Arithmétique modulaire entière en base polynomiale

Pascal Giorgi

University of Perpignan, DALI team

en collaboration avec

C. Nègre (Université de Perpignan),

T. Plantard (University of Wollongong, Australie)

séminaire CASYS-BIBOP,

jeudi 15 mars 2007

Motivations

Le grossissement des clés utilisées par les protocoles classiques en cryptographie asymétrique nécessite une arithmétique modulaire de plus en plus performante.

Protocoles standards :

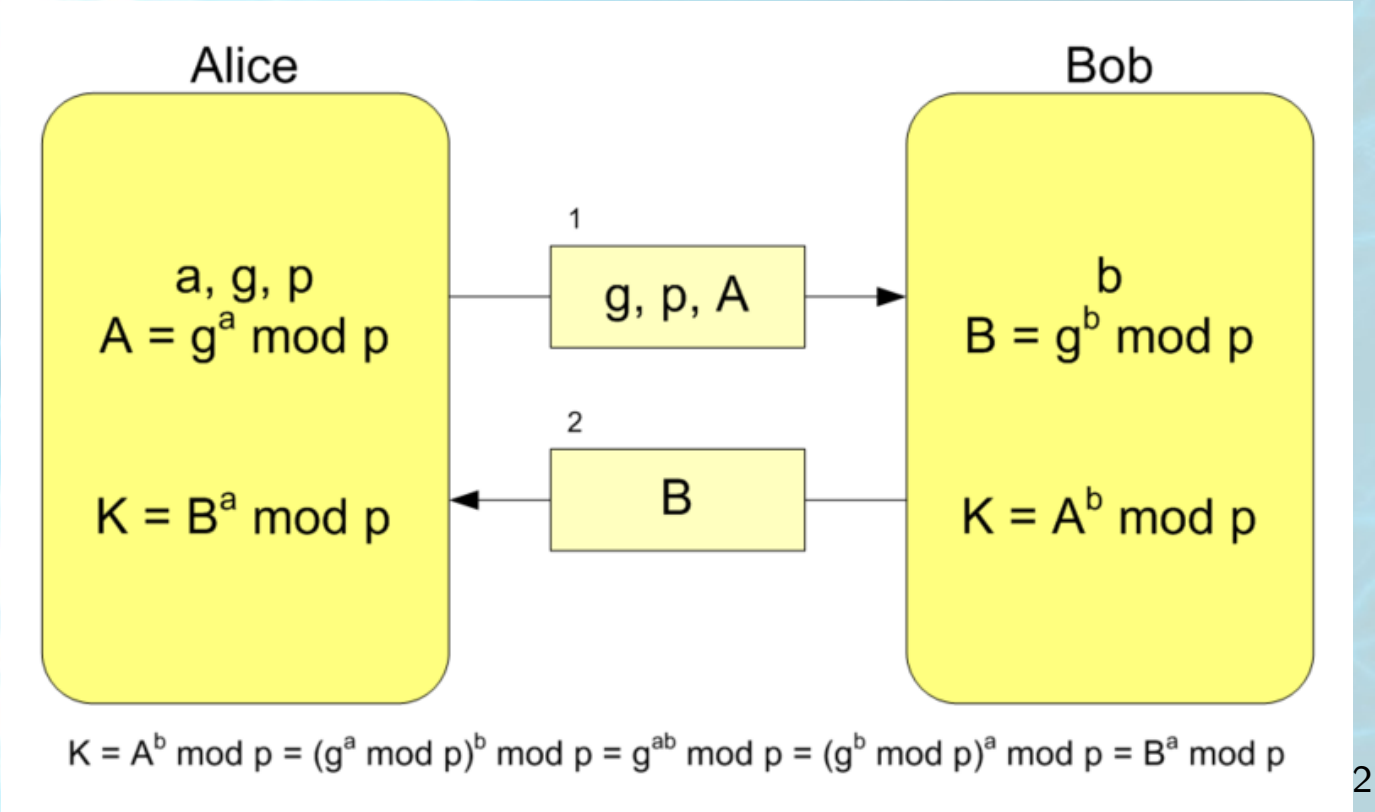
- échange de clés de Diffie-Hellman [Diffie, Hellman 1976],
- cryptosystème RSA [Rivest, Shamir, Adleman 1978],
- cryptosystème de ElGamal [ElGamal 1984],

$\hookrightarrow$ NIST[1] recommande des clés de minimum 1024-2048 bits

[1] National Institute of Standards and Technology

Échange de clés de Diffie-Hellman

objectif : se mettre d'accord sur une clé commune.

