TD 4 – Congruences (suite)

Énoncés

Exercice 1 – Pour tout $m \geq 0$, soit $F_m = 2^{2^m} + 1$ (le nombre de Fermat). Montrer que $\text{pgcd}(F_m, F_n) = 1$ si $m \neq n$. En déduire qu'il y a au moins $\log_2(\log_2(x))$ nombres premiers compris entre 1 et $x > 2$.

Exercice 2 – Soient $a, b \in \mathbf{Z}$. Montrer :

1. si $2 \nmid a$ et $5 \nmid a$, alors on a $a^{100} \equiv 1 \pmod{1000}$.
2. $b^{100} \equiv 0, 1, 376, 625 \pmod{1000}$.

Exercice 3 – Soit $a \in \mathbf{Z}$.

1. Déterminer les valeurs possibles de $a^{12} \pmod 7$, $a^{12} \pmod{13}$ et $a^{12} \pmod{91}$.
2. Idem pour a^6 à la place de a^{12}.
3. Montrer : si $n \geq 1$ est un entier tel que $n \equiv 1 \pmod{12}$, alors on a $a^n \equiv a \pmod{91}$.

Exercice 4 –

1. Calculer $\varphi(64), \varphi(125), \varphi(100), \varphi(108)$.
2. Montrer que $\varphi(2n)/\varphi(n)$ est égal à 1 (resp. à 2) si $n \geq 1$ est impair (resp. si n est pair). Que se passe-t-il si l'on remplace $2n$ par $3n$ (resp. par $6n$) ?
3. Montrer que $\varphi(n) = \frac{n}{2}$ si et seulement si $n = 2^k$, avec $k \geq 1$.
4. Trouver toutes les valeurs de n telles que $\varphi(n) = 4$.
5. Trouver l'exposant minimum m tel que $a^m \equiv 1 \pmod{77}$ pour tout a premier avec 77.
6. Idem en remplacant 77 par 385.

Exercice 5 – Soit $a \in \mathbf{Z}$.

1. Si $17 \nmid a$, alors il est équivalent: $a \pmod{17}$ est un générateur de $(\mathbf{Z}/17\mathbf{Z})^*$ (une racine primitive $\pmod{17}$) $\iff a^8 \neq 1 \pmod{17}$. Trouver un tel générateur.

2. Si $3 \nmid a$, alors il est équivalent: $a \pmod{27}$ est un générateur de $(\mathbf{Z}/27\mathbf{Z})^*$ (une racine primitive $\pmod{27}$) $\iff a^6, a^9 \neq 1 \pmod{27}$. Trouver un tel générateur.

Exercice 6 – Etude de l'équation $x^2 \equiv 1 \pmod{n}$ ($\iff n \mid (x-1)(x+1)$).

1. Montrer que si $n = p$ (premier), les solutions sont $\pm 1 \pmod{n}$.

2. Montrer que si $n = p^r$ ($p > 2$ premier), les solutions sont $\pm 1 \pmod{n}$.

3. Combien y a-t-il de solutions quand $n = 91$? Expliciter les solutions.

4. Combien y a-t-il de solutions quand $n = 105$?

5. Montrer que si $n = 2^r$ ($r > 2$), les solutions sont $\pm 1, \pm(1 + n/2) \pmod{n}$.

Exercice 7 – Etude de l'équation $x^2 \equiv x \pmod{n}$ ($\iff n \mid x(x-1)$).

1. Montrer que si $n = p^r$ (p premier), les solutions sont $x \equiv 0, 1 \pmod{n}$.

2. Combien y a-t-il de solutions quand $n = 10$? Trouver les solutions.

3. Idem avec $n = 100$ et $n = 1000$.

4. Combien y a-t-il de solutions quand $n = 840$?

Exercice 8 – Afin de communiquer en utilisant le protocole RSA, Alice choisit la clé publique $(e, n) = (37, 65)$.

1. Déterminer la clé secrète d d'Alice.

2. Bob transmet le cryptogramme 3. Quel est le message initial?

3. Idem pour $n = 77$.

Exercice 9 – On a

$$1/7 = 0,142857\ldots \quad 2/7 = 0,285714\ldots \quad 3/7 = 0,428571\ldots$$

$$4/7 = 0,571428\ldots \quad 5/7 = 0,714285\ldots \quad 6/7 = 0,857142\ldots$$

Que se passe-t-il et pourquoi?