Exercice 1

1. Calculer le reste dans la division euclidienne par 7 des nombres 561, 143 et 561×143.
2. Déterminer le reste de la division euclidienne de $(8 \times 20 + 12) \times (5 + 13 \times 52)^2$ par 7.
3. Déterminer le reste de la division euclidienne de $(30 \times 14 - 27 \times 18) - 5 \times (15 \times 4 - 13 \times 19)^3$ par 13.
4. Déterminer le reste de la division euclidienne de $(2^8 + 1) \times (2^7 - 1)$ par 2^6.
5. Déterminer le reste de la division euclidienne de 10^{100} par 13.
6. Déterminer le chiffre des unités de 3^{12}.
7. On veut déterminer le chiffre des unités de 7^{7^7}.
   (a) Montrer que $7^4 \equiv 1$ [10].
   (b) Déterminer le reste de la division euclidienne de 7^7 par 4.
   (c) Conclure.

Exercice 2 : critères de divisibilité.
Soit x un entier positif. On considère l'écriture décimale $a_r a_{r-1} ... a_0$ de x, telle que

$$x = a_r.10^r + a_{r-1}.10^{r-1} + ... + a_0$$

1. Montrer que x est divisible par 2 si et seulement si a_0 est divisible par 2.
2. Montrer que x est divisible par 3 si et seulement si $a_r + ... + a_0$ est divisible par 3.
3. Montrer que x est divisible par 4 si et seulement si l'entier d'écriture décimale $a_1 a_0$ est divisible par 4.
4. Montrer que x est divisible par 5 si et seulement si a_0 est divisible par 5.
5. Montrer que x est divisible par 9 si et seulement si $a_r + ... + a_0$ est divisible par 9.
6. Montrer que x est divisible par 11 si et seulement si $a_0 - a_1 + ... + (-1)^r a_r$ est divisible par 11.

Exercice 3

1. Écrire les tables de multiplication de $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/10\mathbb{Z}$.
2. Donner la liste des éléments inversibles de ces anneaux et expliquer les propriétés suivantes :
   (a) les lignes et colonnes correspondant aux éléments inversibles contiennent tous les éléments de l'anneau, représenté une et une seule fois.
   (b) Les lignes et colonnes correspondant aux éléments non inversibles contiennent une suite périodique.
   (c) La dernière ligne et la dernière colonne, correspondant à $\overline{n-1}$ dans $\mathbb{Z}/n\mathbb{Z}$, contient tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ rangé dans l'ordre inverse de l'ordre usuel.
3. Écrire la table du groupe $(\mathbb{Z}/10\mathbb{Z})^*$.

Exercice 4 Résoudre les équations suivantes en $\overline{x}$:

1. $\overline{4} \times \overline{x} = \overline{3}$ dans $\mathbb{Z}/6\mathbb{Z}$.
2. $\overline{4} \times \overline{x} = \overline{2}$ dans $\mathbb{Z}/6\mathbb{Z}$.
3. $\overline{4} \times \overline{x} = \overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$.
4. $\overline{3} \times \overline{x} = \overline{0}$ dans $\mathbb{Z}/9\mathbb{Z}$.
5. $\overline{4} \times \overline{x} = \overline{6} \times \overline{x}$ dans $\mathbb{Z}/10\mathbb{Z}$.
6. Déterminer tous les entiers $x \in \mathbb{Z}$ tels que le reste de la division euclidienne de $4x$ par 7 vaut 3.

Exercice 5 Dans le pays A, on ne dispose que de pièces de valeurs 13 et de pièces de valeur 5.

1. Quelles sont les solutions de $13x + 5y = 47$ où x et y appartiennent à $\mathbb{Z}$?
2. J'achète un produit qui a pour valeur 47. Puis-je le payer sans que l'on me rende la monnaie ?

3. Même question avec 49.
4. J'achète un produit qui a pour valeur 16. Puis-je le payer si on me rend la monnaie ?
5. Montrer que pour $n \in \mathbb{N}$, il existe un unique couple (x, y) d'entiers tels que $0 \leq x \leq 4$ et $n = 13x + 5y$.
6. Montrer que tout achat de produit de valeur plus grande que 48 peut être payé sans rendu de monnaie.
7. Soit a et b deux entiers naturels premiers entre eux.

