Université du Sud-Toulon-Var / UFR-Sciences et Techniques

Maîtrise de mathématiques – TD A

1. Chiffrement à clef secrète

Exercice 1. Le message suivant a été obtenu à l'aide du chiffrement par substitution. Retrouvez la clef secrète et déchiffrez le en utilisant les tables de distributions des lettres qui suivent.

```
  YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
> OURFRIENDFROMPARISEXAMINEDHISEMPTYGLASSWIT
  NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
> HSURPRISEASIFEVAPORATIONHADTAKENPLACEWHILE
  NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
> HEWASNTLOOKINGIPOUREDSOMEMOREWINEANDHESETT
  XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
> LEDBACKINHISCHAIRFACETILTEDUPTOWARDSTHESUN
```

Solution. La clef est `CGHWZQTNMaSXVRYElFDJIKUPBo`, les lettres en minuscules n'ont pas été utilisées dans le message.

Exercice 2. Soit m un entier positif. Montrez que pour tout élément a non-nul de $\mathbf{Z}/m\mathbf{Z}$, les trois propriétés suivantes sont équivalentes :

(1) $a \in (\mathbf{Z}/m\mathbf{Z})^*$;

(2) a n'est pas un diviseur de 0 dans $\mathbf{Z}/m\mathbf{Z}$, autrement dit le seul élément b de $\mathbf{Z}/m\mathbf{Z}$ tel que $ab = 0$ est $b = 0$;

(3) $(a, m) = 1$.

Solution. (1) $\Rightarrow$ (2) est évident. Montrons que (2) $\Rightarrow$ (3) par contraposition : supposons que a ne soit pas premier avec m, il existe donc $k \neq \pm 1$ tel que $a = ka'$ et $m = km'$ et ainsi $am' = a'm$ donc $am' \equiv 0 \pmod m$ et a est alors un diviseur de 0. Reste à montrer que (3) $\Rightarrow$ (1) : si a est premier avec m, d'après Bezout, il existe u et v tels que $au + vm = 1$, donc $au \equiv 1 \pmod m$ et ainsi u est l'inverse de a modulo m.

Exercice 3. Démontrez le théorème suivant du cours : si a et m sont deux entiers, et d leur pgcd, alors la congruence

$$ax \equiv b \pmod m \tag{1}$$

admet exactement d solutions si $d|b$ et n'en admet aucune dans le cas contraire.

Solution. Si $d = 1$, alors d'après l'exercice précédent, la solution est unique et vaut ba^{-1}. L'équation (1) est équivalente à chercher l'ensemble S des solutions (x, k) de l'équation

$$ax - km = b, \tag{2}$$

et de réduire modulo m les $x \in \mathrm{pr}_1(S)$.

Plus généralement, étudions les solutions (x, y) dans $\mathbf{Z}$ d'une équation $ax + by = c$ pour a et b fixés. Comme $\mathbf{Z}$ est principal (voir exercice suivant) et que l'ensemble $\{ax+by,\ (x, y) \in \mathbf{Z}\times\mathbf{Z}\}$ est un idéal de $\mathbf{Z}$(appelé idéal engendré par a et b), il existe un entier c tel que pour tout couple $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, il existe $z \in \mathbf{Z}$ tel que $ax + by = cz$. On en déduit que c divise a et b et réciproquement $(a, b)|a$ et $(a, b)|b$ donc $\forall (x, y) \in \mathbf{Z} \times \mathbf{Z}$, $(a, b)|ax + by$ et ainsi (a, b) divise tout les éléments de l'idéal $c\mathbf{Z}$ donc c en particulier. Finalement l'idéal engendré par a et b est l'idéal $(a, b)\mathbf{Z}$.

