TD2 : Crible par Corps de Nombres, à propos de Sélection Polynomiale

4I905: Représentation des Nombres et Algorithmes : application à la cryptographie

Exercice 1. Sélection polynomiale en moyenne caractéristique

Question 1 : Un exemple simple de 2006. Soit f_1 un polynôme à petits coefficients irréductible sur $\mathbb{F}_p$ (p étant un nombre premier) et de degré n. Posons $f_2 = f_1 + p$. Montrez que ces deux polynômes permettent de définir un diagramme commutatif utile pour le crible par corps de nombres. Quel est le corps fini que l'on considère ? Donnez les paramètres pertinents des deux polynômes.

Question 2 : La sélection par fraction continue (2006). Soit f_1 un polynôme à coefficients entiers, de degré n, irréductible modulo p et tel que l'on puisse écrire $f_1 = g + c \cdot h$ avec g et h des polynômes à petits coefficients, et c un entier de taille[1] $O(\sqrt{p})$. Un algorithme (que l'on ne détaillera pas ici) permet d'obtenir deux entiers a et b de tailles $\sqrt{p}$ tels que $c = a/b \mod p$. Que peut-on dire du polynôme égal à bf_1 modulo p ? Donnez les paramètres pertinents des deux polynômes.

Exercice 2. Calcul de complexité en moyenne caractéristique. Le but de cet exercice est de calculer la complexité asymptotique obtenue en moyenne caractéristique par le Crible par Corps de Nombres lorsque l'on utilise la sélection par fraction continue proposée à l'exercice précédent.

Question 1 : Rappelez la notation en L_Q. De quel paramètre la complexité asymptotique finale va-t-elle dépendre ? On pose $Q = p^n$ avec p premier, et on considère le corps fini à Q éléments.

Question 2 : Dans notre cas, des trois phases principales des algorithmes par calcul d'indice, l'une est négligeable. De laquelle s'agit-il ?

Question 3 : Paramètres. On se donne les paramètres suivants : $p = L_Q(l_p, c_p)$ avec $1/3 < l_p < 2/3$, B la borne de lissité, S la borne de crible, $t-1$ le degré des polynômes sur lequel on crible, et $\mathcal{P}$ la probabilité partant d'un polynôme de l'espace de crible d'obtenir une bonne relation. Ecrivez n en fonction de Q, l_p et c_p.

Question 4 : Coût de l'algèbre linéaire. Donnez en fonction des paramètres précédents la taille du système d'équations linéaires que l'on cherche à résoudre. Indication : on peut grossièrement majorer le nombre de nombres premiers inférieurs à x par x. Quelle est la spécificité de cette matrice ? Quel est alors le coût total de l'algèbre linéaire ?

Question 5 : Coût du crible. S désigne la borne sur les coefficients des polynômes du crible. Quel est le cardinal de l'espace de crible ? Expliquez pourquoi le coût du crible peut être arrondi à cette dernière valeur.

Question 6 : Première contrainte. On se propose, pour réduire le nombre de paramètres, d'égaliser le coût des deux phases non négligeables. Donnez l'égalité qui en résulte.

[1] Rappel : la notation grand O de Landau dénote le caractère dominé d'une fonction par rapport à une autre. Soient f et g deux fonctions de la variable réelle x. On dit que f est dominée par g en $+\infty$ et on note $f(x) = O(g(x))$ $(x \to \infty)$, lorsqu'il existe des constantes N et C telles que $\forall x > N, |f(x)| \leq C\,|g(x)|$.

Question 7 : Deuxième contrainte. Une deuxième contrainte apparait naturellement : il s'agit d'obtenir suffisamment d'équations à l'issue de la face de crible. Nous proposons de traduire cela de nouveau en forçant l'égalité entre le nombre d'équations obtenues et le nombre d'inconnues (telles qu'approximées à la question 3). Quelle égalité en résulte ? Montrez que les deux contraintes mises ensemble forcent l'égalité $B = 1/\mathcal{P}$.

Question 8 : Calcul de la probabilité. Que signifie qu'un entier est B-lisse ? Nous cherchons la probabilité que les deux normes issues d'un même polynôme du crible soient toutes les deux B-lisses. Montrez que chacune des normes peut-être majorée par :

$$(\deg f_i + \deg \phi)! \cdot N(f_i)^{\deg \phi} \cdot N(\phi)^{\deg f_i}$$

où f_i est respectivement f_1 ou f_2 et où $N(P)$ est un majorant de la valeur absolue de chaque coefficient du polynôme P. Nous admettons pour la suite que les paramètres sont tels que la factorielle dans cette dernière expression est négligeable. Montrez que deux entiers x et y indépendants sont tous les deux B-lisse si et seulement si leur produit est B-lisse.

Pour évaluer cette probabilité, nous, utilisons un corollaire du théorème de Canfield, Erdős et Pomerance :

Corollary 0.1. *Soit $(\alpha_1, \alpha_2, c_1, c_2) \in [0,1]^2 \times [0,\infty)^2$ tels que $\alpha_1 > \alpha_2$. Notons $\mathcal{P}$ la probabilité qu'un entier positif inférieur à $x = L_q(\alpha_1, c_1)$ soit y-lisse avec $y = L_q(\alpha_2, c_2)$. Alors l'égalité suivante est satisfaite $\mathcal{P}^{-1} = L_q\left(\alpha_1 - \alpha_2, (\alpha_1 - \alpha_2)c_1 c_2^{-1}\right)$.*

En posant :

$$t = \frac{c_t}{c_p}\left(\frac{\log Q}{\log\log Q}\right)^{2/3-l_p}, \quad S^t = L_Q(1/3, c_s c_t) \quad \text{et} \quad B = L_Q(1/3, c_b)$$

réécrivez l'entier $p^t S^{2n}$ sous une forme adéquate. On s'autorise à arrondir p^{t-1} à p^t. Déduisez-en $\mathcal{P}$, puis c_b. Montrez que :

$$3c_b^2 = c_t + 2c_s \tag{1}$$

Question 9 : Optimisation. Le but est maintenant de minimiser $2c_b$ sous la contrainte (1). Réécrivez cette contrainte de sorte de n'obtenir plus que les paramètres c_b et c_s. Minimisez par la méthode de votre choix (dérivée par rapport à la variable c_s ou calcul de racine d'un polynôme de degré 2...). Quelle la complexité finale obtenue ?

Exercice 3. Borne inférieure sur les paramètres de f_1 et f_2. Nous avons vu en cours que plus les degrés et coefficients des deux polynômes sont petits plus la probabilité d'obtenir de bonnes relations dans la phase de crible est grande, donc plus la complexité s'abaisse. Pourtant, il existe une borne naturelle inférieure sur ces paramètres comme nous allons le montrer.

Question 1 : La condition réelle que l'on souhaite vérifier est le fait que f_1 et f_2 partagent une racine commune m dans $\mathbb{F}_{p^n}$. En effet, si telle est le cas, une égalité du type $P_1(X) + Q_1(X)f_1(X) = P_2(X) + Q_2(X)f_2(X)$ donnera $P_1(m) = P_2(m)$ dans le corps fini. Vérifiez qu'exiger que f_1 et f_2 partagent, modulo p, un facteur commun irréductible de degré n suffit pour que f_1 et f_2 partagent une racine commune dans $\mathbb{F}_{p^n}$.

Question 2 : Donnez une condition nécessaire simple sur le résultant de f_1 et f_2 pour que f_1 et f_2 partagent une racine commune dans $\mathbb{F}_{p^n}$.

Le cas des corps premiers. Dans toute la suite on considère le cas où le corps dont lequel on cherche à résoudre le problème du logarithme discret est $\mathbb{F}_p$ avec p un nombre premier. Par abus de langage, un tel corps sera dit lui aussi premier. On rappelle qu'en présence d'un corps fini de grande caractéristique, cribler sur des polynômes de la forme $a + bX$ suffit. On suppose de plus ici que $0 \leqslant a \leqslant S$ et $-S \leqslant b \leqslant S$ où S est une borne de crible fixée.

Question 3 : Evaluez les normes issue d'un polynôme $a + bX$ dans chacun des deux corps de nombres, en fonction de a, b et f_1 (resp. f_2). On s'appuiera sur le fait que la norme d'un polynôme ϕ dans le corps défini par f un polynôme unitaire est égale au résultant de ϕ et f, au signe près. En particulier on ne demande pas de passer par la matrice de Sylvester.

Question 4 : En notant C_i une borne sur les coefficients de f_i et d_i son degré, donnez l'ordre de grandeur du résultant de f_1 et f_2. Déduisez une borne inférieure sur $d_1 \log_2(C_1) + d_2 \log_2(C_2)$.

Question 5 : Théorie de l'information. La quantité d'information portée par f_1 et f_2 ne peut pas être moins grande que celle de p. On dit en effet que f_1 et f_2 forment un encodage de p, c'est-à-dire qu'à partir de ces deux polynômes il est possible de retrouver p. Expliquez brièvement comment. Déduisez-en une seconde inégalité faisant intervenir C_1, C_2, d_1 et d_2.

Question 6 : Fixons d_1 et d_2. Quelles valeurs de C_1 et C_2 réalisent l'optimum ? Que peut-on dire du cas où les degrés des deux polynômes sont égaux ?

Question 7 : Lorsque $d_1 \neq d_2$ sont fixés, montrez qu'une sélection polynomiale optimale vérifie :

$$\log_2(C_1) + \log_2(C_2) = 2\log_2(p)/(d_1 + d_2 + 1). \tag{2}$$

Exercice 4. Crible Spécial par Corps de Nombres pour les nombres de Fermat.

