Éléments de théorie des nombres

d'algèbre modulaire

et

application à la cryptographie RSA

Introduction

Le principe de la cryptographie est simple. L'émetteur d'un message (suite de caractères formant des mots et ayant du sens) utilise une fonction de cryptage (bijective) qui remplace le message par une suite de symboles. Le récipiendaire utilise la fonction réciproque afin de reconstituer le message d'origine. Toute personne qui intercepte le message sans connaître la fonction de décryptage éprouve des difficultés à lire le message.

L'histoire de la cryptanalyse a montré qu'aucune difficulté de lecture n'est insurmontable. Le véritable enjeu est de rendre le temps de décryptage suffisamment long pour que le message soit obsolète au moment où il est compris par des tiers. Il en résulte que les fonctions de cryptage et de décryptage doivent non seulement être tenues secrètes mais doivent aussi être changées régulièrement.

Durant des millénaires, la sécurité de la cryptographie se basait sur le prétendu secret des fonctions utilisées autant pour le cryptage que pour le décryptage. Mais les correspondants devaient échanger afin de convenir de la fonction utilisée, ce qui limitait fortement la sécurité. Aujourd'hui, la sécurité est assurée par une fonction de cryptage dont la réciproque est prétendument difficile à déterminer. Ceci permet de publier la fonction de cryptage (appelée clé publique) et de la changer aussi souvent que nécessaire. Aucun échange préalable de la fonction de décryptage (appelée clé secrète) n'est nécessaire.

Le système à clé publique RSA est le plus utilisé actuellement. Nous l'utilisons incessamment dans toutes les communications de nos smartphones. Il se base sur la prétendue grande difficulté de factoriser un nombre construit comme le produit de deux nombres premiers possédant plusieurs centaines de chiffres.

Dans ce cours, nous allons développer les outils algébriques permettant de comprendre la cryptographie RSA. Pour cela nous aborderons quelques éléments de théorie des nombres, acquerrons des compétences en algèbre modulaire et étudierons le fonctionnement du système de cryptographie à clé publique RSA.

Nous utiliserons le langage python afin de programmer les algorithmes étudiés en classe et les appliquer à de grands nombres. Nous nous confronterons aux problèmes pratiques liés à l'implémentation du système de cryptographie à clé publique RSA.

Pour ceux qui désirent en savoir plus sur l'histoire de la cryptographie, nous recommandons la lecture du livre tout public de Simon Singh « Histoire des codes secrets, de l'Egypte des pharaons à l'ordinateur quantique ».

1 Arithmétique modulaire

Exercice 1.

L'aiguille des secondes de ma montre indique 17 secondes. Combien de secondes indiquera-t-elle dans

1) 55 secondes ?
2) 555 secondes ?
3) 5555 secondes ?

Exercice 2.

Sachant que le 1er janvier 2002 était un mardi, déterminer les jours correspondant aux dates suivantes :

1) 29 janvier 2002
2) 12 mars 2002
3) 1er janvier 2003
4) 23 avril 2005

Exercice 3.

Quelle est la date du millième dimanche du XXIe siècle ?

Remarque : le premier jour du XXIe siècle est le 1er janvier 2001.

Définition

Soit m un entier naturel non nul.

Deux entiers relatifs a et b sont dits **congrus modulo** m, et on note

$$a \equiv b \mod m$$

si l'une des conditions équivalentes suivantes est satisfaite

1. leur différence est divisible par m, ce qui signifie qu'il existe $k \in \mathbb{Z}$ tel que $a-b = k \cdot m$, ce que l'on note $m \mid (a-b)$
2. il existe $k \in \mathbb{Z}$ tel que $a = b + k\,m$
3. a et b ont même reste dans la division par m

Dans le langage des congruences, les calculs des exercices 1 et 2 s'écrivent

1. $17 + 55 = 72 = 60 + 12$ donc $\mathbf{72 \equiv 12 \mod 60}$
2. $17 + 555 = 572 = 9 \cdot 60 + 32$ donc $\mathbf{572 \equiv 32 \mod 60}$
3. $17 + 5555 = 5572 = 92 \cdot 60 + 52$ donc $\mathbf{5572 \equiv 52 \mod 60}$

1. $28 = 4 \cdot 7$ donc $\mathbf{28 \equiv 0 \mod 7}$
2. $31 + 28 + 11 = 70 = 10 \cdot 7$ donc $\mathbf{70 \equiv 0 \mod 7}$
3. $365 = 52 \cdot 7 + 1$ donc $\mathbf{365 \equiv 1 \mod 7}$
4. $2 \cdot 365 + 366 + 31 + 28 + 31 + 22 = 1208 = 172 \cdot 7 + 4$ donc $\mathbf{1208 \equiv 4 \mod 7}$

Exercice 4.

Trouver le plus petit nombre supérieur ou égal à 0 qui est congru à a modulo m. Un tel nombre s'appelle **le plus petit résidu non négatif** de a modulo m. C'est le reste de la division euclidienne de a par m.

1) $a = 3412$	$m = 4$	2) $a = 177$	$m = 9$
3) $a = 31$	$m = 31$	4) $a = 31$	$m = 25$
5) $a = 365$	$m = 5$	6) $a = -3122$	$m = 3$
7) $a = 31\ 458\ 687\ 312$	$m = 10$	8) $a = -259\ 874\ 629$	$m = 10$

Exercice 5.

Trouver tous les nombres compris entre 1950 et 2000, qui sont congrus à a modulo m :

1) $a = 1 \quad m = 13$ 2) $a = 1776 \quad m = 40$ 3) $a = 1929 \quad m = 15$

Avant de poursuivre, revenons sur quelques éléments d'arithmétique intervenant dans la définition des congruences.

Définition

Soient a et b deux entiers relatifs avec b non nul.
On dit que b **divise** a, ou que b est un **diviseur** de a, s'il existe un entier relatif q tel que $a = b \cdot q$. Si b divise a, on écrit $b \mid a$; dans le cas contraire, on écrit $b \nmid a$.

Exercice 6. Propriétés de la divisibilité

Soient a, b et c des entiers non nuls. Démontrer les propriétés suivantes :

1. $1 \mid a$
2. $a \mid a$
3. $b \mid 0$
4. si $c \mid b$ et $b \mid a$, alors $c \mid a$
5. si $b \mid a$, alors $b\,c \mid a\,c$
6. si $c \mid a$ et $c \mid b$, alors $c \mid (m\,a + n\,b)$ pour tous $m,n \in \mathbb{Z}$

Théorème de la division euclidienne

Soient a un entier relatif et b un entier naturel non nul.
*Il existe un **unique** couple $(q\,;r)$ d'entiers relatifs tels que*

$$a = b\,q + r \quad \text{avec } 0 \leq r < b\,.$$

On dit que a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** dans la division euclidienne de a par b.

Preuve

1. **Existence de q et r pour a positif ou nul.**
   Pour a positif ou nul, considérons la suite arithmétique de premier terme $u_0 = a$ et de raison $-b$, c'est-à-dire de terme général $u_n = a - b\,n$.
   Cette suite est strictement décroissante et à valeurs entières.
   Soit $r = u_q$ le plus petit terme de la suite (u_n) qui soit positif ou nul.
   Par définition, on constate que :
   (a) $r = u_q = a - b\,q$ équivaut à $a = b\,q + r$;
   (b) $r \geq 0$;
   (c) $r - b = u_q - b = a - b\,q - b = a - b\,(q+1) = u_{q+1} < 0$
   c'est-à-dire $r < b$.

Exercice 7.

2. **Montrer l'existence de q et r pour a négatif.**
   On utilise la suite arithmétique de terme général $u_n = a + b\,n$.

Exercice 8.

2. **Montrer l'unicité de q et r**
   Supposons qu'il existe deux couples d'entiers $(q\,;r)$ et $(q'\,;r')$ tels que
   $$a = b\,q + r = b\,q' + r' \quad \text{avec } 0 \leq r < b \text{ et } 0 \leq r' < b\,.$$
   (a) Montrer que $r - r'$ est un multiple de b.
   (b) Montrer que $-b < r - r' < b$.
   (c) En déduire que $r = r'$ et que $q = q'$.

Exercice 9.

Montrer que les conditions énoncées dans la définition de la congruence sont bien équivalentes :

1. $m \mid (a - b)$
2. il existe $k \in \mathbb{Z}$ tel que $a = b + k\,m$
3. a et b ont même reste dans la division par m

Exercice 10.

Soient a, b, c des entiers relatifs et m un entier naturel non nul. Démontrer les propriétés suivantes :

1. $a \equiv a \mod m$
2. si $a \equiv b \mod m$, alors $b \equiv a \mod m$
3. si $a \equiv b \mod m$ et $b \equiv c \mod m$, alors $a \equiv c \mod m$

On résume ces propriétés en disant que la congruence modulo m constitue une **relation d'équivalence** sur l'ensemble des entiers relatifs.

