

Arithmétique modulaire pour la cryptographie

Thomas PLANTARD

Projet ARITH
LIRMM — Université Montpellier II — UMR 5506
106 rue Ada
34592 Montpellier — Cedex 5

web : <http://www.lirmm.fr/~plantard/>
email : plantard@lirmm.fr

Le 15 décembre 2005

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

La cryptographie à clé privée

Alice

m 1010100010011

Bob

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

La cryptographie à clé privée

Alice

m 1010100010011
 k 0110110101001

Bob

k 0110110101001

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

La cryptographie à clé privée

Alice

m	1010100010011
k	0110110101001
$c = m \otimes k$	11000101111010

Bob

k	0110110101001
-----	---------------

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

La cryptographie à clé privée

Alice

m	1010100010011
k	0110110101001
$c = m \otimes k$	1100010111010

Bob

c	1100010111010
k	0110110101001

La cryptographie à clé privée

Alice

m	1010100010011
k	0110110101001
$c = m \otimes k$	1100010111010

Bob

c	1100010111010
k	0110110101001
$m = c \otimes k$	1010100010011

La cryptographie à clé privée

Alice

m	1010100010011
k	0110110101001
$c = m \otimes k$	1100010111010

Bob

c	1100010111010
k	0110110101001
$m = c \otimes k$	1010100010011

La cryptographie à clé publique

Clé publique : g, p

Alice

Clé privée : a

- ① Alice calcule $g^a \bmod p$
- ② Alice envoie à Bob g^a
- ③ Alice calcule $k = (g^b)^a \bmod p$

Clé commune $k = g^{ab} \bmod p$

Bob

Clé privée : b

- ① Bob calcule $g^b \bmod p$
- ② Bob envoie à Alice g^b
- ③ Bob calcule $k = (g^a)^b \bmod p$

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Plan du mémoire

- 1 Besoins arithmétiques en cryptographie
- 2 État de l'art sur l'arithmétique modulaire
- 3 Systèmes de représentation adaptés
- 4 Arithmétique modulaire pour de petits moduli

Arithmétique modulaire

- Introduction
- Présentation**
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

- 1 Introduction**
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide**
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation**
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli**
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 Cas général**
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 Conclusion**

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits ...

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits ...

RSA, Rivest, Shamir et Adleman (1978)

- Une exponentiation sur l'anneau $\mathbb{Z}/n\mathbb{Z}$
- Opération : Multiplication modulo n (composé)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits ...

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits ...

RSA, Rivest, Shamir et Adleman (1978)

- Une exponentiation sur l'anneau $\mathbb{Z}/n\mathbb{Z}$
- Opération : Multiplication modulo n (composé)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits ...

ECC, Koblitz et Miller (1985)

- Une exponentiation sur le groupe des points d'une courbe elliptique
- Opération : Inversion, Addition, Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 160 bits, $2^{112} \Rightarrow$ 224 bits ...

Multiplication Modulaire

- Entrée : a, b et p tel que $0 \leq a, b < p < 2^n$
- Sortie : $r = ab + qp$ tel que $0 \leq r, q < p$

Multiplications modulaires généralistes

- Taylor, 1981 : Mémorisation de la mise au carré modulaire.
- Blakley, 1983 : "Double and Add" avec réduction à chaque étape.
- Montgomery, 1985 : Division par une puissance de la base.
- Barrett, 1986 : Approximation du quotient de la division.
- Takagi, 1992 : "Double and Add" en représentation redondante.

Moduli particuliers

- Trouver des moduli pour les tailles supérieures à 160 bits.
- Avec une réduction modulaire très efficace.

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 **Classes de moduli à réduction rapide**
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 Conclusion

Les nombres de Mersenne

- Nombre premier p de la forme $p = 2^n - 1$

Réduction

- $2^n \equiv 1 \pmod{p}$
- $a = a_1 2^n + a_0$
- $a \equiv a_1 + a_0 \pmod{p}$

$$p = 31 = 2^5 - 1, a = 273$$

- $2^5 \equiv 1 \pmod{31}$
- $a = 8 \times 2^5 + 17$
- $a \equiv 8 + 17 = 25 \pmod{31}$
- Coût = Deux Additions de n bits

Si $p = \beta^n - 1$ premier alors $\beta = 2$

- $\beta^n - 1 = (\beta - 1)(\beta^{n-1} + \dots + 1)$
- Si $\beta > 2$ alors $(\beta - 1) > 1$ divise p

n premier

- Si n pas premier alors $n = uv$ avec $u, v \geq 2$
- $p = 2^n - 1 = 2^{uv} - 1 = (2^u)^v - 1 = \beta^v - 1$ alors p pas premier

Les nombres de Mersenne pour la cryptographie

- Impossible pour les tailles cryptographiques 160, 192, 224, ...
- $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607$
- Le *NIST* et le *SEC* conseillent le nombre de Mersenne $2^{521} - 1$

Les Pseudo nombres de Mersenne

- Nombre premier p
- $p = 2^n - c$ avec $c < 2^{\frac{n}{2}}$

Exemple

- $n = 10$
- $c = 3$
- $p = 1021$

Réduction

- 1 $a = a_1 2^n + a_0$
- 2 $a \leftarrow a_1 c + a_0$
- 3 $a = a_1 2^n + a_0$
- 4 $a \leftarrow a_1 c + a_0$

Le coût

- 2 Multiplications de $\frac{n}{2}$ bits
- 4 Additions de $\frac{n}{2}$ bits

Les Pseudo nombres de Mersenne premiers

n	160	192	224	256	288	320
$ c _2$	6	8	6	8	8	8
	352	384	416	448	480	512
	10	9	9	8	6	10

