6 Congruences dans $\mathbb{Z}$ et applications à la cryptographie

Contenu

1. Définition de la congruence et propriétés
2. Résolution d'équations de congruences par recherche exhaustive de solution
3. TD cryptographie :
   - exemples de chiffrements par substitution monoalphabétique (chiffrement affine)
   - attaque de chiffrements par analyse fréquentielle.
   - chiffrement polyalphabétique de Hill
4. Problème du logarithme discret et (petit) théorème de Fermat
5. TD cryptographie : le protocole d'échange de clefs de Diffie et Hellman
6. TD cryptographie(*) : le chiffrement clef publique Rivest-Shamir-Adleman (RSA)
7. inversion modulo n et applications simples à la résolution d'équations
8. TP Markov Chain Monte Carlo (*)

6.1 Congruence

Définition 6.1 Soit a, b et n des entiers avec $n > 0$.

a et b sont *congrus modulo* n lorsque a–b est divisible par n.

On note $a \equiv b \pmod{n}$ (mais encore : $a \equiv b\,[n]$).

■ **Exemple 6.1**

1. $17 \equiv 5 \pmod{6}$ car 6 divise $17 - 5 = 12$.
2. $4 \equiv 25 \pmod{7}$ car 7 divise $4 - 25 = -21$.
3. $6 \equiv -4 \pmod{5}$ car 5 divise $6 - (-4) = 10$.

R Dans la notation $a \equiv b \pmod{n}$, les symboles $\equiv$ et $\pmod{n}$ sont partie du même symbole. « $a \equiv b$ » seul n'a pas de sens.

Les relations de congruences généralisent les relation d'égalité ($a = b$ signifie $a - b = 0$). Elles possèdent les mêmes propriétés :

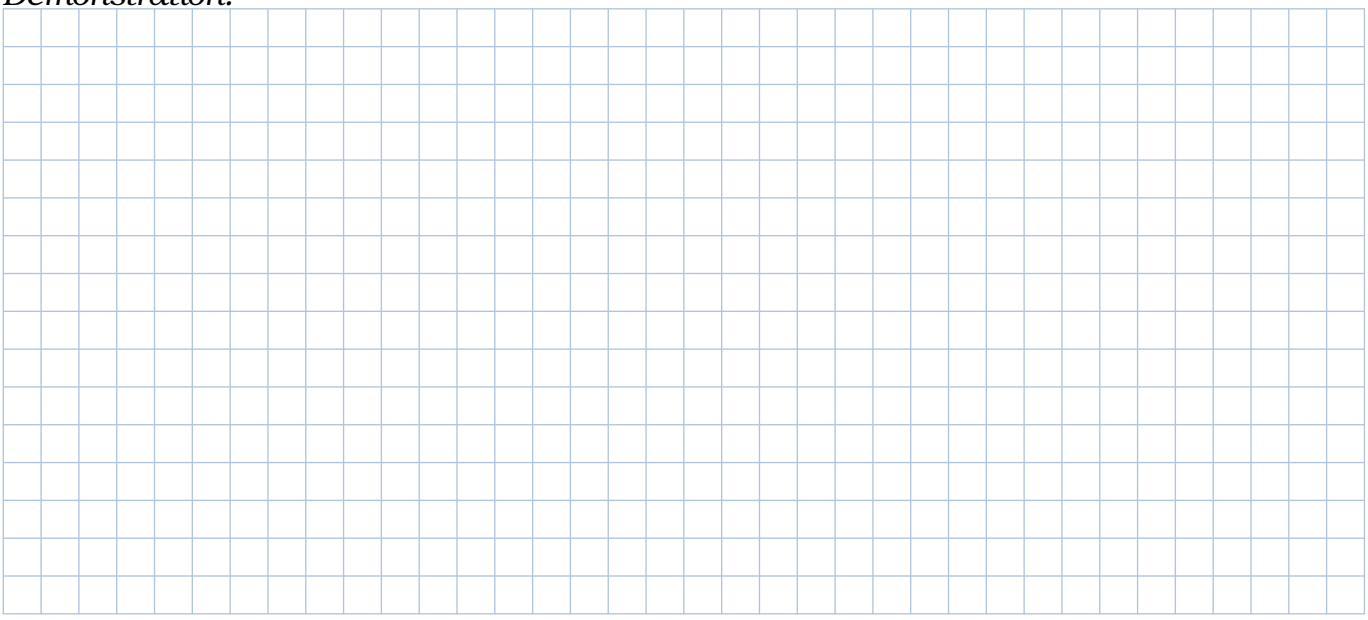
Théorème 6.1 $n > 0$ un entier. Pour tout a, $b \in \mathbb{Z}$.

(i) *(réflexive)* $a \equiv a \pmod{n}$

(ii) *(symétrique)* Si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$.

(iii) *(transitive)* Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$.

Démonstration.



■

Théorème 6.2 Soit n un entier $n > 0$.

Deux nombres a et b sont congrus modulo n si et seulement la division euclidienne de a par n a le même reste que la division euclidienne b par n.

Beaucoup de relations algébriques se base sur le fait que si :

Si $a = b$ et $c = d$ alors $a + c = b + d$ et $ac = bd$.

Nous allons montrer que la congruence dispose de relations similaires :

Théorème 6.3 — compatibilité de la congruence avec les opérations.

