Modular Number Systems: Beyond the Mersenne family

> Jean-Claude Bajard Laurent Imbert Thomas Plantard

> > SAC 2004

LIRMM - Montpellier - France ATIPS - Calgary - Canada

# Contents

- 1 Introduction
  - Context
  - Modular reduction
  - State of the art
- 2 New Number System
  - Number system
  - Adapted Modular Number System
- 3 Coefficient Reduction
  - Coefficient Reduction Algorithm
  - The Algorithm RED
  - An example
- 4 new class of moduli
- 5 Conclusion

- - E - - - E - -

< 177 ▶

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

# Context

- Many cryptographic protocols use modular arithmetic
  - ECC: uses a prime number P, 160 < |P| < 500
  - RSA: uses composite number N, 1024 < |N|
- We need:
  - fast modular algorithm ...
  - ... for a large class of moduli.
- Remark: Any modular operation can be decomposed in the equivalent classical operation, followed by a modular reduction.

< ロト (周) (日) (日)

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

# Modular Reduction

#### Input

- Constant: P with n = |P|, the length of P
- Variable: X, the result of a multiplication:  $0 \le X < P^2$

#### Output

• Variable: R with  $R = X \mod P$ 

・ロト ・ 日 ・ ・ ヨ ト ・ ・ ヨ ト ・

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

# Modular Reduction

#### Input

- Constant: P with n = |P|, the length of P
- Variable: X, the result of a multiplication:  $0 \le X < P^2$

### Output

• Variable: R with  $R = X \mod P$ 

#### Example

- *P* = 31 and *n* = 5
- $X = 21 \times 13 = 273$
- *R* = 25
  - $X = 25 + 8 \times 31 = 273$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004 Modular Number Systems: Beyond the Mersenne family

イロン イヨン イヨン イヨン

э

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

# Some interesting classes of moduli

#### Mersenne's number

•  $P = 2^n - 1$ 

# Algorithm

- $2^n \equiv 1 \pmod{P}$
- $X = X_1 2^n + X_0$
- $X \equiv X_1 + X_0 \pmod{P}$ 
  - Advantage: cost = one addition
  - Drawback: Prime Mersenne's number class is too small

・ロト ・ 日 ・ ・ ヨ ト ・ ・ ヨ ト ・

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

# Some interesting classes of moduli

#### Mersenne's number

•  $P = 2^n - 1$ 

# Algorithm

- $2^n \equiv 1 \pmod{P}$
- $X = X_1 2^n + X_0$
- $X \equiv X_1 + X_0 \pmod{P}$

Example: 
$$P = 31, X = 273$$

• 
$$2^5 \equiv 1 \pmod{31}$$

• 
$$X = 8 \times 2^5 + 17$$

• 
$$R = 8 + 17 = 25$$

・ロト ・ (日)・ ・ (日)・ ・ (日)・ ・

- Advantage: cost = one addition
- Drawback: Prime Mersenne's number class is too small

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

### Pseudo Mersenne

- Introduced by Crandall in 1992.
- $P = 2^n c$  with c small integer
- Example:  $n = 10, c = 3 \rightarrow P = 1021$

イロン イヨン イヨン イヨン

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

#### Pseudo Mersenne

- Introduced by Crandall in 1992.
- $P = 2^n c$  with c small integer
- Example:  $n = 10, c = 3 \rightarrow P = 1021$

#### Generalized Mersenne

- Introduced by Solinas in 1999.
- $P = f(2^t)$  where f is a polynomial with coefficients in  $\{0, 1\}$
- Example:  $t = 3, f(x) = x^3 x 1 \rightarrow P = 8^3 8 1 = 503$

New Number System Coefficient Reduction A new class of moduli Conclusion Context Modular reduction State of the art

#### Pseudo Mersenne

- Introduced by Crandall in 1992.
- $P = 2^n c$  with c small integer
- Example:  $n = 10, c = 3 \rightarrow P = 1021$

#### Generalized Mersenne

- Introduced by Solinas in 1999.
- $P = f(2^t)$  where f is a polynomial with coefficients in  $\{0, 1\}$
- Example:  $t = 3, f(x) = x^3 x 1 \rightarrow P = 8^3 8 1 = 503$

#### More generalized Mersenne

• Introduced by Chung and Hassan in SAC 2003.

