

Un corrigé de l'examen du 20 mai 2011 :

On omet dans la rédaction de ce corrigé les calculs numériques comme l'application de l'algorithme d'Euclide étendu.

Exercice 1 Résoudre en nombres entiers chacune des équations suivantes

$$1539x + 585y = 18 \quad (1)$$

$$1539x + 585y = 15 \quad (2)$$

On commence par calculer $d := \text{pgcd}(1539, 585)$; en effet on sait que la première équation (resp. la deuxième) aura des solutions si et seulement si d divise 18 (resp. 15). Dans le cas présent, on trouve $d = 9$ et, de fait $1539 = 9 \times 171$ et $585 = 9 \times 65$. La deuxième équation n'a aucune solution, la première a des solutions et équivaut (en simplifiant par 9) à l'équation $171x + 65y = 2$. L'algorithme de Bézout étendu fournit $1 = -19 \cdot 171 + 50 \cdot 65$ et on obtient donc une première solution $2 = -38 \cdot 171 + 100 \cdot 65$ c'est-à-dire $(x_0, y_0) = (-38, 100)$, on sait donc que l'ensemble des solutions est

$$S = \{(x, y) = (-38 + 65m, 100 - 171m) \mid m \in \mathbb{Z}\}.$$

Exercice 2 Résoudre en nombres entiers les systèmes d'équations suivants

$$\begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 5 \pmod{36} \end{cases} \quad (3)$$

$$\begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 11 \pmod{36} \end{cases} \quad (4)$$

$$\begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 11 \pmod{36} \\ x \equiv 4 \pmod{5} \end{cases} \quad (5)$$

On commence par calculer $d_1 := \text{pgcd}(117, 36)$; en effet on sait que le premier système de congruences (resp. le deuxième) aura des solutions si et seulement si d_1 divise $3 = 5 - 2$ (resp. si d_1 divise $9 = 11 - 2$). Dans le cas présent, on trouve $d_1 = 9$ donc le premier système de congruences n'a pas de solution, i.e. $S_1 = \emptyset$, alors que le second possède des solutions, en fait on sait déjà que l'ensemble des solutions est une classe de congruence modulo $m_1 := \text{ppcm}(117, 36)$. En

utilisant l'égalité $a \times b = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$, on peut calculer d'ailleurs $m_1 = 117 \times 36/9 = 468$. On peut ensuite observer que :

$$\begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 11 \pmod{36} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 11 \pmod{4} \\ x \equiv 11 \pmod{9} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{117} \\ x \equiv 3 \pmod{4} \end{cases}$$

Pour trouver une solution on cherche $x_0 = 2 + 117h = 3 + 4k$, ce qui amène à résoudre $1 = 117h - 4k$ qui a par exemple (après calculs) pour solution $h = 1$, $k = 29$ d'où l'on tire $x_0 = 119$. Les solutions du deuxième système sont donc

$$S_2 = \{119 + 468m \mid m \in \mathbb{Z}\}.$$

Le troisième système équivaut, d'après ce qui précède, au système

$$\begin{cases} x \equiv 119 \pmod{468} \\ x \equiv 4 \pmod{5} \end{cases}$$

que l'on résout de manière similaire. L'algorithme d'Euclide montre que $d_2 := \text{pgcd}(468, 5) = 1$ et fournit l'identité $1 = 5 \times (-187) + 468 \times 2$. Pour trouver une solution on cherche $x_0 = 119 + 468h = 4 + 5k$, on en tire, après calcul une première solution $h = 3$, $k = 258$ d'où $x_0 = 1523$ et la description des solutions du système :

$$S_3 = \{1523 + 2340m \mid m \in \mathbb{Z}\}.$$

Exercice 3 Si N est un nombre impair, on décompose $N - 1 = 2^s M$ avec M impair et on pose

$$S := \left\{ a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^M = 1 \text{ ou } \exists r \in [0, s-1], a^{2^r M} = -1 \right\}.$$

1. Calculer le cardinal de S pour $N = 59$.
2. Soit $L \geq 1$, combien de solutions modulo 59 possède l'équation $a^L \equiv 1 \pmod{59}$?
3. Combien de solutions modulo 17 possède l'équation $a^2 \equiv -1 \pmod{17}$ (resp. $a^4 \equiv -1 \pmod{17}$) ?
4. Calculer le cardinal de S pour $N = 1003 = 17 \cdot 59$.

