Le problème des chantiers 195

Daniel PERRIN

1 Le problème

1.1 Le problème initial

L'avis de recherche proposé dans *Les chantiers de pédagogie mathématique* numéro 195 est le suivant :

Soit a et b deux entiers.

a) Montrer que les deux propositions suivantes sont équivalentes :
(P_1) $a \equiv 1 \pmod 2$ *et* $b \equiv a \pmod 3$,
(P_2) $a + 2b \equiv 3 \pmod 6$.

b) Soit n et p deux entiers strictement supérieurs à 1 et premiers entre eux. Soit c un entier. Montrer qu'il existe trois entiers relatifs u, v et w tels que les deux propositions suivantes sont équivalentes :
(P_1) $a \equiv c \pmod n$ *et* $b \equiv a \pmod p$,
(P_2) $ua + vb \equiv w \pmod{np}$

c) Problème ouvert : Qu'en est-il lorsque n et p ne sont pas premiers entre eux ?

1.2 Une réécriture

Je n'aime pas trop la formulation de l'énoncé (en particulier l'annonce préalable des entiers a, b). Voilà ce que je propose.

1.1 Question. *Soient n, p deux entiers strictement supérieurs à 1 et c un entier. Existe-t-il trois entiers $u, v, w \in \mathbf{Z}$ (dépendant de n, p, c) tels que les deux ensembles suivants soient égaux :*
$A_{n,p,c} = \{(a, b) \in \mathbf{Z} \mid a \equiv c \pmod n \text{ et } b \equiv a \pmod p\}$,
$B_{n,p,u,v,w} = \{(a, b) \in \mathbf{Z} \mid ua + vb \equiv w \pmod{np}\}$.
Lorsqu'aucune ambiguïté n'est à craindre on désignera seulement ces ensembles par les lettres A et B.

2 Le cas n, p premiers entre eux

2.1 Une solution

Dans ce cas, la propriété est vraie. Il suffit de prendre $u = p - n$, $v = n$ et $w = pc$. En effet, B est alors l'ensemble des couples (a, b) tels que $N :=$

$(p-n)a+nb-pc = p(a-c)+n(b-a)$ soit multiple de np. Comme n et p sont pemiers entre eux, cela équivaut à N multiple de n et de p, ou encore à $p(a-c)$ multiple de n et $n(b-a)$ multiple de p. Mais, toujours parce que n et p sont premiers entre eux, le théorème de Gauss montre que cela équivaut à $a-c$ multiple de n et $b-a$ de p, autrement dit $(a,b) \in A$.

2.2 Analyse

Dans la preuve précédente on a parachuté les valeurs de u, v, w convenables. En fait, on n'a pas vraiment le choix :

2.1 Proposition. *Soient n, p deux entiers strictement supérieurs à 1 et c un entier.*

1) Avec les notations de 1.1, on suppose qu'on a $A_{n,p,c} \subset B_{n,p,u,v,w}$ avec $u, v, w \in \mathbf{Z}$. Alors, il existe $k, l \in \mathbf{Z}$ tels que l'on ait $u = lp - kn$, $v = kn$ et $w \equiv lpc \pmod{np}$.

2) Si, de plus, pour ces valeurs de l et k, on a $pgcd(n,p) = 1$, $pgcd(k,p) = 1$ et $pgcd(l,n) = 1$, l'inclusion inverse est vérifiée.

Démonstration. 1) On note d'abord que, si un nombre w convient, tous les nombres de sa classe modulo np aussi. Mais on a trois éléments évidents de A : (c,c), $(c+n, c+n)$ et $(c, c+p)$. S'ils sont aussi dans B on a les relations $w \equiv (u+v)c \pmod{np}$, $w \equiv (u+v)c+(u+v)n \pmod{np}$ et $w \equiv (u+v)c+vp \pmod{np}$ dont on déduit par différence qu'on a $(u+v)n \equiv 0 \pmod{np}$ et $vp \equiv 0 \pmod{np}$. On voit que p divise $u+v$ et que n divise v et on a donc $v = kn$ et $u = lp - kn$ avec $k, l \in \mathbf{Z}$ et, avec $w \equiv (u+v)c \pmod{np}$, on obtient $w \equiv lpc \pmod{np}$.