   Ecrire un programme en langage naturel donnant le nombre de pièces de valeur a et de pièces de valeur b permettant si c'est possible de payer un produit de valeur n sans rendu de monnaie. On supposera que l'on dispose d'une fonction donnant l'identité de Bézout de a et b.

Exercice 6 Déterminer tous les entiers x tels que $x^2 = 3 \pmod 6$.

Exercice 7

1. Montrer que si x est un entier impair, alors $x^2 = 1 \pmod 8$.
2. Montrer que si x est un entier pair, alors $x^2 = 0 \pmod 8$ ou $x^2 = 4 \pmod 8$.
3. En déduire les solutions en x et y entiers de l'équation $x^2 + y^2 = 2 \pmod 8$.
4. Résoudre les équations suivantes en x, y entiers :
   (a) $x^2 + y^2 = 3 \pmod 9$,
   (b) $x^2 + y^2 = 5 \pmod 9$.

Exercice 8 À l'aide de l'algorithme d'exponentiation rapide, déterminer :

1. $\overline{2}^{65}$ dans $\mathbb{Z}/53\mathbb{Z}$.
2. $\overline{3}^{231}$ dans $\mathbb{Z}/53\mathbb{Z}$.
3. $\overline{7}^{231}$ dans $\mathbb{Z}/238\mathbb{Z}$.

Implémenter l'algorithme d'exponentiation rapide (par exemple la version récursive) et vérifiez les résultats obtenus .

Exercice 9 Les éléments suivants sont-ils des inversibles ? des diviseurs de zéro ?

1. $\overline{4}$ dans $\mathbb{Z}/22\mathbb{Z}$.
2. $\overline{7}$ dans $\mathbb{Z}/16\mathbb{Z}$.
3. $\overline{3}$ dans $\mathbb{Z}/10\mathbb{Z}$.
4. $\overline{21}$ dans $\mathbb{Z}/30\mathbb{Z}$.
5. $\overline{26}$ dans $\mathbb{Z}/45\mathbb{Z}$.

Exercice 10 Montrer que $\overline{2}$, $\overline{3}$, $\overline{4}$ et $\overline{5}$ sont inversibles dans $\mathbb{Z}/13\mathbb{Z}$ et déterminer les sous-groupes de $(\mathbb{Z}/13\mathbb{Z})^*$ engendrés par $\overline{2}$, $\overline{3}$, $\overline{4}$ et $\overline{5}$.

Exercice 11 Montrer que $\overline{4}$ dans $\mathbb{Z}/41\mathbb{Z}$ est inversible et donner son inverse. Déterminer l'ordre de $\overline{4}$ dans $(\mathbb{Z}/41\mathbb{Z})^*$. Déterminer le reste de la division euclidienne de 4^{2017} par 41.

Exercice 12

1. Montrer que $\mathbb{Z}/89\mathbb{Z}$ est un corps.
2. Que peut-on dire, par le théorème de Lagrange, sur l'ordre possible des éléments de $(\mathbb{Z}/89\mathbb{Z})^*$?
3. Déterminer les ordres des éléments $\overline{2}$, $\overline{4}$, $\overline{8}$ et $\overline{1}2$ dans $(\mathbb{Z}/89\mathbb{Z})^*$.

Exercice 13 Déterminer $\overline{3}^{1025}$ dans $\mathbb{Z}/509\mathbb{Z}$ par deux méthodes différentes : le théorème de Lagrange et l'algorithme d'exponentiation rapide.

Exercice 14 On se place dans l'anneau $\mathbb{Z}/201\mathbb{Z}$.

1. Calculer $\overline{2}^{261}$ sans factoriser 201.
2. Calculer $\varphi(201)$.
3. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/201\mathbb{Z}$, déterminer l'ordre de $\overline{2}$ dans le groupe $(\mathbb{Z}/201\mathbb{Z})^*$ et calculer $\overline{2}^{261}$ en utilisant son ordre.

4. Vérifiez que 5 est inversible modulo $\varphi(201)$ et déterminez son inverse s. Calculer $32^s \pmod 2$01 directement et en utilisant le fait que $32 = 2^5$.

Exercice 15 On se place dans l'anneau $\mathbb{Z}/391\mathbb{Z}$.

1. Calculer $\overline{2}^{390}$ sans factoriser 391. Qu'en déduit-on ?
2. Déterminer $\varphi(391)$.
3. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/391\mathbb{Z}$ et déterminer l'ordre de $\overline{2}$ dans le groupe $(\mathbb{Z}/391\mathbb{Z})^*$.

