

## Corrigé de l'envoi 3 — 2006/2007

### Problème 1 :

Déterminer le plus grand entier qui divise tous les nombres de la forme

$$(a - b)(b - c)(c - d)(d - a)(a - c)(b - d)$$

où  $a$ ,  $b$ ,  $c$  et  $d$  sont des entiers.

---

### Notre solution :

La réponse est 12.

On constate dans un premier temps que lorsque  $a = 1$ ,  $b = 2$ ,  $c = 3$  et  $d = 4$ , le produit  $(a - b)(b - c)(c - d)(d - a)(a - c)(b - d)$  vaut 12. Ainsi le plus petit entier que l'on cherche est au moins égal à 12. Pour conclure, il suffit donc de prouver que 12 est toujours un diviseur de  $(a - b)(b - c)(c - d)(d - a)(a - c)(b - d)$  quels que soient les entiers  $a$ ,  $b$ ,  $c$  et  $d$ .

Nous allons montrer successivement que 3 et 4 divisent ce produit (cela permettra de conclure puisque 3 et 4 sont premiers entre eux). Parmi les quatre entiers  $a$ ,  $b$ ,  $c$  et  $d$ , le principe des tiroirs nous dit qu'au moins deux sont congrus modulo 3. Leur différence est donc un multiple de 3 et comme celle-ci apparaît comme facteur dans le produit qui nous intéresse, ce produit est lui-même un multiple de 3.

Pour montrer qu'il est multiple de 4, on va prouver que deux de ses facteurs sont pairs. Parmi les quatre nombres  $a$ ,  $b$ ,  $c$  et  $d$ , soit deux sont pairs et deux sont impairs, soit trois d'entre eux ont même parité. Dans les deux cas, on obtient bien deux facteurs pairs, et la conclusion s'ensuit.

## Corrigé de l'envoi 3 — 2006/2007

### Problème 2 :

Soit  $P$  un polynôme à coefficients entiers tel que  $P(n) > n$  pour tout  $n > 0$ . On suppose que, pour tout entier  $m > 0$ , il existe au moins un terme de la suite  $P(1), P(P(1)), P(P(P(1))), \dots$  qui est divisible par  $m$ . Prouver que  $P(x) = x + 1$ .

---

### Notre solution :

Commençons par une constatation essentielle : comme  $P$  est un polynôme à coefficients entiers, pour tout  $m > 0$ , on a  $P(x) \equiv P(y) \pmod{m}$  dès que  $x \equiv y \pmod{m}$ .

Appliquons à présent l'hypothèse de l'énoncé à  $m = P(1) - 1$  qui est bien un entier strictement positif. On a alors  $P(1) \equiv 1 \pmod{m}$  et par une récurrence immédiate tous les termes de la suite  $P(1), P(P(1)), P(P(P(1))), \dots$  sont congrus à 1 modulo  $m$ . Comme au moins l'un d'entre eux doit être divisible par  $m$ , on a nécessairement  $m = 1$  puis  $P(1) = 2$ .

Nous prouvons maintenant par récurrence (et par un raisonnement analogue) que pour tout entier  $n > 0$ , on a  $P(n) = n + 1$ . On vient de traiter l'initialisation. Supposons à présent que  $P(x) = x + 1$  pour  $x \in \{1, \dots, n - 1\}$  et montrons que  $P(n) = n + 1$ . Pour cela, posons  $m = P(n) - 1$ . On a d'une part  $m > n - 1$ , c'est-à-dire  $m \geq n$ . D'autre part, la suite  $P(1), P(P(1)), P(P(P(1))), \dots$  est alors congrue modulo  $m$  à la suite périodique  $2, 3, \dots, n, 1, 2, 3, \dots, n, 1, \dots$ . Par hypothèse, elle doit contenir un multiple de  $m$  : la seule possibilité est que celui-ci soit  $n$ . Il s'ensuit que  $n = m$  puis  $P(n) = n + 1$ .

Finalement,  $P$  est un polynôme qui prend les mêmes valeurs que le polynôme  $x \mapsto x + 1$  à tous les points entiers. Ils sont donc égaux et l'exercice est résolu.

## Corrigé de l'envoi 3 — 2006/2007

### Problème 3 :

Soit  $k > 0$  un entier. On définit la suite  $(a_n)$  par  $a_1 = k + 1$  et  $a_{n+1} = a_n^2 - ka_n + k$ . Prouver que si  $m \neq n$  alors  $a_m$  et  $a_n$  sont premiers entre eux.