2) Inversement, si (a,b) est dans B, on a $ua + vb \equiv w \pmod{np}$. On voit que np divise $lp(a-c) + kn(b-a)$ et, avec les hypothèses, on en déduit que n divise $a-c$ et que p divise $b-a$, de sorte que (a,b) est dans $A_{n,p,c}$.

3 Une solution élémentaire du cas général

3.1 Analyse

En vertu de 2.1, si l'on a l'égalité des ensembles A et B on a nécessairement $u = lp - kn$, $v = kn$ et $w = lpc$ (modulo np) et on vérifie que l'inclusion $A \subset B$ est acquise. Il s'agit de voir si l'inclusion inverse est encore vraie. Pour cela on note δ le $pgcd$ de n et p et on pose $n = \delta n'$, $p = \delta p'$ avec n' et p' premiers entre eux. Dire que (a,b) est dans B s'écrit alors : np divise $(a-c)lp+(b-a)kn$ ou encore $\delta n'p'$ divise $(a-c)lp'+(b-a)kn'$. Cela implique que n' divise $(a-c)l$ et que p' divise $(b-a)k$.

3.2 Un contre-exemple particulier

On prend $n = 6$, $p = 10$, $c = 0$. On a donc $\delta = 2$, $n' = 3$, $p' = 5$. On a vu que l'on a nécessairement $u = 10l - 6k$, $v = 6k$ et $w = 0$ (modulo 60). Dire que (a, b) est dans A signifie que a est multiple de 6 et $b - a$ de 10. Dire que (a, b) est dans B signifie que $10la + 6k(b - a)$ est multiple de 60, ou encore que 30 divise $5la + 3k(b - a)$. Alors, quels que soient les choix de k et de l, il existe toujours (a, b) qui est dans B et pas dans A. Pour établir cela, on distingue selon les parités de k et l :

• Si l est pair, $a = b = 3$ convient. En effet, on a $5la + 3k(b - a) = 15l$ et ce nombre est multiple de 30 bien que a ne soit pas multiple de 6.

• Si k est pair, $a = 0$ et $b = 5$ convient car on a $5la + 3k(b - a) = 15k$.

• Si k et l sont impairs, $a = 3$ et $b = 8$ convient car on a $5la + 3k(b - a) = 15l + 15k$ et ce nombre est bien multiple de 30.

3.3 Un contre-exemple général

Il repose sur le lemme suivant :

3.1 Lemme. *Soient $\delta, k, l \in \mathbf{Z}$ des entiers avec $\delta \geq 2$. Il existe $\alpha, \beta \in \mathbf{Z}$ tels que δ divise $l\alpha + k\beta$ mais que δ ne divise pas à la fois α et β.*

Démonstration. Si δ divise k et l, il suffit de prendre $\alpha = \beta = 1$. Sinon, on peut supposer, par exemple, que δ ne divise pas k. Soit $\epsilon = pgcd(\delta, k)$. On a donc $\epsilon > 0$ et $\delta = \epsilon\delta'$, $k = \epsilon k'$ avec $pgcd(\delta', k') = 1$ et $\delta' \neq 1$ (sinon δ divise k). Choisissons $\alpha = \epsilon$, de sorte que $\delta = \delta'\epsilon$ ne divise pas α (car $\delta' > 1$). Comme k' est premier avec δ', il existe β tel que δ' divise $l + k'\beta$ (le théorème de Bézout implique que k' est inversible modulo δ'), de sorte que $\delta = \epsilon\delta'$ divise $\epsilon(l + k'\beta) = l\alpha + k\beta$.

