Correction des exercices 6 à 11 de la feuille de TD n°5

- **Exercice 6**

  On va répondre à la question en calculant la classe de congruence de $2^{70}+3^{70}$ modulo 13. On commence par évaluer chacune des puissances 2^{70} et 3^{70} modulo 13. Comme on l'a vu dans les exercices précédents, on pourrait commencer par calculer les puissances modulo 13 de 2 et 3 avec un petit exposant jusqu'à ce qu'on trouve une périodicité. Comme 13 est premier, on peut aussi trouver une périodicité directement en appliquant le petit théorème de Fermat. Comme 13 ne divise pas 2, le petit théorème de Fermat nous indique qu'on a $2^{13-1}\equiv 1 \pmod{13}$ soit $2^{12}\equiv 1 \pmod{13}$. De même, comme 13 ne divise pas 3, on a $3^{12}\equiv 1 \pmod{13}$.

  NB: L'application du petit théorème de Fermat ne nécessite aucun calcul de puissances modulaires, mais ne donne pas nécessairement la plus petite période possible ; dans le présent contexte, il se trouve que 12 est bien la plus petite période possible pour 2, par contre si on avait calculé les puissances successives à la main on aurait constaté qu'on a $3^3\equiv 27\equiv 1 \pmod{13}$.

  On calcule ensuite la division euclidienne de 70 par 12. Elle s'écrit $70=5\times 12+10$. Ainsi on a (toutes les congruences sont modulo 13)

  $$2^{70}=2^{5\times 12+10}=(2^{12})^5\times 2^{10}\equiv 1^5\times 2^{10}\equiv 2^{10} \pmod{13}.$$

  Un calcul similaire montre qu'on a $3^{70}\equiv 3^{10} \pmod{13}$.

  Il reste à calculer 2^{10} et 3^{10} modulo 13. Montrons comment on peut le faire sans calculer toutes les puissances modulaires jusqu'à 10, grâce à l'exponentiation binaire. On a $10=2^3+2$ (autrement dit, 10 s'écrit 1010 en binaire). On calcule alors 2^2, $2^4=(2^2)^2$ et $2^8=(2^4)^2$ modulo 13 par élevations successives au carré (en réduisant à chaque fois le résultat modulo 13)

  $$2^2\equiv 4 \pmod{13},\quad 2^4\equiv 4^2\equiv 16\equiv 3 \pmod{13},\quad 2^8=(2^4)^2\equiv 3^2\equiv 9 \pmod{13}$$

  Ainsi $2^{10}=2^8\times 2^2\equiv 9\times 4\equiv 26\equiv 2\times 13+10\equiv 10 \pmod{13}$.

  Un calcul strictement similaire permet de calculer 3^{10} modulo 13.

  $3^2\equiv 9\equiv -4 \pmod{13},\quad 3^4\equiv (-4)^2\equiv 16\equiv 3 \pmod{13},\quad 3^8=(3^4)^2\equiv 3^2\equiv 9 \pmod{13}.$

  Ainsi $3^{10}=3^8\times 3^2\equiv 9\times -4\equiv -36\equiv (-3)\times 13+3\equiv 3 \pmod{13}$.

  Finalement, on a $2^{70}+3^{70}\equiv 10+3\equiv 13\equiv 0 \pmod{13}$. Ceci montre que 13 divise $2^{70}+3^{70}$.

- **Exercice 7**

  Montrons que l'équation $2x\equiv 3 \pmod{10}$ d'inconnue $x\in\mathbb{Z}$ **n'a pas de solution**. Pour cela raisonnons par l'absurde et supposons l'existence de $x\in\mathbb{Z}$ vérifiant la relation $2x\equiv 3 \pmod{10}$. Par définition des congruences, cela signifie que 10 divise $3-2x$. En particulier, comme 2 divise 10, on obtient que 2 divise $3-2x$. Mais comme 2 divise clairement $2x$, ceci entraîne que 2 divise $(3-2x)+2x=3$. Donc 2 divise 3, contradiction.

  Pour la seconde équation, déterminons tout d'abord une équation équivalente plus simple. Soit $x\in\mathbb{Z}$ vérifiant $4x\equiv 6 \pmod{10}$. Par définition des congruences, ceci équivaut à la propriété : 10 divise $4x-6$, soit encore 2×5 divise $2\times(2x-3)$, ce qui équivaut à 5 divise $2x-3$. Ainsi l'équation initiale est équivalente à l'équation $2x\equiv 3 \pmod{5}$.