On sait donc maintenant que l'équation (2) admet des solutions uniquement si $(a, m)|b$, on suppose donc que $d|b$. Dans ce cas, en notant $a = da'$ et $b = db'$, l'équation (1) devient

$$da'x \equiv db' \pmod m,$$

et on peut également montrer que ce système est équivalent à

$$a'x \equiv b' \pmod{\frac{m}{(d, m)}}.$$

Autrement dit,

$$a'x \equiv b' \pmod{m'} \quad \text{où } m' := \frac{m}{d}.$$

Cette fois, $(a', m') = 1$ et il y a une unique solution t comme nous l'avons déjà montré, donc $x = \lambda m' + t$. On obtient donc toutes les solutions de l'équation (1) avec toutes les valeurs de λ qui donnent des valeurs deux-à-deux distinctes de la quantité $\lambda m' + t$ mod m. On a $\lambda m' + t \equiv \nu m' + t \pmod m$ si et seulement si $m|(\lambda - \nu)m'$, autrement dit si et seulement si $dm'|(\lambda - \nu)m'$ soit $d|(\lambda - \nu)$. Les d valeurs possibles pour λ sont donc $0, 1, 2, \ldots, (d - 1)$ et les solutions sont donc :

$$t, t + m', t + 2m', \ldots, t + (d - 1)m'.$$

Exercice 4. On rappelle qu'un anneau factoriel est un anneau intègre (par hypothèse commutatif) tel que pour tout élément a non-nul, il existe un unique couple (u, ν) avec $u \in A^*$ et ν est une application presque nulle de l'ensemble $\mathcal{P}/\mathcal{R}$ des irréductibles de A quotienté par la relation d'association, tels que

$$a = u \prod_{p \in \mathcal{P}} p^{\nu(p)} \tag{3}$$

On dit que (3) est la décomposition de a en facteurs irréductibles. Démontrez que tout anneau principal A est factoriel. Montrez tout d'abord par l'absurde que dans un anneau principal, il n'existe pas de chaîne d'idéaux strictement croissante pour l'inclusion. Montrez que $\mathbf{Z}$ est un anneau principal et déduisez qu'il est factoriel.

Solution. Supposons qu'il existe une suite strictement croissante pour l'inclusion $(J_n)_{n\in\mathbf{N}}$ d'idéaux de l'anneau principal A. Montrons tout d'abord que $J := \bigcup_{n\in\mathbf{N}} J_n$ est un idéal de A : pour tout couple (x, y) de $J \times J$, il existe un couple d'entiers (n, m) tels que $x \in J_n$ et $y \in J_m$, et on peut supposer que $n \leq m$. Dans ce cas, $J_n \subset J_m$ et les deux éléments x et y appartiennent à J_m donc leur différence $x - y$ également et finalement $x - y \in J$, comme J n'est pas vide c'est bien un sous-groupe additif de A. D'autre part,

pour tout couple $(a, x) \in A \times J$, il existe un entier n tel que $x \in J_n$, ainsi $ax \in J_n$ et $ax \in J$ ce qui prouve que J est un idéal. Comme J est principal, soit a un de ses générateurs. Il existe un entier p tel que $a \in J_p$ et donc $(a) \subset J_p$, soit $J \subset J_p$, mais comme $J \subset J$, pour tout $n \geq p$, $J_n = J_p$ ce qui contredit l'hypothèse.

Pour la deuxième partie de la preuve, il faut montrer que l'ensemble $\mathcal{E}$ des idéaux non-nuls de A dont les générateurs n'admettent pas de décomposition est vide. Supposons que $\mathcal{E}$ ne soit pas vide, dans ce cas on peut construire une séquence $(J_n)_{n\in[1,p]}$ d'idéaux de A strictement croissante à partir d'un idéal arbitraire de $\mathcal{E}$. Le générateur a de l'idéal J_p n'est pas irréductible par hypothèse, il peut donc s'écrire $a = bc$, avec $b, c \notin A^*$, donc $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$ et ainsi b et c admettent une décomposition ce qui est impossible car dans ce cas a en admettrait également une.

Maintenant que l'on sait qu'il existe une décomposition, on laisse la démonstration de son unicité au lecteur.