Exercice 11. Opérations et modulos

Soient a, b, c, d des entiers relatifs et m un entier naturel non nul. On suppose que

$$a \equiv b \mod m \quad \text{et} \quad c \equiv d \mod m\,.$$

Montrer les propriétés suivantes :

1. $a + c \equiv b + d \mod m$
2. $a\,c \equiv b\,d \mod m$
3. $a^n \equiv b^n \mod m$ pour tout $n \in \mathbb{N}$ (par récurrence sur n)

Grâce aux propriétés des congruences, les calculs des exercices 1 et 2 s'écrivent

1. $\mathbf{17 + 55 \equiv 17 - 5 = 12 \mod 60}$ car $55 = 60 - 5$
2. $\mathbf{17 + 555 \equiv 17 + 15 = 32 \mod 60}$ car $555 = 540 + 15 = 60 \cdot 9 + 15$
3. $\mathbf{17 + 5555 \equiv 17 + 35 \equiv 52 \mod 60}$ car $5555 = 5520 + 35 = 60 \cdot 92 + 35$

1. $\mathbf{28 \equiv 0 \mod 7}$
2. $\mathbf{31 + 28 + 11 \equiv 3 + 0 + 4 \equiv 0 \mod 7}$
3. $\mathbf{365 \equiv 1 \mod 7}$ car $365 = 364 + 1 = 52 \cdot 7 + 1$.
4. $\mathbf{2 \cdot 365 + 366 + 31 + 28 + 31 + 22 \equiv 2 \cdot 1 + 2 + 3 + 0 + 3 + 1 \equiv 4 \mod 7}$

Application en théorie des nombres

Les congruences permettent la démonstration d'assertions de théorie des nombres dont en voici quelques-unes.

Exercice 12.

Prouver par récurrence que $6 \cdot 4^n \equiv 6 \mod 9$ pour tout $n \geq 0$ en utilisant la condition $a \equiv b \mod m \Leftrightarrow a = b + k\,m$ (voir définition des entiers congrus modulo, page 3).

Exercice 13.

Montrer que $5^n + 6^n \equiv 0 \mod 11$ pour tout entier naturel impair n.

Exercice 14.

Montrer que $7 \mid (3^{2n} - 2^n)$ pour tout $n \in \mathbb{N}$.

Exercice 15.

1. Constater que $x^2 \equiv 0$ ou $1 \mod 4$ quelque soit l'entier relatif x.
2. Prouver que le cercle centré à l'origine et de rayon $5\sqrt{7}$ ne possède aucun point à coordonnées entières.

2 Éléments de théorie des nombres

Définition

Si a et b sont deux entiers relatifs non tous deux nuls, alors l'ensemble de leurs diviseurs communs $D(a,b)$ est non vide, car il contient 1, et il est fini, car il ne contient que des entiers entre $-a$ et a ou entre $-b$ et b. Par conséquent $D(a,b)$ possède un plus grand élément : on l'appelle le *plus grand commun diviseur* de a et b et on le note pgcd(a,b).

Remarque : pgcd(a,b) = pgcd(b,a) = pgcd$\Big(|a|,|b|\Big)$

Lorsque l'on doit calculer pgcd(a,b), on peut donc supposer a et b positifs, ce que nous ferons dorénavant.

Algorithme d'Euclide

Étant donné deux entiers positifs a et b, effectuons la suite de divisions euclidiennes suivante :

$$\begin{array}{rcrcll} a &=& q_1 \cdot b &+& r_1 & (0 < r_1 < b) \\ b &=& q_2 \cdot r_1 &+& r_2 & (0 < r_2 < r1) \\ r_1 &=& q_3 \cdot r_2 &+& r_3 & (0 < r_3 < r_2) \\ & & & \vdots & & \\ r_{n-2} &=& q_n \cdot r_{n-1} &+& r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} &=& q_{n+1} \cdot r_n & & & \end{array}$$

Alors pgcd$(a,b) = r_n$.

Exercice 16.

Si $a = q\,b + r$, utiliser l'exercice 6 item 6 page 4 $c \mid a\,,\ c \mid b \Rightarrow c \mid (m\,a + n\,b)$ pour montrer que $d \in D(a,b)$ si et seulement si $d \in D(r,b)$.
En déduire que pgcd(a,b) = pgcd(b,r) où r est le reste de la division euclidienne de a par b.
Utiliser cette propriété pour démontrer l'algorithme d'Euclide.

Exercice 17.

Appliquer l'algorithme d'Euclide afin de calculer :

1) pgcd$(308,448)$ 2) pgcd$(120,284)$

Définition

Deux nombres entiers a et b sont dits **premiers entre eux** si pgcd$(a,b) = 1$.

Exercice 18.

Montrer que n^2 et $n+1$ sont premiers entre eux quel que soit $n \in \mathbb{Z}$.

Théorème de Bézout

Soient a et b deux entiers relatifs non tous les deux nuls et $d = pgcd(a,b)$. Alors il existe deux entiers x et y tels que $a\,x + b\,y = d$.

Algorithme d'Euclide étendu

Appliquons l'algorithme d'Euclide et résolvons toutes les équations (sauf la dernière) relativement aux restes successifs :

$$\begin{array}{rcl} a &=& q_1 \cdot b + r_1 \quad \Longrightarrow \quad r_1 = a - q_1 \cdot b \\ b &=& q_2 \cdot r_1 + r_2 \quad \Longrightarrow \quad r_2 = b - q_2 \cdot r_1 \\ r_1 &=& q_3 \cdot r_2 + r_3 \quad \Longrightarrow \quad r_3 = r_1 - q_3 \cdot r_2 \\ & \vdots & \qquad\qquad\quad \vdots \\ r_{n-3} &=& q_{n-1} \cdot r_{n-2} + r_{n-1} \quad \Longrightarrow \quad r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2} \\ r_{n-2} &=& q_n \cdot r_{n-1} + r_n \quad \Longrightarrow \quad r_n = r_{n-2} - q_n \cdot r_{n-1} \end{array}$$

En partant de l'égalité $d = 0 \cdot r_{n-1} + 1 \cdot r_n$, et en remontant, remplaçons successivement chaque r_i pour $i = n, n-1, n-2, \ldots 1$ par sa valeur tirée de l'équation précédente :

$$\begin{aligned} d &= \underbrace{0}_{x_0} \cdot r_{n-1} + \underbrace{1}_{y_0} \cdot r_n \\ &= x_0\, r_{n-1} + y_0\,(r_{n-2} - q_n\, r_{n-1}) = \underbrace{y_0}_{x_1}\, r_{n-2} + \underbrace{(x_0 - y_0\, q_n)}_{y_1}\, r_{n-1} \\ &= x_1\, r_{n-2} + y_1\, r_{n-1} \\ &= x_1\, r_{n-2} + y_1\,(r_{n-3} - q_{n-1}\, r_{n-2}) = \underbrace{y_1}_{x_2}\, r_{n-3} + \underbrace{(x_1 - y_1\, q_{n-1})}_{y_2}\, r_{n-2} \\ &= x_2\, r_{n-3} + y_2\, r_{n-2} \\ &= x_2\, r_{n-3} + y_2\,(r_{n-4} - q_{n-2}\, r_{n-3}) = \underbrace{y_2}_{x_3}\, r_{n-4} + \underbrace{(x_2 - y_2\, q_{n-2})}_{y_3}\, r_{n-3} \\ &= x_3\, r_{n-4} + y_3\, r_{n-3} \\ &\vdots \\ &= x_{n-2}\, r_1 + y_{n-2}\, r_2 \\ &= x_{n-2}\, r_1 + y_{n-2}\,(b - q_2\, r_1) = \underbrace{y_{n-2}}_{x_{n-1}}\, b + \underbrace{(x_{n-2} - q_2\, y_{n-2})}_{y_{n-1}}\, r_1 \\ &= x_{n-1}\, b + y_{n-1}\, r_1 \\ &= x_{n-1}\, b + y_{n-1}\,(a - q_1\, b) = \underbrace{y_{n-1}}_{x_n}\, a + \underbrace{(x_{n-1} - q_1\, y_{n-1})}_{y_n}\, b \\ &= x_n\, a + y_n\, b \end{aligned}$$

Cet algorithme démontre le théorème de Bézout et construit une solution entière de l'équation $a\,x + b\,y = d$.

Exercice 19.

Reprendre les calculs de l'exercice 17, et appliquer l'algorithme d'Euclide étendu afin de déterminer des entiers x et y tels que :

1) $308\,x + 448\,y = 28$ 2) $120\,x + 284\,y = 4$

Corollaire

Deux entiers relatifs a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs x et y tels que $a\,x + b\,y = 1$.

Exercice 20.

Démontrer le corollaire.

Exercice 21.

a) Soient a et b deux entiers et $d = \text{pgcd}(a,b)$. Montrer que $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

b) Soient p et q deux entiers non nuls. Démontrer qu'il existe deux entiers a et b tels que $\dfrac{1}{p\,q} = \dfrac{a}{p} + \dfrac{b}{q}$ si et seulement si p et q sont premiers entre eux.

Lemme de Gauss

Soient a, b, c des entiers non nuls. Si a divise $b\,c$ et si a est premier avec b, alors a divise c.

Exercice 22.

Démontrer le lemme de Gauss grâce au théorème de Bézout.

Définition

Une *équation diophantienne* linéaire à deux variables est une équation de la forme $a\,x + b\,y = c$ où $a,b,c \in \mathbb{Z}$ et dont les solutions doivent être entières.