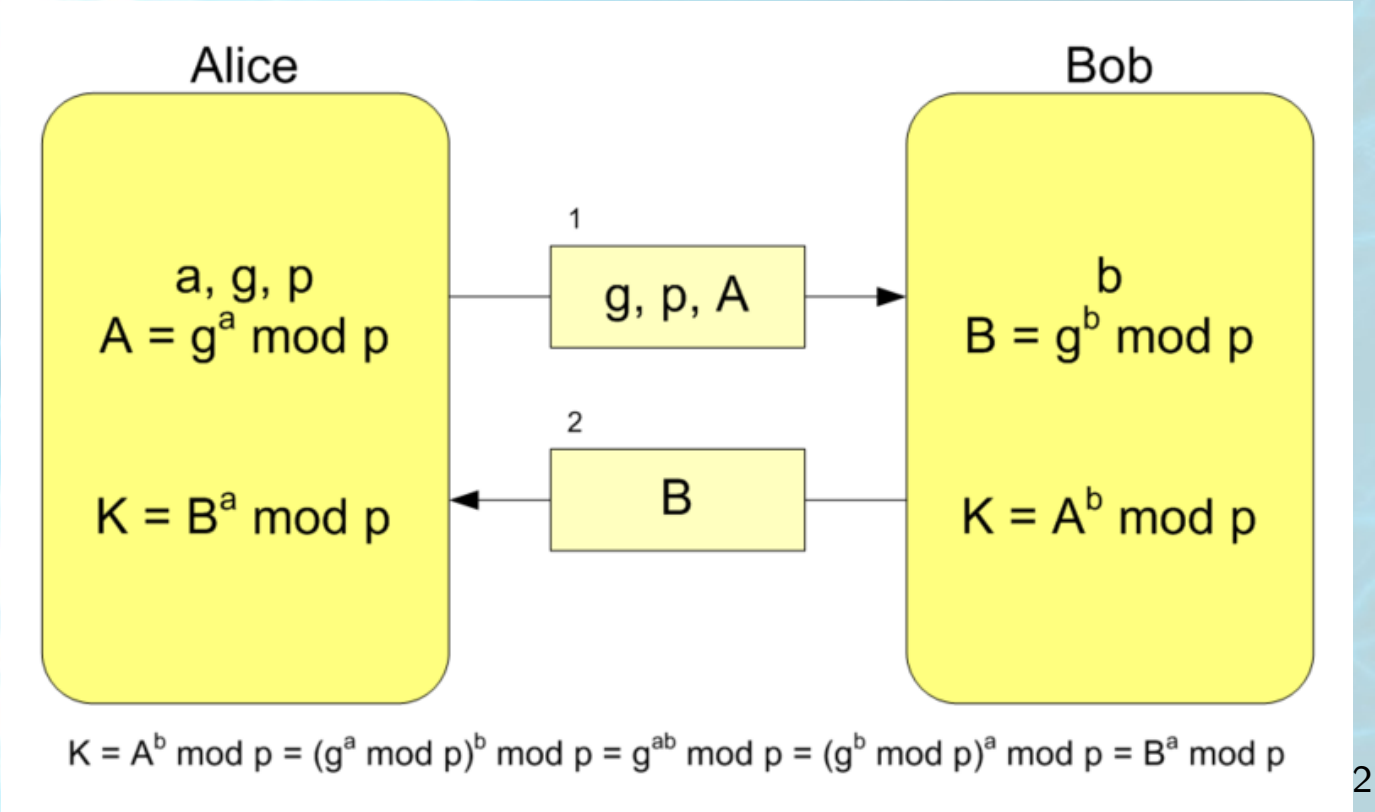


[2]

[2]source Wikipedia

Échange de clés de Diffie-Hellman

objectif : se mettre d'accord sur une clé commune.



[2]

la multiplication joue un rôle central ! ! !

[2] source Wikipedia

Plan de l'exposé

I. multiplication modulaire (*pseudo-Mersenne, Montgomery*)

II. représentation *AMNS* et multiplication

III. multiplication rapide en *AMNS*

IV. conclusion et perspectives

Plan de l'exposé

I. multiplication modulaire (*pseudo-Mersenne, Montgomery*)

II. représentation *AMNS* et multiplication

III. multiplication rapide en *AMNS*

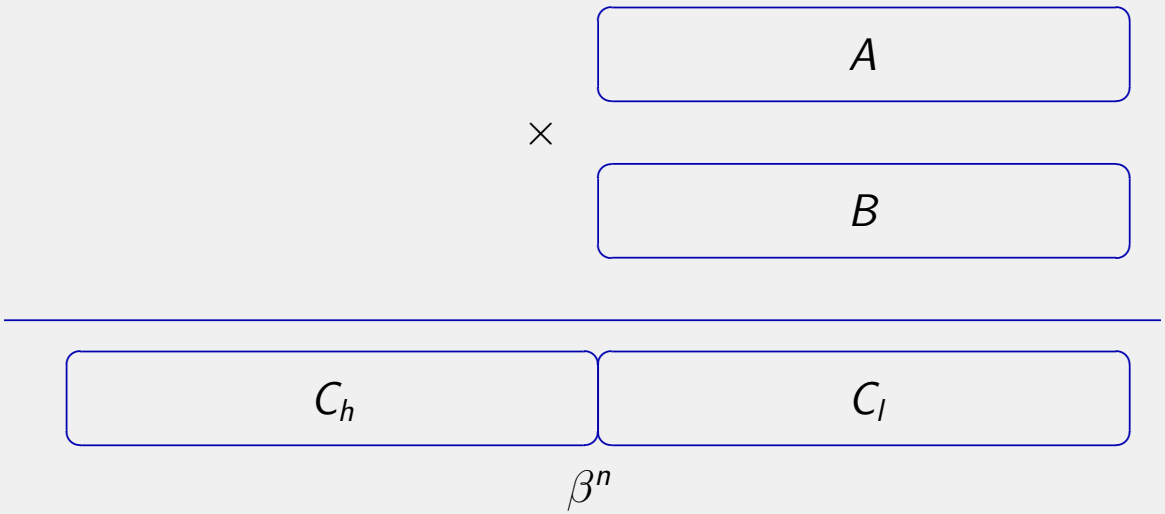
IV. conclusion et perspectives

Multiplication modulaire

Un entier A est généralement représenté par

$$A = \sum_{i=0}^{n} a_i \beta^i, 0 \leq a_i < \beta$$

Le produit de deux entiers A et B s'exprime par



$$C = A \times B = C_l + \beta^n \times C_h.$$

Une multiplication modulaire modulo p correspond à réduire le résultat de la multiplication entière modulo p. $\hookrightarrow$ division.