  Pour résoudre cette équation, on va exploiter le fait que le coefficient de x, soit 2, est premier avec 5 et est donc inversible modulo 5 d'après le cours. Calculons un inverse de 2 modulo 5. Il nous faut une relation de Bezout pour 2 et 5. On calcule (ou on trouve directement) par exemple la relation $5+(-2)\times 2=1$. En particulier on a $(-2)\times 2\equiv 1 \pmod{5}$, donc -2 est un inverse de 2

modulo 5.

Revenons donc à l'équation $2x \equiv 3 \pmod 5$. On va "diviser par 2 modulo 5" soit (pour mémoire : diviser par une quantité, c'est multiplier par son inverse) multiplier l'équation par l'inverse de 2 modulo 5. Concrètement, si on a $2x \equiv 3 \pmod 5$, les propriétés des congruences montrent qu'on a alors $(-2) \times 2x \equiv (-2) \times 3 \pmod 5$ soit $(-4)x \equiv -6 \pmod 5$ soit encore $x \equiv 4 \pmod 5$

Réciproquement, supposons qu'on a $x \equiv 4 \pmod 5$. On a alors $2 \times x \equiv 2 \times 4 \pmod 5$ soit encore $2x \equiv 3 \pmod 5$.

Finalement, *les équations* $2x \equiv 3 \pmod 5$ *et* $x \equiv 4 \pmod 5$ *sont équivalentes*. La dernière équation signifie exactement qu'il existe $k \in \mathbb{Z}$ tel que $x = 4 + 5k$. Ainsi l'ensemble des solutions de l'équation $2x \equiv 3 \pmod 5$ est

$$\{4 + 5k, \quad k \in \mathbb{Z}\}.$$

Nous indiquons à présent une autre méthode pour résoudre l'équation $4x \equiv 6 \pmod{10}$. Cette méthode consiste à se ramener à ce qui a été vu en cours sur les équations diophantiennes linéaires. Plus précisément, pour $x \in \mathbb{Z}$, la condition $4x \equiv 6 \pmod{10}$ est équivalente à l'existence d'un $y \in \mathbb{Z}$ vérifiant $4x - 6 = 10y$ soit $4x - 10y = 6$. Mais on a déjà vu comment déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ vérifiant $4x - 10y = 6$. Sans rentrer dans les détails, on trouve que cet ensemble est l'ensemble $\{(4 + 5k, 1 + 2k), \quad k \in \mathbb{Z}\}$. Ainsi, revenant à l'équation initiale $4x \equiv 6 \pmod{10}$, on trouve que son ensemble de solutions est $\{4 + 5k, \quad k \in \mathbb{Z}\}$, c'est à dire l'ensemble des premières coordonnées des couples (x, y) déterminés précédemment.

- **Exercice 8**

  La fonction suivante prend en entrée une liste d'entiers entre 0 et 25 qui représente le message à coder (par exemple `BONJOUR` est représenté par la liste `[2,15,14,10,15,21,18]`)

```
def cesar_avec_clef_3(mot):
    resultat=[]
    for i in range(0,len(mot)):
        resultat=resultat+[(mot[i]+3) % 26]
    return resultat
```

  Pour déchiffrer César avec clef 3 en utilisant uniquement la fonction précédente, on trouve un entier strictement positif N tel que $3 \times N \equiv -3 \pmod{26}$. Ainsi, si on applique N fois de suite la fonction précédente en partant d'une certaine liste d'entiers, chaque élément $a \in \{0, \ldots, 25\}$ de la liste aura été changé en $a + 3 \times N \pmod{26}$ soit en $a - 3 \pmod{26}$.

  Pour trouver un tel N, on exploite le fait que comme 3 et 26 sont premiers entre eux, 3 est inversible modulo 26. On calcule (ou on trouve directement) une relation de Bezout pour 3 et 26, par exemple $3 \times 9 - 26 = 1$. Ainsi on a $3 \times 9 \equiv 1 \pmod{26}$ et 9 est un inverse de 3 modulo 26.

  On a donc $3 \times 9 \times -3 \equiv 1 \times -3 \pmod{26}$, soit $3 \times (-27) \equiv -3 \pmod{26}$, soit finalement $3 \times 25 \equiv -3 \pmod{26}$. On peut donc prendre $N = 25$.

  Le même type de raisonnement permet d'implémenter le chiffre de César avec clef arbitraire e en utilisant uniquement la fonction `cesar_avec_clef_3`. On a $3 \times 9 \times e \equiv e \pmod{26}$. Ainsi si N est un entier strictement positif tel que $N \equiv 9 \times e \pmod{26}$, appliquer N fois de suite la fonction `cesar_avec_clef_3` revient à appliquer le chiffre de César avec clef e. *Exemple:* pour $e = 5$, on peut prendre $N = 19$.

