Université de Paris-Sud 2002
S2MIAS, option Arithmétique et Histoire des Nombres

Examen
Lundi 10 juin 2002, durée 2h
Les documents et calculettes sont interdits

I

Question de cours. Soient a et b deux entiers premiers entre eux. Montrer que le plus petit commun

Université de Paris-Sud 2002

S2MIAS, option Arithmétique et Histoire des Nombres

Corrigé de l'examen
Lundi 10 juin 2002, durée 2h

I

Notons $p = PPCM(a, b)$. Comme ab est un multiple de a et de b, $ab \geq p$. Pour la réciproque, on peut utiliser le théorème de Gauss. Comme b divise p, il existe $k \in \mathbf{Z}$ tel que $p = kb$. Comme a divise p et a est premier à b, a divise k, donc ab divise p. On conclut que $ab = p$.

On peut aussi utiliser la décomposition en facteurs premiers. Si

$$a = \prod_i p_i^{v_i}, \quad b = \prod_j p_i^{w_i} \quad \text{et} \quad p = \prod_i p_i^{z_i}$$

sont les décompositions en facteurs premiers de a, b et p (où les exposants peuvent être nuls), alors $z_i = \max\{v_i, w_i\}$. Si a et b sont premiers entre eux, pour chaque i, v_i ou w_i est nul, donc z_i vaut v_i ou w_i, donc $p = ab$.

II

1. Un entier est divisible par 9 si et seulement si la somme de ses chiffres l'est. Un entier est divisible par 11 si et seulement si la somme alternée de ses chiffres l'est. Ce dernier critère repose sur le fait que $10 \equiv -1$ (11). Sachant que $100 \equiv -1$ (101), on obtient le critère suivant : étant donné un entier a, groupons ses chiffres deux par deux, et formons la somme alternée s des tronçons t_i. Alors

$$a = \sum_i t_i 100^i \equiv \sum_i t_i (-1)^i \equiv s \ (101),$$

donc a est divisible par 101 si et seulement si s l'est.

2. Supposons n pair, $n = 2k$. Alors les tronçons valent tous 11,

$$s_n = 11 \sum_{i=0}^{k-1} (-1)^i$$

vaut 0 si k est pair, 11 si k est impair. Si n est impair, alors

$$s_n = s_{n-1} \pm 1.$$

Par conséquent, s_n prend les valeurs 1, 11, 10, 0 et ainsi de suite, avec une période de 4. On conclut que a_n est divisible par 101 si et seulement si n est divisible par 4.

3. Ecrivons les nombres inconnus 3xyz2 et 1uvw. Le nombre 1 (resp. 11) de la preuve par 101 est la somme alternée des paquets de deux chiffres de 3xyz2 (resp. de 1uvw) modulo 101. On a donc $z5 - xy \equiv 1$ (101) et $vw - 1u \equiv 11$ (101). Comme $|z5 - xy| < 100$ et $|vw - 1u| < 90$, nécessairement $z5 - xy = 1$ et $vw - 1u = 11$, ce qui donne $5 - y \equiv 1$ (10) et $w - u \equiv 1$ (11). Comme $|5 - y| \leq 5$ et $|w - u| \leq 9$, nécessairement $5 - y = 1$ mais $w - u$ peut prendre deux valeurs, 1 et -9. D'où une discussion.

Supposons d'abord que $w - u = -9$. Ceci ne se produit que si $w = 0$ et $u = 9$, ce qui entraîne $v = 3$. Il s'agit donc de multiplier 3xyz2 par 1930. Le dernier chiffre du produit est forcément 0 et l'avant dernier $3 \times 2 = 6$, contradiction.

On peut donc supposer que $w - u = 1$. Dans ce cas,

$$y = 4, \quad z = x, \quad v = 2, \quad w = u + 1.$$

Posons la multiplication de 3x4x2 par 1u2w. L'avant dernier chiffre du produit vaut $x \times w + \epsilon + 2 \times 2$ où $\epsilon \in \{0, 1\}$ est la retenue éventuelle du produit $2 \times w$. On a donc $x \times w + \epsilon + 4 \equiv 2\ (10)$, donc $x \times w + \epsilon = 8$.

On va discuter suivant la valeur de la retenue, et les valeurs compatibles de x. Si la retenue vaut 1, $x \times w = 7$ donc x vaut 1 ou 7. Sinon, $x \times w = 8$ et x vaut 1, 2, 4 ou 8.