Les Pseudo nombres de Mersenne pour ECC

- ① $secp_{160k1} = 2^{160} - (2^{32} + 2^{14} + 2^{12} + 2^9 + 2^8 + 2^7 + 2^3 + 2^2 + 1)$
- ② $secp_{192k1} = 2^{192} - (2^{32} + 2^{12} + 2^8 + 2^7 + 2^6 + 2^3 + 1)$
- ③ $secp_{224k1} = 2^{224} - (2^{32} + 2^{12} + 2^{11} + 2^9 + 2^7 + 2^4 + 2 + 1)$
- ④ $secp_{256k1} = 2^{256} - (2^{32} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 1)$

Les nombres de Mersenne Généralisés

- Nombre p premier de la forme $p = P(2^k)$
- $P(X) = X^d - C(X)$ avec $Deg(C) \leq \frac{d}{2}$ et $C_i \in \{-1, 0, 1\}$

Un nombre de Mersenne Généralisé

- $P(X) = X^3 - X - 1$
- $P(2^3) = 8^3 - 8 - 1 = 503$

Coût

- $2d$ Additions de k bits

Les nombres de Mersenne Généralisés

- Nombre p premier de la forme $p = P(2^k)$
- $P(X) = X^d - C(X)$ avec $Deg(C) \leq \frac{d}{2}$ et $C_i \in \{-1, 0, 1\}$

Un nombre de Mersenne Généralisé

- $P(X) = X^3 - X - 1$
- $P(2^3) = 8^3 - 8 - 1 = 503$

Coût

- $2d$ Additions de k bits

Réduction

- 1 $A = A_1 X^d + A_0$
- 2 $A \leftarrow A_1 C + A_0$
- 3 $A = A_1 X^d + A_0$
- 4 $A \leftarrow A_1 C + A_0$

Le nombre de nombres de Mersenne Généralisés avec $k = 32$

n	160	192	224	256	288	320
#MG	0	1	1	0	0	1
	352	384	416	448	480	512
	3	2	8	8	13	22

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation**
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Le nombre de nombres de Mersenne Généralisés avec $k = 32$

n	160	192	224	256	288	320
#MG	0	1	1	0	0	1
	352	384	416	448	480	512
	3	2	8	8	13	22

Les nombres de Mersenne Généralisés pour ECC

- ① sec_{192r1} $P(X) = X^3 - (X + 1)$ en 2^{64}
- ② sec_{224r1} $P(X) = X^7 - (X^3 + 1)$ en 2^{32}
- ③ sec_{256r1} $P(X) = X^8 - (X^7 - X^6 - X^3 + 1)$ en 2^{32}
- ④ sec_{384r1} $P(X) = X^{12} - (X^4 + X^3 - X + 1)$ en 2^{32}

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation**
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 **Système de représentation**
 - **Système de représentation modulaire**
 - **Système de représentation adapté**
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 Conclusion

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire**
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Représentation classique en base β

$$a = \sum_{i=0}^{n-1} a_i \beta^i \text{ with } a_i \in \{0, \dots, \beta - 1\}$$

Exemple : $A = 1315 = [2, 4, 4, 3]_8$ $A = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire**
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Représentation classique en base β

$$a = \sum_{i=0}^{n-1} a_i \beta^i \text{ with } a_i \in \{0, \dots, \beta - 1\}$$

Exemple : $A = 1315 = [2, 4, 4, 3]_8$ $A = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$

Représentation modulaire $\mathcal{B} = (p, n, \gamma, \rho)$

$$a = \sum_{i=0}^{n-1} a_i \gamma^i \pmod{p} \text{ with } a_i \in \{0, \dots, \rho - 1\}$$

Forme polynomiale

Le polynôme $A[X]$ représente a dans $\mathcal{B} = (p, n, \gamma, \rho)$ si

- $A[\gamma] \equiv a \pmod{p}$
- $\text{Deg}(A) \leq n$
- $\|A\|_\infty < \rho$

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
6	7	8	9	10	11
12	13	14	15	16	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
6	7	8	9	10	11
	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
12	13	14	15	16	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
6	7	8	9	10	11
	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
12	13	14	15	16	
		[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			[1, 1, 0]
6	7	8	9	10	11
[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
12	13	14	15	16	
[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]	[2, 1, 1]	[2, 1, 2]	[1, 1, 0]
6	7	8	9	10	11
[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]	[2, 2, 0]	[2, 2, 1]
12	13	14	15	16	
[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^2 a_i 7^i \pmod{17}$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \pmod{17} = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]	[2, 1, 1]	[2, 1, 2]	[1, 1, 0]
6	7	8	9	10	11
[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]	[2, 2, 0]	[2, 2, 1]
12	13	14	15	16	
[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Question

- Si p, n et γ sont fixés, comment déterminer ρ_{min} ?
- Si p et n sont fixés, comment "bien" choisir γ ?

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté**
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Définition d'un système de représentation adapté

Un système de représentation modulaire $\mathcal{B} = (\gamma, \rho, n, p)$ sera dit *adapté* si

$$\gamma^n \bmod p = c$$

avec c “petit”.

Définition d'un système de représentation adapté

Un système de représentation modulaire $\mathcal{B} = (\gamma, \rho, n, p)$ sera dit *adapté* si

$$\gamma^n \bmod p = c$$

avec c “petit”.