Un idéal de $\mathbf{Z}$ étant par définition un sous-groupe du groupe additif de $\mathbf{Z}$, montrons que les seuls sous-groupes de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$. Il est aisé de voir que pour tout n, $n\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$. Réciproquement, si H est un sous-groupe de $\mathbf{Z}$, il contient des entiers et leurs inverses, donc des éléments négatifs et positifs. Ainsi l'ensemble $H \cap \mathbf{N}$ est non-vide et le premier axiome des ensembles naturels nous permet d'affirmer qu'il admet un plus petit élément a. Par division euclidienne, pour tout élément $h \in H$, il existe un unique couple (k, r) tel que $h = ka + r$ avec $0 \leq r < a$. Comme H est un sous-groupe de $\mathbf{Z}$, $-ka \in H$ et par conséquent $r \in H$. L'entier r est nécessairement nul sans quoi a ne serait plus le plus petit élément de H puisque $r < a$. Donc $b = ka$. Bien entendu, pour tout $a \in \mathbf{Z}$, $an\mathbf{Z} \subset n\mathbf{Z}$. Finalement $\mathbf{Z}$ est principal et donc factoriel. (N.B. On peut démontrer le théorème fondamental de l'arithmétique de manière élémentaire, sans faire appel aux anneaux factoriels).

Exercice 5. On rappelle l'algorithme d'Euclide étendu :

Algorithme 1 : Euclide étendu

Entrée : deux entiers positifs a et m.
Sortie : deux entiers d et b tels que $d = (a, m)$ et $ba \equiv d \pmod m$.
Règles :

(4a) $\quad (m, a) \mapsto (m, a, 0, 1)$

(4b) $\quad (r, r', t, t') \mapsto (r', r - qr', t', t - qt') \quad$ si $r' \neq 0 \quad$ (avec $q = r \div r'$) ;

(4c) $\quad (r, r', t, t') \mapsto (r, t) \quad$ si $r' = 0$.

Exécutez l'algorithme "à la main" pour $a = 6$ et $m = 33$. Démontrez la justesse de l'algorithme d'Euclide étendu. Pour cela, on note $(r_i, r_{i+1}, t_i, t_{i+1})$ le quadruplet obtenu à chaque application de la règle (4b), avec

$$r_0 = m,\ r_1 = a, \quad t_0 = 0,\ t_1 = 1.$$

On veut donc montrer d'une part qu'il existe un entier k tel que $r_{k+1} = 0$ et que $r_k = (a, m)$. D'autre part, on veut montrer que $t_k a \equiv r_k \pmod m$. Montrez par récurrence que

$$\forall j \in [0, k], \quad r_j \equiv t_j a. \tag{5}$$

En déduire que si $(a, m) = 1$ alors $t_k = a^{-1} \mod m$.

Solution. Montrons tout d'abord que si $0 \leq a < m$, $(a, m) = (a, r)$ où r est le reste de la division euclidienne de m par a (pour l'existence de cette écriture, voir l'exercice suivant). Soit $d := (a, m)$, alors on peut écrire $a = da'$ et $m = dm'$. Comme

$$m = ka + r, \tag{6}$$

avec $0 \leq r < a$, on peut écrire $dm' - kda' = r$, soit $d(m' - ka') = r$ donc d divise a et r, et s'il existait un diviseur commun à a et r plus grand que d, celui-ci diviserait m d'après l'expression (6), ce qui est impossible puisque $d = (a, m)$.