Soient a, b, c et d quatre entiers relatifs et n un entier naturel non nul.

(i) *(addition)* Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv c + d \pmod{n}$.

(ii) *(multiplication)* Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $ac \equiv cd \pmod{n}$.

(iii) *(puissances)* Soit p un entier naturel non nul. Si $a \equiv b \pmod{n}$, alors $a^p \equiv b^p \pmod{n}$.

R La congruence n'est pas compatible avec la division : $6 \equiv 2 \pmod{4}$ mais $3 \not\equiv 1 \pmod{4}$.

Démonstration. Soit les entiers tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$.

Il existe k et $k' \in \mathbb{Z}$ tel que $a - b = kn$ et $c - d = k'n$.

■

■ **Exemple 6.2** On a $7 \equiv 4 \pmod{3}$ et $11 \equiv 2 \pmod{3}$ et $50 \equiv 1 \pmod{7}$.

1. $7 + 11 \equiv 4 + 2 \pmod{3} \equiv 6 \pmod{3} \equiv 6 \pmod{3}$.
2. $7 \times 11 \equiv 4 \times 2 \equiv 8 \pmod{3} \equiv 2 \pmod{3}$.
3. $11^2 \equiv 2^2 \pmod{3} \equiv 4 \pmod{3} \equiv 1 \pmod{3}$, le reste de la division de 11^2 par 3 est 1.
4. $100 \equiv 2 \times 50 \pmod{7} \equiv$ .....
5. $50^{100} \equiv 1^{100} \pmod{7} \equiv$ .....

R Pour tout polynôme à coefficient entiers $P(x)$, si $a \equiv b \pmod{n}$ alors $P(a) \equiv P(b) \pmod{n}$.

6.2 Résolution d'équations par recherche exhaustive

Lemme 6.4 Tout entier x est congru modulo n à un entier unique parmi : 0, 1, 2, 3, ...$n-1$.

Démonstration.

■

Soit un polynôme P. On s'interresse aux solutions dans $\mathbb{Z}$ de l'équation $P(x) \equiv c \pmod{n}$.

Lemme 6.5 Si $P(x) \equiv c \pmod{n}$ et $x \equiv x' \pmod{n}$ alors $P(x') \equiv c \pmod{n}$

Méthode de résolution dans $\mathbb{Z}$ l'équation $P(x) \equiv c \pmod{n}$ pour n raisonnablement petit :

1. Déterminer $P(x)$ pour $x = 0$, 1, ...$n-1$.
2. Identifier les solutions $r \in [\![0, n-1]\!]$ de $P(r) \equiv c \pmod{n}$.
3. Les solutions dans $\mathbb{Z}$ sont $\{r_i + kn \mid k \in \mathbb{Z}\}$

■ **Exemple 6.3** Résoudre dans $\mathbb{Z}$ l'équation $n^2 \equiv 2 \pmod{7}$.

Démonstration.

1.

$n \equiv \ldots \pmod 7$	0	1	2	3	4	5	6
$n^2 \equiv \ldots \pmod 7$	0	1	4	2	2	4	1

2. Les restes possibles de la division de n^2 par 7 sont 0, 1, 2 et 4.

   D'après le tableau, les solutions de $n^2 \equiv 2 \pmod{7}$ sont $n \equiv 3 \pmod{7}$ ou $n \equiv 4 \pmod{7}$.

■

■ **Exemple 6.4** Montrer que $a = n(2n+1)(7n+1)$ est divisible par 6.

Démonstration. 1. Étudions les congruences modulo 2 et modulo 3 :

$n \equiv \ldots \pmod 2$	0	1
$2n+1 \equiv \ldots \pmod 2$	1	1
$7n+1 \equiv \ldots \pmod 2$	1	0
$a \equiv \ldots \pmod 2$	0	0

$n \equiv \ldots \pmod 3$	0	1	2
$2n+1 \equiv \ldots \pmod 3$	1	0	2
$7n+1 \equiv \ldots \pmod 3$	1	2	0
$a \equiv \ldots \pmod 3$	0	0	0

2. a est divisible par 2 et 3, $\text{pgcd}(2,3) = 1$, d'après le théorème de Gauss, a est divisible par 6.

■

6.3 Problème du logarithme discret

Définition 6.2 Soit a un entier positif.

Trouver les solutions $N \in \mathbb{Z}$ $a^N \equiv b \pmod{n}$ est le problème du logarithme discret.

Lemme 6.6 — petit théorème de Fermat. p premier, $a \in \mathbb{Z}$.

Si $p \nmid a$ alors $a^{p-1} \equiv 1 \pmod{p}$

Corollaire 6.7 p premier. Pour tout $a \in \mathbb{Z}$ on a $a^p \equiv a \pmod{p}$.

Démonstration.

1. p ne divise par $(p-1)!$.

2. Aucun de $1a$, $2a$, $3a$, $4a$, ...$(p-1)a$ n'est congru à 0 modulo p.

3. $1a$, $2a$, $3a$, $4a$, ...$(p-1)a$ ne sont pas congrus 2 à 2 modulo p.

4. Conséquence et conclusion :

   Les $p-1$ valeurs $1a$, $2a$, $3a$, $4a$, ...$(p-1)a$ sont congrues modulo p *à l'ordre près* à 1, 2, 3...$p-1$.

   D'après la compatibilité de la multiplication :

$$(1a)(2a)(3a)\cdots(p-1)a \equiv 1(2)(3)\ldots(p-1) \pmod{p}$$

$$a^{p-1} \times (p-1)! \equiv (p-1)! \pmod{p}$$

$$a^{p-1} \times (p-1)! - (p-1)! \equiv \pmod{p}$$

$$(a^{p-1}-1) \times (p-1)! \equiv \pmod{p}$$

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

$p \nmid (p-1)!$

■

Application Pour p premier et a entier.

Si N entier, et la division entière par $p-1$ s'écrit $N = q(p-1)+r$ $(0 \leqslant r < p-1)$:

$$a^N \equiv a^{q(p-1)+r} \pmod{p} \equiv \left(a^{p-1}\right)^q a^r \pmod{p} \equiv a^r \pmod{p}$$

Le problème du logarithme discret $a^N \equiv b \pmod{p}$ (avec p premier) peut donc se ramener à la résolution par recherche exhaustive des solutions de $a^r \equiv 1 \pmod{b}$ pour $r \in [\![1, p-1]\!]$

■ **Exemple 6.5**

Résoudre dans $\mathbb{Z}$ l'équation $2^N \equiv 3 \pmod{11}$.

solution.

1.

$r \equiv \ldots \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$2^r \equiv \ldots \pmod{11}$	1	2	4	8	5	10	9	7	3	6	1

2. Les solutions entières dans $[\![0, 10]\!]$ de $2^r \equiv 3 \pmod{11}$ est 8.

   Les solutions de $a^N \equiv 3 \pmod{11}$ sont les entiers $8 + k(11-1) = 8 + 10k$ $(k \in \mathbb{Z})$.

■

R En prenant un nombre premier suffisamment grand (typiquement $p > 10^{100}$), la recherche exhaustive devient impossible en des temps raisonnables. Et il n'y a pas d'alternatives !

6.4 Résolution d'équations simples de la forme $ax \equiv b \pmod{n}$

Définition 6.3 Un entier a admet un *inverse modulo* n s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$.

Théorème 6.8 a admet un inverse modulo n si et seulement si $\text{pgcd}(a, n) = 1$.

Démonstration.

■

Proposition 6.9 Si a admet b comme inverse modulo n. Alors on a l'équivalence :

$$ax \equiv c \pmod{n} \iff x \equiv bc \pmod{n}$$

■ **Exemple 6.6 — inverse d'un nombre modulo n et résolution d'équation.**

1. Démontrer que 17 est inversible modulo 26.
2. Résoudre Dans $\mathbb{Z}$ l'équation $17x \equiv 15 \pmod{26}$

solution.

1. pgcd$(17; 26) = 1$, d'après le théorème de Bézout il existe u et v tel que $17u + 26v = 1$.

   Par la méthode de Bézout : $(1)26 + (0)17 = 26$

   $$(0)26 + (1)17 = 17$$

   $$(1)26 + (-1)17 = 9$$

   $$(-1)26 + (2)17 = 8$$

   $$(2)26 + (-3)17 = 1$$

   $(-3)17 \equiv 1 - (2)26 \pmod{26} \equiv 1 \pmod{26}$.

   (-3) et 17 sont inverses modulo 26.
2. $17x \equiv 15 \pmod{26} \iff (-3)17x \equiv (-3)15 \pmod{26} x \equiv 7 \pmod{26}$

■

R D'après la compatibilité de la multiplication avec la congruence, si $ab \equiv 1 \pmod{n}$ et $b \equiv c \pmod{n}$ alors $ac \equiv 1 \pmod{n}$.

■ **Exemple 6.7 — recherche d'inverse modulo n pour n assez petit.** Dans la recherche d'un inverse modulo n, nous savons que cet inverse sera congru à 0, 1, 2, ...$n-1$. Il est possible de déterminer cet inverse en par essai erreur sur ces $n - 1$ valeurs.

2 et 7 sont premiers entre eux. 2 est inversible modulo 7.

Testons les entiers de 0 à 6 :

1. $0(2) \equiv 0 \pmod{7}$,
2. $1(2) \equiv 2 \pmod{7}$,
3. $2(2) \equiv 4 \pmod{7}$,
4. $3(2) \equiv 6 \pmod{7}$,
5. $4(2) \equiv 8 \pmod{7} \equiv 1 \pmod{7}$. 4 est un inverse de 2 modulo 7.

6.5 Exercices : congruences

Exercice 1

1. Démontrer que $115 \equiv 27 \pmod{11}$ et simplifier son expression.
2. Démontrer que $-39 \equiv 27 \pmod{11}$ et simplifier son expression.

Exercice 2

Soient a et b deux entiers.

1. Sachant que $a \equiv 16 \pmod{5}$. Quel est le reste de la division euclidienne de a par 5 ?
2. Sachant que $b \equiv 17 \pmod{3}$. Quel est le reste de la division euclidienne de b par 3 ?

Exercice 3

Soient deux entiers a et b tels que $a \equiv 7 \pmod{13}$ et $b \equiv 4 \pmod{13}$.

Donner le reste de la division euclidienne par 13 de :

1. $a+b$ | 2. ab | 3. a^3 | 4. a^2-b^2 | 5. $2b-3a$

Exercice 4

Pour chaque valeur de a, trouver un entier $x \in [\![-4,4]\!]$ tel que $a \equiv x \pmod{9}$.

1. $a=11$ | 2. $a=24$ | 3. $a=62$ | 4. $a=85$ | 5. $a=-12$ | 6. $a=32$

Exercice 5

Déterminer les valeurs de $x \in \mathbb{Z}$ tel que $\begin{cases} x+2 \equiv -1 \pmod{7} \\ 100 \leqslant x < 125 \end{cases}$.

■ **Exemple 6.8 — Déterminer le reste de la division euclidienne via les congruences.**

Déterminer le reste de la division de 2^{457} par 5.

solution. *On cherche à faire apparaitre une puissance de* 2 *qui est égale à* $1 \pmod{5}$.
Pour cela, on calcule premières puissance de 2. *On remarque que* $2^4 = 16$ *et* $16 \equiv 1[5]$.
Comme $457 = 4(114)+2$ on a $2^{457} \equiv 2^{4(114)+1} \pmod{5}$

$$\equiv 2^{4(114)} \times 2^1 \pmod{5}$$
$$\equiv \left(2^4\right)^{114} \times 2^1 \pmod{5}$$
$$\equiv \left(1\right)^{114} \times 2 \pmod{5}$$
$$\equiv 1 \times 2 \pmod{5}$$
$$\equiv 2 \pmod{5}$$

Le reste de la division de 2^{457} par 5 est égal au reste de la division de 2 par 5, soit 2. ■

Exercice 6 À l'aide des règles de compatibilité de la congruence, déterminer :

1. les restes de la division par 7 de $351^{12} \times 85^{15}$ et $16^{12} - 23^{12}$
2. les restes de la division par 11 de : 12^{15}, 10^{7}, 78^{15}, 13^{12}, -2^{19}.

Exercice 7

Montrer que $3^{32} + 2$ est divisible par 11 à l'aide des règles de compatibilité des puissances.

Exercice 8

1. Déterminer le reste de la division de 2^{100} par 10 et en déduire le chiffre des unités de 2^{100}.
2. Déterminer le chiffre des unités de l'écriture décimale de 3^{2024}.

Exercice 9 — entrainement.

1. Déterminer le reste de la division euclidienne de 3^{329} par 13.
2. Déterminer le reste de la division euclidienne de 2^{437} par 7.
3. Déterminer le reste de la division euclidienne de $12\,345^{2000}$ par 7.

Exercice 10

1. Déterminer le reste de la division de 2^{10} par 340.
2. En déduire le reste de la division de 2^{341} par 340.

Exercice 11

Déterminer le plus petit entier divisible par 17 et supérieur à 11^{104}.

Exercice 12

1. Vérifier que $2^4 \equiv -1 \pmod{17}$ et $6^2 \equiv 2 \pmod{17}$ et $346 = 16 \times 21 + 10$.
2. En déduire le reste de la division par 17 de 346^{12} et 1532^{20}.

Exercice 13 — tableau de congruence.

1. Démontrer que pout tout n, que n^2 est congru à 0 ou 1 ou 4 modulo 8.
2. En déduire les solutions dans $\mathbb{Z}$ l'équation $(n+3)^2 \equiv 1 \pmod{8}$.

Exercice 14 Résoudre dans $\mathbb{Z}$ les équations

1. $n^3 \equiv -1 \pmod{7}$ | 2. $4x \equiv 5 \pmod{9}$ | 3. $x^2 + x \equiv 2 \pmod{7}$ | 4. $x^2 + x \equiv 2 \pmod{6}$

Exercice 15 — équation quadratique.

On cherche les solutions dans $\mathbb{Z}$ l'équation (E) : $11x^2 - 7y^2 = 5$.

1. Montrer que si x et y sont solutions de (E), alors $x^2 \equiv 2y^2 \pmod{5}$
2. Déterminer les restes possibles de la division de x^2 et $2y^2$ par 5.
3. En déduire que si x et y sont solutions de (E) alors x et y sont des multiples de 5.
4. Que pouvez vous en déduire pour les solutions de (E).

Exercice 16 — bis. Le but de cet exercice est de démontrer que l'équation diophantienne (non linéaire) $x^3 + 10000 = y^3$ n'a pas de solutions entières x et y.

Nous raisonnons par l'absurde et supposons qu'un couple d'entiers x et y solutions existent.

1. Montrer que $x^3 + 4 \equiv y^3 \pmod 7$.
2. Déterminer les restes possibles de la division de $x^3 + 4$ par 7.
3. Identifier une contradiction et conclure.

Exercice 17

1. Montrer que $n(n^2-1)(n^2-4)$ est divisible par 3, 5 et 8.
2. En déduire que a est divisible par 120 (justifier soigneusement).

Exercice 18 — entrainement.

Démontrer à l'aide d'un tableau de congruence adapté :

1. $n(n+1)(2n+1)$ est divisible par 3
2. $n(5n^2+1)$ est divisible par 6
3. $5(n^2+n)^2$ est divisible par 20
4. $n^7 - n$ est un multiple de 21.

■ **Exemple 6.9**

Montrer que pour tout $n \in \mathbb{N}$: $3^{n+3} - 4^{4n+2}$ est divisible par 11.

solution. On utilise la compatibilité modulo 11 :

$$\left.\begin{aligned} 3^{n+3} &\equiv 3^n \times 3^3 \pmod{11} \\ &\equiv 3^n \times 5 \pmod{11} \end{aligned}\right\rangle\ 3^3 \equiv 27 \pmod{11} \equiv 5 \pmod{11}$$

$$\left.\begin{aligned} 4^{4n+2} &\equiv (4^4)^n \times 4^2 \pmod{11} \\ &\equiv 3^n \times 5 \pmod{11} \end{aligned}\right\rangle\ 4^2 \equiv 5 \pmod{11} \textit{ et } 4^4 \equiv 5^2 \pmod{11} \equiv 3 \pmod{11}$$

$3^{n+3} - 4^{4n+2} \equiv 0 \pmod{11}$. ■

Exercice 19

À l'aide des règles de compatibilité de la congruence :

1. Démontrer que pour tout naturel k : $5^{4k} - 1$ est divisible par 13.
2. Démontrer que pour tout naturel n : $5^{2n} - 14^n$ est divisible par 11.

Exercice 20

1. Vérifiez que $7^4 \equiv 1 \pmod{10}$
2. Déterminer selon les valeurs de n les restes possibles de la division entière de 7^n par 10.
3. En déduire les entiers n tel que $7^n - 1$ est divisible par 10.
4. En déduire le chiffre des unités de 7^{98}.

Exercice 21

1. Trouver un entier n tel que $5^n \equiv 1 \pmod 9$
2. Déterminer selon les valeurs de n les restes possibles de la division entière de 5^n par 9.
3. En déduire les entiers n tel que $5^n - 1$ est divisible par 9.
4. En déduire le chiffre des unités de $212^{2020} \equiv 4 \pmod 9$.

Exercice 22

On cherche les solutions dans $\mathbb{Z}$ l'équation $(E)\colon 3x^2 + 7y^2 = 10^{2n}$.

1. Montrer que $100 \equiv 2 \pmod 7$.
2. Montrer que si x et y sont solutions de (E), alors $3x^2 \equiv 2^n \pmod 7$
3. Déterminer les restes possibles de la division de $3x^2$ par 7.
4. Montrer que 2^n est congru à 1, 2, 4 modulo 7.
5. En déduire que l'équation (E) n'a pas de solutions.

Exercice 23

On considère la suite (u_n) définie pour tout $n \in \mathbb{N}$ par $u_n = 2^n + 2^{2n} + 2^{3n}$.

1. Calculer u_0, u_1 et u_2.
2. Démontrer que, pour tout $n \in \mathbb{N}$, $u_{n+3} \equiv u_n \pmod 7$.

Exercice 24 — suite arithmético-géométrique.

On considère la suite (u_n) définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$.

1. Calculer u_1, u_2, u_3 et u_4. Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?
2. Montrer que, $\forall n \in \mathbb{N}$: $u_{n+2} \equiv u_n \pmod 4$.
3. En déduire que $\forall k \in \mathbb{N}$: $u_{2k} \equiv 2 \pmod 4$ et $u_{2k+1} \equiv 0 \pmod 4$.
4. a) Montrer par récurrence que, $\forall n \in \mathbb{N}$, $2u_n = 5^{n+2} + 3$.
   b) En déduire que, $\forall n \in \mathbb{N}$: $2u_n \equiv 28 \pmod{100}$.
5. Déterminer les deux derniers chiffres de l'écriture décimale de u_n en fonction de n.

Exercice 25 — résoudre équation de congruence par recherche d'inverse.

1. Montrer que 4 est inversible modulo 9.
2. Résoudre dans $\mathbb{Z}$ les équations : $(E_1)\colon 4x \equiv 3 \pmod 9$ $\quad$ $(E_2)\colon 7x \equiv 5 \pmod 9$.

Exercice 26 — entrainement. Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $3x \equiv 5 \pmod 4$ | 2. $6x \equiv 2 \pmod 7$ | 3. $4x \equiv 0 \pmod{10}$ | 4. $7x \equiv 2 \pmod{11}$

6.6 TD : chiffrements par substitution

Le chiffrement par substitution est une technique de chiffrement par substitution mono-alphabétique, qui consiste à remplacer chacune des lettres de l'alphabet par une autre. Le chiffre affine est une classe particulière de chiffrement par substitution qui consiste à :

1. Choisir deux entiers a et b, qui sont les *clefs de la ciffre*.
2. Ignorer espaces, majuscules et accents du texte en clair.
3. Chaque lettre est identifiée par son rang x dans l'alphabet de 0 à 25.
4. Pour chaque lettre en clair de rang x est alors remplacée par la lettre de rang égal au *reste de la division de* $ax+b$ *par* 26 (noté ici $(ax+b) \pmod{26}$) dans le texte chiffré.

Pour déchiffrer le message, on suit la même procédure avec des clefs de déchiffrement c et d (à déterminer).

■ **Exemple 6.10 — Atbash.**

Prenons un chiffrement affine de clefs $a=-1$ et $b=25$, ou lettre de rang x est remplacée par la lettre de rang $-x+25 \pmod{26}$ de l'alphabet.

1. $A : 0 \mapsto (-1(0)+25) \pmod{26} \equiv 25 \pmod{26} : Z$
2. $B : 1 \mapsto (-1(1)+25) \pmod{26} \equiv 24 \pmod{26} : Y$
3. $C : 2 \mapsto (-1(2)+25) \pmod{26} \equiv 23 \pmod{26} : X$
4. ...
5. $Z : 25 \mapsto (-1(25)+25) \pmod{26} \equiv 0 \pmod{26} : A$

Ce cas particulier correspond à une inversion de l'alphabet : on subtitue la première letttre à la dernière, la deuxième à l'avant-dernière, et ainsi de suite.

Les clefs de déchiffrement sont ici les mêmes que le chiffrement. En effet : $x \mapsto y \equiv 25-x \pmod{26}$, alors $25-y \pmod{26} \equiv 25-(25-x) \pmod{26} \equiv x \pmod{26}$.

Les mots suivants on été chiffrées par une chiffre Atbash. Déchiffrer les :

1. ..... | 2. ZOTVYIZ:.....

Table 6.1 – Tableau de chiffrement et déchiffrement Atbash

Lettre clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang clair	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Rang chifrré	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	19	20	21	22	23	24	25
Lettre chiffrée	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

■ **Exemple 6.11 — chiffre de César ou par décalage.**

Prenons un chiffrement affine de clefs $a = 1$ et $b \neq 0$, la lettre de rang x est remplacée par la lettre de rang $(1)x + b \pmod{26}$. On remplace une lettre par celle qui suit par un décalage de b lettres.

Pour déchiffrer on utilisera les clefs $c = 1$ et $d = -b$. En effet $x \mapsto y \equiv x + b \pmod{26}$, alors $(1)y - b \equiv (1)(x + b) - b \pmod{26} \equiv x \pmod{26}$.

Ainsi un décalage de 3 lettres, on prendra $a = 1$ et $b = 3$ on obtient le tableau de conversion :

Table 6.2 – Tableau de chiffrement et déchiffrement Atbash

Lettre clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang clair	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Rang chifrré	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
Lettre chiffrée	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

1. Chiffrer “Julius Cesar was not emporor” à l’aide d’un chiffrement par décalage de +3 :

   .....

2. Combien de chiffre de César différentes y a-t-il ? .....

Exercice 27 — attaquer une chiffre de César.

Si un message est suffisamment long, et si on sait que le chiffrement a été fait par décalage il est très facile de déterminer le décalage et de décripter le texte. Il suffit de chercher la lettre la plus fréquente dans le texte, elle serait probablement un “E” (lettre la plus fréquente en français et anglais).

Soit le message chiffré par décalage suivant :

VXKT BT RWTTHT EATAHT

1. Quelle est la lettre la plus fréquente du message ?
2. En supposant que cette lettre correspond à la lettre E quel est la valeur du décalage par le chiffre de César utilisé ?
3. Écrire les correspondances des lettres entre texte clair et chiffré :

Texte chiffré	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Text clair																										

4. Décrypter le message :

   .....

■ **Exemple 6.12**

Prenons le chiffrement affine de clefs $a = 5$ et $b = 8$. La lettre de rang x est remplacée par la lettre de rang $5x + 8 \pmod{26}$.

1. Compléter les tableau et déterminer le texte chiffré obtenu par cette chiffre :

Texte clair	c	h	i	f	f	r	e		a	f	f	i	n	e
x														
$5x + 8$														
$5x + 8 \pmod{26}$														
Text chiffré														

2. Pour déchiffrer le message on utilise le chiffrement affine $21(y - 8) \pmod{26} \equiv 21y + 14$:

   En effet 21 et 5 sont inverses modulo 26 : $21 \times 5 \equiv 105 \pmod{26} \equiv 1 \pmod{26}$

   Et si $y \equiv 5x + 8 \pmod{26}$, alors $21(y - 8) \pmod{26} \equiv 21(5x) \pmod{26} \equiv 1 \pmod{26}$.

Text chiffré	I	H	H	W	V
y					
$21(y - 8)$					
$21(y - 8) \pmod{26}$					
Texte clair					

Toutes les valeurs de a ne sont pas admissibles pour un chiffrement affine. Ainsi, il ne faut pas que deux rangs différents modulo 26 produisent la même lettre chiffrée. Ou encore :

$$\text{si } au + b \equiv av + b \pmod{26} \quad \text{alors} \quad u \equiv v \pmod{26}$$

Exercice 28

Soit le chiffrement affine de clefs a et b : $x \mapsto ax + b \pmod{26}$

1. On suppose que $\text{pgcd}(a, 26) = 1$.
   a) Montrer que si $au + b \equiv av + b \pmod{26}$ alors $a(u - v) \equiv 0 \pmod{26}$.
   b) Justifier que $u - v = 0$
2. a) On suppose a tel que $\text{pgcd}(a, 26) = 2$ et b entier quelconque. Expliquer pourquoi les lettres A et M donneraient le même caractère chiffré.
   b) On suppose a tel que $\text{pgcd}(a, 26) = 13$ et b quelconque. Expliquer pourqui le chiffrement affine de clefs a et b n'est pas admissible.
3. Déterminer le nombre de chiffrement affine différents.