On peut maintenant montrer que, quels que soient n, p, c donnés avec n, p non premiers entre eux, il n'existe pas u, v, w tels que $A_{n,p,c} = B_{n,p,u,v,w}$ (autrement dit, l'équivalence de P_1 et P_2 n'est jamais vraie avec n, p non premiers entre eux). En effet, si tel était le cas, on a vu qu'on aurait nécessairement $u = lp - kn$, $v = kn$ et $w = lpc$ (modulo np). Soit $\delta = pgcd(n, p)$, $\delta \geq 2$. On peut appliquer 3.1 à δ, k, l et il existe donc α, β tels que δ divise $l\alpha + k\beta$ mais que δ ne divise pas à la fois α et β. On pose $a = c + \alpha n'$ et $b = c + \alpha n' + \beta p'$. Alors, (a, b) n'est pas dans A sinon $\delta n'$ diviserait $a - c = \alpha n'$ et $\delta p'$ diviserait $b - a = \beta p'$ donc δ diviserait α et β. En revanche, comme on a $au + bv - w = (a - c)lp + (b - a)kn = \alpha l n' p' \delta + \beta k n' p' \delta = (\alpha l + \beta k) n' p' \delta$ et comme δ divise $\alpha l + \beta k$, on voit que $np = \delta^2 n' p'$ divise $au + bv - w$, de sorte que (a, b) est dans B.

4 Une solution plus algébrique

4.1 Le lemme chinois

En fait, la question posée tourne autour du lemme chinois, qui relie les congruences modulo n et p à celles modulo np. On peut formaliser ce résultat en considérant l'homomorphisme $\Phi : \mathbf{Z}/np\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ qui associe à $\overline{x}$, classe de x modulo np, ses classes $\widehat{x}$ et $x^\vee$ modulo n et p. On sait que, lorsque n et p sont premiers entre eux, Φ est un isomorphisme (on montre qu'il est injectif, donc aussi surjectif pour une question de cardinal). Lorsque n et p ne sont pas nécessairement premiers entre eux, on a le résultat suivant :

4.1 Théorème. *Soient n, p deux entiers positifs et δ leur pgcd. On pose $n = \delta n'$ et $p = \delta p'$ avec n' et p' premiers entre eux. Le ppcm de n et p est alors $m = \delta n' p'$. Le théorème de Bézout assure qu'il existe $\alpha, \beta \in \mathbf{Z}$ tels que l'on ait $1 = \alpha n' + \beta p'$ ou encore $\delta = \alpha n + \beta p$.*

1) Le noyau de Φ est l'image de $m\mathbf{Z}$ dans $\mathbf{Z}/np\mathbf{Z}$. Il est de cardinal δ.

2) L'image V de Φ est formée des couples $(\widehat{y}, z^\vee)$ tels que $y - z$ soit dans l'idéal $(n, p) = (\delta)$ (autrement dit tels que $y - z$ soit multiple de δ). Elle est de cardinal m.

3) L'homomorphisme Φ induit un isomorphisme

$$\overline{\Phi} : \mathbf{Z}/m\mathbf{Z} \to V \subset \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}.$$

Si $(\widehat{y}, z^\vee)$ est dans V (c'est-à-dire si $y - z$ est multiple de δ) on a $\Phi^{-1}(y, z) = \beta p' y + \alpha n' z$ modulo m.

Démonstration. 1) Dire que $\overline{x}$ est dans le noyau signifie qu'il est multiple de n et de p, donc de leur *ppcm*.

2) Dire que $(\widehat{y}, z^\vee)$ est dans l'image signifie qu'il existe x tel que $x \equiv y \pmod{n}$ et $x \equiv z \pmod{p}$. On a donc $x = y + kn = z + lp$, de sorte que $y - z = -kn + lp$ est dans l'idéal $(n, p) = (\delta)$.