Théorème de résolution des équations diophantiennes

Soient $a,b \in \mathbb{Z}$, $d = pgcd(a,b)$ et l'équation diophantienne $a\,x + b\,y = c$. Alors

1. *si d ne divise pas c, l'équation diophantienne $a\,x + b\,y = c$ n'a pas de solution.*
2. *si d divise c, l'équation diophantienne $a\,x + b\,y = c$ a une infinité de solutions ; de plus, si $(x_0\,;y_0)$ est une solution particulière, alors toutes les solutions sont données par $x = x_0 + \frac{b}{d}\,k$ et $y = y_0 - \frac{a}{d}\,k$ $(k \in \mathbb{Z})$.*

Exercice 23.

Le but de cet exercice est de prouver le théorème de résolution des équations diophantiennes.

1. Prouver la **contraposée** de la première affirmation : si l'équation diophantienne $a\,x + b\,y = c$ admet une solution, alors d divise c.
2. Supposons que d divise c.
   (a) Montrer que le théorème de Bézout garantit l'existence d'une solution particulière : il existe des entiers x_0 et y_0 tels que $a\,x_0 + b\,y_0 = c$.
   (b) Vérifier que l'équation diophantienne $a\,x + b\,y = c$ admet pour solution $x = x_0 + \frac{b}{d}\,k$ et $y = y_0 - \frac{a}{d}\,k$ pour tout $k \in \mathbb{Z}$.
   (c) Il reste encore à montrer que toutes les solutions de l'équation diophantienne sont de cette forme. Soient x,$y \in \mathbb{Z}$ avec $a\,x + b\,y = c$.
      i. Puisque $a\,x_0 + b\,y_0 = c$, vérifier que la soustraction de ces équations donne $a\,(x - x_0) = b\,(-y + y_0)$, puis $\frac{a}{d}\,(x - x_0) = \frac{b}{d}\,(-y + y_0)$.
      ii. En déduire, grâce à l'exercice 21 et au lemme de Gauss, que $\frac{a}{d}$ divise $-y + y_0$.
      iii. En conclure qu'il existe $k \in \mathbb{Z}$ tel que $y = y_0 - \frac{a}{d}\,k$.
      iv. Après substitution dans l'équation $\frac{a}{d}\,(x - x_0) = \frac{b}{d}\,(-y + y_0)$, constater que $x = x_0 + \frac{b}{d}\,k$.

Exercice 24.

Déterminer toutes les solutions entières des équations suivantes :

1) $42\,x + 25\,y = 3$
2) $153\,x - 102\,y = 413$
3) $45\,x + 27\,y = 117$
4) $120\,x + 43\,y = 12$

Exercice 25.

Peut-on trouver sur la droite d'équation $35\,x + 84\,y = 150$ des points à coordonnées entières ?

Exercice 26.

Les pièces de 1 franc ont un diamètre de 23 mm, celles de 50 centimes un diamètre de 18 mm. En alignant de telles pièces, peut-on obtenir une longueur égale à :

1) 1 dm
2) 1 m

Si oui, quelle est, dans chaque cas, la solution la plus économique ?

Exercice 27.

Un homme veut obtenir des chèques pour un montant de 500 €. Les seuls montants disponibles pour ces chèques sont 20 € et 50 €. Comment doit-il s'y prendre ? Donner toutes les solutions.

Exercice 28.

On doit à Euler le petit problème suivant : « Un soir dans une auberge s'arrêtent plusieurs diligences. Des hommes et des femmes, moins nombreuses, s'attablent. Chaque homme doit payer 19 sous et chaque femme 13 sous. Sachant qu'à la fin du repas, l'aubergiste a récolté exactement 1000 sous, retrouvez combien d'hommes et de femmes ont mangé à l'auberge ce jour-là ».

Code

Programmer une fonction `div_eucl` qui prend deux nombres `a` et `b` en paramètre, imprime la relation « dividende égale quotient fois diviseur plus reste » et retourne le quotient et le reste de la division euclidienne de `a` par `b`.

Exemple, l'appel `div_eucl(334,23)` affichera `334 = 14 x 23 + 12` et retournera le tuple `(14,12)`.

Indication : en python, l'instruction `334//23` *retourne le quotient de la division entière* `14` *et l'instruction* `334%23` *retourne le reste de cette division* `12`.

Code

Implémenter l'algorithme d'Euclide sous la forme d'une fonction itérative `pgdc` qui prend deux entiers comme paramètres, fait appel à la fonction `div_eucl` pour l'affichage et retourne le plus grand diviseur commun.

Exemple, l'appel `pgdc(234,27)` affichera

```
Algorithme d'Euclide
--------------------
 234 = 8 x 27 + 18
  27 = 1 x 18 +  9
  18 = 2 x  9 +  0
```

et retournera 9.

Code

Implémenter l'algorithme d'Euclide étendu sous la forme d'une fonction `bezout` qui prend deux entiers a et b comme paramètres et retourne un tuple contenant d le plus grand diviseur commun et les coefficients x, y d'une combinaison linéaire $x \cdot a + y \cdot b = d$.

Exemple, l'appel `bezout(234,27)` retournera (9, -1, 9) après avoir affiché

```
Algorithme d'Euclide
--------------------
 234 = 8 x 27 + 18
  27 = 1 x 18 +  9

Algorithme de Bézout
--------------------
 9 = 1 x 27 + ( -1) x 18 avec 18 = 234 - 8 x 27
 9 = -1 x 234 + 9 x 27
```

Code

Programmer une fonction `diophante` qui prend trois entiers a, b et c comme paramètres et résout l'équation diophantienne $a\,x + b\,y = c$. La fonction appelle la fonction `bezout` afin d'afficher une solution particulière, puis la solution générale et toutes les solutions positives. Enfin elle retourne le nombre de solutions positives.

Exemple, l'appel `diophante(234,27,900)` retournera 1 après avoir affiché

```
Algorithme d'Euclide
--------------------
 234 = 8 x 27 + 18
  27 = 1 x 18 +  9

Algorithme de Bézout
--------------------
 9 = 1 x 27 + ( -1) x 18 avec 18 = 234 - 8 x 27
 9 = -1 x 234 + 9 x 27

Résolution de l'équation 234 x + 27 y = 900
-------------------------------------------
 Solution entière particulière
    234 x (-100) + 27 x 900 = 900
 Solution entière générale
    234(-100+3k) + 27(900-26k) = 900
 Solutions entières positives si 33.33 < k < 34.62 ou k = 34,...,34
    Solution 1 : 234 x 2 + 27 x 16 = 900
```

3 Équations modulaires

La résolution de systèmes d'équations modulaires linéaires est un très ancien problème d'astronomie qui a été résolu par les astronomes chinois afin de prévoir l'apparition simultanée de phénomènes célestes cycliques différents comme des conjonctions de planètes ou des éclipses.

> Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver, si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune ?

En admettant que le solstice d'hiver et la pleine lune se produisent respectivement tous les 365 jours et tous les 28 jours et en posant x le nombre de jour à attendre, les conditions se traduisent par le système :

$$\begin{cases} x \equiv 6 \mod 365 \\ x \equiv 3 \mod 28 \end{cases}$$

Avant de comprendre comment résoudre un tel système, il nous faut déjà comprendre comment résoudre des équations linéaires à une variable comme

$$a\,x \equiv b \mod m \qquad \text{ou} \qquad a\,x + b \equiv c\,x + d \mod m$$

Exercice 29.

Soient a, b, c, des entiers relatifs et m un entier naturel non nul. Montrer à l'aide de l'exercice 11 item 1 que

$$a \equiv b \mod m \iff a + c \equiv b + c \mod m$$

Cela permet d'affirmer qu'il y a une seule forme d'équation de degré 1 à résoudre puisque

$$a\,x + b \equiv c\,x + d \mod m \iff (a - c)\,x \equiv d - b \mod m$$

Exercice 30.

Peut-on simplifier une congruence comme suit ?

$$2\,a \equiv 2\,b \mod m \quad \text{donc} \quad a \equiv b \mod m$$

Même question si m est impair.

Exercice 31.

Soient a,b des entiers relatifs, m un entier naturel non nul et k un entier relatif non nul.

1. À l'aide de l'exercice 11 item 2, montrer l'implication

$$a \equiv b \mod m \implies k\,a \equiv k\,b \mod m$$

2. À l'aide de l'exercice **??**, donner un exemple qui illustre la fausseté de la réciproque

$$a \equiv b \mod m \not\impliedby k\,a \equiv k\,b \mod m$$

3. À l'aide du lemme de Gauss, montrer que la réciproque est vraie lorsque k et m sont

premiers entre eux.

$$a \equiv b \mod m \quad \Longleftarrow \quad k\,a \equiv k\,b \mod m \quad \text{et} \quad \text{pgcd}(k,m) = 1$$

Définition

Soit m un entier naturel non nul et a un entier relatif, on dit que a est **inversible modulo** m s'il existe un entier relatif k tel que $k\,a \equiv 1 \mod m$.

Dans ce cas, on dit que k est un **inverse modulaire** de a modulo m.

Critère d'existence de l'inverse modulaire

L'équation $a\,x \equiv 1 \mod m$ admet une solution si et seulement si a et m sont premiers entre eux.

Exercice 32.

