FEUILLE D'EXERCICES n° 1 [*Correction*]

Arithmétique

Exercice 1 – Tout nombre rationnel est le quotient de deux nombres entiers premiers entre eux. Soit donc $a = p/q$ avec $(p, q) = 1$. Si $18a$ est entier, alors q divise $18p$. On rappelle :

Lemme (Gauss)**.** *a, b, c étant des nombres entiers, si a divise bc et si a est premier avec b alors a divise c.*

Comme $(p, q) = 1$ on peut conclure que q divise 18. De même q divise 25. Finalement, si q divise 18 et 25 alors q divise leur pgcd qui vaut 1, donc $q = 1$, ce qui prouve que a est entier.

Exercice 2 – Rappelons la démonstration du fait qu'il y a une infinité de nombres premiers : si $p_1, \ldots, p_n$ sont premiers alors $N = p_1 \ldots p_n + 1$ n'est divisible par aucun des p_i ; comme c'est un entier au moins égal à 2, il possède un diviseur premier $p \notin \{p_1, \ldots, p_n\}$.

Supposons maintenant qu'en outre $p_i \equiv -1 \mod 4$ pour tout $i = 1, \ldots, n$; ceci implique qu'ils sont impairs. L'idée est de construire un N qui soit premier aux p_i et qui vérifie également $N \equiv -1 \mod 4$. En effet, N possède alors au moins un diviseur premier égal à $-1 \pmod 4$: sinon tous ses diviseurs premiers seraient égaux à $1 \pmod 4$ et donc leur produit aussi.

On a $(p_1 \ldots p_n)^2 \equiv 1 \pmod 4$ donc on peut prendre

$$N = (p_1 \ldots p_n)^2 + 2.$$

Remarquons qu'on utilise ici fondamentalement le fait que les congruences modulo un entier se multiplient !

Exercice 3 – Comme $n^2 - 1 = (n-1)(n+1)$, il est nécessaire que $n - 1 = \pm 1$ ou $n + 1 = \pm 1$ ce qui conduit à examiner les cas $n = 0, 2, -2$, pour lesquels $n^2 - 1$ vaut respectivement $1, 3, 3$. Rappelons que le nombre 1 n'est pas premier.

Exercice 5 –

1) $a^2 - b^2 = (a - b)(a + b)$

2) $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$

3) $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$

4) $a^{2n+1} + b^{2n+1} = (a + b)(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n})$. On a simplement remplacé n par $2n + 1$ et b par $-b$ dans la formule précédence.

5) On applique successivement (1), (2), (3) :

$$\begin{aligned} 5^{10} - 2^{10} &= (5^5 - 2^5)(5^5 + 2^5) \\ &= (5-2)(5^4 + 2\cdot 5^3 + 2^2\cdot 5^2 + 2^3\cdot 5 + 2^4) \\ &\quad \times (5+2)(5^4 - 2\cdot 5^3 + 2^2\cdot 5^2 - 2^3\cdot 5 + 2^4) \\ &= 3\cdot 1031\cdot 7\cdot 451. \end{aligned}$$

On vérifie directement que 3, 7 et 1031 sont premiers et que $451 = 11\cdot 41$.

Exercice 6 –

1) Vous verrez plus tard des critères d'irréductibilité plus efficaces que de vérifier qu'aucun nombre premier plus petit que $\sqrt{N}$ ne divise N.

2) On factorise :

$$\begin{aligned} 2^{32} - 1 &= (2^{16} - 1)(2^{16} + 1) \\ &= (2^8 - 1)(2^8 + 1)(2^{16} + 1) \\ &= (2^4 - 1)(2^4 + 1)(2^8 + 1)(2^{16} + 1) \\ &= (2^2 - 1)(2^2 + 1)(2^4 + 1)(2^8 + 1)(2^{16} + 1) \\ &= (2 - 1)(2 + 1)(2^2 + 1)(2^4 + 1)(2^8 + 1)(2^{16} + 1) \\ &= 3\cdot 5\cdot 17\cdot 257\cdot 65537 \end{aligned}$$

3) Si $k = 2^e b$ avec b impair, alors l'identité

$$y^b + 1 = (y+1)(y^{b-1} - y^{b-2} + \cdots + 1),$$

appliquée en $y = 2^{2^e}$, montre que $2^{2^e} + 1$ divise $2^k + 1$. Si $b \neq 1$ c'est un diviseur non trivial.