Multiplication Modulaire dans \mathcal{B}

- 1 Multiplication polynomiale dans $\mathbb{Z}[X]$: $U(X) \leftarrow A(X) B(X)$
- 2 Réduction polynomiale : $V(X) \leftarrow U(X) \bmod (X^n - c)$
- 3 Réduction des coefficients : $S \leftarrow CR(V)$, avec $S \equiv V(\gamma) \pmod{P}$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté**
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Un système de représentation adapté

- $p = 250043 \Rightarrow |p|_2 = 18$
- $n = 3, \rho = 128$
- $\gamma = 127006$ tel que $c = 2 = \gamma^3 \pmod p$

Entrée

- $A = 7 + 30X + 100X^2 \Rightarrow A = 65842$
- $B = 59 + 2X + 76X^2 \Rightarrow B = 8816$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté**
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Un système de représentation adapté

- $p = 250043 \Rightarrow |p|_2 = 18$
- $n = 3, \rho = 128$
- $\gamma = 127006$ tel que $c = 2 = \gamma^3 \pmod p$

Entrée

- $A = 7 + 30X + 100X^2 \Rightarrow A = 65842$
- $B = 59 + 2X + 76X^2 \Rightarrow B = 8816$

Multiplication Modulaire dans \mathcal{B}

- ① $U(X) = A(X) \times B(X)$
 $U(X) = 413 + 1784X + 6492X^2 + 2480X^3 + 7600X^4$
- ② $V(X) = U(X) \pmod{(X^3 - 2)} \leftarrow 5373 + 16984X + 6492X^2$
- ③ $S(X) = ?$

Un système de représentation adapté

- $p = 250043 \Rightarrow |p|_2 = 18$
- $n = 3, \rho = 128$
- $\gamma = 127006$ tel que $c = 2 = \gamma^3 \pmod p$

Entrée

- $A = 7 + 30X + 100X^2 \Rightarrow A = 65842$
- $B = 59 + 2X + 76X^2 \Rightarrow B = 8816$

Multiplication Modulaire dans \mathcal{B}

- 1 $U(X) = A(X) \times B(X)$
 $U(X) = 413 + 1784X + 6492X^2 + 2480X^3 + 7600X^4$
- 2 $V(X) = U(X) \pmod{(X^3 - 2)} \leftarrow 5373 + 16984X + 6492X^2$
- 3 $S(X) = ?$

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Entrée

- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$

Entrée

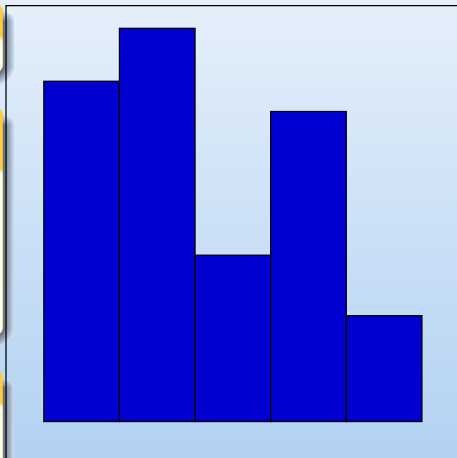
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

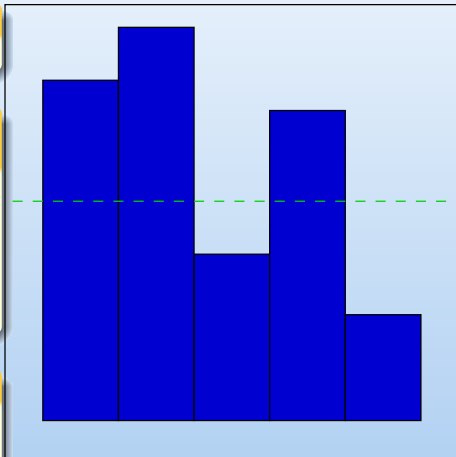
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

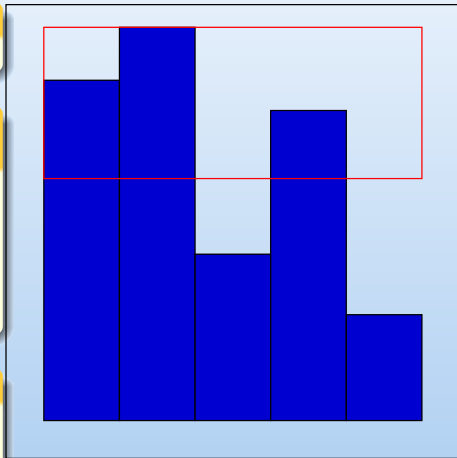
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

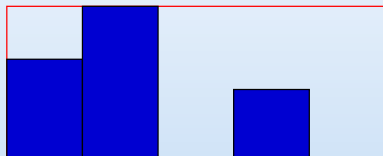
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

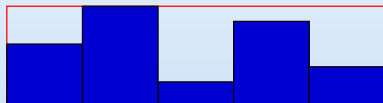
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow \text{RED}(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

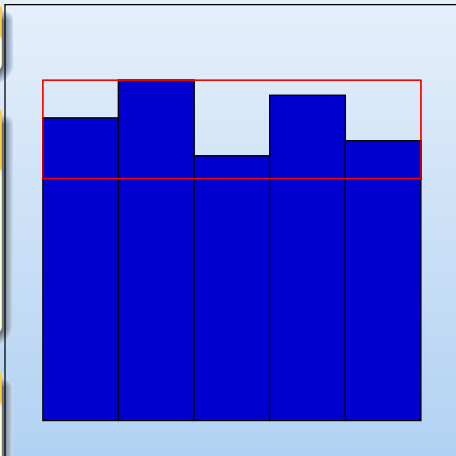
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow \text{RED}(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

