UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2008-2009, Licence 2, MI4
Groupes et arithmétique

Examen du 02/06/08 : corrigé succint

I

On applique l'algorithme d'Euclide :

$$PGCD(17640, 525) = 115 \ .$$

En remontant l'algorithme d'Euclide, on obtient :

$$2 \times 1760 - 67 \times 525 = 105 \ .$$

II

a) 13 et 15 sont premiers entre eux. Le théorème des restes chinois montre que la solution est une classe de congruence modulo $13 \times 15 = 195$. En observant que -10 est solution, on obtient :

$$x = -10 + 195k, \ k \in \mathbb{Z} \ .$$

(La relation de Bezout permet aussi de calculer une solution.)

b)

$$x = -10 + 3315k, \ k \in \mathbb{Z} \ .$$

III

1. 983 n'a pas de diviseur premier inférieur à 31 et $32^2 = 1024 > 983$.
2. $$\begin{array}{rcl} \left(\frac{610}{983}\right) & = & \left(\frac{2}{983}\right)\left(\frac{305}{983}\right) \\ & = & 1 \times \left(\frac{983}{305}\right) = \left(\frac{68}{305}\right) \\ & = & \left(\frac{2^2 \times 17}{305}\right) = \left(\frac{17}{305}\right) \\ & = & \left(\frac{305}{17}\right) \\ & = & \left(\frac{4^2}{17}\right) = 1 \end{array}$$
3. 610 est un carré modulo 983.
4. $610^{491} = 610^{\frac{983-1}{2}}$ est congru à $\left(\frac{610}{983}\right) = 1$ modulo 983.
5. Modulo 983, $(610^{246})^2 = 610^{491+1} = 610^{491} \times 610$ est congru à 610 modulo 983. L'équation $x^2 = 610$ a deux solutions opposées dans $\mathbb{Z}/983\mathbb{Z}$, l'une d'elle est 610^{246}. Donc : x^2 est congru à 610 modulo 983 si et seulement si x est congru à $\pm 610^{246}$ modulo 983.

6. $246 = 2^7 + 2^6 + 2^5 + 2^4 + 2^2 + 2$. On calcule les carrés successifs modulo 983 :
   $610^2 \equiv 526$ modulo 983,
   $610^{2^2} \equiv 453$ modulo 983,
   $610^{2^3} \equiv 745$ modulo 983,
   $610^{2^4} \equiv 613$ modulo 983,
   $610^{2^5} \equiv 263$ modulo 983,
   $610^{2^6} \equiv 359$ modulo 983,
   $610^{2^7} \equiv 108$ modulo 983,
   $610^{246} \equiv 526 \times 453 \times 613 \times 263 \times 359 \times 108 \equiv 278$ modulo 983.

IV

1. (a) $M_p \equiv 0$ modulo q, donc $2^p \equiv 1$ modulo q.
   (b) L'ordre de $\overline{2}$ dans le groupe multiplicatif $\mathcal{U}(\mathbb{Z}/q\mathbb{Z})$ divise p qui est premier : c'est p.
   (c) Par le théorème de Fermat : $2^{q-1} \equiv 1$ modulo q, donc p divise $q - 1$.
2. Les éventuels diviseurs premiers de $M_{11} = 2047$ sont de la forme $11k + 1$. On obtient 23 comme diviseur ; $M_{11} = 2047$ n'est pas premier.