Exercice 16 On se place dans $\mathbb{Z}/49\mathbb{Z}$.

1. Quel est le cardinal de $(\mathbb{Z}/49\mathbb{Z})^*$?
2. Que peut-on en déduire sur l'ordre des éléments de $(\mathbb{Z}/49\mathbb{Z})^*$?
3. Déterminer l'ordre de $\overline{2}$ puis l'ordre de $\overline{3}$ dans $(\mathbb{Z}/49\mathbb{Z})^*$.
4. En déduire qu'il existe $n \in \mathbb{N}$ tel que $\overline{3}^n = \overline{2}$.

Exercice 17 Déteminer un générateur du groupe multiplicatif $(\mathbb{Z}/103\mathbb{Z})^*$

Exercice 18 Soit p un nombre premier. Écrire un algorithme permettant de trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

Exercice 19 On prend au hasard un entier $a \in \{1, ..., 17063\}$. Quelle est la probabilité que a soit un diviseur de 17063 ? un entier non premier à 17063 ?

Exercice 20 On se place dans $\mathbb{Z}/143\mathbb{Z}$.

1. Déterminer $\varphi(143)$.
2. Pour quels entiers x a-t-on $x^{142} \equiv 1$ [143] ? Indication : à l'aide du théorème d'Euler-Fermat, se ramener à une équation plus simple en x, et la résoudre en factorisant 143 et en appliquant les restes chinois.
3. On appelle *menteur* de Fermat d'un entier n non premier les entiers $x \in \{0, \dots, n-1\}$ tels que $x^{n-1} \equiv 1$ $[n]$.
   Combien 143 a-t-il de menteurs de Fermat ? de témoins de Fermat ? Quels sont les autres éléments dans $\{0, \dots, 142\}$?
4. Facultatif : même question en utilisant le test de Miller-Rabin
5. On tire 5 fois de suite au hasard un nombre $x \in \{0, \dots, 142\}$ et on teste si $x^{142} \equiv 1$ [143] (test de primalité de Fermat). Quelle est la probabilité qu'au moins un nombre parmi eux montre que 143 n'est pas premier ?

Exercice 21 Écrire un algorithme effectuant le test de primalité de Fermat pour un entier n donné et N entiers a tirés au hasard. On renverra 0 dès qu'un test renvoie non premier, sinon on renverra 1.

Exercice 22

1. Montrer que pour tout entier impair x, on a $x^4 \equiv 1$ [16]. Indication : distinguer les cas $x \equiv 1$ [4] et $x \equiv -1$ [4].
2. En déduire que le groupe $(\mathbb{Z}/16\mathbb{Z})^*$ n'est pas cyclique.

Exercice 23

1. Montrer que pour tout entier x premier avec 10, on a $x^{4000} \equiv 1$ [10000].
2. Pour quels entiers x a-t-on $x^{9999} \equiv 1$ [10000] ?
3. Montrer que pour tout entier x premier avec 10, on a $x^{500} \equiv 1$ [10000]. Indication : utiliser le théorème des restes chinois.

Exercice 24 : nombre de Carmichaël. On se place dans l'anneau $\mathbb{Z}/561\mathbb{Z}$.

1. Calculer $\overline{2}^{560}$, $\overline{5}^{560}$.
2. Montrer que 561 n'est pas premier et déterminer $\varphi(561)$.
3. En utilisant l'isomorphisme du théorème des restes chinois, montrer que pour tout $a \in (\mathbb{Z}/561\mathbb{Z})^*$, on a $a^{80} = \overline{1}$.
4. En déduire que pour tout $a \in (\mathbb{Z}/561\mathbb{Z})^*$, on a $a^{560} = \overline{1}$.
   Ceci montre qu'il n'y a pas de témoin de Fermat pour l'entier 561, qui n'est pourtant pas premier. On dit que 561 est un nombre de Carmichaël.

5. Déterminer l'ordre de $\overline{2}$ et l'ordre de $\overline{5}$ dans $\mathbb{Z}/561\mathbb{Z}$.

Exercice 25 Écrire un algorithme déterminant la liste des nombres de Carmichael (i.e. les entiers $n > 1$ tels que n n'est pas premier mais $a^{n-1} = 1 \pmod{n}$ si a et n sont premiers entre eux) plus petits qu'un entier N fixé.

