Examen - session 2

ARITHMÉTIQUE

Éléments de correction

Exercice 1.

1) Il est congru à 1 : c'est le petit théorème de Fermat.

2) D'après le 1., pour simplifier le nombre modulo 7, trouvons à quoi est congru 1335 modulo $7-1=6$. Bien sûr, le reste de la division de 1335 par 6 est 3. Donc $3^{1335} \equiv 3^3$ [7]. En effet: $1335 = 6q+3$ donc $3^{1335} \equiv (3^6)^q.3^3 \equiv 1^q.3^3 \equiv 3^3$ [7].

Ainsi $3^{1335} \equiv 27 \equiv 6$ [7]. Donc le reste de la division euclidienne de 3^{1335} par 7 est 6.

Exercice 2.

On utilise les techniques du T.D.: on trouve que ce sont tous les entiers k de la forme: $k = -22 + 180\lambda$ où $\lambda \in \mathbb{Z}$, ou encore tous les entiers k de la forme: $k = 158 + 180m$ où $m \in \mathbb{Z}$.

Exercice 3.

1) Posons $N = 2^q + 1$. Supposons qu'un entier impair $m > 1$ divise q. Alors, on peut écrire: $q = rm$ où $1 \leq r < q$

$$N = (2^r)^m - (-1)^m = \Big(2^r - (-1)\Big)\Big(\sum_{j=0}^{m-1} (2^r)^j.(-1)^{m-1-j}\Big).$$

En particulier $2^r + 1$ divise N, qui est supposé être premier. Or $1 < 2^r + 1 < N$. On a une contradiction.

On en déduit que q n'est divisible par aucun nombre impair donc c'est une puissance de 2.

2) On fait une preuve par récurrence sur $n \geq 1$. Ainsi l'hypothèse $\mathcal{H}_n$ est: $F_n = 2 + \prod_{j=0}^{n-1} F_j$.

$F_1 = 5 = 2 + 3 = 2 + F_0$. donc $\mathcal{H}_1$ est vraie.

Supposons que $\mathcal{H}_n$ soit vraie où $n \geq 1$. On a

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 = (2^{2^n}+1)(2^{2^n}-1) = F_n(F_n - 2).$$

Comme $\mathcal{H}_n$ soit vraie, on a $F_n - 2 = \prod_{j=0}^{n-1} F_j$ donc on obtient

$$F_{n+1} - 2 = \prod_{j=0}^{n} F_j$$

i.e. $\mathcal{H}_{n+1}$ est vraie.

Par récurrence, $\mathcal{H}_n$ est vraie pour tout $n \geq 1$.

3) Ainsi, si $n > m \geq 0$ (donc $n \geq 1$), on a la relation $F_n = 2 + F_m.Q$ avec $Q = \prod_{\substack{0 \leq j < n \\ j \neq m}} F_j$.

Supposons qu'un entier $p \geq 2$ divise F_n et F_m alors p divise 2 mais F_n et F_m sont impairs donc c'est impossible. Ainsi le seul diviseur commun est 1.

4) S'il y avait un nombre fini de nombres premiers: $p_1 < \cdots < p_s$, alors $F_0, \ldots, F_s$ ne peuvent être premiers entre eux deux à deux. En effet, pour tout $0 \leq j \leq s$, il existe i_j dans $\{1, \cdots, s\}$ tel que p_{i_j} divise F_j. D'après 3., ces entiers i_j doivent être distincts, ce qui est impossible: il y en aurait $s + 1$, compris entre 1 et s.