Corrigé de l'EXAMEN du 1er février 2000

Exercice 1

Notons a et b les nombres de voix obtenus par les candidats A et B respectivement. Les hypothèses de l'énoncé se traduisent par l'égalité $a+b=901$ et les congruences $a \equiv 9 \pmod{13}$ et $b \equiv 2 \pmod{64}$. On a donc le système de congruences $a \equiv 9 \pmod{13}$ et $901-a \equiv 2 \pmod{64}$. Ce système équivaut à $a \equiv 9 \pmod{13}$ et $a \equiv 3 \pmod{64}$. Comme 13 et 64 sont premiers entre eux (on a $13.5-64=1$), on peut appliquer le lemme chinois pour obtenir la congruence $a \equiv 451 \pmod{832}$ qui est équivalente au système. Il existe donc $k \in \mathbf{Z}$ tel que $a = 832k + 451$. Comme on a $0 \leq a \leq 901$, on a $k = 0$. On a donc $a = 451$ et $b = 901 - a = 450$.

Exercice 2

Les nombres 2001 et 2002 ne sont pas premiers puisque $3|2001$ et $2|2002$. L'entier 2003 est premier. Pour le prouver, il suffit de vérifier qu'il n'est divisible par aucun nombre premier < 47 car $47^2 = 2209 > 2003$. On a $2 \not| 2003$, $3 \not| 2003$, $5 \not| 2003$ et $11 \not| 2003$ en raison des critères de divisibilité donnés en cours. De plus les calculs de division euclidienne donnent $2003 = 286.7 + 1 = 154.13 + 1 = 117.17 + 14 = 105.19 + 8 = 87.23 + 2 = 69.29 + 2 = 64.31 + 19 = 54.37 + 5 = 48.41 + 35 = 43.46 + 25$.

Exercice 3

1. L'ensemble G est non vide. En effet $\bar{1} \in G$. Soient $x, y \in \mathbf{Z}$ congrus à 1 modulo 5 et inversibles modulo 100. On a $xy \equiv 1.1 \equiv 1 \pmod{5}$. L'ensemble G est donc stable par multiplication. Soit x' un représentant dans $\mathbf{Z}$ de l'inverse de x modulo 100. On a $x'x \equiv 1 \pmod{100}$ et donc $xx' \equiv 1 \pmod{5}$. Comme $x \equiv 1 \pmod{5}$, on a $x' \equiv 1 \pmod{5}$. On a donc $\bar{x}' \in G$. L'ensemble G est donc stable par passage à l'inverse.
2. L'ordre $(\mathbf{Z}/100\mathbf{Z})^*$ est égal à $\phi(100) = \phi(5^2)\phi(2^2) = (25-5)(4-2) = 40$.
3. Remarquons qu'un entier est inversible modulo 100 si et seulement si il est inversible modulo $4 = 2^2$ et modulo $25 = 5^2$, c'est-à-dire si et seulement si il n'est divisible ni par 2 ni par 5 ou encore si et seulement si le dernier chiffre de son écriture décimale n'est divisible ni par 2 ni par 5 ; cela revient à dire que le dernier chiffre de l'écriture décimale est 1, 3, 7 ou 9. Par ailleurs un entier est congru à 1 modulo 5 si et seulement si le dernier chiffre de son écriture décimale est 1 ou 6. Les éléments de G sont donc les classes modulo 100 des entiers dont le dernier chiffre est 1 en écriture décimale. Ils sont donc congrus à 1 modulo 10. Cela permet de donner la liste des éléments de G : $G = \{\bar{1}, \bar{11}, \bar{21}, \bar{31}, \bar{41}, \bar{51}, \bar{61}, \bar{71}, \bar{81}, \bar{91}\}$. Il y a donc 10 éléments dans G.
4. Le groupe G possède des éléments d'ordre 10 : c'est par exemple le cas de $\bar{11}$. En effet, les diviseurs maximaux de 10 sont 2 et 5, comme $\bar{11}^2 = \bar{21} \neq \bar{1}$ et $\bar{11}^5 = \bar{21}^2.\bar{11} = \bar{41}.\bar{11} = \bar{51} \neq \bar{1}$, $\bar{11}$ est bien d'ordre 10. Le groupe G est donc cyclique engendré par $\bar{11}$.

L'élément $\bar{51}$ est d'ordre 2 puisque $51^2 \equiv 2601 \equiv 1 \pmod{100}$. L'élément $\bar{21}$ est d'ordre 5 puisque $\bar{21}^5 = (\bar{11}^2)^5 = \bar{11}^{10} = \bar{1}$.

