Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Feuille 5 — Groupe $(\mathbf{Z}/n\mathbf{Z})^\times$; cryptosystème RSA

Exercice 1. Le but de l'exercice est de montrer l'énoncé suivant, connu sous le nom de théorème de Wilson : « n premier $\Leftrightarrow (n-1)! = -1 \mod n$ » pour $n \geqslant 2$.

1. Soit p un nombre premier. Résoudre $x^2 = 1$ dans $\mathbf{F}_p$.
2. En déduire que $(p-1)! = -1 \mod p$ si p est impair.
3. Soit $n \geqslant 2$ un entier tel que $(n-1)! = -1 \mod n$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ est un corps.
4. Conclure.

Exercice 2. Soient A et B deux anneaux isomorphes. Montrer que $A^\times \approx B^\times$.

Exercice 3.

1. Donner la liste des éléments de $(\mathbf{Z}/14\mathbf{Z})^\times$.
2. Montrer que l'ordre de chaque élément ne peut être que 1, 2, 3 ou 6.
3. Calculer l'ordre de chaque élément et en déduire que $(\mathbf{Z}/14\mathbf{Z})^\times$ est cyclique. Expliciter deux isomorphismes entre ce groupe et $\mathbf{Z}/6\mathbf{Z}$.
4. Montrer que $(\mathbf{Z}/100\mathbf{Z})^\times$ n'est pas cyclique car tous ses éléments sont d'ordre divisant 20.

Exercice 4. Bob décide d'utiliser la méthode RSA avec $(p,q) = (5,7)$. Quelques exposants peut-il utiliser ? Dans chaque cas, donner la clé publique et la clé secrète.

Exercice 5. Alice souhaite envoyer des messages à Bob en utilisant RSA ; la clé publique de Bob est $(n,e) = (253,13)$.

1. Alice veut envoyer $m = 2$ à Bob ; quel est message chiffré c correspondant ?
2. Quelle est la clé secrète de Bob ?
3. Bob reçoit le message chiffré $c' = 22$. Quel est le message clair m' correspondant ?

Exercice 6. Bob souhaite recevoir des messages en utilisant la méthode RSA ; pour cela, il choisit deux nombres premier (p,q) et un exposant de chiffrement e. Il calcule ensuite l'inverse d de e modulo $\phi(pq)$, puis note d_p et d_q les reste de la division de d par $p-1$ et $q-1$. Il calcule enfin l'inverse de p modulo q qu'il note p'.

1. Bob publie alors (n,e) et conserve (p,q,d_p,d_q,p'). Expliquer comment ces informations lui permettent de déchiffrer des messages, sans utiliser d. (Indication : retrouver d'abord $m \mod p$ et $m \mod q$ puis utiliser le théorème chinois.)
2. Appliquer cette méthode avec $(p,q,e) = (11,13,7)$ pour déchiffrer $c = 23$.
3. À votre avis, ces calculs sont-ils plus rapides que la version présentée en cours ? Pourquoi ?

Exercice 7. Soit n le produit de deux nombres premiers p et q. Exprimer p et q en fonction de n et $\phi(n)$. (Indication : exprimer d'abord $p+q$ en fonction de n et $\phi(n)$.)