Question 1 : Si l'on souhait résoudre le problème du logarithme discret sur un corps premier dont la caractéristique p est de forme particulière et non aléatoire, laquelle des deux inégalités de l'exercice précédent ne tient plus ? Qu'en est-il de la seconde ?

Question 2 : Lorsque l'on applique le Crible par Corps de Nombres pour des corps dont la caractéristique est particulière, et que l'on obtient de ce fait des meilleurs paramètres que ceux donnés par (2), on parle de Crible Spécial par Corps de Nombres. Lorsque a et b sont tous les deux bornés en valeur absolue par S, quel vaut le produit des normes d'un polynôme du crible dans chacun des deux corps de nombres ?

Question 3 : En considérant que $D = d_1 + d_2$ est fixée quelle est la quantité à minimiser ? Sous quelle contrainte ?

Question 4 : En supposant que $d_1 \leqslant d_2$, quel est le meilleur choix pour C_1 et C_2 ? Montrez que cela est optimal lorsque l'on sélectionne f_1 comme étant un polynôme de degré 1 et f_2 de degré $D-1$.

Question 5 : Un exemple de Crible Spécial sur un nombre de Fermat. Considérons le p-ième nombre de Fermat $N = 2^{2^p} + 1$. Est-ce un entier aléatoire ? En décomposant 2^p comme produit de deux entiers, construisez deux polynômes avec une racine commune modulo N qui donnent de meilleurs paramètres que ceux imposés par (2).

Question 6 : Cette variante bat-elle le crible par corps de nombres utilisé classiquement en grande caractéristique ?

Exercice 5. Sélection polynomiale de Montgomery pour les corps premiers. Cet exercice présente une construction de deux polynômes quadratiques qui permettent de résoudre le problème du logarithme discret par Crible par Corps de Nombres sur un corps premier de cardinal p.

Question 1 : Soit t un entier proche de $\sqrt{p}$ tel que p soit un résidu quadratique modulo t. Notons c une telle racine carrée. Montrez alors que les nombres t, c et $(c^2 - p)/t$ ont une progression géométrique modulo p. Quelle en est la raison ?

Question 2 : Donnez trois vecteurs (à coefficients dans $\mathbb{F}_p$) linéairement indépendants dont le produit scalaire avec le vecteur $(t, c, (c^2 - p)/t)$ est nul modulo p.

Question 3 : Montrez que chaque vecteur orthogonal à $(t, c, (c^2 - p)/t)$ modulo p peut être transformé en un polynôme dont c/t est une racine modulo p.

Question 4 : Quelle est la taille des coordonnées des vecteurs de la question 2 ? Proposez et une sélection polynomiale pour $\mathbb{F}_p$ et comparez avec la borne donnée par (2).

Question 5 : Pour abaissez la taille des coefficients, Montgommery propose d'utiliser l'algorithme de réduction de réseau LLL. Plus généralement, cela permet de trouver des relations linéaires à petits coefficients. L'idée est la suivante :

Soient α, β, γ et N des entiers positifs. Pour trouver des petits entiers u, v, w tels que:

$$(E) \quad u\alpha + v\beta + w\gamma = 0 \mod N,$$

nous passons par la matrice :

$$M = \begin{pmatrix} \alpha & \beta & \gamma \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Vérifiez que si un vecteur (x, u, v, w) est issu d'un produit matrice-vecteur impliquant M et que $x = 0$ alors (u, v, w) est solution de (E). Nous cherchons un vecteur court solution. Malheureusement, si un vecteur court[2] est obtenu par M, cela ne permet pas de retrouver une solution de (E). Pour contourner ce problème, nous considérons la matrice :

$$M_K = \begin{pmatrix} K\alpha & K\beta & K\gamma \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

où K est un réel suffisamment grand (par exemple K>B). Que peut-on dire cette fois-ci d'un vecteur court engendré par les colonnes de M_K ? L'algorithme LLL appliqué à M_K donnera le réseau réduit :

$$M_{\text{red}} = \begin{pmatrix} 0 & 0 & K \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

où (a_1, a_2, a_3) et (b_1, b_2, b_3) sont des vecteurs courts. Appliquez cet algorithme pour trouver deux polynômes permettant de résoudre le problème du logarithme discret par Crible par Corps de Nombres sur $\mathbb{F}_p$.

Question 6 : Le déterminant d'une matrice A quelconque (en particulier rectangulaire) est définie par :

$$\det A = \sqrt{\det(A \times {}^tA)}.$$

Sachant que la réduction de réseau conserve le déterminant, quelle est la taille des coefficients des polynômes obtenus ? Comparez avec la question 4 puis avec (2).

[2]Lorsque l'on parle de vecteur court, on caractérise implicitement le fait que chacun des coefficients est plus petit qu'une certaine borne B