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

Un corrigé de l'examen du 06.02.96

1) Soit x le nombre d'amies de Miss M. D'après les informations fournies, nous avons

$$\begin{aligned} x &\equiv -11 \ (12) \\ x &\equiv -5 \ (13) \\ x &\equiv -12 \ (17). \end{aligned}$$

Les nombres $12, 13, 17$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $12 \times 13 \times 17 = 2652$ 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

$$\mathbf{Z}/2652 \xrightarrow{\sim} \mathbf{Z}/12 \oplus \mathbf{Z}/13 \oplus \mathbf{Z}/17.$$

Nous avons

$$\begin{array}{llll} 221\,u_1 + 12\,v_1 = 1; & \text{sol. part.} & 221 \times 5 + 12 \times (-92) = 1. & \text{Posons} \quad x_1 = 1105. \\ 204\,u_2 + 13\,v_2 = 1; & \text{sol. part.} & 204 \times 3 + 13 \times (-47) = 1. & \text{Posons} \quad x_2 = 612. \\ 156\,u_3 + 17\,v_3 = 1; & \text{sol. part.} & 156 \times 6 + 17 \times (-55) = 1 & \text{Posons} \quad x_3 = 936. \end{array}$$

Nous avons donc $x \equiv 1 \times 1105 + 8 \times 612 + 5 \times 936 \equiv 73 \ (2652)$. On a donc $x = 73 + k \times 2652$. Puisque $x \leq 1000$, il s'ensuit que $x = 73$. *Miss M. a 73 amies.*

2) a) Nous avons $a = 1 + 16 + \ldots + 16^{299} = (16^{300} - 1)/(16 - 1)$. Or $16 \equiv 3 \ (13)$ et l'ordre de 3 dans $(\mathbf{Z}/13\mathbf{Z})^*$ est égal à 3. Donc $16^{300} \equiv 1 \ (13)$ et $r = 0$.

b) Le nombre 541 est premier et ne divise pas 113. D'après le petit théorème de Fermat, nous avons donc $113^{140} \equiv 1 \ (541)$ et $r = 1$.

c) Le nombre 1000 est premier avec 23×67 et $\phi(23 \times 67) = \phi(23) \times \phi(67) = 22 \times 66 = 1452$. D'après le théorème d'Euler, nous avons donc $1000^{1452} \equiv 1 \ (23 \times 67)$ et $r = 1$.

d) Nous avons $\lambda(12871) = \text{PPCM}\,(\lambda(61), \lambda(211)) = \text{PPCM}\,(60, 210) = 420$. Or, d'après un lemme du cours, nous avons $x^{\lambda(n)} \equiv 1 \ (n)$ pour tout x premier à n. Ainsi, la classe de a modulo b ne dépend que de la classe de 2^{12} modulo 420. Or $420 = 2^2 \times 3 \times 5 \times 7$ et $\lambda(420) = \text{PPCM}\,(2, 2, 4, 6) = 12$. Donc $17^{12} \equiv 1 \ (420)$ et $a \equiv 2 \ (b)$. Donc $r = 2$.

3) a) Par définition, l'ordre maximal d'un élément de $G = (\mathbf{Z}/675\mathbf{Z})^*$ est égal à $\lambda(675) = \lambda(3^3 \times 5^2) = \text{PPCM}\,(18, 20) = 180$.

b) Je dis que la classe de 2 est d'ordre maximal $(= 180)$ dans G. D'après le théorème chinois, il suffit de vérifier que la classe de 2 est d'ordre 18 dans $G_1 = (\mathbf{Z}/27\mathbf{Z})^*$ et d'ordre 20 dans $G_2 = (\mathbf{Z}/25\mathbf{Z})^*$. Or les diviseur maximaux de 18 sont 9 et 6 et nous avons $2^9 \equiv -1 \ (27)$ et $2^6 \equiv 10 \ (27)$. Donc 2 est bien d'ordre 18 dans G_1. Les diviseurs maximaux de 20 sont 10 et 4. Or nous avons $2^10 \equiv -1 \ (25)$ et $2^4 \equiv 16 \ (25)$. Donc 2 est bien d'ordre 20 dans G_2.

4) Par définition, si p est un entier et q un nombre premier, nous avons

$$(\frac{p}{q}) = \begin{cases} 0 & \text{si } p \text{ est divisible par } q, \\ 1 & \text{si } p \text{ est un résidu quadratique modulo } q, \\ -1 & \text{si } p \text{ est un non résidu quadratique modulo } q, \end{cases}$$

a) En utilisant les propriétés du symbole $(\frac{p}{q})$, nous trouvons

$$(\frac{71}{113}) = (\frac{113}{71}) = (\frac{42}{71}) = (\frac{2}{71})(\frac{3}{71})(\frac{7}{71}) = (+1)(-(\frac{71}{3}))(-(\frac{71}{7})) = -(\frac{-1}{3})(-(\frac{1}{7})) = -1.$$

b) Nous avons

$$(\frac{173}{229}) = (\frac{229}{173}) = (\frac{56}{173}) = (\frac{7}{173})(\frac{8}{173}) = (\frac{173}{7})(\frac{2}{173}) = (\frac{5}{7})(-1) = (\frac{7}{5})(-1) = (\frac{2}{5})(-1) = 1.$$