---

### Notre solution :

Considérons deux entiers  $m$  et  $n$  avec  $n < m$ . D'après la relation de l'énoncé, on a  $a_{n+1} \equiv k \pmod{a_n}$ . En injectant cette congruence dans la relation qui définit  $a_{n+2}$ , on obtient :

$$a_{n+2} \equiv k^2 - k^2 + k = k \pmod{a_n}.$$

Une récurrence immédiate montre alors que  $a_{n'} \equiv k \pmod{a_n}$  pour tout  $n' > n$ . En particulier  $a_m \equiv k \pmod{a_n}$ .

Ainsi  $\text{PGCD}(a_n, a_m) = \text{PGCD}(a_n, k)$  et il ne reste plus qu'à montrer que tous les termes de la suite  $(a_n)$  sont premiers avec  $k$ . Pour cela, on calcule  $a_n \pmod{k}$ . On a directement  $a_1 \equiv 1 \pmod{k}$  et  $a_{n+1} \equiv a_n^2 \pmod{k}$ . Ainsi  $a_n \equiv 1 \pmod{k}$  pour tout  $n$ , et la conclusion s'ensuit.

*Remarque.* La méthode que l'on a utilisé pour résoudre l'exercice suit à la lettre l'algorithme d'Euclide usuel pour calculer les PGCD. Dans le premier alinéa, on a montré que le reste de la division euclidienne de  $a_m$  par  $a_n$  est  $k$  : en effet, la congruence  $a_m \equiv k \pmod{a_n}$  nous dit qu'il existe un entier  $q$  tel que  $a_m = qa_n + k$  et on vérifie de plus facilement que  $0 \leq k < a_n$ . Ensuite, l'algorithme d'Euclide demande de calculer le reste de la division euclidienne de  $a_n$  par  $k$ , et le deuxième alinéa de la solution prouve exactement que c'est 1. Le PGCD cherché est donc lui aussi égal à 1.

## Corrigé de l'envoi 3 — 2006/2007

### Problème 4 :

Soient  $n > 1$  un entier et  $p$  un nombre premier tel que  $n$  divise  $p - 1$  et  $p$  divise  $n^3 - 1$ . Prouver que  $4p - 3$  est un carré.

---

### Notre solution :

La factorisation  $n^3 - 1 = (n - 1)(n^2 + n + 1)$  montre que  $p$  divise  $n - 1$  ou  $n^2 + n + 1$ . Or, pour des raisons d'inégalités, on ne peut pas avoir simultanément  $p$  divise  $n - 1$  et  $n$  divise  $p - 1$ . Il en résulte que  $p$  divise  $n^2 + n + 1$ , c'est-à-dire qu'il existe un entier  $q$  tel que  $n^2 + n + 1 = pq$ .

Nous allons montrer que  $q = 1$ . Déjà l'égalité précédente prouve que  $q \equiv 1 \pmod{n}$  puisque par hypothèse  $p \equiv 1 \pmod{n}$ . On raisonne par l'absurde. La congruence précédente entraîne alors  $n \leq q - 1$  et puis :

$$n^2 + n + 1 \leq (q - 1)^2 + (q - 1) + q = q^2 - q < q^2$$

d'où  $q < p$ . Le raisonnement que l'on vient de faire est encore valable si l'on permute  $p$  et  $q$ , ce qui amène à la conclusion  $p < q$ . C'est une contradiction et on a donc prouvé  $q = 1$ .

Il en résulte  $p = n^2 + n + 1$  puis  $4p - 3 = 4n^2 + 4n + 1$  est le carré de  $2n + 1$ .

## Corrigé de l'envoi 3 — 2006/2007

### Problème 5 :

Soit  $p > 1$  un entier fixé. Soit  $(n_i)_{i \geq 0}$  une suite périodique (depuis le début) d'entiers positifs ou nuls. Montrer qu'il existe des suites d'entiers  $(m_i)$  et  $(q_i)$  telles que  $0 \leq m_i < p$  et  $pq_i + m_i = q_{i+1} + n_i$  pour tout entier  $i \geq 0$ .

### Notre solution :

Notons  $d$  la période de la suite  $(n_i)$ . Remarquons tout d'abord que si  $d = 1$ , c'est-à-dire si la suite  $(n_i)$  est constante, disons égale à  $n$ , on peut choisir pour  $(q_i)$  et  $(m_i)$  également des suites constantes respectivement égales au quotient et au reste de la division euclidienne de  $n$  par  $p - 1$ . On a même alors  $m_i < p - 1$ . On suppose donc à partir de maintenant que  $d \geq 2$ .