• 
$$P = f(2^t - c)$$
 with  $f_i = \{0, 1\}$ 

• Example:  $f(x) = x^4 - x^3 - 1 \rightarrow P = f(2^4 - 2) = 35671$ 

Number system Adapted Modular Number System

(日) (周) (王) (王)

# Number system

#### Classical number system with radix $\beta$

$$X = \sum_{i=0}^{n-1} x_i \beta^i \text{ with } x_i \in \{0, ... \beta - 1\}$$

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

Number system Adapted Modular Number System

・ロト ・ 同ト ・ ヨト ・ ヨト

# Number system

#### Classical number system with radix $\beta$

$$X = \sum_{i=0}^{n-1} x_i \beta^i$$
 with  $x_i \in \{0, ... \beta - 1\}$ 

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

#### Modular number system $(\gamma, \rho, n, P)$

$$X = \sum_{i=0}^{n-1} x_i \gamma^i \mod P \text{ with } x_i \in \{0, \dots, \rho-1\}$$

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i$$
 mod 17 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i \mod 17$$
 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i$$
 mod 17 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i$$
 mod 17 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i \mod 17$$
 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

・ロト ・四ト ・ヨト ・ヨト

3

# Example

## MNS

• 
$$(\gamma = 7, \rho = 3, n = 3, P = 17)$$

• 
$$X = \sum_{i=0}^{2} x_i 7^i \mod 17$$
 with  $x_i \in \{0, 1, 2\}$ 

# Table with $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

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

Number system Adapted Modular Number System

< ロト (周) (日) (日)

How find a "good" Modular Number System?

#### Definition: AMNS

A modular number system  $\mathcal{B} = MNS(\gamma, \rho, n, P)$  is called Adapted Modular Number System (AMNS) if  $\gamma^n \mod P = c$  with c small integer.

Number system Adapted Modular Number System

(日) (周) (王) (王)

How find a "good" Modular Number System?

### Definition: AMNS

A modular number system  $\mathcal{B} = MNS(\gamma, \rho, n, P)$  is called Adapted Modular Number System (AMNS) if  $\gamma^n \mod P = c$  with c small integer.

#### Modular Multiplication in AMNS

- **O** Polynomial multiplication in  $\mathbb{Z}[X]$ :  $U(X) \leftarrow A(X)B(X)$
- **2** Polynomial reduction:  $V(X) \leftarrow U(X) \mod (X^n c)$
- Coefficient reduction:  $S \leftarrow CR(V)$ , gives  $S \equiv V(\gamma) \pmod{P}$

Number system Adapted Modular Number System

## AMNS

- $P = 250043 \Rightarrow |P| = 18$
- $n = 3, \ \rho = 2^7$
- $\gamma = 127006$  such that  $c = 2 = \gamma^3 \bmod P$

#### Input

• 
$$A = 7 + 30X + 100X^2 \Rightarrow A = 65842$$

• 
$$B = 59 + 2X + 76X^2 \Rightarrow B = 8816$$

## Algorithm

• 
$$U(X) = A(X) \times B(X)$$
  
 $U(X) = 413 + 1784X + 6492X^2 + 2480X^3 + 7600X^4$ 

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

• WHILE 
$$t > k + 1$$
 DO

$$S = S2^{t-3k/2} + S$$

$$S \leftarrow RED(\overline{S})$$

$$S \leftarrow \overline{S}2^{t-3k/2} + S$$

$$t \leftarrow t - (k/2 - 1)$$

#### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004 Modular Number Syste

Modular Number Systems: Beyond the Mersenne family

◆□> ◆□> ◆目> ◆目> ◆日> 三日 のへで

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

## Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

• 
$$S = S2^{t-3k/2} + S$$
  
•  $\overline{S} \leftarrow RED(\overline{S})$   
•  $S \leftarrow \overline{S}2^{t-3k/2} + S$   
•  $t \leftarrow t - (k/2 - 1)$ 

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆圖> ◆臣> ◆臣> ―臣 ─の�?

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

## Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

$$S = S2^{t-3k/2} + S$$

$$S \leftarrow RED(\overline{S})$$

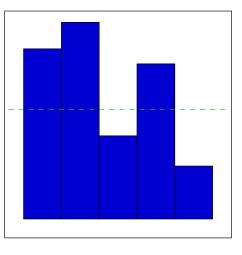
$$S \leftarrow \overline{S}2^{t-3k/2} + S$$

$$t \leftarrow t - (k/2 - 1)$$

. . . . .

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆圖> ◆臣> ