Feuille TD 1 - L'anneau $\mathbb{Z}/n\mathbb{Z}$ - Cryptographie à clef privée

Exercice 1. Calcul modulaire et Théorème chinois des restes.

1. Résoudre les équations : a) $17x = 10[50]$; b) $35y = 10[50]$; c) $35y = 11[50]$.

2. Démontrer le théorème suivant, appelé **Théorème Chinois des restes** :
   Soient $(n_1, \ldots, n_k)$ k entiers premiers deux à deux et $N = \prod_{i=1}^{k} n_i$.
   L'application $\Psi : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ définie par

   $$\Psi(u) = [u \mod n_1; \ldots; u \mod n_k]$$

   est un isomorphisme d'anneau, d'inverse Ψ^{-1} définie par (en posant $N_i = N/n_i$) :

   $$\Psi^{-1}([u_1, \ldots, u_k)) = \left(\sum_{i=1}^{k} u_i.N_i.(N_i^{-1} \mod n_i) \right) \mod N.$$

3. Trouver tous les x entiers tels que $x \equiv 4 \pmod 5$ et $x \equiv 5 \pmod{11}$. En déduire l'inverse de 49 modulo 55.

4. Pour le système de résidus [3,4,5] expliciter l'isomorphisme du théorème chinois des restes $\Phi : \mathbb{Z}/60\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et son inverse Φ^{-1}.
   Application: Calculer de tête avec ce système $x = (36 * 43 - 39 * 27 - 12)/23$ sachant que $0 \leq x < 60$.

5. Trouver les entiers dont les restes par 2, 3, 4, 5, et 6 sont respectivement 1, 2, 3, 4, 5.

Exercice 2. Un algorithme à clef secrète.
Soit p un nombre premier et soient a, b deux entiers non nuls choisis dans $\{1, \ldots, p-1\}$. On note $\Phi_{a,b,p}$ la fonction de $\mathbb{Z}/p\mathbb{Z}$: $\Phi_{a,b,p}(x) = (a.x + b) \mod p$.
Pour un message dans $\{0, \ldots, p-1\}$, on considère la fonction de codage $E = \Phi_{a,b,p}$.

1. Expliciter la fonction de décodage D associée à E en montrant qu'elle s'écrit sous la forme $D = \Phi_{\alpha,\beta,p}$: expliciter α et β en fonction de a et b.

2. On suppose $p = 43, a = 5, b = 37$; on reçoit le message $E(x) = 28$. Que valait x ?

3. On suppose que l'on connaît a, b et p. Soit M un message de n bits avec $n \gg \log_2 p$. Expliquer comment crypter M avec E et donner une estimation du temps nécessaire au cryptage de M avec E en fonction de n et p.

4. On désire maintenant utiliser les fonctions précédentes dans un système à clef privée, en supposant que p est connu : a, b et α, β sont privés, connus par Alice et Bob seulement.
   Un espion sait qu'Alice envoie en secret à Bob les 2 messages différents x_1 et x_2, avec $0 \leq x_1, x_2 < p$. L'espion voit donc passer sur le réseau $y_1 = a.x_1 + b \mod p$ et $y_2 = a.x_2 + b \mod p$.
   Connaissant (x_1, y_1) et (x_2, y_2), montrer que l'espion peut alors facilement casser le code.

Exercice 3. Fonction ϕ d'Euler et inversion modulaire.
On étudie ici la fonction $\varphi(n)$, introduite par Euler, et dont les propriétés sont à la base de la méthode RSA.
On pose $\varphi(1) = 1$ et pour $n > 1$, $\varphi(n)$ est le nombre d'entiers $m \in \{1, \ldots, n-1\}$ premiers avec n (i.e. $\gcd(m, n) = 1$).

1 Pour $n = p^k$ où p est premier et $k \in \mathbb{N}^*$, montrer que $\varphi(n) = \left(1 - \frac{1}{p}\right).n$.

2 Montrer que si n_1 et n_2 sont premiers entre eux : $\varphi(n_1.n_2) = \varphi(n_1).\varphi(n_2)$. Indication : utiliser l'isomorphisme entre les anneaux $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ et $(\mathbb{Z}/n_1n_2\mathbb{Z})$.

3 En déduire que, dans $\mathbb{Z}/n\mathbb{Z}$, le cardinal du groupe des éléments inversibles est

$$\varphi(n) = n.\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

où les p_i $(i = 1, \ldots, k)$ sont les k facteurs premiers distincts de n. e déduit directement de 1 et 2.

4 On rappelle[1] que dans un groupe fini commutatif $(G, \times, e)$ de cardinal c, on a $\forall x \in G$: $x^c = e$. En déduire que pour tout x inversible dans $\mathbb{Z}/n\mathbb{Z}$: $x^{\varphi(n)} = 1 \mod n$ et proposer un algorithme de calcul de l'inverse dans $\mathbb{Z}/n\mathbb{Z}$.
Application : calculer (le plus vite possible) $22^{-1} \mod 63$ et $5^{2001} \mod 24$. On pourra utiliser: $22^2 \mod 63 = 43; 22^4 \mod 63 = 22$.

5 Donner trois algorithmes différents pour calculer l'inverse de y modulo $N = p_1^{\delta_1}.p_2^{\delta_2}.\ldots.p_k^{\delta_k}$, où les p_i sont des entiers premiers distincts.

[1] **Propriété** *Dans un groupe fini commutatif $(G, \times, e)$ de cardinal c, $\forall x \in G$: $x^c = e$.*
Preuve. Soit a un élément quelconque de G. Comme G est un groupe, a est inversible. Donc, l'application f_a de G dans G définie par $f_a : x \mapsto a \times x$ est une bijection. On a donc $Im(f_a) = G$; d'où $\prod_{y \in Im(f_a)} y = \prod_{x \in G} x$. Or $\prod_{y \in Im(f_a)} y = \prod_{x \in G} a \times x = a^n \prod_{x \in G} x$ (commutativité de $\times$). Ainsi $a^n \prod_{x \in G} x = \prod_{x \in G} x$, d'où $a^n = e$.