Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 4 : Logarithme discret

Exercice 1. Cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p-1$. Montrer qu'il existe $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $y^{(p-1)/q} \neq 1$. En déduire qu'il existe un élément x d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Soit q^α la plus grande puissance de q qui divise $p-1$. Montrer qu'il existe un élement y de $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que $y^{(p-1)/(q^\alpha)} \neq 1$.
3. Soit $x_y = y^{(p-1)/q^\alpha}$. Montrer que l'ordre de x est q^k avec $0 \leq k \leq \alpha$.
4. Supposons que $k \leq \alpha-1$ pour tout x. Montrer que tout élément du groupe vérifie $x^{(p-1)/q^{\alpha-k}} = 1$. En déduire l'existence d'un élément x_{q^α} d'ordre q^α.
5. Dans $(\mathbb{Z}/p\mathbb{Z})^\times$, si x est un élément d'ordre a et y d'ordre b, avec $\text{pgcd}(a,b) = 1$, quel est l'ordre de xy. Conclure.

Exercice 2. Le logarithme discret

Soit G un groupe cyclique d'ordre n dont la loi est notée multiplicativement et α un générateur de G.

1. Monter que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que l'application exponentielle de base α est une bijection de $\{0, 1, \ldots, n-1\}$ sur G. Le logarithme est son application réciproque.
3. Soit $G = (\mathbb{Z}/11\mathbb{Z})^\times$. Vérifier que 2 est un générateur de G. Calculer le logarithme en base 2 de 3.

Exercice 3. Calculs d'indices

Soit $p = 227$. $\alpha = 2$ est un élément primitif dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Calculer α^{32} modulo p. De même, on obtient $\alpha^{40} = 110, \alpha^{59} = 60$ et $\alpha^{156} = 28$ modulo p.
2. Factoriser ces puissances sur la base $\{2, 3, 5, 7, 11\}$. En déduire les valeurs de $\log_2(3), \log_2(5), \log_2(7)$ et $\log_2(11)$.
3. On veut calculer $\log_2(173)$. On choisit une puissance de 2 au hasard, disons 2^{177}. Le calcul donne $2^{177} = 123 \pmod p$. En factorisant 173.2^{177} modulo p sur notre base, trouver la valeur de $\log_2(173)$.

Exercice 4. Chiffrement d'ElGamal

Soit p un nombre premier et α un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit a un entier tel que $1 \leq a \leq p-1$ et $\beta = \alpha^a \pmod p$. Pour chiffrer $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ avec le chiffrement d'ElGamal, on choisit $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. La fonction de chiffrement est alors :

$$e(x,k) = \big(\alpha^k \pmod p, x\beta^k \pmod p\big)$$

et la fonction de déchiffrement est :

$$d(y_1, y_2) = \quad y_2(y_1^a)^{-1} \pmod p.$$

1. Précisez les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$. Quelle est la clé publique ? la clé privée ?
2. Montrer que si $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ alors $d \circ e(x) = x$.
3. Quelle est l'utilité de k.
4. On considère dans cette question la clé K suivante : $(p = 31, \alpha = 3, a = 16, \beta = 28)$
   (a) Peut on prendre une telle clé ?
   (b) Chiffrer le message $x = 5$ à l'aide de cette clé (on prendra $k = 8$).
   (c) Le message $(22, 14)$ a été chiffré à l'aide de la clé K, déchiffrez-le.

Exercice 5. Factorisation avec un logarithme

Soit p et q des nombres premiers impairs distincts et $n = pq$.

1. Soit α un inversible de $\mathbb{Z}/n\mathbb{Z}$. On note (α_p, α_q) son image dans $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Montrer que :
$$o(\alpha) = \text{ppcm}(o(\alpha_p), o(\alpha_q))$$
où $o(x)$ est l'ordre de x.
2. Soit $d = \text{pgcd}(p-1, q-1)$. Montrer qu'il existe un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre $\frac{\varphi(n)}{d}$.
3. Dans la suite on suppose de plus que $p > 3$ et $q > 3$ et $\text{pgcd}(p-1, q-1) = 2$. Encadrer $\varphi(n)$ par des fractions de n.
4. Soit α un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre $\frac{\varphi(n)}{2}$ et $a \in \{0, 1, \ldots, \frac{\varphi(n)}{2} - 1\}$ le logarithme de α^n en base α. Montrer que $n - a = \varphi(n)$.
5. Ecrire un algorithme qui prend pour entrées n et a et qui renvoie les facteurs p et q de n.
6. Montrer que le coût de votre algorithme est polynomial en la taille de n. On utilisera une méthode dichotomique pour le calcul de la racine carré dans $\mathbb{Z}$.

Exercice 6. [Test de Fermat]

Dans cet exercice on décrit un test de primalité utilisant le petit théorème de Fermat et plus précisément en étudiant sa réciproque.

1. Rappeler le petit théorème de fermat.
   On dit qu'un nombre n est pseudo premier en base a si n n'est pas premier et vérifie l'égalité :
$$a^{n-1} \equiv 1 \pmod{n}$$
2. Dans cette question on montre l'existence d'une infinité de nombre premier en base a.
   (a) Soit $a \geq 2$ un entier, $p > 2$ un nombre premier tel que $p \nmid a(a^2 - 1)$. On pose :
$$n = \frac{a^{2p} - 1}{a^2 - 1}$$
   Montrer que n n'est pas premier.
   (b) Montrer que $a^{2p} \equiv 1 \pmod{n}$.
   (c) Calculer $(a^2 - 1)(n - 1)$, puis montrer que $p \mid n - 1$.
   (d) Montrer que $2 \mid n - 1$.
   (e) Conclure que n est pseudo premier en base a. En déduire que pour tout $a \geq 2$ il existe une infinité de nombre pseudo premier en base a.
3. Un entier $n \geq 2$ est appelé nombre de Carmichaël si n n'est pas premier et si pour tout a premier avec n on a $a^{n-1} \equiv 1 \pmod{n}$.
   (a) Soit $n = p_1 \ldots p_k$ tel que $p_i - 1 \mid n - 1$ pour tout $1 \leq i \leq k$. Montrer que $a^{n-1} \equiv 1 \pmod{p_i}$ pour tout a premier avec $n$et pour tout $1 \leq i \leq k$.
   (b) Conclure.