5) a) Nous trouvons les valeurs suivantes

$$0:0, 1:1, 2:1, 3:2, 4:3, 5:5, 6:8, 7:13, 8:21, 9:34, 10:55, 11:89, 12:144,$$
$$13:233, 14:377, 15:610, 16:987, 17:1597, 18:2584, 19:4181, 20:6765.$$

b) Notons $b_n = 3 \times (8^n - 4^n)$. Nous avons $b_0 = 0 = a_0$ et $b_1 = 3 \times 4 = 1 = a_0$ dans $\mathbf{Z}/11\mathbf{Z}$. Supposons que nous avons montré que $a_p = b_p$ pour $p < n+2$. Alors

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n = b_{n+1} + b_n = 3 \times (8^{n+1} - 4^{n+1} + 8^n - 4^n) \\ &= 3 \times (8^n(8+1) - 4^n \times (4+1)) = 3 \times (8^{n+2} - 4^{n+2}) \\ &= b_{n+2}. \end{aligned}$$

c) D'après la question précédente, nous avons $a_n \equiv 0\ (11)$ si et seulement si $8^n = 4^n$ dans $\mathbf{Z}/11\mathbf{Z}$ ou encore $(8 \times 4^{-1})^n = 1$. Or $4^{-1} = 3$ dans $\mathbf{Z}/11\mathbf{Z}$ et $8 \times 4^{-1} = 2$. Donc $a_n \equiv 0\ (11)$ ssi $2^n \equiv 1\ (11)$. Or l'ordre de 2 dans $(\mathbf{Z}/11\mathbf{Z})^*$ est égal à 10. Donc finalement, $a_n \equiv 0\ (11)$ ssi $n \equiv 0\ (10)$.

d) Si $p \equiv \pm 1\ (5)$, alors p est impair et 2 est inversible dans $\mathbf{Z}/p\mathbf{Z}$. Nous notons $1/2$ son inverse. Nous affirmons en outre que 5 est un carré dans $\mathbf{Z}/p\mathbf{Z}$. En effet, nous avons

$$(\frac{5}{p}) = (\frac{p}{5}) = (\frac{\pm 1}{5}) = 1.$$

Soit $\alpha \in \mathbf{Z}/p\mathbf{Z}$ tel que $\alpha^2 = 5$. Notons que $\alpha \neq -\alpha$ puisque $p \neq 2$.
Nous avons

$$x^2 - x - 1 = (x - 1/2)^2 - 5/4$$

et l'équation $x^2 - x - 1 = 0$ est équivalente à

$$x = 1/2 \pm \alpha/2.$$

Comme $\alpha \neq -\alpha$ les deux solutions $x_1 = 1/2 - \alpha/2$ et $x_2 = 1/2 + \alpha/2$ sont distinctes.

e) En notation matricielle le système devient

$$\begin{bmatrix} 1 & 1 \\ x_1 & x_2 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Le déterminant de la matrice 2×2 à gauche vaut $x_2 - x_1 \neq 0$ et le système admet donc une unique solution donnée par

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \frac{1}{x_2 - x_1} \begin{bmatrix} x_2 & -1 \\ -x_1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\alpha} \begin{bmatrix} -1 \\ 1 \end{bmatrix}.$$

Montrons par récurrence que nous avons

$$a_n \equiv c_1 x_1^n + c_2 x_2^n \quad \text{dans } \mathbf{Z}/p\mathbf{Z}.$$

En effet, pour $n = 0, 1$ cette égalité se réduit à la première resp. à la deuxième équation du système que vérifient c_1, c_2. Pour $n \geq 0$, nous avons

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n = c_1(x_1^{n+1} + x_1^n) + c_2(x_2^{n+1} + x_2^n) \\ &= c_1 x_1^n(x_1 + 1) + c_2 x_2^n(x_2 + 1) = c_1 x_1^{n+2} + c_2 x_2^{n+2} \end{aligned}$$

car x_1, x_2 sont solutions de $x^2 = x + 1$.

f) D'après e), nous avons

$$a_n = \frac{1}{\alpha}(-x_1^n + x_2^n) \quad \text{dans } \mathbf{Z}/p\mathbf{Z}.$$

Donc $a_n = 0$ ssi $x_1^n = x_2^n$, c'est-à-dire que $(x_1/x_2)^n = 1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$. Cette dernière condition est remplie ssi n est multiple de l'ordre de x_1/x_2 dans $(\mathbf{Z}/p\mathbf{Z})^*$. Donc d'après le théorème de Lagrange, nous avons $a_n = 0$ si n est multiple de $p-1$, l'ordre de $(\mathbf{Z}/p\mathbf{Z})^*$.