Réduction modulaire avec des pseudo-Mersenne

Un pseudo-Mersenne p est un premier tels que

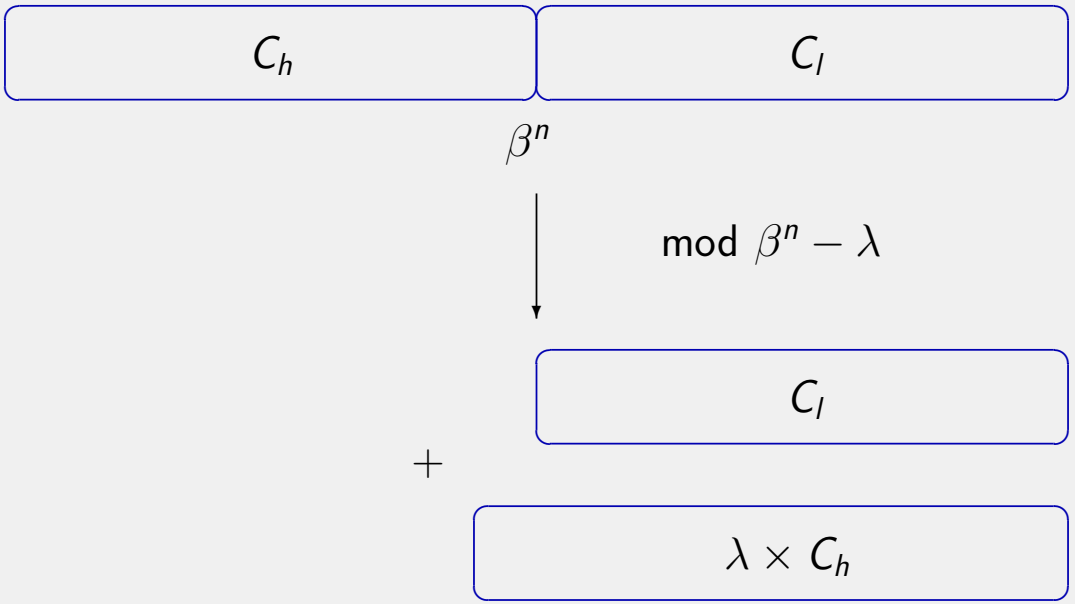
- $p = \beta^n - \lambda$.
- λ étant petit par rapport à p, donc $\beta \cong p^{1/n}$
- $\beta^n \equiv \lambda \mod p$,

Réduction modulaire avec des pseudo-Mersenne

Un pseudo-Mersenne p est un premier tels que

- $p = \beta^n - \lambda$.
- λ étant petit par rapport à p, donc $\beta \cong p^{1/n}$
- $\beta^n \equiv \lambda \mod p$,

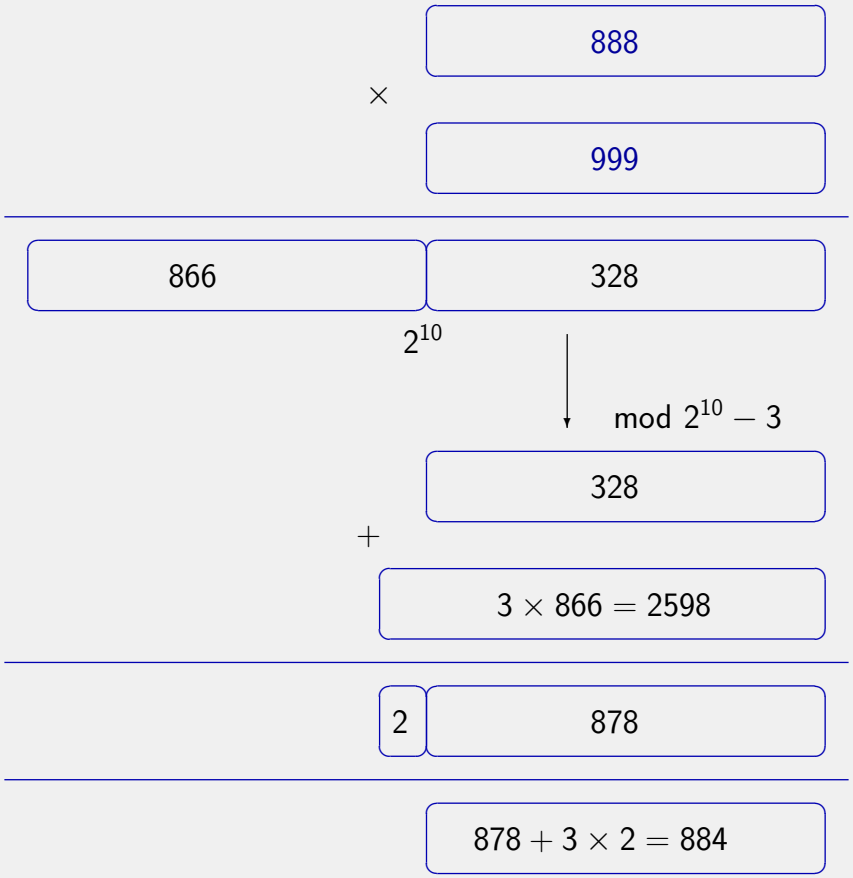
La réduction de C revient à : $R = C_l + \lambda \times C_h \equiv C \mod p$.



Exemple :

- choix d'un premier pseudo Mersenne $1021 = 2^{10} - 3$

calcul de $A \times B \mod P$: $A = 888$, $B = 999$, $P = 1021$



$888 \times 999 \mod 1021 = 884$

Réduction de Montgomery (1)

Alternative quand le modulo n'a aucune structure

[Montgomery 1986] : remplacer la division par quelques multiplications

approche : mettre à zéro la partie basse du produit

Idée

Soit P un modulo quelconque représenté en base β tel $P < \beta^n$, et $gcd(P, \beta^n) = 1$. Soit deux entiers $0 \leq A, B < P$ et $P' = -P^{-1} \mod \beta^n$.

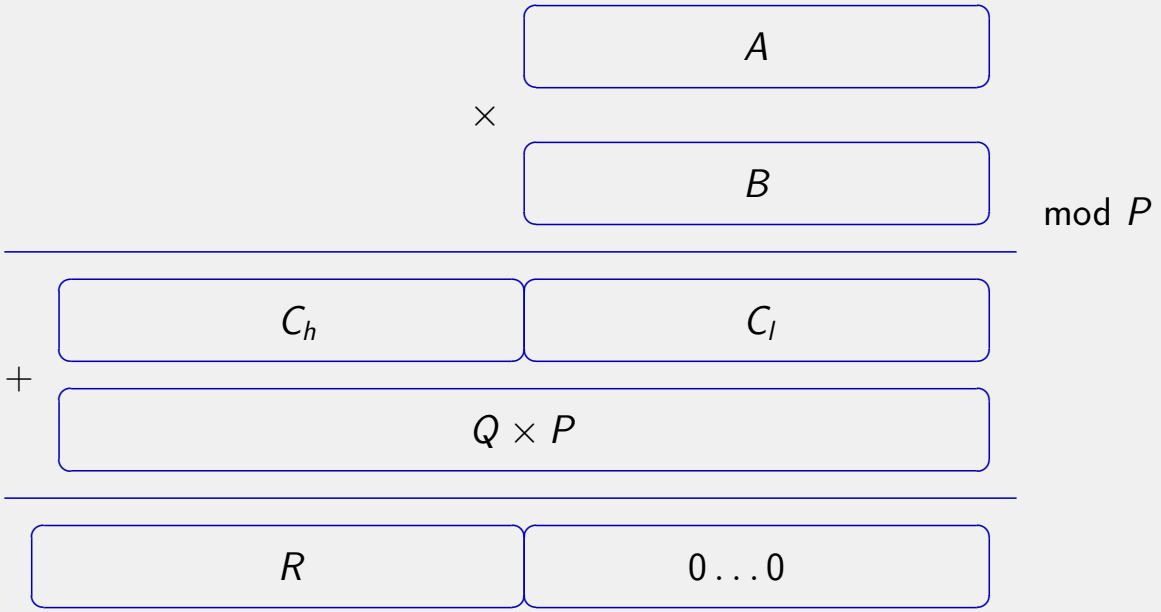
- $Q = A \times B \times P' \mod \beta^n$
- $R = A \times B + Q \times P$

Alors R est divisible par β^n et $R \equiv A \times B \mod P$

Remarque : $R \times \beta^{-n} < 2P$

Réduction de Montgomery (2)

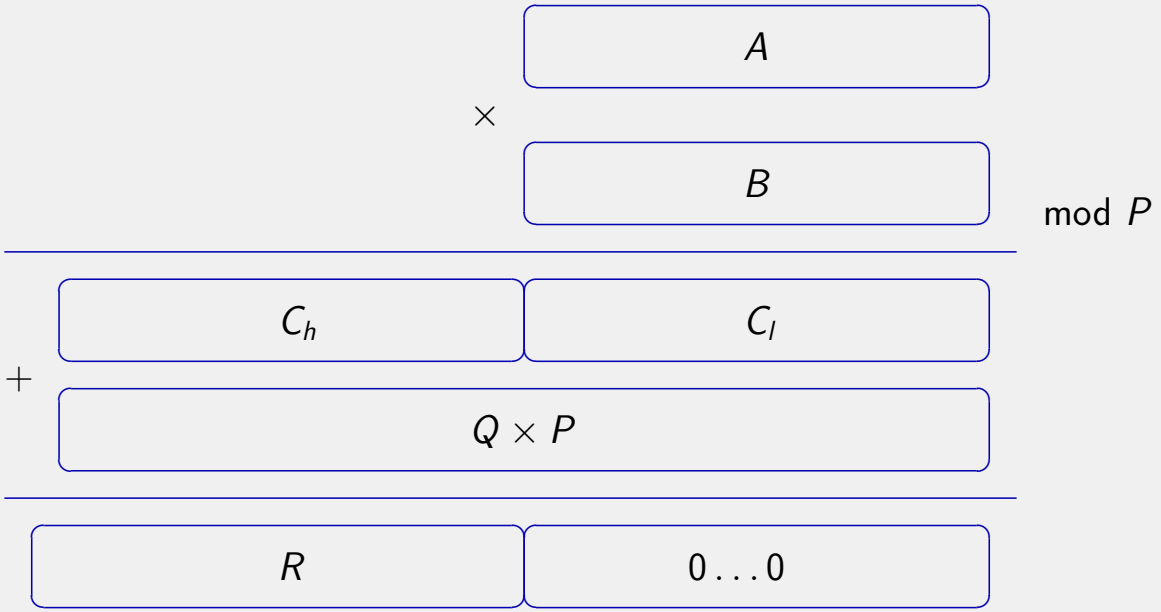
Multiplication de Montgomery



R est un autre codage de $C = A \times B \mod P$

Réduction de Montgomery (2)

Multiplication de Montgomery



R est un autre codage de $C = A \times B \mod P$

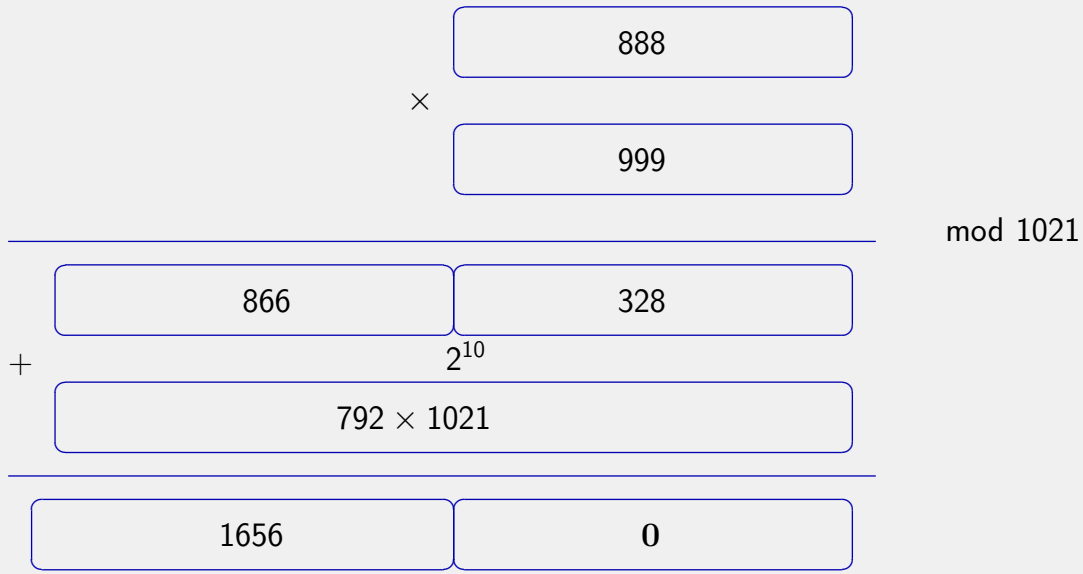
Représentation de Montgomery

Coder les entiers $0 \leq x < p$ par $\bar{x} = x\beta^n \mod p$

- stable par addition classique,
- stable par la multiplication de Montgomery.

Exemple :

- calcul de $A \times B \mod P$:
  $$A = 296, \quad B = 333, \quad P = 1021$$
- en représentation de Montgomery ($\beta^n = 2^{10}$) :
  $$\bar{A} = 888, \quad \bar{B} = 999$$
- <u>résultat</u> :
  $$C = AB \mod P = 552 \rightarrow \bar{C} = 635$$



$$1656 \mod 1021 = 635$$

Plan de l'exposé

I. multiplication modulaire (*pseudo-Mersenne, Montgomery*)

II. représentation *AMNS* et multiplication

III. multiplication rapide en *AMNS*

IV. conclusion et perspectives

Système de représentation modulaire adaptée (AMNS)

Motivations

- relâcher la contrainte sur les chiffres $a_i < \beta$, maintenant $\beta \cong p$ non plus $\beta \cong p^{1/n}$
- plus de choix pour β tel que $\beta^n \equiv \lambda$ avec λ petit.

Définition de l'AMNS [Bajard,Imbert,Plantard 2005]

Un système $\mathcal{B} = (p, n, \gamma, \rho)$ est appelé *système de représentation modulaire adapté (AMNS), si tout entier* $A \in [1, p]$ *peut s'écrire*

$$A \equiv \sum_{i=0}^{n} a_i \gamma^i \mod p, \text{ avec } |a_i| < \rho.$$

et s'il existe un petit entier λ *tel que* $\gamma^n = \lambda \bmod p$

Système de représentation modulaire adaptée (AMNS)

Motivations

- relâcher la contrainte sur les chiffres $a_i < \beta$, maintenant $\beta \cong p$ non plus $\beta \cong p^{1/n}$
- plus de choix pour β tel que $\beta^n \equiv \lambda$ avec λ petit.

Définition de l'AMNS [Bajard,Imbert,Plantard 2005]

Un système $\mathcal{B} = (p, n, \gamma, \rho)$ est appelé *système de représentation modulaire adapté (AMNS), si tout entier* $A \in [1, p]$ *peut s'écrire*

$$A \equiv \sum_{i=0}^{n} a_i \gamma^i \mod p, \text{ avec } |a_i| < \rho.$$

et s'il existe un petit entier λ *tel que* $\gamma^n = \lambda \bmod p$

permet un représentation des entiers modulo p par des polynômes en γ

$\mathcal{B} \cong \mathbb{Z}[\gamma]/(\gamma^n - \lambda)$ avec des contraintes sur les coefficients

Exemple d'AMNS

On considère l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$ suivant

$$p = 17 \quad n = 4$$
$$\gamma = 7, \quad \rho = 2$$

γ vérifie $\gamma^3 = 3 \mod 17$.

0	1	2	3	4
0	1	$-x^2$	$1 - x^2$	$-1 + x + x^2$

5	6	7	8	9
$x + x^2$	$-1 + x$	x	$1 + x$	$-x - 1$

10	11	12	13	14
$-x$	$-x + 1$	$-x - x^2$	$1 - x - x^2$	$-1 + x^2$

15	16
x^2	-1

Multiplication en AMNS

On considère 2 entiers A, B et leur représentation polynomiale $A(x), B(x)$ suivant l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$

Multiplication de $A(x) \times B(x)$ en 3 étapes :

- Multiplication polynomiale dans $\mathbb{Z}[x]$: $C(x) = A(x) \times B(x)$.
- Réduction du degrés : $C'(x) = C(x) \mod x^n - \lambda$.
- Réduction des coefficients de C' : $R = CoeffRed(C')$.

Multiplication en AMNS

On considère 2 entiers A, B et leur représentation polynomiale $A(x), B(x)$ suivant l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$

Multiplication de $A(x) \times B(x)$ en 3 étapes :

- Multiplication polynomiale dans $\mathbb{Z}[x]$: $C(x) = A(x) \times B(x)$.
- Réduction du degrés : $C'(x) = C(x) \mod x^n - \lambda$.
- Réduction des coefficients de C' : $R = CoeffRed(C')$.

En particulier,

$$|C'_j| \leq \sum_{i=1}^{n} ||A||.||B||.\lambda < n\rho^2\lambda$$

Les C'_i doivent être réduits tels que

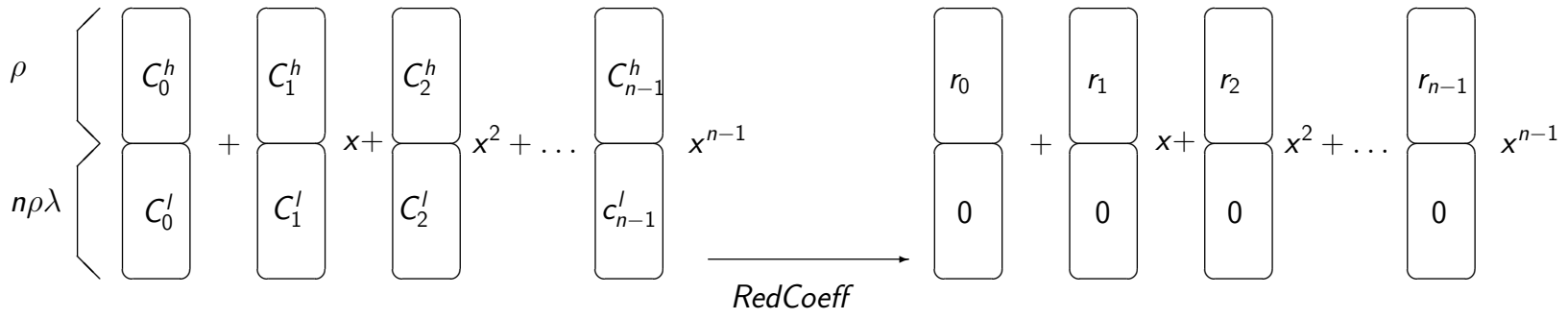
$$|R_i| < \rho \text{ et } R(\gamma) \equiv C'(\gamma) \mod p$$

Comment réduire efficacement les coefficients de C' ?

Comment réduire efficacement les coefficients de C' ?

Approche à la Montgomery

Ajouter un multiple de p pour éliminer la partie basse des coefficients



Réduction des coefficients *à la Montgomery*

Idée : ajouter un multiple de p

En AMNS, cela revient à ajouter un polynôme équivalent à p

$$AMNS(p) : \{M(x) \text{ tel que } M(\gamma) \equiv 0 \mod p\}$$

Réduction :

On suppose un polynôme $M(x)$ et un entier $m > 2n\rho|\lambda|$ tel que $M^{-1}(x) \mod m$ existe.