Problème

1. Comme $(K,+)$ est un groupe d'ordre 8, l'ordre de 1_K pour l'addition divise 8. On a donc $8_K = 1_K + 1_K + 1_K + 1_K + 1_K + 1_K + 1_K + 1_K = 0$.
2. On a $8_K = 1_K+1_K+1_K+1_K+1_K+1_K+1_K+1_K = (1_K+1_K).(1_K+1_K+1_K+1_K) = (1_K+1_K).(1_K+1_K).(1_K+1_K) = 2_K^3$.

Comme K est un corps, tout élément $\neq 0_K$ de K est inversible pour la multiplication. Supposons que $2_K \neq 0_K$. Notons x l'inverse de 2_K dans K. On a (en utilisant l'égalité $2_K.x = x.2_K$, due à la commutativité de K) $0_K = 0_K.x^2 = 8_K.x^2 = 2_K^3.x^2 = 2_K.(2_K.x).(2_K.x) = 2_K.1_K.1_K = 2_K$. C'est absurde ; on a donc $2_K = 0_K$.

On a $0_K = 0_K.x = 2_K.x = (1_K + 1_K).x = 1_K.x + 1_K.x = x + x$.
3. On a, en utilisant que K est commutatif, (*i.e.* $x.y = y.x$), $\phi_2(x+y) = (x+y)^2 = (x+y)(x+y) = x^2 + x.y+y.x+y^2 = x^2+2_K.x.y+y^2 = x^2+y^2 = \phi_2(x)+\phi_2(y)$, $\phi_2(x.y) = (x.y)^2 = x.y.x.y = x^2.y^2 = \phi_2(x).\phi_2(y)$ et $\phi_2(1_K) = 1_K^2 = 1_K$ (x, $y \in K$). On a bien un homomorphisme d'anneaux. (NB : En fait ϕ_2 est même un isomorphisme d'anneaux.)
4. Démontrons que K_ϕ est un sous-groupe de $(K,+)$. Soient x, $y \in K_\phi$. On a $\phi(0_K) = 0_K$, car ϕ est un homomorphisme d'anneaux et donc $0_K \in K_\phi$. On a $\phi(x+y) = \phi(x) + \phi(y) = x + y$ et donc $x+y \in K_\phi$. De plus on $\phi(-x) + x = \phi(-x) + \phi(x) = \phi(-x+x) = \phi(0_K) = 0_K$ et donc $\phi(-x) = -x \in K_\phi$. Cela prouve que K_ϕ est un sous-groupe de $(K,+)$.

Vérifions que K_ϕ est stable par multiplication. On a $\phi(x.y) = \phi(x).\phi(y) = x.y$ et donc $x.y \in K_\phi$. De plus on a $\phi(1_K) = 1_K$, car ϕ est un homomorphisme d'anneaux, et donc $1_K \in K_\phi$. C'est pourquoi K_ϕ est un sous-anneau de K.

Appliquons cela au cas où $\phi = \phi_2$. On a $K_{\phi_2} = \{x \in K / x^2 = x\}$.
5. Comme K est un corps, un polynôme de degré 2 a au plus 2 racines dans K. Or 0_K et 1_K sont des racines du polynôme $X^2 - X$, qui a donc deux racines dans K.

Par conséquent on a $\{x \in K / x^2 = x\} = \{0_K, 1_K\} = K_0$. C'est un sous-corps de K car $K_{\phi_2} = K_0$ est un anneau d'après la question 4. et 1_K, qui est le seul élément inversible de K_0, est son propre inverse dans K_0.
6. On a $K^* = K - \{0_K\}$, car K est un corps. Comme K possède 8 éléments, K^* possède 7 éléments.

D'après le théorème de Lagrange, tout élément x de K^* est d'ordre divisant 7 et vérifie donc $x^7 = 1_K$.

Tout élément y de K vérifie donc $y = 0_K$ ou $y^7 = 1_K$ ce qui implique dans tous les cas $y^8 = y$.

Soit x_0 un élément de K^* distinct de 1_K. L'ordre de x_0 divise 7 mais est différent de 1. C'est donc 7, puisque 7 est premier. C'est pourquoi K^* est un groupe cyclique engendré par x_0.
7. Le groupe $(K_1,+)$ est un sous-groupe de $(K,+)$. Son ordre divise donc l'ordre de K qui est 8. Comme un corps contient au moins 2 éléments, K_1 possède 2, 4 ou 8 éléments.

Le groupe $(K_1^*,.)$ est un sous-groupe de $(K^*,.)$, son ordre divise donc 7.

Notons n le nombre d'éléments de K_1. On a donc $n-1|7$, c'est-à-dire $n = 2$ ou $n = 8$. Dans le deuxième cas on a $K_1 = K$. Si $n = 2$, le corps K_1 contient les éléments 0_K et K_1 de K ; on a alors $K_1 = K_0$.