1. Comme 59 est premier, on sait que $S = (\mathbb{Z}/59\mathbb{Z})^*$ et a donc 58 éléments.
2. Le groupe $(\mathbb{Z}/59\mathbb{Z})^*$ est cyclique de cardinal 58 donc le nombre d'éléments vérifiant $a^L = 1$ est $\text{pgcd}(L, 58)$.
3. Le groupe $(\mathbb{Z}/17\mathbb{Z})^*$ est cyclique de cardinal 16 donc le nombre d'éléments vérifiant $a^L = 1$ est $\text{pgcd}(L, 16)$; le nombre d'éléments vérifiant $a^L = -1$ est donc 0 ou $\text{pgcd}(L, 16)$. Pour voir qu'il existe a tel que $a^2 \equiv -1 \pmod{17}$ (resp. $a^4 \equiv -1 \pmod{17}$) on peut exhiber un exemple $4^2 \equiv -1 \pmod{17}$ (resp. $2^4 \equiv -1 \pmod{17}$); on peut aussi raisonner sans calcul à partir d'un générateur g de $(\mathbb{Z}/17\mathbb{Z})^*$ et en remarquant que $x^2 = 1$ équivaut à

$x = \pm 1$: l'élément g^2 est d'ordre 8 donc $(g^2)^8 = 1$ mais $(g^2)^4 \neq 1$ donc $(g^2)^4 = -1$ et de même $(g^4)^2 = -1$. Dans tous les cas on peut conclure que

$$\text{card}\{a \in (\mathbb{Z}/17\mathbb{Z})^* \mid a^4 = -1\} = 4 \quad \text{et} \quad \text{card}\{a \in (\mathbb{Z}/17\mathbb{Z})^* \mid a^2 = -1\} = 2$$

4. Écrivons $N - 1 = 2.501$, on a donc $S = \{a \in (\mathbb{Z}/17\mathbb{Z})^* \mid a^{501} = 1\} \cap \{a \in (\mathbb{Z}/17\mathbb{Z})^* \mid a^{501} = -1\}$ égal disons $S_0 \cup T_0$. On a $-1 \in T_0$ donc T_0 est non vide et $|S_0| = |T_0|$. D'après le cours

$$|S_0| = \text{pgcd}(16, 501) \text{pgcd}(58, 501) = 1, \quad \text{donc} \quad |S| = 1 + 1 = 2.$$

Exercice 4 Soit $L := 225 = 3^2.5^2$, $M := 143 = 11.13$ et $N := 248 = 2^3.31$.

1. Calculer $\phi(L)$, $\phi(M)$ et $\phi(N)$.
 2. Calculer $\lambda(L)$, $\lambda(M)$ et $\lambda(N)$.
 3. Montrer que les groupes $(\mathbb{Z}/225\mathbb{Z})^*$ et $(\mathbb{Z}/143\mathbb{Z})^*$ sont isomorphes. Les groupes $(\mathbb{Z}/225\mathbb{Z})^*$ et $(\mathbb{Z}/248\mathbb{Z})^*$ sont-ils isomorphes ?
1. On calcule d'abord les valeurs de ϕ en utilisant que, pour p premier, on a $\phi(p^m) = p^m - p^{m-1}$ et que, lorsque $\text{pgcd}(a, b) = 1$, on a $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(225) = \phi(3^2.5^2) = \phi(3^2)\phi(5^2) = (3^2 - 3)(5^2 - 5) = 120$$

$$\phi(143) = \phi(11.13) = \phi(11)\phi(13) = 10.12 = 120$$

$$\phi(248) = \phi(2^3.31) = \phi(2^3)\phi(31) = 4.30 = 120$$

2. On calcule ensuite les valeurs de λ en utilisant que, pour p premier impair, on a $\lambda(p^m) = p^m - p^{m-1}$ tandis que $\lambda(2^m) = 2^{m-2}$ (pour $m \geq 3$) et que, lorsque $\text{pgcd}(a, b) = 1$, on a $\lambda(ab) = \text{ppcm}(\lambda(a), \lambda(b))$.