- $Q(x) = -C'(x)M^{-1}(x) \mod (x^n - \lambda, m)$
- $R(x) = C'(x) + Q(x)M(x) \mod x^n - \lambda$

Alors $R(X)$ est divisible par m et $R(\gamma) \equiv C'(\gamma) \mod p$

Réduction des coefficients *à la Montgomery*

Idée : ajouter un multiple de p

En AMNS, cela revient à ajouter un polynôme équivalent à p

$$AMNS(p) : \{M(x) \text{ tel que } M(\gamma) \equiv 0 \mod p\}$$

Réduction :

On suppose un polynôme $M(x)$ et un entier $m > 2n\rho|\lambda|$ tel que $M^{-1}(x) \mod m$ existe.

- $Q(x) = -C'(x)M^{-1}(x) \mod (x^n - \lambda, m)$
- $R(x) = C'(x) + Q(x)M(x) \mod x^n - \lambda$

Alors $R(X)$ est divisible par m et $R(\gamma) \equiv C'(\gamma) \mod p$

conséquence :

$$\text{si } \rho > 2n|\lambda|.||M|| \text{ alors } ||R.m^{-1}|| < \rho$$

Réduction des coefficients *à la Montgomery*

Idée : ajouter un multiple de p

En AMNS, cela revient à ajouter un polynôme équivalent à p

$$AMNS(p) : \{M(x) \text{ tel que } M(\gamma) \equiv 0 \mod p\}$$

Réduction :

On suppose un polynôme $M(x)$ et un entier $m > 2n\rho|\lambda|$ tel que $M^{-1}(x) \mod m$ existe.

- $Q(x) = -C'(x)M^{-1}(x) \mod (x^n - \lambda, m)$
- $R(x) = C'(x) + Q(x)M(x) \mod x^n - \lambda$

Alors $R(X)$ est divisible par m et $R(\gamma) \equiv C'(\gamma) \mod p$

conséquence :

$$\text{si } \rho > 2n|\lambda|.||M|| \text{ alors } ||R.m^{-1}|| < \rho$$

nécessite de connaître un $M(x)$ avec des petits coefficients

La théorie des réseaux à la rescousse

Objectif : trouver un polynôme $M(X)$ ayant des petits coefficients

Sous-ensemble de $\mathbb{Z}[x]$

$$M(X) \in \mathcal{L} = \{A(X) \in \mathbb{Z}[x] \text{ tels que } \deg A < n,\ A(\gamma) \equiv 0 \mod p\}$$

La théorie des réseaux à la rescousse

Objectif : trouver un polynôme $M(X)$ ayant des petits coefficients

Sous-ensemble de $\mathbb{Z}[x]$

$$M(X) \in \mathcal{L} = \{A(X) \in \mathbb{Z}[x] \text{ tels que } \deg A < n,\ A(\gamma) \equiv 0 \mod p\}$$

équivalent à un réseau dans $\mathbb{Z}^n$

- un polynôme est représenté par un vecteur ligne
- le réseau $\mathcal{L}$ contient le sous-réseau $\mathcal{L}'$ suivant

$$\mathcal{L}' = \begin{pmatrix} p & 0 & 0 & 0 & \dots & 0 \\ -\gamma & 1 & 0 & 0 & \dots & 0 \\ -\gamma^2 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ -\gamma^{n-2} & 0 & 0 & \dots & 1 & 0 \\ -\gamma^{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow p \\ \leftarrow x - \gamma \\ \leftarrow x^2 - \gamma^2 \\ \vdots \\ \leftarrow x^{n-2} - \gamma^{n-2} \\ \leftarrow x^{n-1} - \gamma^{n-1} \end{matrix} .$$

Polynôme le plus court

La théorie des réseaux nous dit qu'il existe un polynômes court $M(x)$ correspondant au vecteur le plus court du sous-réseau $\mathcal{L}'$.

- Le théorème de Minkowski [Minkovski 1896] propose une borne pour le vecteur le plus court :

$$||M(x)||_\infty \leq (det\mathcal{L}')^{1/n} = p^{1/n}$$

- Une approximation du vecteur court par le célèbre algorithme LLL [Lenstra, Lenstra, Lovász 1982] est suffisante pour $M(x)$ dans l'AMNS.

Contraintes pour la multiplication AMNS *à la Montgomery*

$$\begin{aligned} ||M|| &= \sigma \cong p^{1/n} \\ \rho &> 2n\sigma|\lambda| \\ m &> 2n\rho|\lambda| > 4n^2\sigma|\lambda|^2 \end{aligned}$$

Exemple d'AMNS (*polynôme court*)

Soit l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$ avec

$$p = 247\,649,\ n = 4,\ \gamma = 106\,581,\ \lambda = -1.$$

Nous construisons la base du sous-réseau $\mathcal{L}'$:

$$\vec{B} = \begin{pmatrix} p & 0 & 0 & 0 \\ -\gamma \mod p & 1 & 0 & 0 \\ -\gamma^2 \mod p & 0 & 1 & 0 \\ -\gamma^3 \mod p & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 247\,649 & 0 & 0 & 0 \\ 141\,068 & 1 & 0 & 0 \\ 150\,069 & 0 & 1 & 0 \\ 93\,424 & 0 & 0 & 1 \end{pmatrix}$$

Exemple d'AMNS (*polynôme court*)

Soit l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$ avec

$$p = 247\,649,\ n = 4,\ \gamma = 106\,581,\ \lambda = -1.$$

Nous construisons la base du sous-réseau $\mathcal{L}'$:

$$\vec{B} = \begin{pmatrix} p & 0 & 0 & 0 \\ -\gamma \mod p & 1 & 0 & 0 \\ -\gamma^2 \mod p & 0 & 1 & 0 \\ -\gamma^3 \mod p & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 247\,649 & 0 & 0 & 0 \\ 141\,068 & 1 & 0 & 0 \\ 150\,069 & 0 & 1 & 0 \\ 93\,424 & 0 & 0 & 1 \end{pmatrix}$$