3) Comme on est passé au quotient par le noyau, il est clair que $\overline{\Phi}$ est injectif, donc un isomorphisme pour une raison de cardinal. On peut exhiber son inverse. Si $(\widehat{y}, z^\vee)$ est dans V, on pose $x = \beta p' y + \alpha n' z$ et on a $x - y = (\beta p' - 1)y + \alpha n' z = \alpha n'(z - y)$ et, comme $z - y$ est multiple de δ, on voit que $x - y$ est bien multiple de n. On montre, de même, que $x - z$ est multiple de p et on a bien $\overline{x} = \overline{\Phi}^{-1}(\widehat{y}, z^\vee)$.

4.2 *Remarque.* Attention, on ne peut pas espérer que l'antécédent de $(\widehat{y}, z^\vee)$ soit défini modulo np. Par exemple, dans le cas $n = 6$, $p = 10$, l'élément $(0, 0)$ admet deux antécédents, $x = 0$, mais aussi $x = 30$, qui ne sont pas égaux modulo $np = 60$.

4.2 Application à une question analogue à 1.1

On déduit de 4.1 le résultat suivant :

4.3 Proposition. *Soient n, p deux entiers strictement supérieurs à 1 et c, d deux entiers. Soit $\delta = pgcd(n,p)$ et $m = ppcm(n,p)$. On suppose que δ divise $c-d$. Il existe trois entiers $u, v, w \in \mathbf{Z}$ (dépendant de n, p, c, d) tels que les deux ensembles suivants soient égaux :*
$A_{n,p,c,d} := A = \{(a,b) \in \mathbf{Z} \mid \delta \,\text{divise}\, b-a,\ a \equiv c \pmod{n} \text{ et } b \equiv d \pmod{p}\}$,
$B_{n,p,u,v,w} := B = \{(a,b) \in \mathbf{Z} \mid \delta \,\text{divise}\, b-a \text{ et } ua+vb \equiv w \pmod{m}\}$.

Autrement dit, l'analogue de la question 1.1 est vrai à trois conditions :
0) On suppose que δ divise $c-d$.
1) On se restreint aux couples (a,b) tels que δ divise $b-a$,
2) On se contente des congruences modulo m (et pas modulo np).

Démonstration. C'est essentiellement 4.1. En effet, si l'on reprend les notations ci-dessus : $n = \delta n'$, $p = \delta p'$, $\alpha n' + \beta p' = 1$ et si l'on pose $u = \beta p'$, $v = \alpha n'$ et $w = uc + vd$, on a $\Phi(w) = (c,d)$ et $\Phi(ua+vb) = (a,b)$ (voir la preuve de 4.1). Dire que (a,b) est dans A signifie que $(a,b) = (c,d)$ dans $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ et comme ces points sont dans l'image de Φ c'est équivalent à $\overline{\Phi}^{-1}(a,b) = ua+vb \equiv \overline{\Phi}^{-1}(c,d) = w$ dans $\mathbf{Z}/m\mathbf{Z}$.

4.3 Application au problème initial

L'application de 4.3 avec n, p, c donnés et $d = 0$, au couple $(a, b-a)$ donne le corollaire suivant :

4.4 Corollaire. *Soient n, p des entiers strictement supérieurs à 1 et soit c un entier. Soit $\delta = pgcd(n,p)$ et $m = ppcm(n,p)$. On suppose que δ divise c. Il existe trois entiers $u, v, w \in \mathbf{Z}$ (dépendant de n, p, c, d) tels que les deux ensembles suivants soient égaux :*
$A_{n,p,c,d} := A = \{(a,b) \in \mathbf{Z} \mid a \equiv c \pmod{n} \text{ et } b \equiv a \pmod{p}\}$,
$B_{n,p,u,v,w} := B = \{(a,b) \in \mathbf{Z} \mid \delta \,\text{divise}\, b-a \text{ et } ua+vb \equiv w \pmod{m}\}$.