

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

Examen du 25/06/09 (corrigé succinct)

I

1. 12 est premier avec 25, donc est inversible dans $\mathbb{Z}/25\mathbb{Z}$. On a une relation de Bezout : $-2 \times 12 + 25 = 1$. L'inverse de 12 modulo 25 est -2 (ou 23).
2. $12x \equiv 7$ modulo 25 équivaut à $x \equiv -14$, i.e. $x \equiv 11$ modulo 25 .
3. Le système équivaut à :

$$\begin{cases} x & \equiv 11 \text{ modulo } 25 \\ x & \equiv 2 \text{ modulo } 21 \end{cases}$$

21 et 25 sont premiers entre eux, donc il y a une solution unique modulo 525. L'algorithme d'Euclide permet d'obtenir : $6 \times 21 - 5 \times 25 = 1$. On déduit que : $6 \times 21 \times 11 - 5 \times 25 \times 2 = 1136 \equiv 86$ modulo 525 est solution. La solution est : $86 + 525k$, $k \in \mathbb{Z}$.

II

1. $\mathcal{U}(\mathbb{Z}/20\mathbb{Z}) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ (éléments premiers avec 20).
2. Le groupe $\mathcal{U}(\mathbb{Z}/20\mathbb{Z})$ est isomorphe à $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/5\mathbb{Z})$. On en déduit que pour tout x dans $\mathcal{U}(\mathbb{Z}/20\mathbb{Z})$, $x^4 = \bar{1}$. Il n'y a pas d'élément d'ordre 8 : le groupe n'est pas cyclique.
3. $383^{127} \equiv 3^{127} \equiv 3^3 \equiv 7$ modulo 20.

III

1. $6601 = 7 \times 23 \times 41$.
2. 6601 est un nombre de Carmichael, car pour tout diviseur premier p de 6601, p^2 ne divise pas 6601 et $p - 1$ divise $6601 - 1$: 6600 est divisible par 40, 22 et 6.
3. $N_k - 1 = 36k(36k^2 + 11k + 1)$ est divisible par $36k$. Si les trois nombres a_k , b_k et c_k sont premiers, alors N_k est un nombre sans facteur carré. De plus $N_k - 1$ est divisible par $36k$, donc par $a_k - 1 = 6k$, $b_k - 1 = 12k$ et $c_k - 1 = 18k$. Donc N_k est un nombre de Carmichael.
4. $a_6 = 37$, $b_6 = 73$ et $c_6 = 109$ sont des nombres premiers, donc N_6 est un nombre de Carmichael.

IV

1. $F_2 = 17$ et $F_3 = 257$ sont premiers.
2. $\left(\frac{F_1}{3}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\left(\frac{F_2}{3}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$ pour $n \geq 1$.
3. On applique la loi de réciprocité quadratique ; ici $F_n \equiv 1$ modulo 4.

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1 .$$

4. Si F_n , $n \geq 1$, est premier alors $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right)$ est égal à -1 modulo F_n .
5. $F_4 = 65537$. On calcule $3^{2^{4-1}}$ modulo F_4 par élévation au carré successive. Le résultat est : $65536 \equiv -1$ modulo F_4 .
6. L'ordre de 3 dans la groupe $\mathcal{U}(\mathbb{Z}/F_4\mathbb{Z})$ divise $F_4 - 1 = 2^{2^4}$. C'est donc une puissance de 2 : 2^ν avec $\nu \leq 16$. Le calcul précédent montre que $\nu > 15$. 3 est donc d'ordre $2^{16} = 65536 = F_4 - 1$; on déduit que $\mathbb{Z}/F_4\mathbb{Z}$ est un corps, et que F_4 est premier.
7. $F_5 = 4294967297$ n'est pas premier : $3^{\frac{F_5-1}{2}} \equiv 10324303$ n'est pas congru à -1 modulo F_5 .