$$\lambda(225) = \lambda(3^2.5^2) = \text{ppcm}(\lambda(3^2), \lambda(5^2)) = \text{ppcm}(6, 20) = 60$$

$$\lambda(143) = \lambda(11.13) = \text{ppcm}(\lambda(11), \lambda(13)) = \text{ppcm}(10, 12) = 60$$

$$\lambda(248) = \lambda(2^3.31) = \text{ppcm}(\lambda(2^3), \lambda(31)) = \text{ppcm}(2, 30) = 30$$

3. Comme $\lambda(N) \neq \lambda(L) = \lambda(M)$, on peut conclure que $(\mathbb{Z}/248\mathbb{Z})^*$ n'est pas isomorphe aux deux autres groupes. Les deux groupes $(\mathbb{Z}/225\mathbb{Z})^*$ et $(\mathbb{Z}/143\mathbb{Z})^*$ ont le même cardinal et le même exposant mais cela ne suffit pas à montrer qu'ils sont isomorphes. Pour montrer cela on utilise le lemme chinois et les théorèmes de cyclicité pour décomposer :

$$(\mathbb{Z}/L\mathbb{Z})^* \cong (\mathbb{Z}/3^2\mathbb{Z})^* \times (\mathbb{Z}/5^2\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$(\mathbb{Z}/M\mathbb{Z})^* \cong (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

d'où l'on déduit bien que les deux groupes sont isomorphes.

Exercice 5 On suppose que $N = pq$ est le produit de deux premiers distincts, que c est le paramètre pour coder, i.e. on transforme un message m en $m' = m^c \pmod N$ avant de l'envoyer. On note d l'inverse de $c \pmod{\phi(N)}$, de sorte que le décodage s'effectue en calculant $m = m'^d \pmod N$. Dans le système RSA les paramètres (N, c) sont publics, le paramètre d est secret.

1. Soit $N = 55$ et $c = 7$. Coder le message $m = 2$ et vérifiez le résultat en le décodant.
 2. Vos paramètres publics sont $(N, c) = (649, 83)$, vous savez que $649 = 11 \cdot 59$ et vous recevez le message $m' = 3$. Quel est le message original qui vous a été envoyé ?
1. Le message codé est $m' = 2^7 \pmod{55}$, on calcule par exemple $2^3 = 8$, $2^6 = 64 \equiv 9 \pmod{55}$ donc $m' = 18$. On a $N = 5 \cdot 11$, donc $\phi(N) = 4 \cdot 10 = 40$ et l'inverse de $7 \pmod{40}$ est $d = 23$. Le théorème d'Euler garantit que $(m')^d \equiv m \pmod{55}$, vérifions-le avec le schéma $a^{23} = ((a^4)^2 a)^2 a$ (calculs modulo 55) : $18^2 = 324 \equiv 49$, $18^4 \equiv 36$, $18^5 = 648 \equiv 43$, $18^{10} \equiv 34$, $18^{11} = 612 \equiv 7$, $18^{22} = 49 \equiv 34$, $18^{23} = 882 \equiv 2$ (oui!).
 2. Nous avons $\phi(N) = 10 \cdot 58 = 580$, l'inverse de $c = 83 \pmod{580}$ est 7 (noter que $7 \cdot 83 = 581$ et donc le message initial est $m \equiv (m')^7 \equiv 3^7 \equiv 240 \pmod{649}$ (en omettant le détail des calculs)).