MT 282
03/09/95

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

Un corrigé de l'examen du 05.09.95

1) Soit x le nombre de candidats. D'après les informations fournies, nous avons

$$\begin{aligned} x &\equiv 3 \ (5) \\ x &\equiv 3 \ (6) \\ x &\equiv 4 \ (7). \end{aligned}$$

Les nombres $5, 6, 7$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $5 \times 6 \times 7 = 210$ 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

$$\mathbf{Z}/210 \xrightarrow{\sim} \mathbf{Z}/5 \oplus \mathbf{Z}/6 \oplus \mathbf{Z}/7.$$

Nous avons

$$\begin{array}{llll} 42\,u_1 + 5\,v_1 = 1; & \text{sol. part.} & 42 \times 3 + 5 \times (-25) = 1. & \text{Posons} \quad x_1 = 126. \\ 35\,u_2 + 6\,v_2 = 1; & \text{sol. part.} & 35 \times (-1) + 6 \times 6 = 1. & \text{Posons} \quad x_2 = -35. \\ 30\,u_3 + 7\,v_3 = 1; & \text{sol. part.} & 30 \times (-3) + 7 \times 13 = 1. & \text{Posons} \quad x_3 = -90. \end{array}$$

Nous avons donc $x \equiv 3 \times 126 + 3 \times (-35) + 4 \times (-90) \equiv -87 \equiv 123 \ (210)$. En conclusion, 123 **candidats participertont à l'épreuve.**

2) Supposons que H est distingué et que $x \in G$. Nous avons $xHx^{-1} = H$, donc $xH = Hx$ et $x' = x$ convient.

Réciproquement, supposons la condition vérifiée. Soit $x \in G$ et soit $x' \in G$ tel que $xH = Hx'$. Alors $x' = ex' = xh$ pour un $h \in H$ car $ex' \in Hx'$. Donc $xH = Hx' = Hxh$. En multipliant cette égalité à droite par h^{-1}, nous trouvons $xH = Hx$, c'est-à-dire que $xHx^{-1} = H$ et que H est bien distingué.

3) a) Nous avons

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

et $r = 0$.

b) Le nombre $p = 47$ est premier. D'après le petit théorème de Fermat, nous avons $x^p \equiv x \ (p)$ pour tout entier x. En particulier $a = 23^p \equiv 23 \ (p)$ et $r = 23$.

c) D'après le théorème d'Euler, nous avons $x^{\varphi(36)} \equiv 1 \ (36)$ pour tout entier x premier à 36. Or, $\varphi(36) = \varphi(4)\varphi(9) = 2 \times 6 = 12$. Donc $17^{13} \equiv 17^1 \ (36)$ et $r = 17$.

d) Nous avons $495 = 5 \times 9 \times 11$ et les nombres $5, 9$ et 11 sont premiers entre eux deux à deux. Ainsi, d'après le théorème chinois (appliqué deux fois), pour connaître le reste de a modulo 495, il suffit de déterminer les restes de a modulo 5, 9 et 11.
Nous avons $191 \equiv 1 \ (5)$ et donc $a \equiv 1 \ (5)$.

Nous avons $191 \equiv 4 \ (11)$. Comme 4 et 11 sont premiers entre eux, le reste de $4^{(141^{128})}$ ne dépend que du reste de 141^{128} modulo 10. Ce dernier vaut 1, car $141 \equiv 1 \ (10)$.

Finalement nous avons $191 \equiv 2 \ (9)$ et comme 2 et 9 sont premiers entre eux, le reste de $2^{(141^{128})}$ modulo 9 ne dépend que du reste de 141^{128} modulo $\varphi(9) = 6$. Nous avons $141 \equiv 3 \ (6)$ et $3^2 \equiv 3 \ (6)$. En appliquant plusieurs fois la seconde congruence, nous trouvons

$$3^{128} = (3^2)^{64} \equiv 3^{64} \equiv (3^2)^{32} \equiv 3^{32} \equiv \ldots \equiv 3 \ (6).$$

Ainsi, $2^{(141^{128})} \equiv 2^3 \equiv -1 \ (9)$.
Nous obtenons ainsi le système de congruences

$$\begin{aligned} a &\equiv 1 \ (5) \\ a &\equiv -1 \ (9) \\ a &\equiv 4 \ (11). \end{aligned}$$

Nous le résolvons par la méthode bien connue (voir le corrigé de l'exercice 1) pour trouver $a \equiv 26 \ (495)$. En conclusion, **le reste de la division de** $191^{(141^{128})}$ **par** 495 **est égal à** 26.

4) Montrons que (i) implique (ii). Si n est premier on sait que le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique. Soit a un entier dont la classe engendre $(\mathbf{Z}/n\mathbf{Z})^*$. Alors a est d'ordre $n-1$ et on a donc $a^{(n-1)} \equiv 1 \ (n)$ et $a^d \not\equiv 1 \ (n)$ pour tout diviseur propre d de $n-1$. En particulier, $a^{(n-1)/q} \not\equiv 1 \ (n)$ pour tout facteur premier q de $n-1$.