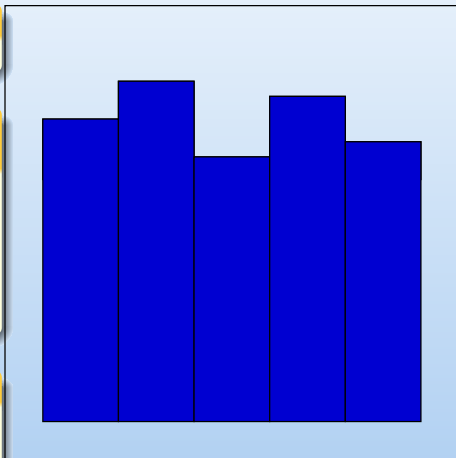
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Arithmétique modulaire

Introduction
 Présentation
 Contexte
 Multiplication
 Classes de moduli
 Mersenne
 Pseudo Mersenne
 Généralisation
 Représentation
 Modulaire
Adapté
 Nouvelle classe
 RED
 Propriété
 Construction
 Cas général
 Réseaux Euclidiens
 Théorème
 Conclusion

Entrée

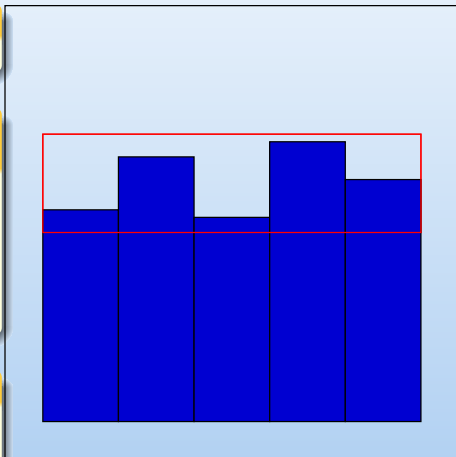
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow \text{RED}(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

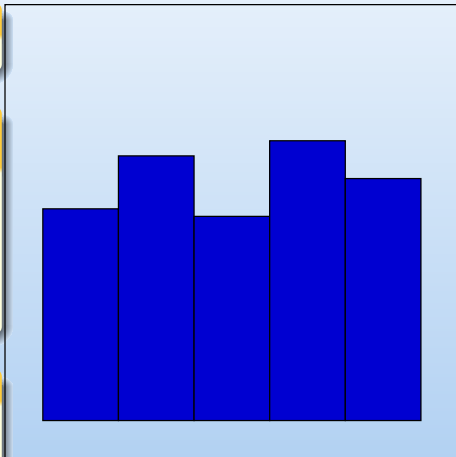
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle

Entrée

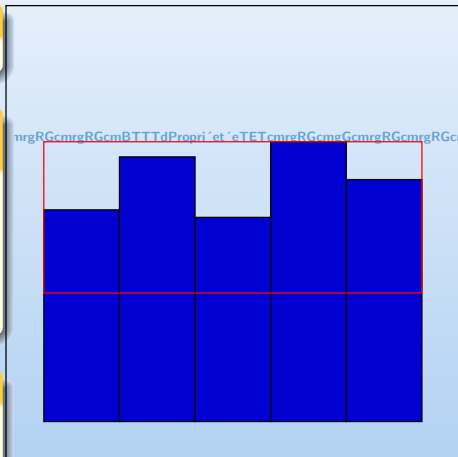
- Un vecteur V

Réduction des coefficients

- $S \leftarrow V$
- WLE $\rho \geq s_i$ DO
 - ① $t \leftarrow |S|_2$
 - ② $S = S_1 2^{t-k_1} + S_0$
 - ③ $S_1 \leftarrow RED(S_1)$
 - ④ $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

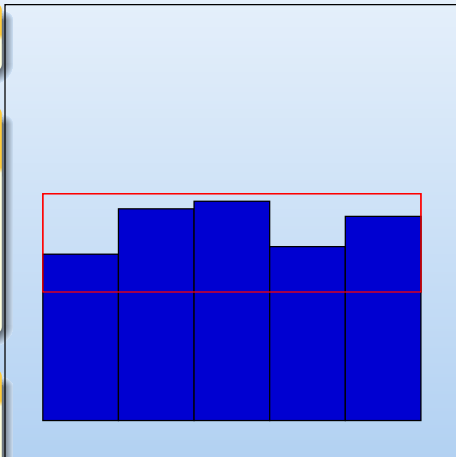
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow \text{RED}(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Arithmétique modulaire

Introduction
 Présentation
 Contexte
 Multiplication
 Classes de moduli
 Mersenne
 Pseudo Mersenne
 Généralisation
 Représentation
 Modulaire
Adapté
 Nouvelle classe
 RED
 Propriété
 Construction
 Cas général
 Réseaux Euclidiens
 Théorème
 Conclusion

Entrée

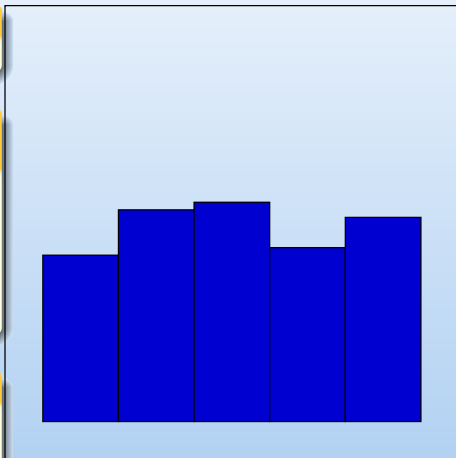
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Entrée