Après une LLL-réduction nous obtenons

$$\vec{B'} = LLL(\vec{B}) = \begin{pmatrix} -8 & -5 & -17 & 11 \\ -5 & -17 & 11 & 8 \\ -17 & 11 & 8 & 5 \\ 11 & 8 & 5 & 17 \end{pmatrix}$$

Exemple d'AMNS (*polynôme court*)

Soit l'AMNS $\mathcal{B} = (p, n, \gamma, \rho)$ avec
$$p = 247\,649,\ n = 4,\ \gamma = 106\,581,\ \lambda = -1.$$

Nous construisons la base du sous-réseau $\mathcal{L}'$:

$$\vec{B} = \begin{pmatrix} p & 0 & 0 & 0 \\ -\gamma \mod p & 1 & 0 & 0 \\ -\gamma^2 \mod p & 0 & 1 & 0 \\ -\gamma^3 \mod p & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 247\,649 & 0 & 0 & 0 \\ 141\,068 & 1 & 0 & 0 \\ 150\,069 & 0 & 1 & 0 \\ 93\,424 & 0 & 0 & 1 \end{pmatrix}$$

Après une LLL-réduction nous obtenons

$$\vec{B'} = LLL(\vec{B}) = \begin{pmatrix} -8 & -5 & -17 & 11 \\ -5 & -17 & 11 & 8 \\ -17 & 11 & 8 & 5 \\ 11 & 8 & 5 & 17 \end{pmatrix}$$

En choisissant $M(x) = -8 - 5x - 17x^2 + 11x^3$ nous avons bien

$$M(\gamma) = 0 \mod p \quad \text{et } \|M\|_\infty = 17 \cong p^{1/n}.$$

On peut donc borner ρ par $\rho < 2 \times 4 \times 17 = 136$

Exemple d'AMNS (*multiplication*)

Rappel : $p = 247\,649,\ n = 4,\ \gamma = 106\,581,\ \lambda = -1, \rho = 136$

$$M(x) = -8 - 5x - 17x^2 + 11x^3$$

Soit 2 éléments A et B exprimé en AMNS $\mathcal{B}$

$$A(x) = 10 + 20x + 30x^2 + 40x^3, \qquad A(\gamma) \mod p = 8\,611$$
$$B(x) = 60 + 70x + 80x^2 + 90x^3, \qquad B(\gamma) \mod p = 157\,651$$
$$A(\gamma)B(\gamma) \mod p = 168\,592$$

On pose $m = 2^8$ et on calcule

$$M^{-1}(x) \mod (x^4 + 1, m) = 8 + 197x + 31x^2 + 85x^3$$

Exemple d'AMNS (*multiplication*)

Rappel : $p = 247\,649,\ n = 4,\ \gamma = 106\,581,\ \lambda = -1, \rho = 136$

$$M(x) = -8 - 5x - 17x^2 + 11x^3$$

Soit 2 éléments A et B exprimé en AMNS $\mathcal{B}$

$$A(x) = 10 + 20x + 30x^2 + 40x^3, \qquad A(\gamma) \mod p = 8\,611$$
$$B(x) = 60 + 70x + 80x^2 + 90x^3, \qquad B(\gamma) \mod p = 157\,651$$
$$A(\gamma)B(\gamma) \mod p = 168\,592$$

On pose $m = 2^8$ et on calcule

$$M^{-1}(x) \mod (x^4 + 1, m) = 8 + 197x + 31x^2 + 85x^3$$

Multiplication *à la Montgomery*

- $C = AB \mod (x^4 + 1) = -5\,800 - 5\,000x - 200x^2 + 6\,300x^3$
- $Q = -CM^{-1} \mod (x^4 + 1, m) = 236 + 4x + 12x^2 + 72x^3$
- $R = C + QM \mod (x^4 + 1) \times m^{-1} = -28 - 20x - 20x^2 + 32x^3$

$$R(\gamma) \times 256 \mod p = 168\,592$$

Limiter le grossissement des coefficients dans les calculs

On remarque que $C(x) = A(x)B(x) \mod x^n - \lambda$ à des grand coefficients ($\cong n\rho^2|\lambda|$) comparer au modulo m ($\cong 2n\rho|\lambda|$).

De même, le calcul de $R(x)$ nécessite le calcul de grand coefficients ($\cong n\rho^2|\lambda|$)

Multiplication *à la Montgomery* modifiée

choisir deux moduli $m1$ et $m2$ tel que $gcd(m1, m2) = 1$

$$m2 < 2n\rho|\lambda| \text{ et } m1 < \rho$$

- $Q(x) = -A(x)B(x)M^{-1}(x) \mod (x^n - \lambda, m2)$
- $R(X) = (A(x)B(x) + Q(x)M(x)) \times m_2^{-1} \mod (x^n - \lambda, m1)$

Plan de l'exposé

I. multiplication modulaire (*pseudo-Mersenne, Montgomery*)

II. représentation *AMNS* et multiplication

III. multiplication rapide en *AMNS*

IV. conclusion et perspectives

Multiplication rapide à base de FFT

Motivations

- Utiliser des algorithmes de multiplication sous-quadratique (e.g. quasi-linéaire avec FFT).
- Limiter le grossissement des degrés durant les calculs.

Idée :

Utiliser une représentation de Lagrange des polynômes
$\hookrightarrow$ évaluation multi-points

intérêts : multiplication linéaire en le nombre de points

Représentation de la Lagrange

Base de Lagrange

La représentation de Lagrange d' un polynôme $A \in \mathbb{Z}/m\mathbb{Z}[x]$ de degré $\leq n$ en n points distincts notés $\{\alpha_i\}_{i=1}^{n}$ est définie par

$$A_{Lag,\alpha_i} = [A(\alpha_1) \mod m, \ldots, A(\alpha_n) \mod m]$$

Motivation pour l'*AMNS*

- choisir m tels que $x^n - \lambda$ se scinde totalement modulo m

$$x^n - \lambda = \prod_{i=1}^{n}(x - \mu\omega^i) \mod m,$$

$$\text{avec } \mu^n = \lambda \mod m \text{ et } \omega^n = 1 \mod m$$

- représentation de Lagrange en racine nième de l'unité

$$A_{Lag,\mu\omega^i} = \widehat{A}_{Lag,\omega^i} \text{ avec } \widehat{A} = \sum_{i=0}^{n} a_i \mu^i x^i$$