Premier cas : $x = 1$ et $w = 7$. Dans ce cas, $u = 6$. Or $31412 \times 1627 > 5.10^7$, contradiction.

Deuxième cas : $x = 7$ et $w = 1$. Dans ce cas, $u = 0$. Or $37472 \times 1021 < 4.10^7$, contradiction.

Troisième cas : $x = 1$ et $w = 8$. Dans ce cas, $u = 7$. Or $31412 \times 1728 > 5.10^7$, contradiction.

Quatrième cas : $x = 4$ et $w = 2$. Dans ce cas, $u = 1$. Or $34442 \times 1728 > 5.10^7$, contradiction.

Cinquième cas : $x = 8$ et $w = 1$. Dans ce cas, $u = 0$. Or $38482 \times 1021 < 4.10^7$, contradiction.

C'est donc le sixième cas, $x = 2$ et $w = 4$, qui est le bon. Dans ce cas, $u = 3$. On trouve $32422 \times 1324 = 42926728$.

III

1. D'après le théorème de Bézout, comme a et b sont premiers entre eux, il existe des entiers u et v tels que $au + bv = 1$. Alors $n = 1 + au = 2 - bv$ est congru à 1 modulo a et à 2 modulo b.

2. Pour $a = 3$ et $b = 4$, il suffit de prendre $n = 10$. Pour $a = 26$ et $b = 47$, on emploie la méthode du cours. On écrit les divisions euclidiennes successives

$$47 = 26 + 21, \quad 26 = 21 + 5, \quad 21 = 4 \times 5 + 1$$

et on remonte

$$1 = 21 - 4 \times 5 = 21 - 4 \times (26 - 21) = 5 \times 21 - 4 \times 26 = 5 \times (47 - 26) - 4 \times 26 = 5 \times 47 - 9 \times 26$$

d'où une solution $u = -9$, $v = -5$, $n_0 = -233$.

3. Soient n et n_0 deux entiers n tels que $n \equiv 1\ (a)$ et $n \equiv 2\ (b)$. Alors $n - n_0$ est divisible par a et par b, donc par leur PPCM ab. Inversement, tout nombre de la forme $n = n_0 + kab$ est congru à 1 modulo a et à 2 modulo b. Par conséquent, les solutions du système sont exactement les entiers congrus à n_0 modulo ab.

4. D'après 3., les solutions du système sont les nombres de la forme $-233 + k \times 1222$ où k décrit $\mathbf{Z}$. La plus petite solution positive est donc $-233 + 1222 = 989$.

IV

1. D'après le théorème de Fermat, lorsque p est premier distinct de 13, $13^{p-1} \equiv 1\ (p)$. Cela donne en particulier $13^4 \equiv 1\ (5)$ et $13^{16} \equiv 1\ (17)$.

Les entiers non premiers avec 9 sont les entiers divisibles par 3. Entre 0 et 8, il y en a 3 : 0, 3 et 6, donc les entiers compris entre 0 et 8 premiers avec 9 sont 1,2,4,5,7,8. En particulier, l'in dicatrice d'Euler $\phi(9)$ vaut 6. D'après le théorème d'Euler, comme 13 est premier avec 9, $13^6 \equiv 1\ (9)$.

2. On constate que $13^4 \equiv 1\ (17)$ et $13^3 \equiv 1\ (9)$, donc les restes modulo 5 (resp. 9, resp. 17) des puissances de 13 sont périodiques de période 4 (resp. 3, resp. 4). C'est pourquoi le tableau ci-dessous ne comporte que 5 colonnes.

n	0	1	2	3	4
13^n mod 5	1	3	4	2	1
13^n mod 9	1	4	7	1	4
13^n mod 17	1	13	16	4	1

3. De 2., il résulte que $13^n \equiv 4\ (5)$ si et seulement si $n \equiv 2\ (4)$, et que $13^n \equiv 4\ (17)$ si et seulement si $n \equiv 3\ (4)$. Par conséquent, $13^n - 4$ n'est jamais divisible à la fois par 5 et 17.

4. De 2., il résulte que $13^n \equiv 4\ (5)$ si et seulement si $n \equiv 2\ (4)$, et que $13^n \equiv 4\ (9)$ si et seulement si $n \equiv 1\ (3)$. D'après l'exercice III, il existe $n \in \mathbf{N}$ tel que $n \equiv 1\ (3)$ et $n \equiv 2\ (4)$ simultanément, et $n = 10$ convient. On conclut que $13^{10} - 4$ est divisible à la fois par 5 et 9.