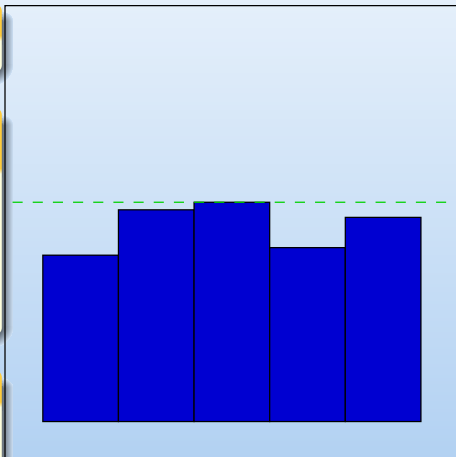
- Un vecteur V

Réduction des coefficients

- 1 $S \leftarrow V$
- 2 WHILE $\rho \geq s_i$ DO
 - 1 $t \leftarrow |S|_2$
 - 2 $S = S_1 2^{t-k_1} + S_0$
 - 3 $S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

Sortie

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Problématique

- Entrée : Un vecteur V avec $v_i < 2^{k_1}$
- Sortie : Un vecteur S avec $s_i < 2^{k_0}$ ($k_0 < k_1$)
- Avec $V \equiv S$ dans \mathcal{B} : $V(\gamma) \equiv S(\gamma) \pmod{p}$

Méthodes possibles

- 1 Particulière : Classe de moduli avec une réduction efficace.
- 2 Généralisation : Classe de moduli avec une réduction efficace.

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation Modulaire
- Adapté
- Nouvelle classe**
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 **Une nouvelle classe de moduli**
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 Conclusion

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED**
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Entrée

- Un vecteur V avec $v_i < 2^{k_1}$ et $k_1 = k + t$

Algorithme *RED*

- ① $V = \overline{V}2^k + \underline{V} \iff V = \overline{V}2^k Id + \underline{V}$
- ② $S \leftarrow \overline{V}M + \underline{V}$, où $M \equiv 2^k Id$ dans \mathcal{B}

Sortie

- Un vecteur $S \equiv V$ dans \mathcal{B}
- Avec $s_i < 2^{k_0}$ et $k_0 = k + 1$

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1}\gamma^{n-1} + \xi_{n-2}\gamma^{n-2} \cdots + \xi_1\gamma + \xi_0 \pmod{p}$
- $\gamma^n \equiv c \pmod{p}$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété**
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1}\gamma^{n-1} + \xi_{n-2}\gamma^{n-2} \cdots + \xi_1\gamma + \xi_0 \pmod{p}$
- $\gamma^n \equiv c \pmod{p}$

Construction de M

$$\begin{pmatrix} 2^k & 0 & \cdots & 0 & 0 \\ 0 & 2^k & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 2^k & 0 \\ 0 & 0 & \cdots & 0 & 2^k \end{pmatrix} \equiv \begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{pmatrix} \quad (1)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété**
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".

$$2^k \equiv \xi_{n-1}\gamma^{n-1} + \xi_{n-2}\gamma^{n-2} \cdots + \xi_1\gamma + \xi_0 \pmod{p}$$

$$\gamma^n \equiv c \pmod{p}$$

Construction de M

$$\begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ 0 & 0 & \cdots & 0 & 2^k \end{pmatrix} \equiv \begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_1 & \xi_0 \end{pmatrix} \quad (1)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété**
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1}\gamma^{n-1} + \xi_{n-2}\gamma^{n-2} \cdots + \xi_1\gamma + \xi_0 \pmod{p}$
- $\gamma^n \equiv c \pmod{p}$

Construction de M

$$\begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ 0 & 0 & \cdots & 2^k & 0 \\ 0 & 0 & \cdots & 0 & 2^k \end{pmatrix} \equiv \begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ \xi_{n-2} & \xi_{n-3} & \cdots & \xi_0 & c\xi_{n-1} \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_1 & \xi_0 \end{pmatrix} \quad (1)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété**
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1}\gamma^{n-1} + \xi_{n-2}\gamma^{n-2} \cdots + \xi_1\gamma + \xi_0 \pmod{p}$
- $\gamma^n \equiv c \pmod{p}$

Construction de M

$$\begin{pmatrix} 2^k & 0 & \cdots & 0 & 0 \\ 0 & 2^k & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 2^k & 0 \\ 0 & 0 & \cdots & 0 & 2^k \end{pmatrix} \equiv \begin{pmatrix} \xi_0 & c\xi_{n-1} & \cdots & c\xi_2 & c\xi_1 \\ \xi_1 & \xi_0 & \cdots & c\xi_3 & c\xi_2 \\ \vdots & & & & \vdots \\ \xi_{n-2} & \xi_{n-3} & \cdots & \xi_0 & c\xi_{n-1} \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_1 & \xi_0 \end{pmatrix} \quad (1)$$

Entrée

- $\mathcal{B} = (p = 250043, n = 3, \gamma = 127006, \rho = 128)$ avec $\gamma^n \equiv 2$
- $\gamma^3 = 2 \pmod p$ et $2^6 = 1 + \gamma^2 \pmod p$

$$\begin{pmatrix} 2^6 & 0 & 0 \\ 0 & 2^6 & 0 \\ 0 & 0 & 2^6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \quad (2)$$

- Un vecteur $V = [22, 444, 120]$ avec $V_i < 2^9$

RED

- 1 $V = [0, 6, 1]2^6 + [22, 60, 56]$
- 2 $S \leftarrow [0, 6, 1]M + [22, 60, 56] = [12, 8, 1] + [22, 60, 56]$

Sortie

$$S = [57, 68, 34] \text{ avec } S_i < 2^{k+1} = 2^7 = 128$$

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Entrée

- $\mathcal{B} = (\gamma = 127006, \rho = 128, n = 3, P = 250043)$ avec $\gamma^n \equiv 2$
- $V = [6492, 16984, 5373]$