Représentation de la Lagrange

Base de Lagrange

La représentation de Lagrange d' un polynôme $A \in \mathbb{Z}/m\mathbb{Z}[x]$ de degré $\leq n$ en n points distincts notés $\{\alpha_i\}_{i=1}^{n}$ est définie par

$$A_{Lag,\alpha_i} = [A(\alpha_1) \mod m, \ldots, A(\alpha_n) \mod m]$$

Motivation pour l'*AMNS*

- choisir m tels que $x^n - \lambda$ se scinde totalement modulo m

$$x^n - \lambda = \prod_{i=1}^{n}(x - \mu\omega^i) \mod m,$$

$$\text{avec } \mu^n = \lambda \mod m \text{ et } \omega^n = 1 \mod m$$

- représentation de Lagrange en racine nième de l'unité

$$A_{Lag,\mu\omega^i} = \widehat{A}_{Lag,\omega^i} \text{ avec } \widehat{A} = \sum_{i=0}^{n} a_i \mu^i x^i$$

<u>double intérêts</u> :

évaluation/interpolation rapide avec FFT

réduction modulo $x^n - \lambda$ intégrée à la base de Lagrange

Multiplication AMNS en base de Lagrange

On note $A_{Lag(m)}$ la représentation de Lagrange relative au modulo m d'un élément A appartenant à l'AMNS.

Multiplication en base de Lagrange

Entrées : $A_{Lag(m_1)}, A_{Lag(m_2)}, B_{Lag(m_1)}, B_{Lag(m_2)}$
Sorties : $(ABm_2^{-1})_{Lag(m_1)}, (ABm_2^{-1})_{Lag(m_2)}$
Données : $M_{Lag(m_1)}, M^{-1}_{Lag(m_2)}$

- $Q_{Lag(m_2)} = A_{Lag(m_2)} B_{Lag(m_2)} M^{-1}_{Lag(m_2)}$
- $Q_{Lag(m_1)} = \ conversion(Q_{Lag(m_2)})$
- $R_{Lag(m_1)} = (A_{Lag(m_1)} B_{Lag(m_1)} + Q_{Lag(m_1)} M_{Lag(m_1)}) m_2^{-1}$
- $R_{Lag(m_2)} = \ conversion(R_{Lag(m_1)})$

Nombre de FFT dans la multiplication modulaire

Soit p le modulo tel que $k = \log p$ représente le nombre de bits de p.

Approche classique de Montgomery avec multiplication rapide

On utilise ici l'approche de Montgomery classique avec la multiplication quasi-linéaire de Schonäge-Strassen. L'algorithme nécessite 3 multiplications d'entiers de k bits.

La multiplication d'entiers de taille k avec Schonäge-Strassen nécessite : 3 FFT d'ordre $2\sqrt{k}$ avec des entiers de taille $\cong 2\sqrt{k}$

soit un total de 9 FFT d'ordre $2\sqrt{k}$ avec des entiers de taille $\cong 2\sqrt{k}$.

Nombre de FFT dans la multiplication modulaire

Soit p le modulo tel que $k = \log p$ représente le nombre de bits de p.

Approche classique de Montgomery avec multiplication rapide

On utilise ici l'approche de Montgomery classique avec la multiplication quasi-linéaire de Schonäge-Strassen. L'algorithme nécessite 3 multiplications d'entiers de k bits.

La multiplication d'entiers de taille k avec Schonäge-Strassen nécessite :
3 FFT d'ordre $2\sqrt{k}$ avec des entiers de taille $\cong 2\sqrt{k}$

soit un total de 9 FFT d'ordre $2\sqrt{k}$ avec des entiers de taille $\cong 2\sqrt{k}$.

Approche *AMNS* en base de Lagrange (on fixe $n = \sqrt{k}$)

La multiplication *AMNS* en base de Lagrange nécessite :
4 FFT d'ordre $\sqrt{k}$ avec des entiers de taille $\cong \sqrt{k} + O(\log k)$.

Quelques considérations sur une implantation efficace

Malheureusement, la théorie n'est pas totalement corrélée par les implantations !

Une première approche (exponentiation modulaire)

- GMP est malheureusement souvent le meilleur,
- l'*AMNS* semble intéressant pour des grands corps (e.g $> 5\,000$ bits),
- l'approche *AMNS* en représentation monomiale n'est pas compétitive, même pour des petit corps (e.g. $< 1\,000$ bits)

Quelques considérations sur une implantation efficace

Malheureusement, la théorie n'est pas totalement corrélée par les implantations !

Une première approche (exponentiation modulaire)

- GMP est malheureusement souvent le meilleur,
- l'*AMNS* semble intéressant pour des grands corps (e.g $> 5\,000$ bits),
- l'approche *AMNS* en représentation monomiale n'est pas compétitive, même pour des petit corps (e.g. $< 1\,000$ bits)

Difficultés à surmonter :

- gérer le facteur de redondance de l'*AMNS*
- maximiser les opérations machines (m_1, m_2 pas toujours $< 2^{32}$)
- le degrés des polynômes dans l'AMNS ne doit pas être trop grand (Pb avec LLL, $max = 256$)

Plan de l'exposé

I. multiplication modulaire (*pseudo-Mersenne, Montgomery*)

II. représentation *AMNS* et multiplication

III. multiplication rapide en *AMNS*

IV. conclusion et perspectives

Conclusion & Perspectives

La représentation *AMNS*

- permet de se ramener à une arithmétique polynomiale $\mod x^n - \lambda$,
- améliore la multiplication modulaire pour des modulis quelconques,
- est très proche de la théorie des réseaux,
- offre des caractéristiques parallèles intéressantes pour le matériel,
- n'est pas encore satisfaisante au niveau pratique sur des tailles « cryptographiques »

Perspectives :

- Optimiser les implantations (mot machine, découpage, FFT).
- Autres algorithmes sous-quadratique (Karatsuba, Toom-Cook).
- Généraliser l'approche au cas des extensions (i.e. $\mathtt{GF}(2^n), \mathtt{GF}(p^n)$).
- Approche complexe (*stabilité numérique, mesure d'erreurs*).