Licence première année 2011-2012

M1MI2016 Codes et Cryptologie : feuille d'exercices 6

– Exercice 1.

1. Trouver l'entier x modulo 72 tel que $x = 1 \bmod 8$ et $x = 2 \bmod 9$.
2. Trouver l'entier x modulo $210 = 2 \times 3 \times 5 \times 7$ tel que

$$x = 1 \bmod 2$$
$$x = 2 \bmod 3$$
$$x = 3 \bmod 5$$
$$x = 4 \bmod 7$$

– Exercice 2. On cherche tous les $x \in \mathbb{Z}/143\mathbb{Z}$ tels que $x^2 = 114 \bmod 143$.

1. Remarquer que $143 = 11 \times 13$ et trouver les valeurs possibles de x^2 modulo 11 et modulo 13.
2. En déduire les valeurs possibles de x modulo 11 et modulo 13.
3. En déduire les valeurs possibles de x modulo 143.

– Exercice 3.

1. Montrer que si $x^a = 1 \bmod n$ et $x^b = 1 \bmod n$ alors $x^{\mathrm{pgcd}(a,b)} = 1 \bmod n$.
2. Si p et q sont premiers entre eux, et si $x^a = 1 \bmod p$ et $x^b = 1 \bmod q$ montrer que $x^{\mathrm{ppcm}(a,b)} = 1 \bmod (pq)$.
3. Montrer que pour tout x premier avec 63, on a

$$x^6 = 1 \bmod 63.$$

– Exercice 4. Les entiers 25 et 76 ont la propriété d'être un nombre x tel que x^2 en écriture décimale se termine par x. Utiliser le théorème chinois pour trouver les entiers à 3 chiffres avec cette propriété, puis les entiers à 4 chiffres. Montrer qu'il n'y a jamais plus de 2 entiers à n chiffres avec cette propriété.

– Exercice 5. Utiliser le théorème chinois pour montrer que si f est une fonction polynomiale à coefficients entiers telle que pour tout entier n, $f(n)$ est soit multiple de 2, soit multiple de 3, alors $f(n)$ est :
– *toujours* multiple de 2,

– ou bien *toujours* multiple de 3.

– EXERCICE 6. Utiliser le théorème chinois pour trouver trois entiers *consécutifs* $n, n+1, n+2$, tels que le premier soit divisible par 9, le deuxième par 16, et le troisième par 25. Montrer plus généralement qu'il existe k entiers consécutifs tels que chacun est divisible par un carré parfait.

– EXERCICE 7. Calculer les valeurs de $\phi(n)$ pour $1 \leq n \leq 20$.

– EXERCICE 8. On a calculé les congruences modulo $5, 7, 8, 9$ et 11 d'un entier x compris entre 1 et 250. Il a été trouvé, nous dit-on :
– $x = 4 \bmod 5$
– $x = 5 \bmod 7$
– $x = 3 \bmod 8$
– $x = 4 \bmod 9$
– $x = 7 \bmod 11$.
Cependant, une erreur de calcul ou de copie s'est introduite, et un de ces résultats est faux. Retrouvez x quand même, et corrigez l'erreur.