- **Exercice 9**

  En utilisant la définition de φ et en dénombrant à la main les entiers premiers avec n et compris entre 1 et n, on trouve

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Par exemple pour $n = 9$, les entiers compris entre 1 et 9 sont $1, 2, 3, 4, 5, 6, 7, 8, 9$ et leurs pgcd respectifs avec 9 sont $1, 1, 3, 1, 1, 3, 1, 1, 9$. On trouve donc bien $\varphi(9) = 6$.

Soit p un nombre premier. Ses diviseurs positifs sont donc 1 et p. Si k est un nombre entier compris entre 1 et $p-1$, k ne peut pas être divisible par p. Ainsi 1 est le seul diviseur positif commun à k et p, et donc k et p sont premiers entre eux. Comme p n'est pas premier avec lui même, le nombre d'entiers compris entre 1 et p qui sont premiers avec p est donc $p-1$. Ainsi on a bien $\varphi(p) = p - 1$.

- **Exercice 10**
  - **Question 1**

    Il s'agit de calculer 15^3 modulo 187. On calcule $15^2 = (10+5)^2 = 10^2 + 2 \times 5 \times 10 + 5^2 = 225$. Or $225 = 187 + 38$ donc $15^2 \equiv 38 \pmod{187}$. Ainsi $15^3 \equiv 38 \times 15 \pmod{187}$ On a $38 \times 15 = 30 \times 10 + 30 \times 5 + 8 \times 10 + 8 \times 5 = 300 + 150 + 80 + 40 = 570$. La division euclidienne de 570 par 187 s'écrit $570 = 3 \times 187 + 9$. Donc finalement on a $15^3 \equiv 9 \pmod{187}$.

  - **Question 2**

    On sait que N est le produit de deux nombres premiers p et q distincts. On sait qu'alors on a $\varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N - p - q + 1$. Ainsi on a $pq = N = 187$ et $p + q = N + 1 - \varphi(N) = 187 + 1 - 160 = 28$.

    À partir de là, soit on détermine à la main les paires $\{p, q\}$ de nombres premiers telles que $p + q = 28$ et on regarde pour chaque paire le produit correspondant, soit on se rappelle que les condition $pq = 187$ et $p + q = 28$ signifient que p et q sont les solutions de l'équation du second degré $x^2 - 28x + 187$, que l'on sait résoudre. On trouve finalement $\{p, q\} = \{17, 11\}$.

    Trouver la clef privée de Bruno revient à déterminer une relation de Bezout pour $e = 3$ et $\varphi(N) = 160$. La division euclidienne de 160 par 3 s'écrit $160 = 3 \times 53 + 1$ d'où $160 + 3 \times (-53) = 1$. Or on a $-53 \equiv 107 \pmod{160}$. Donc Bruno peut utiliser $d = 107$ comme clef privée de déchiffrement.

- **Exercice 11**

  Eve connaît les valeurs N, e_1, e_2 et les valeurs c_1 et c_2 de m^{e_1} et m^{e_2} modulo N. Comme e_1 et e_2 sont premiers entre eux, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $ue_1 - ve_2 = 1$, couple qu'Eve peut facilement déterminer en appliquant l'algorithme d'Euclide étendu. Comme e_1 et e_2 sont strictement supérieurs à 1, on a nécessairement $u > 0$ et $v > 0$. Eve peut alors calculer c_1^u et c_2^v modulo N. Comme on a $ue_1 = 1 + ve_2$, on a

  $$c_1^u \equiv m^{ue_1} \equiv m^{1+ve_2} \equiv m \times c_2^v \pmod{N}$$

  Par ailleurs $c_2^v = m^{ve_2}$ et N sont premiers entre eux. En fait ce ne sera pas le cas si m est divisible par p ou q, mais statistiquement cette dernière possibilité a une probabilité ridiculement faible de se produire ; si cela se produisait, Eve pourrait calculer p ou q en calculant le pgcd de N et c_2^v, donc trouver la factorisation de N et les clefs secrètes.

  Ainsi Eve peut également calculer a un inverse de c_2^v modulo N (Bezout via Euclide étendu). On a $c_1^u \equiv m \times c_2^v \pmod{N}$ soit $ac_1^u \equiv m \times (ac_2^v) \pmod{N}$ or $ac_2^v \equiv 1 \pmod{N}$ donc $ac_1^u \equiv m \pmod{N}$. Ainsi Eve peut retrouver m.