M1MI2016 Codes et Cryptologie

DS n° 1.

19 Mars 2013, durée 1h20

Documents interdits, calculatrices autorisées

1 Alice doit communiquer à Bob confidentiellement une date de l'année 2013. Pour cela ils décident ensemble du système cryptographique suivant : les jours de l'année 2013 sont numérotés de 0 à 364 puis ils choisissent deux entiers a et b. Le chiffrement de la date x sera $(ax + b) \bmod 365$.

1. Si $a = 57$ et $b = 44$, et si Bob reçoit 249, quelle est la date qu'Alice a voulu lui transmettre ?
2. Dans le cas général, quelle(s) propriété(s) doivent vérifier a et b pour que Bob puisse déchiffrer correctement les messages d'Alice ? Explicitez dans ce cas la fonction de déchiffrement.
3. Alice et Bob, qui ne sont pas très forts en arithmétique, ont choisit $a = 55$ et $b = 1$. Bob reçoit 221, que peut-il en déduire sur la date qu'Alice veut lui transmettre ?

2 Dans tout l'exercice, x et y désignent des entiers relatifs.

1. Montrez que, si $x = y \bmod 2$, alors $x^2 = y^2 \bmod 4$.
2. Déduisez-en que $x^2 = 0$ ou $1 \bmod 4$.
3. Utilisez ce qui précède pour montrer que la somme de deux carrés d'entiers n'est jamais congrue à 3 modulo 4.
4. Montrez que, plus généralement, si $x = y \bmod 2^k$, alors $x^2 = y^2 \bmod 2^{k+1}$.
5. Déduisez-en les valeurs possibles de $x^2 \bmod 8$.
6. Montrez que la somme de trois carrés d'entiers n'est jamais congrue à 7 modulo 8.

3 Critère de divisibilité par 7 :

1. Calculez les 8 premiers termes de la suite $10^k \bmod 7$ $(k \geq 0)$ puis montrez que cette suite est périodique de période 6.
2. En déduire un critère de divisibilité par 7 sur l'écriture décimale d'un nombre entier.
3. Application : l'entier 8641969 est-il divisible par 7 ?