Le but de cet exercice est de prouver le critère d'existence de l'inverse modulaire.

1. Montrer que l'équation $a\,x \equiv 1 \mod m$ est satisfaite si et seulement s'il existe un entier y tel que $a\,x + m\,y = 1$.
2. Démontrer la proposition précédente à l'aide du théorème de Bézout.

Remarque. C'est un cas particulier du théorème de résolution des équations diophantiennes.

Exercice 33.

Montrer, à l'aide de la proposition précédente, que si a et m sont premiers entre eux, alors l'équation $a\,x \equiv b \mod m$ admet une solution pour tout $b \in \mathbb{Z}$.

Critère d'existence de la solution d'une équation modulaire

L'équation $a\,x \equiv b \mod m$ admet une solution si et seulement si le plus grand diviseur commun de a et m divise b.

Exercice 34.

Le but de cet exercice est de prouver le critère d'existence de la solution d'une équation modulaire.

1. Montrer que l'équation $a\,x \equiv b \mod m$ est satisfaite si et seulement s'il existe un entier y tel que $a\,x + m\,y = b$.
2. Démontrer la proposition précédente à l'aide du théorème de résolution des équations diophantiennes.

Exercice 35.

Résoudre les équations suivantes :

1) $12\,x \equiv 5 \mod 25$
2) $12\,x \equiv 5 \mod 36$
3) $12\,x \equiv 5 \mod 47$
4) $12\,x \equiv 5 \mod 58$
5) $313\,x \equiv 1 \mod 543$
6) $7\,x \equiv 1 \mod 215$
7) $7\,x \equiv 13 \mod 215$

Exercice 36.

Montrer que si $a \equiv b \mod m$ et si d divise m, alors $a \equiv b \mod d$.

Exercice 37.

Soient a,b,m et n des entiers.

Montrer que si $a \equiv b \mod m$, $a \equiv b \mod n$ et si m et n sont premiers entre eux, alors $a \equiv b \mod m\,n$.

Théorème chinois des restes

Soient $m_1, m_2, \ldots, m_n$ des entiers distincts, deux à deux premiers entre eux, et $b_1, b_2, \ldots, b_n$ des entiers quelconques. Alors le système de congruences

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \qquad \vdots \\ x \equiv b_n \mod m_n \end{cases}$$

admet une solution unique modulo $M = m_1\,m_2\,\ldots\,m_n$.

Exercice 38.

Le but de cet exercice est de prouver le théorème chinois des restes.

1. Prouvons d'abord l'existence d'une solution.
   Pour tout $1 \leq i \leq n$, on pose $M_i = \frac{M}{m_i}$.
   (a) Montrer, grâce au critère d'existence de l'inverse, que chacune des équations $M_i\,x \equiv 1 \mod m_i$ admet une solution x_i.
   (b) On pose $x = b_1\,M_1\,x_1 + b_2\,M_2\,x_2 + \ldots + b_n\,M_n\,x_n$.
   Montrer que x constitue une solution du système de congruences.
2. Prouvons ensuite l'unicité de la solution modulo M.
   Soient x et x' deux solutions du système de congruences. Montrer, à l'aide de l'exercice **??**, que $x \equiv x' \mod M$.

Exercice 39.

Le but de cet exercice est de résoudre le système $\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 6 \mod 8 \\ x \equiv -1 \mod 15 \end{cases}$.

1. En reprenant les notations de l'exercice **??**, calculer M, M_1, M_2 et M_3.
2. (a) Calculer $120 \mod 11$. En déduire une solution évidente de l'équation $120\,x \equiv 1 \mod 11$.
   (b) L'équation $165\,x \equiv 1 \mod 8$ équivaut à $165\,x + 8\,y = 1$ pour un certain $y \in \mathbb{Z}$. Résoudre l'équation diophantienne $165\,x + 8\,y = 1$ et en déduire une solution de l'équation $165\,x \equiv 1 \mod 8$.
   (c) Déterminer une solution de l'équation $88\,x \equiv 1 \mod 15$.
3. Résoudre le système de congruences $\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 6 \mod 8 \\ x \equiv -1 \mod 15 \end{cases}$.

Exercice 40.

Résoudre le système $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 0 \mod 4 \end{cases}$.

Exercice 41.

Trouver les nombres dont la division par 3 donne le reste 1, celle par 5 le reste 2 et celle par 7 le reste 3.

Exercice 42.

Un premier phare émet un signal toutes les 15 minutes et un second phare un signal toutes les 28 minutes. On a aperçu le signal du premier à 0 h 02 et celui du second à 0 h 08. À quelle heure au plus tôt les deux signaux coïncideront-ils ?

Exercice 43.

Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver, si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune ?

Remarque : on admet que le solstice d'hiver et la pleine lune se produisent respectivement tous les 365 jours et tous les 28 jours.

Exercice 44.

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la

. fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Exercice 45.

1. Pourquoi ne peut-on pas appliquer le théorème chinois des restes pour résoudre le système $\begin{cases} x \equiv 1 \mod 6 \\ x \equiv 4 \mod 15 \end{cases}$?
2. (a) À l'aide des exercices 3.?? et 3.??, montrer l'équivalence
$$x \equiv 1 \mod 6 \iff \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \end{cases}$$
(b) Montrer l'équivalence $x \equiv 4 \mod 15 \iff \begin{cases} x \equiv 1 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$.
3. En déduire l'équivalence $\begin{cases} x \equiv 1 \mod 6 \\ x \equiv 4 \mod 15 \end{cases} \iff \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$
et résoudre ce système.

Exercice 46.

Résoudre le système $\begin{cases} x \equiv 8 \mod 12 \\ x \equiv 10 \mod 14 \\ x \equiv 3 \mod 7 \end{cases}$

Exercice 47.

L'adjudant-chef a un problème. S'il fait défiler ses hommes par rangs de quatre, il n'a que trois hommes sur le dernier rang. S'il les fait défiler par rangs de cinq, il lui manque trois hommes sur ce dernier rang et par rangs de six, il lui manque un homme.

Sachant que la compagnie comporte entre 100 et 150 hommes, combien d'hommes l'adjudant-chef doit-il faire défiler ?

Exercice 48.

Résoudre le système $\begin{cases} 5\,x \equiv 2 \mod 24 \\ 3\,x \equiv -26 \mod 88 \\ x \equiv 28 \mod 99 \end{cases}$.

Exercice 49.

Une vieille femme se rend à un marché pour y vendre ses œufs. Un cheval piétine sa corbeille et casse tous ses œufs. Le propriétaire du cheval offre de payer les dommages et lui demande combien d'œufs elle avait apportés. Elle ne se souvient pas du nombre exact, mais si elle les avait groupés par paquets de 2,3,4,5 ou 6, il en serait resté chaque fois 1, alors qu'en

les groupant par paquets de 7, il n'en serait resté aucun. Quel nombre minimum d'œufs pouvait-elle avoir ?

Code

Programmer une procédure `inv_mod` qui prend deux entiers comme paramètres et retourne le plus petit résidu positif de l'inverse modulaire du premier modulo le deuxième.

Indication : adapter la procédure `diophante`.

Code

Programmer une procédure `resol_mod` qui prend trois entiers a, b et m comme paramètres et retourne le plus petit résidu positif modulo m de la solution de l'équation modulaire $a\,x \equiv b \mod m$.

Réponses

Solution 1.

1) 12 secondes
2) 32 secondes
3) 52 secondes

Solution 2.

1) mardi
2) mardi
3) mercredi
4) samedi

Solution 3. 1er mars 2020

Solution 4.

1) 0
2) 6
3) 0
4) 6
5) 0
6) 1
7) 2
8) 1

Solution 5.

1) $1951\,;1964\,;1977\,;1990$
2) 1976
3) $1959\,;1974\,;1989$

Solution 15.

1)
2) 0, 1 ou 2

Solution 17.

1) 28
2) 4

Solution 19.

1) $308\cdot 3+448\cdot(-2)=28$
2) $120\cdot(-26)+284\cdot 11=4$

Solution 24.

1) $S=\left\{(9-25\,k\,;-15+42\,k):k\in\mathbb{Z}\right\}$
2) $S=\emptyset$
3) $S=\left\{(2+3\,k\,;1-5\,k):k\in\mathbb{Z}\right\}$
4) $S=\left\{(228+43\,k\,;-636-120\,k):k\in\mathbb{Z}\right\}$

Solution 25. Non

Solution 26.

1) 2 fois 1 fr. et 3 fois 50 ct.
2) 2 fois 1 fr. et 53 fois 50 ct.

Solution 27. $5\,k$ chèques de 20 € et $10-2\,k$ chèques de 50 € avec $0\leq k\leq 5$

Solution 28. 41 hommes et 17 femmes

Solution 35.

1) $x \equiv 15 \mod 25$
2) impossible
3) $x \equiv 20 \mod 47$
4) impossible
5) $x \equiv 229 \mod 543$
6) $x \equiv 123 \mod 215$
7) $x \equiv 94 \mod 215$

Solution 39.

1. $M = 1320$, $M_1 = 120$, $M_2 = 165$ et $M_3 = 88$.
2. (a) $120 \equiv -1 \mod 11$ $x_1 = -1$ (b) $x_2 = -3$ (c) $x_3 = 7$
3. $x \equiv 14 \mod 1320$

Solution 40. $x \equiv 32 \mod 60$

Solution 41. $52 + 105\,k$ où $k \in \mathbb{Z}$

Solution 42. 1 h 32

Solution 43. 9131 jours $= 25$ ans et 6 jours

Solution 44. 785 pièces d'or

Solution 45.

1) pgcd$(6,15) \neq 1$
3) $x \equiv 19 \mod 30$

Solution 46. $x = 80 + 84\,k$ où $k \in \mathbb{Z}$

Solution 47. 107

Solution 48. $x = 226 + 792\,k$ où $k \in \mathbb{Z}$

Solution 49. 301

4 Classes de congruence

Définition

Soit $m \in \mathbb{N}$.

On appelle **classe de congruence** de a modulo m l'ensemble de tous les entiers qui sont congrus à a modulo m ; on la note $\overline{a}_m$ ou simplement $\overline{a}$ s'il n'y a aucune ambiguïté sur m.

$$\overline{a}_m = \{b \in \mathbb{Z} : a \equiv b \mod m\} = \{a + k\,m : k \in \mathbb{Z}\}$$

Un élément d'une classe de congruence s'appelle **représentant** de cette classe.

On peut désigner une classe de congruence par n'importe quel représentant de cette classe. Cependant, il est souvent utile de la désigner par son plus petit représentant non négatif.

On note $\mathbb{Z}/m\mathbb{Z}$ l'ensemble de toutes les classes modulo m :

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}_m\,;\,\overline{1}_m\,;\ldots;\,\overline{(m-1)}_m\}$$

On définit une addition et une multiplication dans $\mathbb{Z}/m\mathbb{Z}$:

$$\overline{a}_m + \overline{b}_m = \overline{a+b}_m \qquad \overline{a}_m \cdot \overline{b}_m = \overline{a\,b}_m$$

L'exercice 11 garantit que ces définitions ont un sens, c'est-à-dire que le résultat ne dépend pas du choix des représentants de ces classes.

Ces opérations vérifient les propriétés suivantes :

1. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
2. $\overline{a} + \overline{0} = \overline{a}$
3. $\overline{a} + \overline{(-a)} = \overline{0}$
4. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$
5. $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$
6. $\overline{a} \cdot \overline{1} = \overline{a}$
7. $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$
8. $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$

Les propriétés 1) à 4) signifient que $\mathbb{Z}/m\mathbb{Z}$ forme un *groupe commutatif*.

Les propriétés 1) à 8) signifient que $\mathbb{Z}/m\mathbb{Z}$ constitue un *anneau commutatif*.

Un ensemble d'entiers $\{r_1\,;r_2\,;\ldots;r_m\}$ constitue un **ensemble complet de représentants** de $\mathbb{Z}/m\mathbb{Z}$ si $\mathbb{Z}/m\mathbb{Z} = \{\overline{r_1}\,;\overline{r_2}\,;\ldots;\overline{r_m}\}$.

Exercice 50.

Lesquels des ensembles suivants sont-ils des ensembles complets de représentants de $\mathbb{Z}/7\mathbb{Z}$:

1) $\{1\,;3\,;5\,;7\,;9\,;11\,;13\}$
2) $\{1\,;4\,;9\,;16\,;25\,;36\,;49\}$
3) $\{1\,;8\,;27\,;64\,;125\,;216\,;343\}$
4) $\{0\,;1\,;3\,;9\,;27\,;81\,;243\}$
5) $\{0\,;1\,;4\,;16\,;128\,;512\,;2048\}$

Exercice 51.

Montrer que $\{0\,;2\,;2^2\,;2^3\,;\ldots\,;2^{11}\,;2^{12}\}$ est un ensemble complet de représentants de $\mathbb{Z}/13\mathbb{Z}$.

Définition

Un élément $\overline{a}$ de $\mathbb{Z}/m\mathbb{Z}$ est dit **inversible** s'il existe $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tel que $\overline{a}\cdot\overline{b} = \overline{1}$. L'élément $\overline{b}$, s'il existe, s'appelle **inverse** de $\overline{a}$.

Exercice 52.

Montrer que si $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ est inversible, son inverse est unique.

Indication : si $\overline{b}$ et $\overline{c}$ sont deux inverses de $\overline{a}$, calculer $\overline{c}\cdot(\overline{a}\cdot\overline{b})$ et $(\overline{c}\cdot\overline{a})\cdot\overline{b}$.

Exercice 53.

Dans $\mathbb{Z}/13\mathbb{Z}$, trouver les inverses de $\overline{2}$, $\overline{4}$, $\overline{5}$ et $\overline{7}$.

Exercice 54.

Dans $\mathbb{Z}/25\mathbb{Z}$, trouver les inverses de $\overline{3}$, $\overline{11}$ et $\overline{23}$.

On appelle **unité** de $\mathbb{Z}/m\mathbb{Z}$ tout élément inversible de $\mathbb{Z}/m\mathbb{Z}$.

Le critère de la page **??** implique que $\overline{a}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ si et seulement si a et m sont premiers entre eux.

Exercice 55.

Dans $\mathbb{Z}/12\mathbb{Z}$, trouver les éléments qui ont un inverse et, pour chacun des éléments trouvés, calculer l'inverse.

Exercice 56.

Mêmes questions avec $\mathbb{Z}/14\mathbb{Z}$.

Exercice 57.

Mêmes questions avec $\mathbb{Z}/20\mathbb{Z}$.

La fonction indicatrice φ d'Euler

Le nombre d'unités de $\mathbb{Z}/m\mathbb{Z}$ se note $\varphi(m)$.

La fonction φ s'appelle la **fonction indicatrice d'Euler**.

Ainsi, $\varphi(m)$ est le nombre d'entiers a tels que $1 \leq a \leq m$ et pgcd$(a,m) = 1$.

Exercice 58.

À l'aide des exercices 4.34, 4.35 et 4.36, calculer $\varphi(12)$, $\varphi(14)$ et $\varphi(20)$.

Exercice 59.

Soit p un nombre premier. Que vaut $\varphi(p)$?

Exercice 60.

Soient p un nombre premier et $k \in \mathbb{N}$.

1. Soit a un entier. Montrer l'équivalence suivante :
   a et p^k ne sont pas premiers entre eux $\iff$ a est un multiple de p.
2. Combien d'éléments contient $\{a \in \mathbb{Z} : 1 \leq a \leq p^k$ et $\text{pgcd}(a,p^k) \neq 1\}$?
3. En déduire que $\boxed{\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)}$.

Exercice 61.

Calculer $\varphi(125)$ et $\varphi(121)$.

Exercice 62.

Soient m et n des entiers positifs premiers entre eux.

Le but de cet exercice est de prouver que $\varphi(mn) = \varphi(m)\,\varphi(n)$.

On désigne respectivement par $(\mathbb{Z}/m\mathbb{Z})^\star = \{\overline{r}_1\,;\overline{r}_2\,;\ldots\,;\overline{r}_{\varphi(m)}\}$ et $(\mathbb{Z}/n\mathbb{Z})^\star = \{\overline{s}_1\,;\overline{s}_2\,;\ldots\,;\overline{s}_{\varphi(n)}\}$ l'ensemble des unités de $\mathbb{Z}/m\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

1. Justifier que l'on puisse définir une application *injective*
   $$\begin{array}{ccc}(\mathbb{Z}/m\mathbb{Z})^\star \times (\mathbb{Z}/n\mathbb{Z})^\star & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (\overline{r}_i\,;\overline{s}_j) & \longmapsto & \overline{a}_{ij}\end{array}$$
   telle que $\begin{cases} a_{ij} \equiv r_i \mod m \\ a_{ij} \equiv s_j \mod n \end{cases}$ pour tous $1 \leq i \leq \varphi(m)$ et $1 \leq j \leq \varphi(n)$.
2. Soient $1 \leq i \leq \varphi(m)$ et $1 \leq j \leq \varphi(n)$.
   (a) À l'aide de l'exercice 3.5 1), montrer que $\text{pgcd}(a_{ij},m) = \text{pgcd}(m,r_i)$ et en déduire que a_{ij} et m sont premiers entre eux.
   (b) Montrer de même que a_{ij} et n sont premiers entre eux.
   (c) En conclure que a_{ij} et mn sont premiers entre eux, c'est-à-dire que $\overline{a}_{ij}$ est une unité de $\mathbb{Z}/mn\mathbb{Z}$.
3. Soit $\overline{a} \in \mathbb{Z}/mn\mathbb{Z}$ avec $\overline{a} \neq \overline{a}_{ij}$ pour tous $1 \leq i \leq \varphi(m)$ et $1 \leq j \leq \varphi(n)$.
   (a) Posons $r \equiv a \mod m$ et $s \equiv b \mod n$.
   Montrer que $r \notin (\mathbb{Z}/m\mathbb{Z})^\star$ ou que $s \notin (\mathbb{Z}/n\mathbb{Z})^\star$.
   (b) Supposons que $r \notin (\mathbb{Z}/m\mathbb{Z})^\star$, c'est-à-dire que $\text{pgcd}(r,m) > 1$.

Montrer, grâce à l'exercice 3.5 1), que pgcd$(a,m) > 1$.
En tirer que $\overline{a}$ n'est pas une unité de $\mathbb{Z}/mn\mathbb{Z}$.

(c) Prouver que si $s \notin (\mathbb{Z}/n\mathbb{Z})^\star$, alors $\overline{a}$ n'est pas une unité de $\mathbb{Z}/mn\mathbb{Z}$.

4. Conclure que $\left\{\overline{a}_{ij} : 1 \leq i \leq \varphi(m) \text{ et } 1 \leq j \leq \varphi(n)\right\}$ constitue l'ensemble des unités de $(\mathbb{Z}/mn\mathbb{Z})$. En déduire la formule $\varphi(mn) = \varphi(m)\,\varphi(n)$.

Exercice 63.

Soit n un entier dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1}\, p_2^{\alpha_2}\, \ldots\, p_k^{\alpha_k}$.
Montrer que

$$\boxed{\varphi(n) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\ldots\left(1 - \tfrac{1}{p_k}\right)}$$

Exercice 64.

Calculer :

1) $\varphi(100)$ 2) $\varphi(720)$ 3) $\varphi(1001)$ 4) $\varphi(10!)$

Exercice 65.

Montrer que $\varphi(5186) = \varphi(5187) = \varphi(5188)$.

Exercice 66.

Trouver tous les entiers positifs n tels que $\varphi(n)$ soit égal à

1) 1 2) 2 3) 3 4) 6 5) 14

Théorème d'Euler

Exercice 67.

Montrer que si pgcd$(a,m) = 1$ et si pgcd$(b,m) = 1$, alors pgcd$(a\,b,m) = 1$.

Indication : il y a trois preuves possibles :

1. utiliser les théorèmes de Bézout et de Bachet de Mériziac ;
2. utiliser la formule de l'exercice 4.18 ;
3. utiliser la proposition de la page 5.1.

Exercice 68.

Montrer que si pgcd$(a,m) = 1$, alors pgcd$(a^n,m) = 1$ pour tout $n \in \mathbb{N}$.

Ordre d'un élément

Exercice 69.

Calculer $2, 4, 8, 16, 32, 64, \ldots, 2^n$

1) modulo 7 2) modulo 10

Que remarque-t-on ?

Exercice 70.

Montrer que si on élève un entier a à des puissances positives : $a, a^2, a^3, \ldots$, alors nécessairement deux de ces puissances seront congrues modulo m.

Indication : combien d'éléments y a-t-il dans $\mathbb{Z}/m\mathbb{Z}$?

Exercice 71.

Montrer que les conditions suivantes sont équivalentes :

1. a et m sont premiers entre eux ;
2. il existe $k \in \mathbb{N}$ avec $1 \leq k < m$ tel que $a^k \equiv 1 \mod m$.

Indications :

1. Supposons qu'il existe $k \in \mathbb{N}$ avec $1 \leq k < m$ tel que $a^k \equiv 1 \mod m$.
   Montrer que a et m sont premiers entre eux, grâce à la proposition de la page 5.1.
2. Supposons a et m premiers entre eux.
   (a) Justifier, à l'aide de l'exercice 4.47, que les classes $\overline{1}$, $\overline{a}$, $\overline{a^2}$, $\overline{a^3}$, ..., $\overline{a^{m-1}}$ sont des unités de $\mathbb{Z}/m\mathbb{Z}$.
   (b) Combien y a-t-il au plus d'unités dans $\mathbb{Z}/m\mathbb{Z}$?
   (c) En déduire qu'il existe $n \geq 0$ et $1 \leq k \leq m-1$ tels que $\overline{a^{n+k}} = \overline{a^n}$, c'est-à-dire $a^{n+k} \equiv a^n \mod m$.
   (d) Conclure que $a^k \equiv 1 \mod m$, grâce à l'exercice 5.2.

Soit a un entier premier à m. L'exercice précédent implique l'existence d'un entier k avec $1 \leq k < m$ tel que $a^k \equiv 1 \mod m$.

Le plus petit entier positif α tel que $a^\alpha \equiv 1 \mod m$ s'appelle l'**ordre** de a modulo m.

Exercice 72.

Trouver l'ordre des éléments non nuls de $\mathbb{Z}/5\mathbb{Z}$.

Exercice 73.

Trouver l'ordre des unités de $\mathbb{Z}/9\mathbb{Z}$.

Exercice 74.

Trouver l'ordre de $\overline{2}$ dans $\mathbb{Z}/m\mathbb{Z}$ pour les valeurs 11, 17, 31, 9 et 14 de m.

Exercice 75.

Trouver l'ordre des éléments non nuls de $\mathbb{Z}/11\mathbb{Z}$.

Théorème d'Euler

Si a et m sont premiers entre eux, alors $a^{\varphi(m)} \equiv 1 \mod m$.

Exercice 76.

Le but de cet exercice est de prouver le théorème d'Euler.

1. Soit $(\mathbb{Z}/m\mathbb{Z})^\star = \{\overline{r}_1 ; \overline{r}_2 ; \ldots ; \overline{r}_{\varphi(m)}\}$ l'ensemble des unités de $\mathbb{Z}/m\mathbb{Z}$.
   (a) Justifier, à l'aide de l'exercice 4.46, que $\overline{a\,r_i}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ quel que soit $1 \leq i \leq \varphi(m)$.
   (b) Montrer que l'application
   $$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\star & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\star \\ \overline{r_i} & \longmapsto & \overline{a\,r_i} \end{array}$$
   est bijective.
2. En déduire que $(a\,r_1)\,(a\,r_2)\,(a\,r_3)\,\ldots\,(a\,r_{\varphi(m)}) \equiv r_1\,r_2\,r_3\,\ldots\,r_{\varphi(m)} \mod m$ et conclure que $a^{\varphi(m)} \equiv 1 \mod m$.

Exercice 77.

Soit $\overline{a}$ une unité de $\mathbb{Z}/m\mathbb{Z}$. Montrer que son inverse vaut $\overline{a^{\varphi(m)-1}}$.

Exercice 78.

(Petit) théorème de Fermat

Si p est premier et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \mod p$.

Démontrer ce théorème à l'aide du théorème d'Euler.

Exercice 79.

Soient a et m deux entiers premiers entre eux. Montrer que si l'ordre de a modulo m est α et si $a^k \equiv 1 \mod m$, alors α divise k.

Indication : la division euclidienne de k par α donne $k = \alpha q + r$ avec $0 \leq r < \alpha$; montrer que $r = 0$.

Exercice 80.

Trouver l'ordre des éléments non nuls de $\mathbb{Z}/13\mathbb{Z}$.

Exercice 81.

Trouver l'ordre des éléments non nuls de $\mathbb{Z}/17\mathbb{Z}$.

Exercice 82.

Trouver l'ordre des unités de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 83.

Trouver le plus petit résidu non négatif de 2^{47} modulo 23.

Exercice 84.

Montrer, à l'aide du petit théorème de Fermat, que si 7 ne divise pas n, alors 7 divise $n^{12} - 1$.

Exercice 85.

Montrer que $n^{13} - n$ est divisible par 2, 3, 5, 7 et 13 pour tout entier n.

Indication : montrer par exemple que $n^{13} \equiv n \mod 5$ en montrant que ou bien 5 divise n, ou bien $n^4 \equiv 1 \mod 5$.

Exercice 86.

Montrer que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ est un entier pour tout entier n.

Indication : multiplier l'expression par 15 et montrer que l'entier obtenu est divisible par 5 et par 3 en utilisant le petit théorème de Fermat.

Exponentiation modulaire

On verra que le système de cryptage RSA nécessite d'effectuer une exponentiation modulaire, c'est-à-dire de calculer $a^n \mod m$, lorsque m et n sont très grands. Heureusement, il existe un algorithme, appelé l'**exponentiation binaire**, qui réduit considérablement le nombre des opérations.

Illustrons-le en calculant $15^{52} \mod 23$.

On commence par écrire 52 en base 2 comme on l'a fait au chapitre 1 :

52	2
0	26
0	13
1	6
0	3
1	1
1	0

On a donc trouvé $52 = \overline{110100} = 2^5 + 2^4 + 2^2$.

Par conséquent $15^{52} = 15^{2^5+2^4+2^2} = 15^{2^5} \cdot 15^{2^4} \cdot 15^{2^2}$.

Il reste encore à déterminer $15^{2^n} \mod 23$ pour $0 \leq n \leq 5$. Ces valeurs se calculent facilement si l'on remarque que $15^{2^{n+1}} = 15^{2^n \cdot 2} = \left(15^{2^n}\right)^2$: les valeurs successives de 15^{2^n} s'obtiennent en calculant le carré de la précédente :

n	$15^{2^n} \mod 23$
0	15
1	$15^2 \equiv 225 \equiv 18$
2	$18^2 \equiv 324 \equiv 2$
3	$2^2 \equiv 4$
4	$4^2 \equiv 16$
5	$16^2 \equiv 256 \equiv 3$

Finalement, $15^{52} \equiv 15^{2^5} \cdot 15^{2^4} \cdot 15^{2^2} \equiv 3 \cdot 16 \cdot 2 \equiv 96 \equiv 4 \mod 23$.

On peut aussi synthétiser cette démarche sous la forme d'un seul tableau :

x	reste r	n	$15^{2^n} \mod 23$	contribution (si $r = 1$)
52	0	0	15	
26	0	1	$15^2 \equiv 18$	
13	1	2	$18^2 \equiv 2$	2
6	0	3	$2^2 \equiv 4$	
3	1	4	$4^2 \equiv 16$	16
1	1	5	$16^2 \equiv 3$	3

Exercice 87.

Calculer :

1) $3^{100} \mod 19$ 2) $12^{364} \mod 34$ 3) $5^{51} \mod 97$ 4) $9^{71} \mod 113$

5 Cryptographie (RSA)

La cryptographie à clé privée

Les algorithmes de chiffrement utilisés jusqu'à la veille des années 1970, aussi sophistiquées que soient leur méthode de codage, présentent deux inconvénients majeurs : la transmission des clés et l'authentification de l'expéditeur.

Les méthodes traditionnelles de cryptage sont dites **symétriques** ou encore à **clé privée**, parce qu'elles se fondent sur une même clé pour chiffrer et déchiffrer un message. Le problème de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. Toute interception, quelle que soit la sécurité du codage, détruit la confidentialité du message. Dans son ouvrage *Histoire des codes secrets*, Simon Singh illustre bien le problème :

> Dans les années 70, les banques essayèrent de faire distribuer les clés par des coursiers spécialement sélectionnés qui comptaient parmi les employés les plus sûrs de l'entreprise. Ces messages devaient courir le monde munis de cartables cadenassés et remettre en mains propres les clés aux destinataires des messages de la banque la semaine suivante. Plus les contacts se multipliaient, plus les réseaux s'étendaient, et tant de clés durent être distribuées que la logistique nécessaire, avec ses frais prohibitifs, devint un véritable cauchemar.

L'autre problème est qu'il est impossible de savoir si l'expéditeur d'un message est bien celui que l'on croit. Un intrus, s'étant emparé de la clé, pourrait très bien fabriquer de faux messages, ou changer subrepticement une partie d'un message intercepté. En l'absence d'une **signature** de l'expéditeur, ces falsifications demeurent indétectables.

La cryptographie à clé publique

Le problème de la transmission des clés a été résolu grâce à la cryptographie à clé publique. Pour illustrer son fonctionnement, imaginons qu'Alice et Bob vivent dans un pays à ce point corrompu que le système postal n'offre plus aucune sécurité : toutes les lettres et tous les paquets sont susceptibles d'être ouverts par les employés de la poste. Alice doit faire parvenir à Bob un message très personnel, mais elle n'a ni le temps ni les moyens de le lui transmettre personnellement. Elle ne peut l'envoyer que par la poste. Existe-t-il un moyen de le faire, en étant sûr que Bob reçoive le message sans qu'il ait été lu par un tiers ?

La solution de cette énigme a été trouvée en 1976 par Whitfield Diffie et Martin Hellman. Alice envoie à Bob son message secret dans un coffret qu'elle a verrouillé à l'aide d'un cadenas dont elle est la seule à posséder la clé. Bob, à la réception du coffret, ajoute au coffret son propre cadenas et renvoie le coffret à Alice, qui le reçoit donc muni de deux cadenas. Elle retire le sien, ne laissant que celui de Bob. Puis elle renvoie le coffret à Bob qui peut l'ouvrir et prendre connaissance du message, puisqu'il est détenteur de la clé du seul cadenas qui verrouille le coffret. À aucun moment, un employé indélicat ne peut prendre connaissance du secret d'Alice.

Cette historiette prouve qu'il existe une suite d'opérations qui assure la transmission d'un message secret sans échange de clés. Ainsi, l'antique nécessité de la distribution de clés est mise hors jeu. Deux personnes qui ne se sont jamais rencontrées ou qui n'ont jamais échangé d'informations peuvent s'envoyer un message qui restera secret, même s'il passe par un canal non sécurisé.

Après avoir élaboré ces principes, Diffie et Hellman cherchent à les mettre en œuvre eux-mêmes, mais ils ne parviennent pas à trouver un équivalent cryptographique à cet échange de coffret à deux cadenas.

Le système cryptographique à clé publique RSA

En 1977, trois mathématiciens américains, Ronald Rivest, Adi Shamir et Leonard Adleman, trouvent un système asymétrique qui reste le meilleur et le plus utilisé à ce jour : le système RSA (nommé à partir des initiales des trois auteurs).

Supposons que Bob attende un message d'Alice. Nous allons expliquer en trois étapes ce qui doit être fait.

Création de la clé RSA

Bob opère de la manière suivante.

1. Il détermine au hasard deux nombres premiers p et q distincts.
2. Il calcule $n = p\,q$ et $\varphi(n) = (p-1)\,(q-1)$.
   L'entier n s'appelle le **modulo RSA**.
3. Il choisit un entier e tel que $1 < e < \varphi(n)$ et $\text{pgcd}\big(e,\varphi(n)\big) = 1$.
   En général, on choisit le nombre e le plus petit possible.
   L'entier e s'appelle l'**exposant d'encryptage RSA**.
4. Il résout l'équation diophantienne $e\,x+\varphi(n)\,y = 1$ ou recourt à l'exercice 7.11 pour déterminer l'unique entier d tel que $1 < d < \varphi(n)$ et $e\,d \equiv 1 \mod \varphi(n)$.
   L'entier d s'appelle l'**exposant de décryptage RSA**.
5. Il publie dans un annuaire le couple (n,e), appelé **clé publique RSA**, et garde secrets les nombres p, q et d, qui constituent la **clé secrète RSA**.

Exercice 88.

Bob choisit sa clé RSA en prenant $p = 11$ et $q = 23$.

1. Calculer n et $\varphi(n)$.
2. Quel est le plus petit exposant d'encryptage RSA que Bob peut choisir ?
3. Quel est l'exposant de décryptage RSA correspondant ?
4. Quels nombres constituent la clé publique et la clé secrète de Bob ?

Encryptage RSA

Si Alice veut envoyer un message à Bob, elle doit procéder comme suit :

1. Elle prend connaissance de la clé publique (n,e) de Bob.
2. Elle traduit chaque lettre du texte en clair en un équivalent numérique adéquat (le code ASCII par exemple). Elle partage les chiffres de ce message en blocs de même taille.
3. Elle encrypte chaque bloc m séparément en calculant $c \equiv m^e \mod n$.
4. Elle envoie chaque bloc c à Bob.

Exercice 89.

Alice a pris connaissance de la clé publique de Bob : $(253,3)$. Elle veut lui envoyer le message SALUT.

1. Elle numérise son message selon le code suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	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

Quelle est la transcription numérique de son message en clair ?

2. Si elle divise son message en blocs de 2 chiffres, quel message crypté envoie-t-elle à Bob ?

Décryptage RSA

Théorème RSA *Soient (n,e) une clé publique RSA et d la clé secrète RSA correspondante. Alors $(a^e)^d \equiv a \mod n$ pour tout entier a.*

Exercice 90.

Le but de cet exercice est de prouver le théorème RSA.

On rappelle que $e\,d \equiv 1 \mod \varphi(n)$ et que $\varphi(n) = (p-1)\,(q-1)$.

1. Montrer qu'il existe un entier $k \geq 0$ tel que $(a^e)^d = a\left(a^{\varphi(n)}\right)^k$.
2. (a) Supposons $p \nmid a$ et $q \nmid a$.
   Établir que $(a^e)^d \equiv a \mod n$ grâce au théorème d'Euler.
   (b) Supposons $p \mid a$ et $q \nmid a$.
      i. Vérifier que $a \equiv 0 \mod p$ et en tirer que $(a^e)^d \equiv a \mod p$.
      ii. Montrer que $(a^e)^d \equiv a\left(a^{(q-1)}\right)^{(p-1)} \equiv a \mod q$ à l'aide du petit théorème de Fermat.
      iii. Conclure que $(a^e)^d \equiv a \mod n$, grâce à l'exercice 5.4.
   (c) Supposons $p \nmid a$ et $q \mid a$.
   Montrer, de même que précédemment, que $(a^e)^d \equiv a \mod n$.
   (d) Supposons $p \mid a$ et $q \mid a$.
   Vérifier que $a \equiv 0 \mod n$ et en déduire que $(a^e)^d \equiv a \mod n$.

En vertu du théorème RSA, lorsque Bob reçoit le message codé c, il utilise sa clé privée d pour calculer $c^d \mod n$ et obtenir ainsi le message décodé.

Exercice 91.

Bob reçoit le message crypté $13\ 00\ 66\ 157\ 28$ d'Alice. Déchiffrer ce message.

Exercice 92.

Crypter le message m en utilisant le système RSA avec les données suivantes :

1) $p = 3 \quad q = 11 \quad e = 7 \quad m = 5$
2) $p = 7 \quad q = 11 \quad e = 17 \quad m = 8$
3) $p = 17 \quad q = 31 \quad e = 7 \quad m = 2$

puis retrouver m à partir du message crypté.

Exercice 93.

Effectuer le chiffrement du message SOS en utilisant le système RSA de clé publique $(3233,17)$, puis retrouver SOS à partir du message crypté.

Indication : $3233 = 53 \cdot 61$

Exercice 94.

Un système RSA a pour paramètres $p = 97$ et $q = 109$. Parmi les nombres ci-dessous, lesquels peuvent être choisis comme clé publique d'encryptage :

1) $e = 123$ 2) $e = 865$ 3) $e = 169$

Exercice 95.

Un professeur envoie votre moyenne de cryptographie au secrétariat via un courriel crypté en RSA. La clé publique du secrétariat est $(55,7)$ et le message crypté envoyé est 25. Quelle est votre moyenne ?

Exercice 96.

Un ennemi intercepte le message chiffré $c = 10$, dont le destinataire possède la clé publique $(35,5)$. Quel est le texte clair m ?

Sécurité du système RSA

Supposons qu'un intrus intercepte le message c et cherche à le décrypter. Il connaît aussi la clé publique, à savoir les nombres n et e. En revanche, il ne connaît pas d. Pour découvrir ce nombre, il doit trouver p et q.

En effet, la seule façon connue de découvrir d en connaissant n et e est de factoriser n pour connaître $\varphi(n) = (p-1)(q-1)$, et de calculer ensuite la solution de l'équation $e\,d \equiv 1 \mod \varphi(n)$.

La difficulté vient de ce que la factorisation de n est une tâche impossible à effectuer en un temps raisonnable, dans l'état des connaissances actuelles, pour autant que n soit suffisamment grand. On prend aujourd'hui des premiers p et q tels que leur produit soit un nombre s'écrivant avec plus de 200 chiffres. Le système est donc sûr, du moins tant que l'on ne découvre pas un algorithme rapide pour factoriser les entiers.

Authentification par signature

La cryptographie à clé publique permet également de résoudre le problème de l'authenticité et de l'intégrité des informations transmises. Imaginons par exemple qu'Alice possède un compte dans une banque administrée par Bob. Elle veut envoyer par courriel l'ordre de payer la somme de $100\ 000$ francs à l'un de ses créanciers. La banque a deux problèmes à résoudre :

1. Comment convaincre Bob que c'est bien Alice qui est l'expéditrice et non pas un escroc qui aurait usurpé l'identité d'Alice ? Ou encore, comment empêcher qu'Alice nie après coup avoir donné un tel ordre ?
2. Comment Bob peut-il être sûr que c'est bien $100\ 000$ francs qu'il faut verser à un tel et non $50\ 000$ francs à tel autre ? Un intrus n'aurait-il pas pu modifier le message ?

Montrons comment le système à clé publique RSA permet de résoudre ces problèmes.

Phase de signature et d'encryptage (par Alice)

Pour envoyer un message signé m à Bob, Alice procède ainsi :

1. Elle crypte m au moyen de sa clé privée d_A : $d_A(m) = s$. L'expression s est la **signature** du message m et le couple (m,s) est le **message signé** par Alice.
2. Elle crypte le message signé (m,s) à l'aide de la clé publique e_B de Bob et lui envoie le couple $\Big(e_B(m),e_B(s)\Big)$.

Phase de vérification et de décryptage (par Bob)

À la réception de $\Big(e_B(m),e_B(s)\Big)$, Bob procède ainsi :

1. Il le décrypte au moyen de sa clé privée d_B et obtient ainsi :
   $\Big(d_B\Big(e_B(m)\Big),d_B\Big(e_B(s)\Big)\Big) = (m,s)$.
2. Il vérifie la signature d'Alice à l'aide de la clé publique e_A d'Alice en calculant $e_A(s)$. Le message provient d'Alice si et seulement si $e_A(s) = m$.

Exercice 97.

Admettons qu'Alice choisisse $p_A = 11$, $q_A = 23$ et $e_A = 3$, comme à l'exercice 5.67. Elle obtient $n_A = 253$ et $d_A = 147$. Sa clé publique est $(253,3)$ et sa clé privée est $d_A = 147$.

De son côté, Bob a choisi $p_B = 13$, $q_B = 19$ et $e_B = 5$. Il obtient $n_B = 247$ et $d_B = 173$. Sa clé publique est $(247,5)$ et sa clé privée est $d_B = 173$.

Alice veut faire verser à Charles la somme de 111 francs. Le message en clair est donc $m = 111$.

1. Quelle est la signature s qu'Alice calcule avec sa clé privée ?
2. Quel est le message signé codé qu'elle envoie à Bob ?
3. En utilisant la clé privée de Bob, décoder le message codé par Alice.
4. Comment Bob vérifie-t-il l'authenticité et l'intégrité du message reçu ?

Exercice 98.

Supposons qu'Alice a pour clé publique RSA $(638\ 611{,}251)$. Après avoir décrypté un message envoyé par Alice, Bob obtient la paire $(11\ 911{,}341\ 076)$. Expliquer ce qu'il doit faire pour vérifier la signature. Doit-il considérer le message comme valide ?

Indication : $638\ 611 = 701 \cdot 911$

Exercice 99.

La clé publique d'Alice est $(437{,}17)$.

Quelle est la signature du message $m = 100$?

Exercice 100.

Pour assurer l'authenticité des messages contenant les notes, le secrétariat demande au professeur de signer ses messages codés en RSA. On sait que la clé publique du professeur est $(15{,}3)$ et celle du secrétariat $(77{,}7)$.

1. Quel est le message envoyé par le professeur pour indiquer la note 4 ?
2. Quelle note correspond au message crypté $(41{,}41)$ reçu par le secrétariat ? Ce message a-t-il vraiment été envoyé par le professeur ?
3. Le secrétariat reçoit le message crypté $(12{,}27)$. Ce message a-t-il été envoyé par le professeur ?

Réponses

Solution 50. 1) et 4)

Solution 53. $\overline{7}$, $\overline{10}$, $\overline{8}$ et $\overline{2}$

Solution 54. $\overline{17}$, $\overline{16}$ et $\overline{12}$

Solution 55. Sont inversibles $\overline{1}$, $\overline{5}$, $\overline{7}$ et $\overline{11}$.
Ce sont leurs propres inverses.

Solution 56. Sont inversibles $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{9}$, $\overline{11}$ et $\overline{13}$.
Leurs inverses respectifs sont $\overline{1}$, $\overline{5}$, $\overline{3}$, $\overline{11}$, $\overline{9}$ et $\overline{13}$.

Solution 57. Sont inversibles $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$, $\overline{11}$, $\overline{13}$, $\overline{17}$ et $\overline{19}$.

Solution 58. $\varphi(12) = 4 \qquad \varphi(14) = 6 \qquad \varphi(20) = 8$

Solution 59. $\varphi(p) = p - 1$

Solution 61. $\varphi(125) = 100$ et $\varphi(121) = 110$

Solution 64.

1) 40 2) 192 3) 720 4) $829\ 440$

Solution 65. $\varphi(5186) = \varphi(5187) = \varphi(5188) = 2592$

Solution 66.

1) 2 2) 3 3) 4 4) 7 ou 12

5) pas de solution

Solution 69.

1) $2^n \equiv \begin{cases} 2 & \text{si } n \equiv 1 \mod 3 \\ 4 & \text{si } n \equiv 2 \mod 3 \\ 1 & \text{si } n \equiv 3 \mod 3 \end{cases}$

2) $2^n \equiv \begin{cases} 2 & \text{si } n \equiv 1 \mod 4 \\ 4 & \text{si } n \equiv 2 \mod 4 \\ 8 & \text{si } n \equiv 3 \mod 4 \\ 6 & \text{si } n \equiv 4 \mod 4 \end{cases}$

Les puissances de 2^n reprennent de façon cyclique les puissances précédentes.

Solution 72.

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
Ordre :	1	4	4	2

Solution 73.

Élément :	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
Ordre :	1	6	3	6	3	2

Solution 74.

m :	11	17	31	9	14
Ordre :	10	8	5	6	non inversible

Solution 75.

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
Ordre :	1	10	5	5	5	10	10	10	5	2

Solution 80.

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
Ordre :	1	12	3	6	4	12	12	4	3	6	12	2

Solution 81.

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$
Ordre :	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

Solution 82.

Élément :	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$	$\overline{19}$	$\overline{23}$
Ordre :	1	2	2	2	2	2	2	2

Solution 83. 8

Solution 87.

1) 16 2) 4 3) 69 4) 91

Solution 88.

1) $n = 253$ $\varphi(n) = 220$
2) $e = 3$
3) $d = 147$
4) clé publique : (253,3)
clé secrète : (11,23,147)

Solution 89.

1) 18 00 11 20 19
2) 13 00 66 157 28

Solution 91. 18 00 11 20 19 → salut

Solution 92.

1) $c = 14$ 2) $c = 57$ 3) $c = 128$

Solution 93. 2100 2549 2100

Solution 94. $e = 865$ et $e = 169$

Solution 95. 5

Solution 96. $m = 5$

Solution 97.

1) $s = 89$ 2) $(232,33)$ 3) $(111,89)$ 4) $89^3 \equiv 111 \mod 253$

Solution 98. Bob vérifie que $341\ 076^{251} \equiv 11\ 911 \mod 638\ 611$: le message est valide.

Solution 99. $s = 156$

Solution 100.

1. $(60,60)$
2. La note est 6. Le message a été envoyé par le professeur.
3. La signature est correcte... mais le message correspond à la note 12 ?!