout $k \in \mathbb{Z}\setminus\{0\}$. Qu'en déduisez-vous pour $\omega([-1]a)$ et dans le cas où k est premier avec $\omega(a)$.

4. Soit a et b deux éléments d'un groupe fini (commutatif). Montrer que $\omega(a \circ b)$ est un diviseur de ppcm$(\omega(a), \omega(b))$. Qu'en déduisez-vous dans le cas où $\omega(a)$ et $\omega(b)$ sont premiers entre eux.
5. Montrer que tout groupe d'ordre premier est cyclique.
6. Montrer que pour tout diviseur d de l'ordre n d'un groupe G cyclique fini, il existe un unique sous-groupe H de G d'ordre d. (Si G est engendré par g, le sous-groupe H sera engendré par $[\frac{n}{d}]g$).

Exercice 20 – Arithmétique modulaire et Complexité

1. Soit n un en entier et a un élément de $\mathbb{Z}/n\mathbb{Z}$. Si a est inversible peut-il être un diviseur de zéro (argumentez votre réponse) ? Si a est diviseur de zéro, comment calculer l'entier $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 0$?
2. (**Algorithme d'Euclide étendu**) Estimer *a priori* le nombre de calculs à effectuer pour déterminer le pgcd et la relation de Bézout entre 1014 et 5005. Effectuer l'ensemble des calculs intermédiares et présenter les sous la forme d'un tableau comme vu en cours et en TD.
3. (**Inverse ou Diviseur de zéro ?**) L'entier 1014 est-il un inverse ou un diviseur de zéro dans $\mathbb{Z}/5005\mathbb{Z}$? Si c'est un inverse calculer l'entier $b \in \mathbb{Z}/5005\mathbb{Z}$ tel que $1014 \times b = 1 \mod 5005$. Si c'est un diviseur de zéro calculer l'entier $b \in \mathbb{Z}/5005\mathbb{Z}$ tel que $1014 \times b = 0 \mod 5005$.
4. Donner un algorithme et estimer sa complexité pour déterminer si un entier donné dans $\{1 \ldots, n\}$ est un diviseur de zéro modulo n.