Montrons que (ii) implique (i). Si on a $a^{n-1} \equiv 1 \ (n)$, alors a est clairement inversible dans $\mathbf{Z}/n\mathbf{Z}$ (d'inverse a^{n-2}). L'ordre de a dans le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ divise $(n-1)$ et ne divise pas $(n-1)/q$, pour tout facteur premier q de $n-1$. Donc l'ordre est égal à $n-1$ et le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ a $n-1$ éléments (au moins). Les classes de $1, \ldots, n-1$ appartiennent donc à $(\mathbf{Z}/n\mathbf{Z})^*$ ce qui montre que tout entier positif inférieur à n est premier à n. Donc n est bien premier.

5) a) Le nombre 5 admet la décomposition en facteurs premiers $5 = (1+2i)(1-2i)$ dans $\mathbf{Z}[i]$. Donc $5^n = (1+2i)^n(1-2i)^n$ est une décomposition en facteurs premiers dans $\mathbf{Z}[i]$. Nous avons $(x+iy)(x-iy) = (1+2i)^n(1-2i)^n$. D'après l'unicité de la décomposition en facteurs premiers dans $\mathbf{Z}[i]$, **la décomposition en facteurs premiers de $(x+iy)$ doit être de la forme**

$$x + iy = u(1+2i)^a(1-2i)^b$$

où u est une unité de $\mathbf{Z}[i]$ et a, b sont des entiers positifs tels que $a+b=n$ (car la norme de $x+iy$ est de $5^n = N(1+2i)^a N(1-2i)^b = 5^a \times 5^b$).

b) D'après a), si (x,y) est une solution, alors $x+iy = u(1+2i)^a(1-2i)^{n-a}$, où $u \in \{1,-1,i,-i\}$ et $0 \leq a \leq n$. Il y a donc au plus $4(n+1)$ solutions.

6) a) Les classes de 1 et de -1 sont des solutions évidentes de $x^2 = 1$ dans $\mathbf{Z}/p^m\mathbf{Z}$. Il n'y a pas d'autres solutions. En effet, comme p est impair, le groupe $(\mathbf{Z}/p^m\mathbf{Z})^*$ est cyclique d'ordre pair. Il contient donc exactement deux éléments qui vérifient $x^2 = 1$. En conclusion, **les solutions ont les nombres $\pm 1 + k \times p^m$, $k \in \mathbf{Z}$.**

b) Ecrivons $n = q_1 q_2 \ldots q_r$ où les q_i sont des puissances strictement positives de nombres premiers distincts d eux à deux. D'après le lemme chinois, la projection canonique p est un isomorphisme d'anneaux

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} (\mathbf{Z}/q_1\mathbf{Z}) \times (\mathbf{Z}/q_2\mathbf{Z}) \times \ldots \times (\mathbf{Z}/q_r\mathbf{Z}).$$

Si on note $p(x) = (x_1, \ldots, x_r)$, l'équation $x^2 = 1$ se traduit par

$$(x_1, \ldots, x_r)^2 = (1, \ldots, 1)$$

c'est-à-dire par les équations $x_i^2 = 1$ dans $\mathbf{Z}/q_i\mathbf{Z}$, $i = 1, \ldots, r$. Comme n est impair, les q_i le sont aussi, et d'après a), chaque équation $x_i^2 = 1$ admet exactement 2 solutions. Ainsi, l'équation $(x_1, \ldots, x_r)^2 = (1, \ldots, 1)$ admet 2^r solutions. En conclusion, **le nombre de solutions modulo n de l'équation $x^2 = 1$ est de 2^r, où r est le nombre de facteurs premiers distincts de n. Il y a exactement 2 solutions si et seulement si n est puissance d'un nombre premier (impair).**

c) Ecrivons $n = 2^m u$ où u est impair. D'après le lemme chinois, la projection p est un isomorphisme d'anneaux

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} (\mathbf{Z}/u\mathbf{Z}) \times (\mathbf{Z}/2^m\mathbf{Z}).$$

Si l'on note $p(x) = (x_1, x_2)$, l'équation $x^2 = 1$ dans $\mathbf{Z}/n\mathbf{Z}$ se traduit par les équations $x_1^2 = 1$ dans $\mathbf{Z}/u\mathbf{Z}$ et $x_2^2 = 1$ dans $\mathbf{Z}/2^m\mathbf{Z}$. D'après b), nous connaissons le nombre de solutions de $x_1^2 = 1$ dans $\mathbf{Z}/u\mathbf{Z}$. Nous savons que $(\mathbf{Z}/2^m\mathbf{Z})^*$ est isomorphe à $\{1\}$ si $m \leq 1$; à $\mathbf{Z}/2\mathbf{Z}$ si $m = 2$; à $\mathbf{Z}/2 \times \mathbf{Z}/2^{(m-2)}\mathbf{Z}$ si $m \geq 3$. Léquation $x_2 = 1$ admet donc 1, resp. 2, resp. 4 solutions si $m \leq 1$, resp. $m = 2$, resp. $m \geq 3$. En conclusion, **si 2^m est la puissance maximale de 2 qui divise n et que r est le nombre de facteurs premiers impairs de n, le nombre de racines modulo n de l'équation $x^2 = 1$ est de 2^r si $m \leq 1$, de 2^{r+1} si $m = 2$, et de 2^{r+2} si $m \geq 3$.**