Licence 3 – 4TTI603U  Université de Bordeaux
2024/2025

# Feuille d'entraînement maths info

**Exercice 1.**

Trouver toutes les solutions $x$, si elles existent, au système de congruences suivant :

$$\begin{aligned} 2x &\equiv 6 \pmod{14} \\ 3x &\equiv 9 \pmod{15} \\ 5x &\equiv 20 \pmod{60} \end{aligned}$$

Nous souhaitons d'abord simplifier ce système. Puisque $\gcd(2, 14) = 2$, nous pouvons diviser les termes de la première équivalence par 2 et écrire $x \equiv 3 \pmod 7$. De même, nous simplifions les deux autres équivalences pour réduire le système à :

$$\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{12} \end{aligned}$$

Nous pouvons maintenant appliquer la méthode du théorème des restes chinois. En suivant les notations du théorème, nous obtenons :

$$\begin{aligned} m_1 &= 5 \times 12 = 60 \equiv 4 \pmod{7}; \quad y_1 \equiv 4^5 = 1024 \equiv 2 \pmod{7} \\ m_2 &= 7 \times 12 = 84 \equiv 4 \pmod{5}; \quad y_2 \equiv 4^3 = 64 \equiv 4 \pmod{5} \\ m_3 &= 7 \times 5 = 35 \equiv 11 \pmod{12}; \quad y_3 \equiv 11^3 \equiv (-1)^3 \equiv -1 \equiv 11 \pmod{12} \end{aligned}$$

Ainsi, nous avons :

$$x = y_1 m_1 b_1 + y_2 m_2 b_2 + y_3 m_3 b_3 = 2 \times 60 \times 3 + 4 \times 84 \times 3 + 11 \times 35 \times 4 = 2908.$$

Par conséquent, toute solution est donnée par $x \equiv 2908 \equiv 388 \pmod{420}$.

**Exercice 2.**

Alice utilise le système de chiffrement RSA. Elle choisit deux nombres premiers $p$ et $q$ vérifiant $p \equiv 9 \pmod{10}$ et $q \equiv 7 \pmod{10}$.

1. Montrer que le choix $e = 25$ pour l'exposant de chiffrement est possible. Il s'agit de montrer que $e$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Or $\varphi(N) \equiv \varphi(p)\varphi(q) \equiv 8 * 6 \equiv 8 \pmod{10}$. Il reste à montrer que $\mathrm{pgcd}(e, \varphi(N)) = 1$, or un diviseur qui n'est pas 1 de $e$ ne peut jamais diviser $\varphi(N)$ qui termine par 8 en base 10, donc $e$ est un exposant possible pour RSA.
2. Alice choisit $p$ et $q$ vérifiant ces congruences modulo 10. Elle obtient $N = pq = 13843$ et $\varphi(N) = 13608$. Retrouver $p$ et $q$. On retrouve $p = 109$ et $q = 127$.

3. Alice choisit $e = 25$ comme exposant de chiffrement public. Quelle est sa clef secrète ? Donner le détail du calcul. On doit trouver l'inverse de $e$ modulo $\varphi(N) = 13608$. On va utiliser l'algorithme d'Euclide étendu pour trouver une relation de bézout entre $e = 25$ et $\varphi(N) = 13608$ Nous cherchons à résoudre l'équation suivante :

$$25x \equiv 1 \pmod{13608}$$

Ceci revient à trouver des entiers $x$ et $y$ tels que :

$$25x + 13608y = 1$$

En appliquant l'algorithme d'Euclide étendu, nous obtenons :

$$25 * 1633 - 3 * 13608 = 1$$

donc

$$25^{-1} \equiv 1633 \pmod{13608}$$

ainsi la clé privée est $(d, \varphi(N)) = (1633, 13608)$

4. Alice déchiffre un chiffré $c$ en utilisant le théorème des restes chinois : elle calcule d'abord

$$d_p \equiv d \pmod{p-1} \quad \text{et} \quad d_q \equiv d \pmod{q-1}$$

puis

$$m_p \equiv c^{d_p} \pmod{p} \quad \text{et} \quad m_q \equiv c^{d_q} \pmod{q}.$$

Enfin, elle obtient $m \in \mathbb{Z}/NZ$ en résolvant le système :

$$\begin{cases} m \equiv m_p \pmod{p} \\ m \equiv m_q \pmod{q} \end{cases}$$

Justifier que si $m$ est solution du système ci-dessus alors on a bien $m \equiv c^d \pmod{N}$. On l'a fait en TD3 exerice 2

5. Oscar chiffre un message $m$ en $c$ pour Alice. En déchiffrant comme dans la question précédente, Alice se trompe en calculant $m_q$ : elle obtient une mauvaise valeur modulo $q$, mais son calcul de $m_p$ est correct. Elle ne s'aperçoit pas de son erreur et obtient un résultat erroné $m'$ modulo $N$. Oscar apprend cette valeur de $m'$. Montrer qu'il peut factoriser $N$.

Oscar fait la soustraction $m - m' \mod n$ par la question précédente et le fait que Alice s'est trompé dans le calcul de $m_q$. La relation de Bézout entre $p$ et $q$ est donné par $1 = up + vq$. Alors pour $(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, le théorème des restes chinois envoi $(x, y) \mapsto (xvq + yup) \in \mathbb{Z}/N\mathbb{Z}$. On a alors

$$m = m_p \cdot vq + m_q \cdot up$$
$$m' = m_p \cdot vq + m'_q \cdot up$$

Donc Oscar peut calculer $(m - m') = (m_q - m'_q) \cdot up \mod N$, et en faisant le pgcd$(m - m', N)$ on retrouve exactement $p$. Il reste à faire $N/p = q$ et donc Oscar a trouvé une factorisation de $N$.

