MT 282
30/11/95

Université Paris 7
U.F.R. de Mathématiques
B. Keller

Un corrigé de l'examen partiel du 03.12.95

1) Soit x le nombre de pistolets à eau que possède Jean. D'après les informations fournies, nous avons

$$\begin{aligned} x &\equiv 9 \ (7) \\ x &\equiv -1 \ (9) \\ x &\equiv 4 \ (8). \end{aligned}$$

Les nombres $7, 9, 8$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $7 \times 9 \times 8 = 504$ est unique. Pour trouver x, nous déterminons d'abord x_1, x_2, x_3 dont les classes sont les images réciproques de $(1,0,0), (0,1,0), (0,0,1)$ par la projection

$$\mathbf{Z}/504 \xrightarrow{\sim} \mathbf{Z}/7 \oplus \mathbf{Z}/9 \oplus \mathbf{Z}/8.$$

Nous avons

$$\begin{array}{llll} 72\,u_1 + 7\,v_1 = 1; & \text{sol. part.} & 72 \times (-3) + 7 \times 31 = 1. & \text{Posons} \quad x_1 = -216. \\ 56\,u_2 + 9\,v_2 = 1; & \text{sol. part.} & 56 \times (-4) + 8 \times 25 = 1. & \text{Posons} \quad x_2 = -224. \\ 63\,u_3 + 8\,v_3 = 1; & \text{sol. part.} & 63 \times (-1) + 8 \times 8 = 1 & \text{Posons} \quad x_3 = -63. \end{array}$$

Nous avons donc $x \equiv 9 \times (-216) - 1 \times (-224) + 4 \times (-63) \equiv -1972 \equiv 44 \ (504)$. On a donc $x = 44 + k \times 504$ et si y désigne le nombre d'amis de Jean, on a $y = (x-9)/7 = 5 + 72\,k$. Puisque $y \leq 100$, il s'ensuit que $x = 44$ et $y = 5$. *Jean possède 44 pistolets à eau et il a 5 amis.*

2) a) Nous avons $16 \equiv 2 \ (7)$, donc $16^2 \equiv 4 \ (7)$, $16^3 \equiv 1 \ (7)$ et $16^k \equiv 16^l \ (7)$ si $k \equiv l \ (3)$. Par conséquent

$$a \equiv B \times (1+2+4+1+2+4) + A \times (1+2+4+1+2+4) \equiv 0 \ (7)$$

et $r = 0$.

b) Le nombre 31 est premier et ne divise pas 19. Le petit théorème de Fermat permet donc de conclure que $19^{30} \equiv 1 \ (31)$. Puisque $330 = 11 \times 30$, nous avons $19^{330} \equiv 1 \ (31)$ et $r = 1$.

c) Nous avons $2025 = 25 \times 81$ et $\phi(2025) = \phi(25)\phi(81) = 20 \times 54 = 1080$. Le nombre $532 = 4 \times 7 \times 19$ est premier avec 2025. D'après le théorème d'Euler, nous avons $532^{1080} \equiv 1 \ (2025)$ et donc $532^{2160} \equiv 1 \ (2025)$ car $2160 = 2 \times 1080$. Donc $r = 1$.

d) Nous avons $437 = 19 \times 23$. Comme 19 et 23 sont premiers entre eux, il suffit de calculer les restes de a par 19 et 23 pour connaître le reste de a par 437, d'après le lemme chinois. Nous avons

$$\begin{aligned} a &\equiv 217^{18} \equiv 8^{18} \equiv 1 \ (19) \\ a &\equiv 217^{18} \equiv 10^{18} \ (23). \end{aligned}$$

Ici, nous avons utilisé le petit théorème de Fermat pour calculer que $8^{18} \equiv 1 \ (19)$. Nous avons $10^2 \equiv 8 \ (23)$, $10^4 \equiv 18 \ (23)$, $10^8 \equiv 2 \ (23)$, $10^{16} \equiv 4 \ (23)$ et $10^{18} \equiv 8 \times 4 \equiv 9 \ (23)$. Donc

$$\begin{aligned} a &\equiv 1 \ (19) \\ a &\equiv 9 \ (23). \end{aligned}$$

Nous avons $5 \times 23 - 6 \times 19 = 1$ et donc $a \equiv 5 \times 23 - 9 \times 6 \times 19 \equiv -37 \ (437)$. Donc $r = 400$.

3) Supposons que p ne divise pas n. Alors p et n sont premiers entre eux et on a donc

$$\phi(p\,n) = \phi(p^{k+1}\,n') = \phi(p)\,\phi(n).$$

Puisque p est premier, on a $\phi(p) = p-1$. Donc on a $\phi(p\,n) = (p-1)\,\phi(n)$, si p ne divise pas n.

