DS n°1 : corrigé

Exercice 1. L'entier 193 est-il inversible modulo 2014 ? Si oui, calculer son inverse.

Solution. On applique l'algorithme d'Euclide étendu :

x_k	u_k	v_k	q_k
2014	1	0	
193	0	1	2
84	1	-10	2
25	-2	21	3
9	7	-73	2
7	-16	167	1
2	23	-240	3
1	-85	887	

De sorte que

$$-85 \times 2014 + 887 \times 193 = 1$$

ce qui implique que $\mathsf{pgcd}(193, 2014) = 1$, *i.e.* 193 est inversible modulo 2014, d'inverse 887 modulo 2014.

Exercice 2. Déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $19x + 3y = 2014$.

Solution. Commençons par trouver une solution particulière. On a l'égalité de Bezout évidente $19 - 6 \times 3 = 1$, donc $2014 \times 19 - 12084 \times 3 = 2014$. Si maintenant $(x, y) \in \mathbb{Z}^2$ vérifie $19x+3y = 2014$, on a $19(x-2014)+3(y+12084) = 0$: comme $\mathsf{pgcd}(3, 19) = 1$, on a $3 \mid x-2014$, et il existe $k \in \mathbb{Z}$ tel que $x = 2014+3k$. On a alors $19 \times 3k+3(y+12084) = 0$, donc $y = -12084 - 19k$. L'ensemble des solutions est donc

$$\{(2014 + 3k, -12084 - 19k),\ k \in \mathbb{Z}\}$$

Exercice 3. Montrer que pour tout $n \in \mathbb{Z}$, les fractions $\frac{21n+4}{14n+3}$ et $\frac{n^3+n}{2n^2+1}$ sont irréductibles.

Solution. Il s'agit de montrer que pour tout $n \in \mathbb{Z}$, on a $\mathsf{pgcd}(21n + 4, 14n + 3) = 1$ et $\mathsf{pgcd}(n^3 + n, 2n^2 + 1) = 1$. Pour le premier, cela résulte de l'égalité de Bezout $3(14n + 3) - 2(21n + 4) = 1$. Pour le deuxième, on a $\mathsf{pgcd}(2n^2 + 1, n) = 1$ et $\mathsf{pgcd}(2n^2 + 1, n^2 + 1) = 1$ (car $2(n^2 + 1) - (2n^2 + 1) = 1$), donc $\mathsf{pgcd}(2n^2 + 1, n^3 + n) = 1$.

Exercice 4. On veut déterminer les solutions de l'équation diophantienne

$$(*) \qquad x^2 - 13y^2 = 7$$

Soit donc $(x, y) \in \mathbb{Z}^2$ une solution de $(*)$.

(1) Montrer que ni x, ni y n'est divisible par 7.
(2) Montrer que $x^2 \equiv -y^2 \mod 7\,\mathbb{Z}$.
(3) En déduire que -1 est un carré modulo 7.

(4) Déterminer les carrés modulo 7, et en déduire que $(*)$ n'a pas de solutions entières.

Solution. (1) Si x est divisible par 7, alors $x = 7a$ avec $a \in \mathbb{Z}$, donc $13y^2 = x^2 - 7 = 7(7a^2 - 1)$ est divisible par 7. Comme 13 est premier à 7, on a $7 \mid y^2$, et donc $7 \mid y$ parce que 7 est premier : on peut écrire $y = 7b$ avec $b \in \mathbb{Z}$. L'égalité $(*)$ s'écrit alors $7^2(a^2 - 13b^2) = 7$, *i.e.* $7(a^2 - 13b^2) = 1$, ce qui est absurde : x n'est pas divisible par 7. De même, y n'est pas divisible par 7.

(2) En réduisant $(*)$ modulo $7\,\mathbb{Z}$, on a $x^2 \equiv -y^2 \mod 7\,\mathbb{Z}$ vu que $-13 \equiv 1 \mod 7\,\mathbb{Z}$.

(3) Comme $\mathsf{pgcd}(y, 7) = 1$, l'entier y est inversible modulo 7 : il existe $z \in \mathbb{Z}$ tel que $yz \equiv 1 \mod 7\,\mathbb{Z}$. En multipliant la congruence de la question précédente par z^2, on en déduit $(xz)^2 \equiv -1 \mod 7\,\mathbb{Z}$, et -1 est un carré modulo 7.

(4) Dressons la table des carrés modulo 7 :

a	0	± 1	± 2	± 3
a^2	0	1	4	2

Comme -1 n'est congru modulo $7\,\mathbb{Z}$ à aucun des entiers de la deuxième ligne, ce n'est pas un carré modulo 7. Cela implique que l'existence d'un couple $(x, y) \in \mathbb{Z}^2$ solution de $(*)$ est absurde.

Exercice 5. Démontrer que si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab.

Solution. Il existe $u, v \in \mathbb{Z}^2$ tels que $au + bv = 1$. Observons d'abord que $a + b$ est premier à a : cela résulte par exemple de l'égalité de Bezout $(a + b)v + a(u - v) = 1$. De même, $a + b$ est premier à b, et $(a + b)u + b(v - u) = 1$. Il en résulte que $a + b$ est premier à ab, une égalité de Bezout s'obtenant en prenant le produit des égalités de Bezout :

$$\big((a + b)v + a(u - v)\big)\big((a + b)u + b(v - u)\big) = 1$$
$$(a + b)\big((a + b)uv + vb(v - u) + ua(u - v)\big) - ab(u - v)^2 = 1$$

Remarquons qu'on peut aussi raisonner par l'absurde : si $d = \mathsf{pgcd}(a + b, ab) \neq 1$, soit p premier divisant d. On a $p \mid ab$, donc $p \mid a$ ou $p \mid b$: quitte à échanger a et b, on peut supposer $p \mid a$. Comme en outre $p \mid a + b$, on a aussi $p \mid b$, de sorte que $p \mid \mathsf{pgcd}(a, b)$, ce qui contredit l'hypothèse a et b premiers entre eux.