Supposons qu'une telle suite existe et analysons les contraintes que cela implique. Supposons en outre que l'on cherche des suites  $(m_i)$  et  $(q_i)$  également périodiques de période  $d$ . La relation de l'énoncé appliquée à  $i = 0, 1, \dots, d - 1$  donne les égalités :

$$\begin{aligned} p^d q_0 + p^{d-1} m_0 &= p^{d-1} q_1 + p^{d-1} n_0 \\ p^{d-1} q_1 + p^{d-2} m_1 &= p^{d-2} q_2 + p^{d-2} n_1 \\ &\vdots \\ p q_{d-1} + m_{d-1} &= q_d + n_{d-1} = q_0 + n_{d-1}. \end{aligned}$$

Ainsi si l'on pose  $s = p^{d-1} n_0 + p^{d-2} n_1 + \dots + n_{d-1}$  et  $t = p^{d-1} m_0 + p^{d-2} m_1 + \dots + m_{d-1}$  et que l'on somme les égalités précédentes on obtient :

$$q_0(p^d - 1) + t = s.$$

Par ailleurs de la condition  $m_i \leq p - 1$ , on déduit  $t \leq p^d - 1$  et donc la relation précédente devrait être (sauf si  $m_i$  est constante égale à  $p - 1$ ) la division euclidienne de  $s$  par  $p^d - 1$ .

Bref, cette analyse amène à définir  $q_0$  (resp.  $t_0$ ) comme le quotient (resp. le reste) de la division euclidienne de  $s = p^{d-1} n_0 + p^{d-2} n_1 + \dots + n_{d-1}$  par  $p^d - 1$  et  $m_0$  comme le quotient de la division euclidienne de  $t_0$  par  $p^{d-1}$ . De façon générale définissons  $q_i$ ,  $m_i$  et  $r_i$  par la formule :

$$s_i = p^{d-1} n_i + p^{d-2} n_{i+1} + \dots + n_{i+d-1} = q_i(p^d - 1) + p^{d-1} m_i + r_i$$

avec  $0 \leq p^{d-1} m_i + r_i < p^d - 1$  et  $0 \leq r_i < p$ . Nous allons montrer que les suites ainsi définies vérifient les conditions de l'énoncé. La première relation implique  $m_i < \frac{p^d - 1}{p^{d-1}} < p$  comme voulu. Pour vérifier l'autre condition, remarquons que  $s_{i+1} + n_i(p^d - 1) = p s_i$ . Si  $A$  désigne ce nombre, on obtient en remplaçant par les expressions de  $s_i$  et  $s_{i+1}$  l'égalité :

$$A = (q_{i+1} + n_i)(p^d - 1) + p^{d-1} m_{i+1} + r_{i+1} = p q_i (p^d - 1) + p^d m_i + p r_i = (p q_i + m_i)(p^d - 1) + m_i + p r_i.$$

Le premier et le dernier terme de cette égalité sont des écritures de la division euclidienne de  $A$  par  $p^d - 1$ . En effet, pour le premier c'est évident puisque par hypothèse  $0 \leq p^{d-1} m_{i+1} + r_{i+1} < p^d - 1$ . Pour le second, cela résulte de l'inégalité  $m_i + p r_i \leq (p - 1) + p(p - 1) = p^2 - 1 \leq p^d - 1$  après avoir remarqué que le cas d'égalité ne peut pas se produire car il impliquerait  $d = 2$  et  $m_i = r_i = p - 1$ , puis  $p^{d-1} m_i + r_i = p(p - 1) + (p - 1) = p^2 - 1$  alors qu'il doit y avoir entre ces nombres une inégalité stricte. Finalement, on en déduit que les quotients  $q_{i+1} + n_i$  et  $p q_i + m_i$  sont égaux, ce qui termine l'exercice.

*Remarque.* Les entiers  $m_i$  et  $q_0$  peuvent s'interpréter de la façon suivante. Considérons le réel :

$$x = \sum_{i=0}^{\infty} a_i p^{-i}.$$

C'est moralement le nombre dont l'écriture (après la virgule) en base  $p$  est donnée par la suite  $(n_i)$  sauf que celle-ci ne contient pas nécessairement que des chiffres inférieurs à  $p - 1$ . Dans ce cas  $q_0$  est la partie entière de  $x$  et les  $m_i$  sont les (véritables) chiffres après la virgule de  $x$  écrit en base  $p$ .

Ce point de vue « montre » que la conclusion de l'énoncé demeure encore lorsque la suite  $(n_i)$  n'est pas supposée périodique. De plus si l'on interdit à la suite  $(m_i)$  n'être constante égale à  $p - 1$ , alors celle-ci est uniquement déterminée.

## Corrigé de l'envoi 3 — 2006/2007

### Problème 6 :

Soit  $(p_n)$  la suite des nombres premiers dans l'ordre croissant. Soit  $m > 0$  un entier. Prouver qu'il existe une infinité d'entiers  $i$  tels que  $p_i - p_{i-1} > m$  et  $p_{i+1} - p_i > m$ .

---

Notre solution :