D34: Méthodes de calcul efficaces
Arithmétique dans $\mathbb{F}_p$ et $\mathbb{F}_{2^n}$

1 Exercices

Exercice 1. Algorithme de Barrett

1. Calculer $m \mod p$ pour les valeurs de m et p suivantes:
   (i) $m = 1254, p = 56$
   (ii) $m = 9956, p = 56$
   (iii) $m = 10101101_2, p = 1001_2$
2. Écrire la version décimale de l'algorithme de Barrett. Montrer que le nombre d'itérations de la boucle `while` est le même que dans le cas binaire.

Exercice 2. Algorithme de Montgomery en base β

Le but est d'écrire une version générale de l'algorithme de Montgomery vu en cours. On veut réaliser la multiplication modulaire de $A = (a_{n-1}...a_0)_\beta$ par $B = (b_{n-1} \dots b_0)_\beta$ modulo $P = (p_{n-1} \dots p_0)_\beta$ (on notera M le résultat).

1. Quel résultat calcule la multiplication de Montgomery?
2. Rappeler l'algorithme de multiplication des livres d'écoles en base β.
3. Posons $M' = M + a_i B + qP$ pour un M et un i donnés. Calculer q pour que M' soit divisible par β. Montrer que si $M \leq 2p - 1$ alors $M' \leq 2p - 1$.
4. Déduire de ce qui précède l'algorithme de Montgomery en base β.

Exercice 3. Nombre de Crandall et Solinas

1. Calculer les réduction modulaire suivantes:
   (i) $869 \mod 10^2 - 3$
   (ii) $123456 \mod 1009$
   (iii) $25612864321 \mod 1003001$
   (iv) $(10101010100101010101)_2 \mod (1111111111)_2$
2. On admettra que le nombre $p_{224} = f(2^{32})$ où $f(X) = X^7 - X^3 + 1$ est premier. Proposer un algorithme de réduction modulaire efficace (6 additions/soustractions de nombres de 224 bits).

Exercice 4. Multiplication de polynomes dans $\mathbb{F}_{2^n}$

1. À l'aide de l'algorithme `shift-and-add`, calculer le produit $(X^{12} + X^7 + X^6 + X^3 + 1)(X^{11} + X^5 + X + 1)$ dans $\mathbb{F}_2[X]/(X^{13} + X^{11} + X^2 + X + 1)$.
2. Calculer $(X^{10}+X^8+X^6+X^2+X+1)^2$ dans $\mathbb{F}_2[X]/(X^{13}+X^{11}+X^2+X+1)$.

Exercice 5. Carré dans $\mathbb{F}_{2^n}$

1. En remarquant que $(x + y)^2 = x^2 + y^2$ dans $\mathbb{F}_{2^n}$, proposer un algorithme de réduction spécifique à l'élévation d'un élément au carré.
2. Quel est le coût relatif de cette algorithme par rapport à celui de la multiplication généraliste.

Exercice 6.

On considère le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3 + X + 1)$.

1. Donner les matrices de structure M_i de la multiplication par un polynome $A[X] = a_2X^2 + \dots a_0$. En déduire la matrice du produit M_A.
2. Transformer la matrice M_A en matrice de Toeplitz.
3. On considère maintenant une matrice de Toeplits de taille $n = 3^t$. Proposer un algorithme de calcul du produit AB en décomposant la matrice en 9 blocs. Montrer que l'on peut effectuer ce calcul en seulement 6 multiplications matrice/vecteur de taille $n/3$.
4. En déduire un algorithm général de multiplication dans les corps $\mathbb{F}_{2^{3^b}}$. Quelle est la complexité de la méthode?

Exercice 7. Bases normales

On considère le corps $\mathbb{F}_{2^7} = \mathbb{F}_2[X]/(X^7 + X^6 + 1)$.

1. Montrer que l'élément X est un élément normal de $\mathbb{F}_{2^7}$.
2. Calculer la matrice de structure M_0 et en déduire les autres matrices de structures.

2 Programmation

Exercice 1. Multiplication de polynomes

L'objectif de cet exercice est d'implanter est de créer un type pour les polynomes de $F_2[X]$ en `C` et de comparer l'efficacité des algorithmes élémentaires sur ce type par rapport à l'implantation pour les entiers de `gmp`.

On considérera le type `F2_pol_t`:

```
typedef unsigned char uchar;
typedef struct{
  uchar *coeff;
  int deg;
  int nblimb;
} F2_pol_t;
```

1. Implanter les fonctions de bases permettant la gestion du type `F2_pol_t` (initialisation, affectation, décalage à gauche, somme).
2. Implanter l'algorithme de multiplication `shift-and-add`.
3. Comparer l'efficacité des algorithmes d'addition et de multiplication dans F_2 avec leur équivalent entier de la bibliothèque `gmp`.
4. On rappelle que que $\left(\sum_{i=0}^{n-1} a_i X^i\right)^2 = \sum_{i=0} a_i X^{2i}$. Implanter une procédure d'élévation carré dans $\mathbb{F}_{2^n}$ et comparer son efficacité avec les résultats précédents.

On pourra utiliser les polynomes irréductibles suivants:

$X^{15}+X+1$	$X^{31}+X^3+1$	$X^{47}+X^5+1$	$X^{63}+X+1$	$X^{79}+X^9+1$
$X^{95}+X^{11}+1$	$X^{111}+X^{10}+1$	$X^{127}+X+1$	$X^{159}+X^{31}+1$	$X^{191}+X^9+1$
$X^{223}+X^{33}+1$	$X^{255}+X^{52}+1$	$X^{287}+X^{71}+1$	$X^{319}+X^{36}+1$	$X^{383}+X^{90}+1$
$X^{447}+X^{73}+1$	$X^{511}+X^{10}+1$	$X^{575}+X^{146}+1$	$X^{639}+X^{16}+1$	$X^{767}+X^{168}+1$