Pour la récurrence sur la congruence (5), elle se fait sur j. Pour $j = 0$ et $j = 1$, c'est évident. Supposons que ce soit vrai pour $j = i - 1$ et $j = i - 2$, on a $r_{i-2} \equiv t_{i-2}a \pmod m$ et $r_{i-1} \equiv t_{i-i}a \pmod m$. D'autre part,

$$\begin{aligned} r_i &= r_{i-2} - q_{i-1}r_{i-1} \\ &\equiv t_{i-2}a - q_{i-1}t_{i-1}a \pmod m \\ &\equiv (t_{i-2} - q_{i-1}t_{i-1})a \pmod m \\ &\equiv t_i a \pmod m \end{aligned}$$

Exercice 6. Montrez que l'anneau $\mathbf{Z}$ est archimédien et en déduire que l'on peut réaliser une division euclidienne dans $\mathbf{Z}$:

$$\forall (a, b) \in \mathbf{Z} \times \mathbf{Z} \setminus \{0\},\ \exists!(q, r) \in \mathbf{Z}^2, \quad a = bq + r \text{ et } 0 \leq r \leq |b|.$$

On rappelle qu'une anneau est archimédien si son groupe additif est archimédien, autrement dit si son groupe additif G est abélien, totalement ordonné et tel que

$$\forall (x, y) \in G_+ \times G_+ \setminus \{0\}, \exists n \in \mathbf{N}, \quad x \leq ny.$$

2. Théorie de Shannon

Exercice 7. Montrez qu'un système cryptographique tel que $|P| = |C| = |K|$ est à confidentialité parfaite si et seulement si les clefs suivent une distribution uniforme et si

$$\forall (x, y) \in P \times C,\ \exists!k \in K, \quad e_k(x) = y.$$

Exercice 8. Montrez que l'entropie d'une distribution de probabilité $p_1, p_2, \ldots, p_n$ satisfait :

$$H(p) \leq \log_2(n).$$

Utilisez l'inégalité de Jensen : si est f est une fonction continue strictement concave sur un intervalle I de $\mathbf{R}$ (l'image du milieu de deux points est strictement supérieure au milieu des images), alors pour tout ensemble de points $x_1, \ldots, x_n$ de I, et toute pondération $a_1, a_2, \ldots, a_n$, $a_i > 0$ ($\sum a_i = 1$),

$$\sum_{i=1}^{n} a_i f(x_i) \leq f\left(\sum_{i=1}^{n} a_i x_i\right).$$

L'égalité étant satisfaite si $x_i = x_j$ pour tout i, j.

Exercice 9. Démontrez que dans un système cryptographique,

$$H(K|C) = H(K) + H(P) - H(C).$$

3. Cryptographie à clef publique, complexité

Exercice 10. Ecrivez un programme sur une machine de Turing qui part d'une bande vierge, écrit n bâtons sur la bande et revient sur le bâton le plus à gauche. Quel est le nombre d'états de cette machine ?

Exercice 11. Ecrivez un programme sur une machine de Turing qui réalise la fonction $n \mapsto 2.n$ sur l'alphabet unaire. Quel est le nombre d'états de cette machine ?

Exercice 12. *(T. Rado).* On définit la productivité $P(T)$ d'une machine de Turing T comme le nombre de 1 sur la bande si elle s'arrête en configuration standard en partant de la bande vierge et 0 sinon. Notons $q(T)$ le nombre d'états d'une machine de Turing T. On définit la fonction $p : \mathbf{N} \setminus \{0\} \to \mathbf{N}$ par

$$p(n) = \max_T \{P(T),\ q(T) = n\}$$

autrement dit on définit la *productivité maximale* des machines de Turing à n états.

(1) Montrez que $p(1) \geq 1$.

(2) Montrez que $p(n + 11) \geq 2n$. Indication : inspirez vous de l'exercice 3 pour construire une machine qui écrit n batons sur la bande et de la machine vue en cours qui écrit la séquence 1^n de n batons.

(3) Montrez que $p(n + 1) > p(n)$ et en déduire que $\forall i \geq j,\ p(i) \geq p(j)$.

(4) Montrez que s'il existe une machine de Turing T_p qui calcule la fonction p avec k états, alors

$$p(n + 2 + 2k) \geq p(p(n)).$$

Indication : composez deux fois cette machine avec la machine qui écrit la chaîne 1^n (exercice 3).

(5) Conclure que la fonction p n'est pas T-calculable en mettant en évidence une contradiction à l'aide des points 2 et 3.