Étape

- 1 $S = [2524, 984, 1853]$
- 2 $S = [532, 544, 357]$
- 3 $S = [32, 56, 121]$

Sortie

$S = [32, 56, 121]$ avec $s_i < 128$

Un système de représentation adapté : $\mathcal{B} = (p, n, \gamma, \rho)$

- ① Le modulo p
- ② Le nombre de chiffres n
- ③ La base γ
- ④ Le majorant des chiffres ρ

Création d'un modulo p et du système \mathcal{B} correspondant

- En fonction de la taille des chiffres (32, 64...), nous déduisons n .
- Nous voulons $c = -2, -1, 2$.
- Nous voulons $\|\xi\|_\infty = 1, 2$.
- Construire M avec ξ et c .
- Nous savons que $p \mid \det(2^k Id - M)$
- Nous en déduisons p tel que p premier et $p \sim 2^{kn}$
- Calculer γ racine $\gcd(X^n - c, 2^k - \xi(X)) \bmod p$

Exemple

- Taille des chiffres, 32 bits et taille du modulo, 256 bits $\Rightarrow n = 8$
- $c = 2$
- $\xi = [0, 0, 1, 0, 0, 0, 0, 1]$ ($\xi(X) = X^5 + 1$)
- $p = 115792089021636622262124715160334756877804245386980633020041035952359812890593$
 p est premier et $p \sim 2^{256}$
- γ racine $\gcd(X^8 - 2, 2^{32} - X^5 - 1) \pmod{p}$
 $\gamma = 14474011127704577782765589395224532314179217058921488395049827733759590399996$

Exemple

- Taille des chiffres, 32 bits et taille du modulo, 256 bits $\Rightarrow n = 8$
- $c = 2$
- $\xi = [0, 0, 1, 0, 0, 0, 0, 1]$ ($\xi(X) = X^5 + 1$)
- $p = 115792089021636622262124715160334756877804245386980633020041035952359812890593$
 p est premier et $p \sim 2^{256}$
- γ racine $\gcd(X^8 - 2, 2^{32} - X^5 - 1) \pmod{p}$
 $\gamma = 14474011127704577782765589395224532314179217058921488395049827733759590399996$

Propriété de la classe

- ① Généralisation : elle contient les classes de la "famille des nombres de Mersenne".
- ② Bonne densité : elle contient de nouveau moduli.
- ③ Grande efficacité : coût inférieur et parallélisation.

Proposition pour la cryptographie

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Moduli				Coût en additions k bits			
\mathcal{B}	$ p $	n	k	RedExt	RedInt	Total	Gain
\mathcal{B}_{128}	128	4	32	6	8	14	-26%
\mathcal{B}_{160}	160	5	32	8	10	18	-10%
\mathcal{B}_{192_a}	192	6	32	10	12 + 6	28	+17%
\mathcal{B}_{192_b}	192	6	32	10	12	22	-8%
\mathcal{B}_{224}	224	7	32	12	14	26	-11,5%
\mathcal{B}_{256}	256	8	32	14	16	30	-50%
\mathcal{B}_{288_a}	288	9	32	36	14	50	
\mathcal{B}_{288_b}	288	9	32	16	18	34	
\mathcal{B}_{320_a}	320	10	32	36	11	47	
\mathcal{B}_{320_b}	320	10	32	18	20	38	
\mathcal{B}_{352}	352	11	32	20	22	42	
\mathcal{B}_{384_a}	384	12	32	54	19	73	-13%
\mathcal{B}_{384_b}	384	12	32	22	24	46	-45%
\mathcal{B}_{384_c}	384	12	32	22	24	46	-45%
\mathcal{B}_{416}	416	13	32	24	26	50	
\mathcal{B}_{448_a}	448	14	32	26	28	54	
\mathcal{B}_{448_b}	448	14	32	26	28	54	
\mathcal{B}_{480_a}	480	15	32	28	30	58	
\mathcal{B}_{480_b}	480	15	32	56	16	78	
\mathcal{B}_{512}	512	16	32	30	32	62	

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général**
- Réseaux Euclidiens
- Théorème
- Conclusion

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 **Cas général**
 - **Les Réseaux Euclidiens**
 - **Théorème fondamental**
- 6 Conclusion

Définition d'un réseau euclidien

- Un réseau \mathcal{L} est l'ensemble des combinaisons linéaires entières de d vecteurs \mathbf{b}_i indépendants de \mathbb{R}^n avec $d \leq n$:

$$\mathcal{L} = \mathbb{Z} \mathbf{b}_1 + \cdots + \mathbb{Z} \mathbf{b}_d = \{ \lambda_1 \mathbf{b}_1 + \cdots + \lambda_d \mathbf{b}_d : \lambda_i \in \mathbb{Z} \}$$

- d est la dimension.
- $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_d)$ est une *base*.

"SVP" : Le problème du plus court vecteur

- NP-Dur
- Approximation de SVP par LLL (Lenstra, Lenstra, Lovasz), 1982

"CVP" : Le problème du plus proche vecteur

- NP-Dur
- Approximation de CVP par Babai, 1986

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

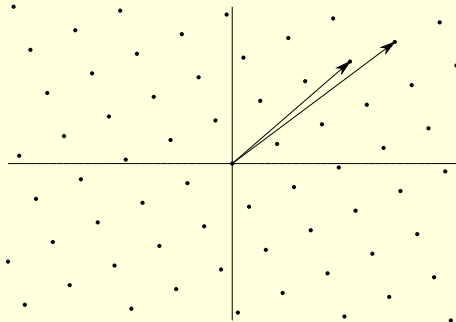
Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

$$\mathcal{B} = \begin{pmatrix} 29 & 31 \\ 21 & 26 \end{pmatrix} \quad (3)$$

"SVP" : Le problème du plus court vecteur



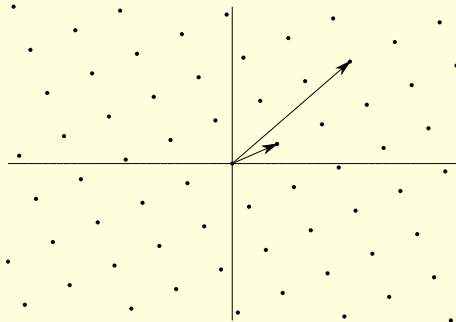
Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 21 & 26 \end{pmatrix} \quad (4)$$