Les chiffrements par substitution monoalphabétique (affine ou quelconque) peuvent être cassé par une simple analyse fréquentielle. Cette découverte est due à Al-Kindi vers 850. Al-kindi constata que pour tout texte assez long, la fréquence d'apparition de chaque lettre se rapproche d'une valeur générique propre à la langue du message. Si la langue du texte est

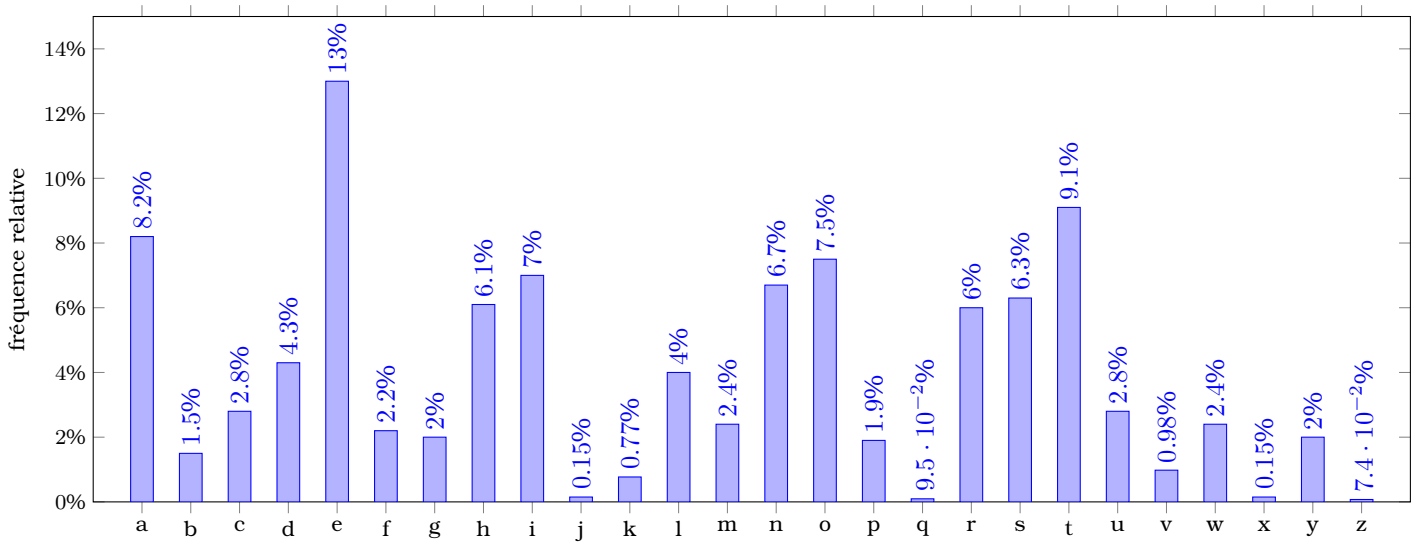


Figure 6.1 – Les lettres les plus courantes dans la langue anglaise sont, dans l'ordre, ETAON RISHD LFCMU GYPWB VKJXZQ.

connue, et si la longueur du texte est suffisante, une analyse fréquentielle aboutira avec un peu de patiente.

Exercice 29 — Breaking the code!.

The following text uses a substitution cipher. Your task is to decipher the passage and complete the substitution alphabet. Several hints are given to help you.

AUHC MVKFC V BYZUGC V IZMC CJ GUMBZYAZD

UKUVM VC HZZGZB CJ GZ V HCJJB PD CFZ VYJM KUCZ

AZUBVMK CJ CFZ BYVWZ UMB OJY U IFVAZ V TJNAB

MJC ZMCZY OJY CFZ IUD IUH PUYYZB CJ GZ.

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
tally																										
frequency																										
Plaintext																										

Hint n° 1: The three most frequently occurring letters in the passage concur with the three most frequent letters in the English language. Find the three most commonly occurring letters in the cipher and substitute the letters you think they could represent.

Hint n° 2: Note that there are some one-letter words; one of these you should already have found. What would the other one be? Use this information to find a fourth letter.

Hint n° 3: The next most frequently occurring letter in the cipher can now be assigned its real letter, So you now have a fifth letter

Hint n° 4: If you have done everything correctly, you should have a couple of words that look like "T?E". Use this information to find a sixth letter.

Hint n° 5: Look at the word "?ATE". There are a few possibilities: DATE, FATE, GATE, LATE, MATE, RATE, SATE. Note that whatever the letter K stands for it stands for the same thing in the second word "?I?HT".

Hint n° 6: Word 20 has a very common ending. By now you should have enough to work out/guess (a very important skills in cipher analysis) to decipher the whole message!

Hint n° 7: Once you have deciphered the whole message, are you able to give the complete substitution table? If not, what would you need to finish the task?

■ **Exemple 6.13 — chiffrement de Hill.**

Le chiffrement de Hill a été publié en 1929. C'est un chiffrement polygraphique dans lequel on chiffre les lettres par paquet. Pour simplifier on travaillera avec des paquets de 2 et un chiffrement de Hill de *matrice clef* $\begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$.

— On regroupe les lettres du message par paquets de 2.

— On remplace les deux lettres par leur rang pour obtenir un couple $(x_1\ ;\ x_2)$ dans $[\![0, 15]\!]$.

— On calcule $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 11x_1 + 3x_2 \pmod{26} \\ 7x_1 + 4x_2 \pmod{26} \end{pmatrix}$

— On prend les lettres de rang y_1 et y_2 pour le texte chiffré.