Exercice 26 En utilisant le test de Miller-Rabin, vérifiez que 561 n'est pas premier. Déterminez tous les entiers $a \in [1, 560]$ qui passent le test de Miller-Rabin pour 561, vérifiez qu'il y a (nettement) moins d'un quart de valeurs de a qui renvoient Vrai pour ce test.

Exercice 27 Montrer que les relations suivantes dans $\mathbb{Z}$ sont des relations d'équivalence. Existe-il une loi $+$ sur l'ensemble quotient $\mathbb{Z}/\sim$ telle pour tous entiers a, b, on a $Cl(a) + Cl(b) = Cl(a + b)$?

1. $a \sim b$ si et seulement si a et b ont même chiffre des unités dans leurs écritures décimales.
2. $a \sim b$ si et seulement si a et b ont même chiffre des dizaines dans leurs écritures décimales.

Exercice 28 On considère l'application suivante :

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{Z}/20\mathbb{Z} & \rightarrow & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \overline{x} & \rightarrow & (\overline{x}, \overline{x}) \end{array} \right.$$

où $\overline{x}$ désigne la classe de l'entier x dans l'anneau considéré.

1. Expliquez rapidement pourquoi Φ est bien définie
2. Donner les images par Φ de tous les éléments de $\mathbb{Z}/20\mathbb{Z}$ et vérifier que Φ est bien une bijection.
3. Résoudre de deux manières :
   (a) $\left\{ \begin{array}{ccll} x & \equiv & 2 & [4] \\ x & \equiv & 4 & [5] \end{array} \right.$
   (b) $\left\{ \begin{array}{ccll} x & \equiv & 1 & [4] \\ x & \equiv & 2 & [5] \end{array} \right.$
4. On munit l'ensemble $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ des lois $+$ et $\times$ définies par

$$(x, y) + (x', y') = (x + x', y + y'),\ (x, y) \times (x', y') = (x \times x', y \times y').$$

   (a) Montrer que $+$ et $\times$ sur $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ possède des éléments neutres.
   (b) On admet (vérification facile) que $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est un anneau pour les lois $+$ et $\times$. Montrer qu'un élément $(\overline{x}, \overline{y})$ de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est inversible si et seulement si $\overline{x}$ est inversible dans $\mathbb{Z}/4\mathbb{Z}$ et $\overline{y}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$
   (c) Déterminer les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$ et ceux de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, et montrer qu'ils sont en relation par Φ.
   (d) Trouver l'inverse de $\overline{13}$ dans $\mathbb{Z}/20\mathbb{Z}$ en utilisant l'image par Φ de $\overline{13}$ dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Justifier le résultat trouvé en calculant $\Phi(\overline{13}.\overline{13}^{-1})$.

Exercice 29 : chiffrement affine

Soit n un entier, $n \geq 2$. Pour tous $a, b \in \mathbb{Z}/n\mathbb{Z}$, on définit l'application $\Phi_{a,b}$ sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\Phi_{a,b}(x) = ax + b$$

1. Trouver une condition nécessaire et suffisante pour que $\Phi_{a,b}$ soit bijective.
2. On prend $n = 27$ et on code l'alphabet de la manière suivante :

   $\sqcup$ (espace) $\leftrightarrow\ \overline{0}$, $A \leftrightarrow\ \overline{1}$, $B \leftrightarrow\ \overline{2}$, ..., $Z \leftrightarrow\ \overline{26}$.

   Lorsque la fonction $\Phi_{a,b}$ est inversible, elle peut être utilisée comme application de chiffrement. C'est le *chiffrement affine* sur $\mathbb{Z}/27\mathbb{Z}$, de clef (a, b) privée (cryptographie symétrique).

   (a) En utilisant la clef $(\overline{4}, \overline{21})$, coder la phrase : LA CLEF EST DANS LE COFFRE
   (b) À l'aide d'une analyse de fréquence, déchiffrer le cryptogramme suivant utilisant un chiffrement affine sur $\mathbb{Z}/27\mathbb{Z}$:

   RKCTP ILUAPCHPTCHOGGPPTCGCPTACWKTCEKLKGAUPCWKLC PC MUXXLPZPGA

   (c) Combien y a-t-il de clefs possibles pour le chiffrement affine sur $\mathbb{Z}/27\mathbb{Z}$?

Exercice 30 : Logarithme discret On se place dans $\mathbb{Z}/11\mathbb{Z}$.