"SVP" : Le problème du plus court vecteur



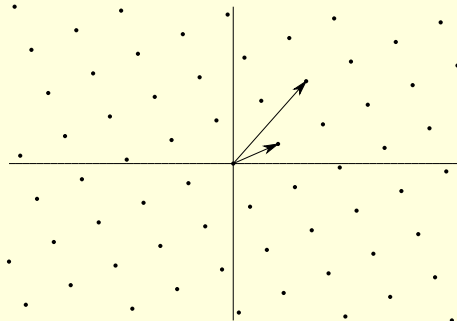
Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 13 & 21 \end{pmatrix} \quad (5)$$

"SVP" : Le problème du plus court vecteur



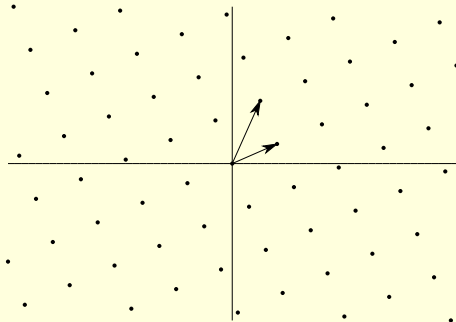
Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \quad (6)$$

"SVP" : Le problème du plus court vecteur



Arithmétique modulaire

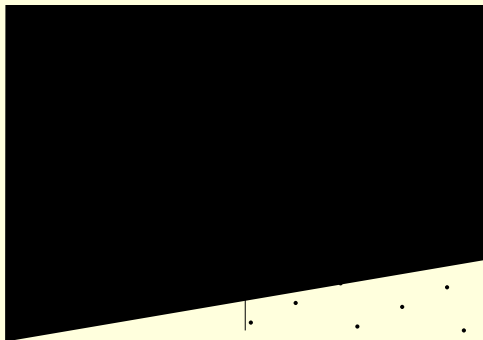
- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens**
- Théorème
- Conclusion

Un réseau \mathcal{L}

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : (8, 5).

“SVP” : Le problème du plus court vecteur



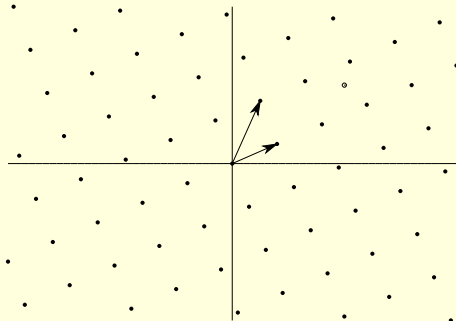
Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : $(8, 5)$.

Le plus proche vecteur : $(20, 20) \equiv (20, 20) \pmod{\mathcal{L}}$

“CVP” : Le problème du plus proche vecteur



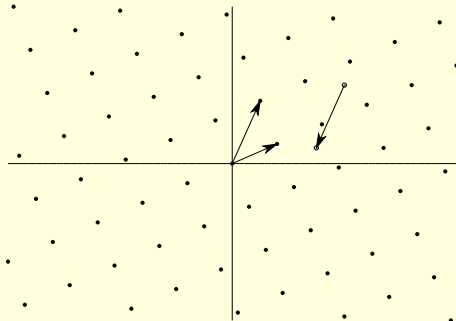
Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : $(8, 5)$.

Le plus proche vecteur : $(20, 20) \equiv (15, 4) \pmod{\mathcal{L}}$

“CVP” : Le problème du plus proche vecteur



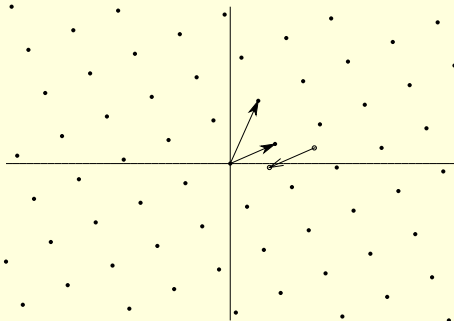
Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : $(8, 5)$.

Le plus proche vecteur : $(20, 20) \equiv (7, -1) \pmod{\mathcal{L}}$

"CVP" : Le problème du plus proche vecteur



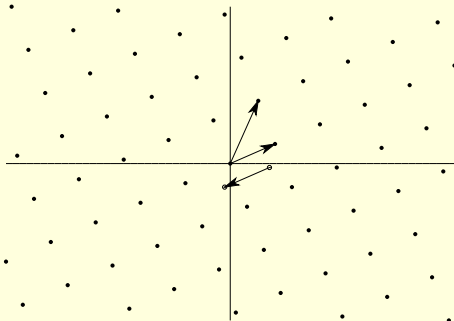
Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : $(8, 5)$.