Supposons maintenant que p divise n et que $n = p^k\,n'$ où $k \geq 1$ et p ne divise pas n'. Alors toute puissance de p est première avec n' et on a donc $\phi(p\,n) = \phi(p^{k+1})\,\phi(n)$. Comme p est premier, on a $\phi(p^{k+1}) = p^{k+1} - p^k$. Donc finalement, on a

$$\begin{aligned}\phi(p\,n) &= \phi(p^{k+1}\,n') = (p^{k+1} - p^k)\,\phi(n') = p\,(p^k - p^{k-1})\,\phi(n') \\ &= p\,\phi(p^k)\,\phi(n') = p\,\phi(p^k\,n') \\ &= p\,\phi(n).\end{aligned}$$

4) a) Nous avons $75 = 3 \times 25$ et $45 = 9 \times 5$. Comme $\mathrm{PGCD}\,(3, 25) = 1$ et $\mathrm{PGCD}\,(9, 5) = 1$, le lemme chinois montre que le système est équivalent au système de quatre congruences

$$\begin{array}{rcll} x & \equiv & c & (3) \\ x & \equiv & c & (25) \end{array} \qquad \begin{array}{rcll} x & \equiv & 6 & (9) \\ x & \equiv & 1 & (5). \end{array}$$

Nous réécrivons ces congruences dans un ordre différent :

$$\begin{aligned} x &\equiv 6 \ (9) && (1) \\ x &\equiv c \ (3) && (2) \\ x &\equiv c \ (25) && (3) \\ x &\equiv 1 \ (5). && (4) \end{aligned}$$

Si ce système possède une solution $x \in \mathbf{Z}$, la congruence (1) implique que $x \equiv 0\ (3)$. La congruence (2) montre alors que $c \equiv 0\ (3)$. De même la congruence (3) implique que $x \equiv c\ (5)$ et la congruence (4) donne que $c \equiv 1\ (5)$. Ainsi, le nombre entier c doit satisfaire les conditions

$$\begin{aligned} c &\equiv 0 \ (3) \\ c &\equiv 1 \ (5). \end{aligned}$$

Réciproquement, si ces conditions sont remplies, la congruence (2) résulte de (1), et (4) résulte de (3). Ainsi les conditions ci-dessus sont nécessaires et suffisantes pour que le système admette une solution. Par le lemme chinois ($\mathrm{PGCD}\,(3, 5) = 1$), nous pouvons conclure que le système admet une solution ssi $c \equiv 6\ (15)$ c'est-à-dire que *la classe* $\overline{c}$ *de* c *modulo* 75 *est* $\overline{6}, \overline{21}, \overline{36}, \overline{51}$ *ou* $\overline{66}$.

b) Nous avons vu dans a) que si $c \equiv 6\ (9)$, le système est équivalent à

$$\begin{aligned} x &\equiv 6 \ (9) \\ x &\equiv c \ (25) \end{aligned}$$

Les nombres 9 et 25 sont premiers entre eux et nous avons l'identité de Bézout $(-11) \times 9 + 4 \times 25 = 1$. Le système est donc équivalent à

$$x \equiv 6 \times 4 \times 25 + c \times (-11) \times 9 \equiv 150 - 99 \times c \ \ (225).$$

Si c *est congru à* $6, 21, 36, 51$ *et* 66 *modulo* 75 *nous trouvons que* x *est congru à* $6, 96, 186, 51$ *et* 141 *modulo* 225, *respectivement.*

5) a) On a $\sigma(1) = 1$, $\sigma(2) = 1 + 2 = 3$, $\sigma(3) = 4$, $\sigma(5) = 6$, $\sigma(6) = 1 + 2 + 3 + 6 = 13$, $\sigma(7) = 8$, $\sigma(8) = 1 + 2 + 4 + 8 = 15$, $\sigma(9) = 1 + 3 + 9 = 12$ et $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

b) La liste des diviseurs positifs de p^k est $1, p, p^2, \ldots, p^k$. Donc

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

c) Soient

$$r = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ et } s = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$$

les décompositions de r et s en produit de puissances strictement positives de nombres premiers distincts deux à deux. Comme r et s sont premiers deux à deux, les ensembles des p_i et celui de q_j sont disjoints. Ainsi,

$$rs = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\, q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$$

est la décomposition de rs en produit de puissances strictement positives de nombres premiers distincts deux à deux. Un diviseur de rs est un nombre de la forme

$$n = p_1^{e_1'} p_2^{e_2'} \cdots p_k^{e_k'}\, q_1^{f_1'} q_2^{f_2'} \cdots q_k^{f_k'}$$

où $e_i' \leq e_i$ et $f_j' \leq f_j$ pour tous i, j. Il s'écrit de façon unique comme le produit d'un diviseur d de r par un diviseur e de s, à savoir

$$d = p_1^{e_1'} p_2^{e_2'} \cdots p_k^{e_k'}\ ,\ e = q_1^{f_1'} q_2^{f_2'} \cdots q_k^{f_k'}.$$

L'application ψ est donc injective et surjective.

d) En utilisant c) nous calculons que

$$\begin{aligned} \sigma(rs) &= \sum_{f \in D(rs)} f = \sum_{(d,e) \in D(r) \times D(s)} de = \sum_{d \in D(r)} \sum_{e \in D(s)} de = \Big(\sum_{d \in D(r)} d\Big)\Big(\sum_{e \in D(s)} e\Big) \\ &= \sigma(r)\,\sigma(s). \end{aligned}$$