4) Montrons les deux observations :

a) $641 = 2^9 + 2^7 + 1$ donc $2^7\cdot 5 = 2^7(2^2+1) = 2^9 + 2^7 = 641 - 1 \equiv -1 \pmod{641}$.

b) En effet $5^4 = 625 \equiv -16 \pmod{641}$.

Comme $32 = 4\cdot 7 + 4$, on a dans $\mathbb{Z}/641\mathbb{Z}$:

$$\begin{aligned} 2^{32} = (2^7)^4\cdot 2^4 &= (2^7)^4\cdot(-5^4) \\ &= -(2^7\cdot 5)^4 \\ &= -(-1)^4 = -1 \end{aligned}$$

donc 641 divise $2^{32} + 1$.

Exercice 7 – Comme $10^k \equiv 0 \pmod 4$ pour $k \geqslant 2$, un nombre N d'écriture décimale $\overline{a_n \ldots a_1 a_0} = 10^n a_n + \cdots + a_0$ est congru à $\overline{a_1 a_0} = 10a_1 + a_0 \pmod 4$.

Exercice 8 – L'algorithme d'Euclide appliqué à un couple de nombres entiers $(a, b) \neq (0, 0)$ calcule le pgcd de a et b. On effectue les divisions euclidiennes successives en posant $r_0 = a$, $r_1 = b$, puis en effectuant les divisions euclidiennes suivantes :

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\dots \\ r_{i-1} &= r_i q_i + r_{i+1} \\ &\dots \\ r_{t-1} &= r_t q_t + r_{t+1}, \quad \text{avec } r_t \neq 0,\ r_{t+1} = 0. \end{aligned}$$

Le pgcd de a et b est alors $d = r_t$, le dernier reste non nul. Une relation de Bezout est une équation de la forme $d = au + bv$ où $d = (a, b)$. Rappelons que a est inversible modulo b, c'est-à-dire $a \in (\mathbb{Z}/b\mathbb{Z})^*$ si et seulement si $(a, b) = 1$. Une relation de Bezout $au + bv = 1$ montre que $au \equiv 1 \pmod{b}$ et donc $a^{-1} = u$ dans $(\mathbb{Z}/b\mathbb{Z})^*$; de même, $b^{-1} = v$ dans $(\mathbb{Z}/a\mathbb{Z})^*$.

Pour extraire une relation de Bezout, on peut « remonter » les équations données par les divisions euclidiennes successives de l'algorithme d'Euclide, mais il est plus efficace d'appliquer l'algorithme dit d'*Euclide étendu* : celui-ci calcule en même temps que la suite des q_i et des r_i, deux suites u_i et v_i vérifiant les relations de récurrence :

$$\begin{aligned} u_{i+1} &= u_{i-1} - q_i u_i \\ v_{i+1} &= v_{i-1} - q_i v_i \end{aligned}$$

et les conditions initiales :

$$\begin{pmatrix} u_0 & v_0 \\ u_1 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Le dernier couple (u_t, v_t) calculé donne une relation de Bezout entre a et b. L'intérêt de cet algorithme réside dans le fait que son exécution ne nécessite pas de garder en mémoire tous les (q_i, r_i, u_i, v_i) mais seulement les deux précédents.

Exemple. $a = 34$, $b = 21$.

i	r_i	q_i	u_i	v_i	
0	34		1	0	
1	21	1	0	1	
2	13	1	1	-1	$L_2 \leftarrow L_0 - q_1 L_1$
3	8	1	-1	2	$L_3 \leftarrow L_1 - q_2 L_2$
4	5	1	2	-3	$L_4 \leftarrow L_2 - q_3 L_3$
5	3	1	-3	5	$L_5 \leftarrow L_3 - q_4 L_4$
6	2	1	5	-8	$L_6 \leftarrow L_4 - q_5 L_5$
7	1	2	-8	13	$L_7 \leftarrow L_5 - q_6 L_6$
8	0				

On trouve la relation de Bezout $(-8) \cdot 34 + 13 \cdot 21 = 1$; dans $\mathbb{Z}/21\mathbb{Z}$, on a $34^{-1} = -8$; dans $\mathbb{Z}/34\mathbb{Z}$, on a $21^{-1} = 13$.