Le plus proche vecteur : $(20, 20) \equiv (-1, 6) \pmod{\mathcal{L}}$

"CVP" : Le problème du plus proche vecteur



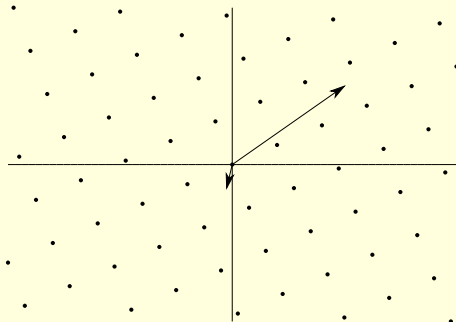
Un réseau \mathcal{L}

$$B = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (7)$$

Le plus court vecteur : $(8, 5)$.

Le plus proche vecteur : $(20, 20) \equiv (-1, 6) \pmod{\mathcal{L}}$

“CVP” : Le problème du plus proche vecteur



Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Redéfinition de la réduction des coefficients

- Entrée : Un vecteur V de \mathbb{Z}^n
- Sortie : Un vecteur S de \mathbb{Z}^n plus "court" pour la norme $\|\cdot\|_\infty$
- Avec $V \equiv S \pmod{\mathcal{L}}$ où \mathcal{L} est l'ensemble des vecteurs représentant 0 (Si $V(\gamma) \equiv 0 \pmod{p}$ alors $V \in \mathcal{L}$)
- Approximation CVP_∞ sur des réseaux totaux.

Redéfinition de la réduction des coefficients

- Entrée : Un vecteur V de \mathbb{Z}^n
- Sortie : Un vecteur S de \mathbb{Z}^n plus "court" pour la norme $\|\cdot\|_\infty$
- Avec $V \equiv S \pmod{\mathcal{L}}$ où \mathcal{L} est l'ensemble des vecteurs représentant 0 (Si $V(\gamma) \equiv 0 \pmod{p}$ alors $V \in \mathcal{L}$)
- Approximation CVP_∞ sur des réseaux totaux.

Théorème

- Si $X^n - c$ irréductible dans \mathbb{Z} alors

$$\rho_{min} \leq |c|p^{\frac{1}{n}}$$

- $\mathcal{B} = (p, n, c^{1/n}, |c|p^{\frac{1}{n}})$ est un système de représentation modulaire.

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}

$$\mathbf{B} = \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \quad (8)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}

$$\mathbf{B} = \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \quad (8)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}

$$\mathbf{B} = \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ 0 & 0 & \dots & 0 & p & \end{pmatrix} \quad (8)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}

$$\mathbf{B} = \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ 0 & 0 & \cdots & 1 & & -\gamma \\ 0 & 0 & \cdots & 0 & & p \end{pmatrix} \quad (8)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -\gamma^{n-1} \\ 0 & 1 & \cdots & 0 & -\gamma^{n-2} \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & -\gamma \\ 0 & 0 & \cdots & 0 & p \end{pmatrix} \quad (8)$$

Le réseau \mathcal{L}

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -\gamma^{n-1} \\ 0 & 1 & \cdots & 0 & -\gamma^{n-2} \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & -\gamma \\ 0 & 0 & \cdots & 0 & p \end{pmatrix} \quad (8)$$

Analyse du réseau \mathcal{L}

- Le déterminant $\text{Det}(\mathcal{L}) = p$ et la dimension $d = n$
- Théorème de Minkowski $\Rightarrow \exists \mathbf{m} \in \mathcal{L}$ tel que $\|\mathbf{m}\|_\infty \leq p^{1/n}$
- $\|(m_{n-1}, m_{n-2}, \dots, m_1, m_0)\|_\infty \leq p^{1/n}$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}'

$$\mathbf{B}' = \left(\begin{array}{c} \\ \\ \\ \\ \end{array} \right) \quad (9)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}'

$$\mathbf{B}' = \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 & \end{pmatrix} \quad (9)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}'

$$\mathbf{B}' = \begin{pmatrix} m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix} \quad (9)$$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème**
- Conclusion

Le réseau \mathcal{L}'

$$\mathbf{B}' = \begin{pmatrix} m_0 & cm_{n-1} & \cdots & cm_2 & cm_1 \\ m_1 & m_0 & \cdots & cm_3 & cm_2 \\ \vdots & & & & \vdots \\ m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix} \quad (9)$$

Le réseau \mathcal{L}'

$$\mathbf{B}' = \begin{pmatrix} m_0 & cm_{n-1} & \cdots & cm_2 & cm_1 \\ m_1 & m_0 & \cdots & cm_3 & cm_2 \\ \vdots & & & & \vdots \\ m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix} \quad (9)$$

Analyse du réseau \mathcal{L}'

- $\mathcal{L}' \subseteq \mathcal{L}$
- $\|\mathbf{B}'_i\|_\infty \leq |c|p^{\frac{1}{n}}$
- Si \mathbf{B}' est une base alors $\forall \mathbf{v}, \exists \mathbf{u}, \mathbf{v} \equiv \mathbf{u} \pmod{\mathcal{L}}$

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion**

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- 5 Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 **Conclusion**

Arithmétique modulaire

- Introduction
- Présentation
- Contexte
- Multiplication
- Classes de moduli
- Mersenne
- Pseudo Mersenne
- Généralisation
- Représentation
- Modulaire
- Adapté
- Nouvelle classe
- RED
- Propriété
- Construction
- Cas général
- Réseaux Euclidiens
- Théorème
- Conclusion

Système de représentation modulaire

- Une nouvelle représentation adaptée au modulaire
- Une nouvelle classe de moduli efficace pour ECC
- Des algorithmes généralistes pour RSA

Autre ...

- Multiplications modulaire à précalculs calibrables
- Optimisation du changement de base en RNS
- Algorithmique modulaire à forte mémorisation

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Système de représentation modulaire

- Implantation
- Étude des possibilités de parallélisation
- Interpolation

Autre ...

- Implantation
- Étude des réseaux en norme $\|\cdot\|_\infty$