Ainsi pour chiffrer TE : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv \begin{pmatrix} 11(19) + 3(4) \pmod{26} \\ 7(19) + 4(4) \pmod{26} \end{pmatrix} \equiv \begin{pmatrix} 13 \pmod{26} \\ 19 \pmod{26} \end{pmatrix}$ et donne NT.

1. Quel est le texte chiffré correspondant à ST ?
2. Chiffrer les mots PALACE et RAPACE. Que constatez vous ?
3. Vérifier que $\begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix} \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$.

   En déduire que $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \pmod{26}$
4. Déchiffrer le mot "DQM". Vous rajouterez une lettre pour avoir 4 lettres.

6.7 TD : Protocole d'échange de clefs de Diffie et Hellman

Diffie et Hellman ont proposé en 1976 un protocole d'échange de clés totalement sécurisé. Le problème est le suivant. *Alice et Bob*[1] veulent s'échanger un message crypté de clef k. Ils veulent s'échanger cette clef k, mais ne disposent pas de canal sécurisé et sont sous la surveillance des oreilles indiscrètes d'*Eve*[2]. Le protocole d'échange de clefs de Diffie et Hellman répond à ce problème lorsque k est un nombre entier. Il repose sur l'arithmétique modulaire, et sur le postulat suivant :

— Connaissant a et N, il est facile de déterminer $a^N \pmod n$.

— Connaissant $a^N \pmod n$ et a, il est très difficile de déterminer N.

Table 6.3 – Protocole d'échange de clé de Diffie et Hellman

	Alice	**Bob**
Étape 1	Alice et Bob échangent publiquement un nombre premier p et une base $a \in [\![0, p-1]\!]$.	
Étape 2	Alice choisit secrètement s	Bob choisit secrètement t
Étape 3	Alice envoie publiquement $a^s \pmod p$ à Bob	Bob envoie publiquement $a^t \pmod p$ à Alice
Étape 4	Alice calcule secrètement $k = (a^t)^s \pmod p$	Bob calcule secrètement $k = (a^s)^t \pmod p$

À la fin du protocole, A et B n'ont pas révélé s, t ni k. E peut voir a, p, $a^s \pmod p$ et $a^t \pmod p$ mais ne peut pas retrouver suffisamment rapidement les logarithmes discrets s et t, et donc ne peut trouver la clef $k = a^{st} \pmod p$

■ **Exemple 6.14** Pour des paramètres publics $a = 2$ et $p = 11$:

1. A choisit $s = 4$ et envoie $2^4 \equiv 5 \pmod{11}$ à B. B choisit $t = 8$ et envoie $2^8 \equiv 3 \pmod{11}$ à A.
2. A recoit 3 et calcule $k = 3^s = 3^4 \equiv 4 \pmod{11}$. B recoit 5 et calcule $k = 5^t = 5^8 \pmod 4 \pmod{11}$.
3. La clef secrète de communication est $k = 4$. Et sera alors utilisée par A et B pour le chiffrement de la communication.

L'écouteur E, récupère publiquement $5 \equiv 2^s \pmod{11}$ et $3 \equiv 2^t \pmod{11}$, mais doit déterminer s et t par recherche exhaustive du logarithme discret.

[1] noms utilisés par Rivest, Shamir et Adleman dans leur présentation de l'algorithme de chiffrement RSA
[2] E comme "eavesdropper", écouteuse externe

Dans cet exemple, la recherche exhaustive des logarithmes discrets aboutit rapidement. Dans la pratique, $p > 10^{100}$, s et t sont des entiers avec plus de 100 chiffres. Une recherche exhaustive est impossible.

6.8 TD : le chiffrement clef publique Rivest-Shamir-Adleman (RSA)

après Fermat.

6.9 Exercices : solutions et éléments de réponse

exemple 6.13.

1. Vérifier que TE est chiffré par NT.
2. $ST \mapsto VU$.
3. a) PALACE$\mapsto$ JBRZIE et RAPACE$\mapsto$ FPJBIE.
   b) Que constatez vous ?
4. ETE.

■

6.10 Extra

Exercice 30 Pour $n \in \mathbb{N}$:

1. Démontrer que (n^2+5n+4) et (n^2+3n+2) sont divisibles par $(n+1)$.
2. Déterminer n tel que $(3n^2+15n+19)$ est divisible par $(n+1)$.
3. En déduire que $(3n^2+15n+19)$ n'est jamais divisible par (n^2+3n+2)

⋆⋆ **Exercice 17**

Pour coder un message, on peut procéder de la façon suivante : chaque lettre du message munie de son numéro d'ordre n (voir tableau ci-dessous) est remplacée par la lettre de l'alphabet munie du numéro d'ordre p où $0 \leq\leq 25$ obtenu à l'aide de la formule :

$$p \equiv 3n+7[26]$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(1) Vérifier qu'avec ce chiffrement le S est remplacé par le J.

(2) Coder le mot SECRET.

(3) Montrer que si $p \equiv 3n+7[26]$ alors $n \equiv 9p+15[26]$.

(4) Déchiffrer le message suivant : KGHSX

Pour le DS sur les congruences :

Questions de cours : une démo de cours

Exercice 1 : diviseurs avec combinaison linéaire

Exercice 2 : équation avec congruences

Exercice 3 : congruences et puissances

Exercice 4 : un truc de codage - Yvan Monka