1. Montrer que $(\mathbb{Z}/11\mathbb{Z})^*$ est un groupe cyclique engendré par $\overline{2}$.
2. Dans ce groupe, calculer le logarithme en base $\overline{2}$ de $\overline{3}$.

Exercice 31 : Attaque sur le logarithme discret.
On considère le nombre premier 101 et on cherche, s'il existe, un entier $x \in \mathbb{N}$ tel que $3^x = 2$ [101].

1. Déterminer $\phi(101)$ et le factoriser en nombres premiers.
2. À l'aide de l'algorithme d'exponentiation modulaire, calculer 3^4, 2^4, 3^{25} et 2^{25} modulo 101.
3. Montrer à l'aide du théorème d'Euler-Fermat que $(3^4)^{25} = 1$ [101].
4. Déterminer des entiers a, b tels que $(3^4)^a = 2^4$ et $(3^{25})^b = 2^{25}$ modulo 101 (pour déterminer a, on pourra chercher les puissances successives de 3^4 modulo 101).
5. Montrer qu'il existe un entier x tel que $x = a$ [25] et $x = b$ [4]. Calculer un tel entier $x \geq 0$.
6. Vérifier que pour cet x, on a $3^x = 2$ [101] (on pourra soit effectuer le calcul à l'aide de l'algorithme d'exponentiation modulaire, soit utiliser le calcul de x et les propriétés de a et b).

Exercice 32 Bob propose le système de chiffrement RSA. Il choisit $p = 17$ et $q = 13$ donc $n = 221$.

1. Déterminer $\varphi(n)$.
2. Vérifier qu'il peut utiliser $e = 7$ comme exposant de chiffrement.
3. Calculer l'exposant de déchiffrement d.
4. Quelle est la clef publique ? quelle est la clef privée ?
5. Chiffrer $M = 3$.
6. Que doit calculer Bob pour déchiffrer $C = 198$ et quel est le résultat ?

Exercice/TP RSA
Cf. `www-fourier.ujf-grenoble.fr/~parisse/mat249/rsa231.pdf`

Cryptographie RSA, problème donné en juin 21
Première partie, un exemple :
On rappelle que pour crypter un message a à un destinataire dont la clef publique est (c, n), il faut lui envoyer $b = a^c \pmod n$. Pour pouvoir faire les calculs, on suppose dans cette question que $c = 17, n = 55$.

1. Crypter le message $a = 3$ en donnant le détail des calculs par la méthode de la puissance rapide.
2. Déterminer $\phi(n)$, le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 55$.
3. Déterminer d l'inverse de 17 modulo $\phi(55)$ en donnant les étapes intermédiaires.
4. Déterminer $b^d \pmod n$.
5. Pourquoi ne doit-on pas prendre $n = 55$ si on souhaite que le message codé reste confidentiel ?

Deuxième partie, utiliser 3 comme clef publique.
Ici n n'est plus égal à 55, c'est le produit de deux nombres premiers quelconques. On se propose de prendre $c = 3$.

1. À quelle condition sur $\phi(n)$ peut-on prendre $c = 3$?
2. Comparer le nombre d'opérations nécessaires au cryptage d'un message lorsque $c = 3$ avec $c = 17$.
3. Écrire un algorithme en langage naturel ou en C ou en Python permettant de connaitre le nombre d'opérations nécessaires au cryptage en fonction de c.
4. Un espion envoie le même message a à trois destinataires différents, ayant chacun leur clef publique $c = 3, n_1 = 187$, $c = 3, n_2 = 46$ et $c = 3, n_3 = 253$ (on a pris des petites valeurs de n pour que les calculs soient faisables à la calculatrice). Les services de contre-espionnage arrivent à intercepter les trois messages codés :

$$b_1 = 98 \pmod{187}, \quad b_2 = 15 \pmod{46}, \quad b_3 = 126 \pmod{145}$$

   Il s'agit de déterminer a *sans chercher à factoriser les entiers* n_i.

   (a) Montrer qu'il existe un unique entier $b \in [0, n_1 n_2 n_3[$ tel que

   $$b = b_1 \pmod{n_1}, \quad b = b_2 \pmod{n_2}, \quad b = b_3 \pmod{n_3}$$

   (b) Expliquer comment calculer b, et donner le détail des calculs si vous avez le temps,

   (c) On trouve $b = 9261$, en déduire a sachant que $a \in [0, n_1[$.