UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2007-2008, Licence 2, MI4
Groupes et arithmétique

Examen du 13/05/08 : corrigé

I

Il s'agit de résoudre le système de congruence ($1000 \leq x \leq 3000$) :

$$\begin{cases} x & \equiv & 0 & (\text{mod } 11) \\ x & \equiv & 5 & (\text{mod } 9) \\ x & \equiv & 8 & (\text{mod } 13) \end{cases}$$

Le théorème des restes chinois résout un système de deux congruences modulo des entiers a et b premiers entre eux. Si on a une relation de Bezout : $ua + vb = 1$, alors on a l'équivalence :

$$\begin{cases} x & \equiv & \alpha & (\text{mod } a) \\ x & \equiv & \beta & (\text{mod } b) \end{cases} \Leftrightarrow x \equiv \alpha vb + \beta ua \pmod{ab}$$

On applique d'abord aux deux premières congruences : $-4 \times 11 + 9 \times 5 = 1$ (11 et 9 sont premiers entre eux) ; on a : $5 \times 11 \times (-4) + 0 \times 9 \times 5 = -220 \equiv 77 \pmod{99}$. Le système étudié est équivalent à :

$$\begin{cases} x & \equiv & 77 & (\text{mod } 99) \\ x & \equiv & 8 & (\text{mod } 13) \end{cases}$$

On applique une seconde fois le théorème : $5 \times 99 - 38 \times 13 = 1$ (99 et 13 sont premiers entre eux) ; on a : $77 \times 13 \times (-38) + 8 \times 99 \times 5 = -34078 \equiv 671 \pmod{1287}$. Le système étudié est équivalent à :

$$x \equiv 671 \pmod{1287}$$

On a donc $x = 671 + 1287k$ avec k entier. Compte tenu de l'encadrement, seul $k = 1$ convient. L'effectif de l'armée est **1958**.

II

1. Pour montrer qu'un nombre n est premier, il suffit de tester la divisibilité par tous les nombres premiers de carré inférieur à n.
   Application : 787 n'est divisible par aucun des nombres : 2, 3, 5, 7, 11, 13, 17, 19, 23 ; et $29^2 > 787$. Le nombre 787 est donc premier.

2. $238 = 2 \times 7 \times 17$; $\left(\frac{238}{787}\right) = \left(\frac{2}{787}\right) \times \left(\frac{13}{787}\right) \times \left(\frac{17}{787}\right)$.
   On a : $787 \equiv 3 \pmod 8$, donc $\left(\frac{2}{787}\right) = -1$.
   On utilise la loi de réciprocité quadratique : $787 \equiv 3 \pmod 4$, $7 \equiv 3 \pmod 4$ et $17 \equiv 1 \pmod 4$. Donc :
   $\left(\frac{7}{787}\right) = -\left(\frac{787}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{7}{3}\right) = 1$, et
   $\left(\frac{17}{787}\right) = \left(\frac{5}{17}\right) = \left(\frac{2}{5}\right) = -1$.
   Finalement : $\left(\frac{238}{787}\right) = 1$
3. Comme 787 est premier, le symbole de Legendre égal à 1 indique que 238 est un carré modulo 787 ?

III

1. Soit $p = 8k + 7$ un nombre premier.
   (a) $p \equiv -1 \bmod 8$, dons $\left(\frac{2}{p}\right) = 1$
   (b) $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv 1 \bmod p$. Donc $2^{4k+3} - 1$ est divisible par p.
2. (a) 263 n'est pas divisible par 2, 3, 5, 7, 11, 13 ; et $17^2 > 263$; 263 est donc premier.
   (b) $131 = 4k + 3$, avec $k = 32$; $p = 8k + 7 = 263$ est premier. La question 1b montre que $M_{131} = 2^{131} - 1$ est divisible par 263.

IV

1. a) montre que $\overline{b}$ est inversible modulo N et que son ordre dans le groupe des inversibles de $\mathbb{Z}/N\mathbb{Z}$ divise $N-1$. D'après b), cet ordre n'est aucun des diviseurs de $N - 1$ différent de $N - 1$, il est donc égal à $N - 1$.
2. On démontre que l'hypothèse c) entraîne l'hypothèse b).
   Supposons que c) est vrai. Soit δ un diviseur de $N-1$ qui n'est pas égal à $N-1$. Il a au moins un facteur premier en moins par rapport à ceux de $N - 1$. Il a donc un multiple de la forme $d = \frac{N}{q}$ avec q premier. On a $b^d \not\equiv 1 \bmod N$, donc $\delta^d \not\equiv 1 \bmod N$.
3. $8460 = 2^2 \cdot 3^2 \cdot 5 \cdot 47$
4. On calcule 23^d modulo 8461 pour les valeurs de d : $\frac{8460}{2} = 4230$, $\frac{8460}{3} = 2820$, $\frac{8460}{5} = 1692$ et $\frac{8460}{47} = 180$.
   On obtient successivement : $8460 \equiv -1$, 6684, 3405 et 3773. (Calcul *rapide* des puissances, cf feuille de calcul pour tableur ; on peut évidemment compléter le même tableau avec une calculatrice.)
   Le nombre 8461 est premier.
5. Le nombre 8461 étant premier, le groupe des inversibles de $\mathbb{Z}/8461\mathbb{Z}$ est un groupe à 8460 éléments et cyclique. Il est isomorphe au groupe additif $\mathbb{Z}/8460\mathbb{Z}$; le nombre de ses générateurs est donné par l'indicateur d'Euler :

$$\phi(8460) = \phi(2^2)\phi(3^2)\phi(5)\phi(47) = 2 \cdot (9-3) \cdot 4 \cdot 46 = 2208 \ .$$