Preuve de l'algorithme d'Euclide étendu. on exprime le passage de (r_{i-1}, r_i) à (r_i, r_{i+1}) par la relation matricielle

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix},$$

ce qui conduit par itération à :

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}.$$

En posant, pour $i \geqslant 1$,

$$U_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}, \quad \text{et} \quad U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

on a

$$U_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} U_{i-1}, \quad \text{pour tout } i \geqslant 1.$$

En posant $U_i = \left(\begin{smallmatrix} u_i & v_i \\ s_i & t_i \end{smallmatrix}\right)$, on en déduit les relations

$$\begin{cases} u_i = s_{i-1}, \\ v_i = t_{i-1}, \\ s_i = u_{i-1} - q_i u_i \ = u_{i+1}, \\ t_i = v_{i-1} - q_i v_i \ = v_{i+1}. \end{cases}$$

À la dernière étape, on a

$$\begin{pmatrix} r_t = (a, b) \\ r_{r+1} = 0 \end{pmatrix} = U_t \begin{pmatrix} a \\ b \end{pmatrix}$$

dont la première ligne donne la relation de Bezout $(a, b) = u_t a + v_t b$.

Une dernière optimisation. puisque le calcul des u_i ne fait pas intervenir les v_i, ce n'est pas la peine de remplir la colonne des v_i dans le tableau ci-dessus, on peut se contenter des u_i, puisque de $d = (a, b)$, $u = u_t$, a, et b, on déduit $v = (d - au)/b$.

Exercice 9 – $32x + 10y = 6$ ssi $16x + 5y = 3$. Comme $(16, 5) = 1$ et que $16 - 3 \cdot 5 = 1$ on a $16^{-1} = 1 \mod 5$ et $5^{-1} = -3 \mod 16$. On a $16x = 3 \mod 5$ ssi $x = 3 \mod 5$ et $5y = 3 \mod 16$ ssi $y = -9 \mod 16$. En remplaçant $x = 3 + 5x'$ et $y = -9 + 16y'$ on trouve que $16x + 5y = 3$ ssi $x' = -y'$. finalement les solutions (x, y) sont tous les $(3 + 5q, -9 - 16q)$ avec $q \in \mathbb{Z}$.

Exercice 10 – On doit donc résoudre $12J + 31M = 442$. Par l'algorithme d'Euclide étendu on trouve $13 \cdot 12 - 5 \cdot 31 = 1$. Comme dans l'exercice précédent on a $J = 11 \mod 31$ et $M = 10 \mod 12$. Comme $1 \leqslant M \leqslant 12$ la seule solution est $M = 10$ et donc $J = 11$.

Exercice 11 –

1) $(3, 37) = 1$ donc $3 \in (\mathbb{Z}/37\mathbb{Z})^*$; une relation de Bezout $37 - 3 \cdot 12 = 1$ montre que $3^{-1} = 12 \mod 37$.

2) $(4, 14) = 2 > 1$ donc 4 n'est pas inversible modulo 14.

Exercice 12 – On rappelle que a est un inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $(a, n) = 1$. On a donc : $(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\}$, $(\mathbb{Z}/6\mathbb{Z})^* = \{1, 3, 5\}$, $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. Si p est premier, les inversibles de $\mathbb{Z}/p^2\mathbb{Z}$ sont les $a \mod p^2$ tels que p ne divise pas a. Il y en a donc $p^2 - p$.