**Exercice 3.**

Les deux questions sont indépendantes.

1. Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés. Elle choisit comme clé publique le couple $(e, n) = (147, 253)$. Bob lui envoie le cryptogramme $5 + n\mathbb{Z}$. Quel est le message secret que Bob souhaite transmettre à Alice ?

   (a) On a $n = 11 \times 23$ et $\varphi(n) = 220$. Déterminons l'inverse de 147 modulo 220. Pour cela, on vérifie avec l'algorithme d'Euclide pour retrouver

   $$-2 \times 220 + 3 \times 147 = 1$$

   Par suite, 3 est l'inverse cherché. Le message secret que Bob souhaite envoyer à Alice est donc $5^3 \mod 253$, c'est-à-dire $125 \mod 253$.

2. Alice souhaite communiquer de manière sécurisée en utilisant le cryptosystème de Rabin. Sa clé publique est $n = 87$. Bob lui envoie le message $7 + n\mathbb{Z}$.

   (a) Montrer que 7 est un carré modulo $n$. On a $n = 3 \times 29$. On a $7 \equiv 1 \pmod 3$, donc 7 est un carré modulo 3 et il reste à montrer que 7 est un carré modulo 29.

   Parce que 7 est un carré modulo 3 et 29, c'est donc un carré modulo $n$ par le théorème des restes chinois.

   (b) Quels sont les quatre décryptages possibles du message envoyé par Bob ? Soit $S$ l'ensemble des solutions de l'équation $x^2 = 7$ dans $\mathbb{Z}/n\mathbb{Z}$. Les quatre messages décryptés possibles sont les éléments de $S$. Modulo 3, les racines carrées de 7 sont $\pm 1$. Modulo 29, les racines carrées de 7 sont $\pm 6$. On est ainsi amené à résoudre les deux systèmes de congruences

   $$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 6 \pmod{29} \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv -6 \pmod{29} \end{cases}$$

   On obtient comme solutions particulières respectivement $x = 64$ et $x = 52$. En tenant compte des solutions opposées, on en déduit que l'on a

   $$S = \left\{\overline{23}, \overline{35}, \overline{52}, \overline{64}\right\}.$$

**Exercice 4.**

Les deux questions sont indépendantes.

1. Afin de pouvoir se faire envoyer des messages secrets, un utilisateur du cryptosystème RSA utilise comme clé publique le couple $(e, n) = (23, 209)$. Quelle est sa clé secrète ?
   On a $n = 209 = 11 \times 19$, d'où $\varphi(n) = 180$. Il s'agit de déterminer l'inverse $d$ de 23 modulo 180. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

| | 7 | 1 | 4 | 1 | 3 | |
|---|---|---|---|---|---|---|
| 180 | 23 | 19 | 4 | 3 | 1 | 0 |
| 1 | 0 | 1 | $-1$ | 5 | $-6$ | |
| 0 | 1 | $-7$ | 8 | $-39$ | 47 | |

   On en déduit que l'on a l'égalité :

$$23 \times 47 - 6 \times 180 = 1.$$

Par suite, l'inverse de 23 modulo $\varphi(n)$ est 47 et la clé secrète cherchée est donc $(d, \varphi(n)) = (47, 180)$.

2. Posons $n = 7807$. Sachant que $n$ est le produit de deux nombres premiers $p$ et $q$, avec $p < q$, et que $\varphi(n) = 7560$ où $\varphi(n)$ est l'indicateur d'Euler de $n$, déterminer $p$ et $q$.
   On a $n = pq$ et $p + q = n - \varphi(n) + 1$. Par suite, $p$ et $q$ sont racines du polynôme
   $$X^2 - 248X + 7807.$$
   Son discriminant réduit est $7569 = 3^2 \cdot 29^2$, d'où $p = 37$ et $q = 211$.
3. Posons $n = 176399$.
   (a) Factoriser $n$ en un produit de deux nombres premiers avec la méthode Fermat. La partie entière de la racine carrée de $n$ est 419. On constate que l'on a $420^2 - 1 = n$, d'où $n = 419 \times 421$. Par ailleurs, 419 et 421 sont premiers car ils ne sont pas divisibles par un nombre premier plus petit que 20.
   (b) Calculer l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

**Exercice 5.** Cryptosystème RSA

Soit $n \geq 1$ un entier. Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés par des éléments de $\mathbb{Z}/n\mathbb{Z}$. Soit $(e, n)$ sa clé publique.

1. Déterminer sa clé secrète si $(e, n) \in \{(139, 265), (31, 3599)\}$.
2. Alice choisit le couple $(e, n) = (107, 187)$. Bob lui envoie le cryptogramme 9. Quel est le message secret que Bob souhaite transmettre à Alice ?
3. Alice a perdu sa clé publique et ne possède que sa clé privée égale à $(3, 88)$. Parmi ses papiers, elle retrouve le cryptogramme 7 envoyé par Bob, ainsi que le message décrypté égal à 113. Déterminer sa clé publique.