Exercice 14 – Comme $2 \in (\mathbb{Z}/5\mathbb{Z})^*$ et $3 \in (\mathbb{Z}/7\mathbb{Z})^*$, on obtient

$$\left\{\begin{array}{rcll} 2x & = & 37 & \mod 5 \\ 3x & = & 48 & \mod 7 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcll} 2x & = & 2 & \mod 5 \\ 3x & = & 6 & \mod 7 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcll} x & = & 1 & \mod 5 \\ x & = & 2 & \mod 7 \end{array}\right.$$

On utilise la relation de Bezout $3 \cdot 5 - 2 \cdot 7 = 1$ pour remarquer que

$$15 = \begin{cases} 0 & \mod 5 \\ 1 & \mod 7 \end{cases} \quad \text{et} \quad -14 = \begin{cases} 1 & \mod 5 \\ 0 & \mod 7 \end{cases}.$$

On en déduit que

$$2 \cdot 15 - 14 = 16 = \begin{cases} 1 & \mod 5 \\ 2 & \mod 7 \end{cases}.$$

Alors x vérifie le système $\Leftrightarrow x - 16$ est divisible par 5 et $7 \Leftrightarrow x - 16$ est divisible par 35. Finalement l'ensemble des solutions est l'ensemble des $x = 16 \mod 35$.

Exercice 15 – Pour résoudre une équation du second degré du type $x^2+2bx+c = 0$ dans un anneau A, on peut procéder comme dans $\mathbb{R}$ en « complétant le carré » :

$$x^2 + 2bx + c = 0 \Leftrightarrow (x + b)^2 - b^2 + c = 0.$$

Il faut ensuite discuter :

- Si $b^2 - c$ n'est pas un carré dans A, il n'y a pas de solution.
- Si $b^2 - c = a^2$ alors

$$x^2 + bx + c = 0 \Leftrightarrow (x + b)^2 - a^2 = 0 \Leftrightarrow (x + b - a)(x + b + a) = 0.$$

  Alors $x = -b + a$ ou $x = -b - a$ ou $(x + b - a, x + b + a)$ est un couple de diviseurs de zéro (attention à ne pas oublier ce dernier cas...).

L'équation $ax^2 + bx + c = 0$ se ramène au cas précédent si d'une part a est un inversible de A et d'autre part si 2 est inversible dans A : on peut alors toujours écrire $a^{-1}b = 2b'$.

a) $x^2+x+7 = 0$ dans $\mathbb{Z}/13\mathbb{Z} : x^2+x+7 = (x+7)^2-49+7 = (x+7)^2-3 \mod 13$. On a $3 = 16 = 4^2 \mod 13$ donc on obtient $(x+7-4)(x+7+4) = (x+3)(x+11)$ soit $x = 10, 2 \mod 13$.

b) $x^2 - 2x + 3 = 0$ dans $\mathbb{Z}/4\mathbb{Z} : x^2 - 2x + 3 = (x - 1)^2 + 2$. Les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont $0, 1$. Comme 2 n'est pas un carré il n'y a pas de solutions.

c) $x^2 - 4x + 3 = 0$ dans $\mathbb{Z}/12\mathbb{Z} : x^2 - 4x + 3 = (x - 2)^2 - 1 = (x - 3)(x - 1)$. Les diviseurs de zéro dans $\mathbb{Z}/12\mathbb{Z}$ sont : $\{2, 3, 4, 6, 8, 9, 10\}$. À part les solutions $x = 1, 3 \mod 12$, il faut examiner les couples de diviseurs de $0 : x - 1 = 2, 3, 4, 6, 8, 9, 10$, correspond respectivement à $x - 3 = 0, 1, 2, 4, 6, 7, 8$. Les couples $(x - 1, x - 3) = (6, 4), (8, 6)$ donnent deux nouvelles solutions $x = 7, 9 \mod 12$. On obtient 4 solutions en tout.

En fait, sur cet exemple, il est plus rapide et moins risqué de rechercher tous les y modulo 12 tels que $y^2 = 1$, et poser $x = y + 2$. Un tel y est inversible, donc à chercher parmi $\pm 1, \pm 5$ modulo 12 : tous les 4 conviennent (leur carré est 1) et on retrouve les mêmes solutions que par l'autre méthode.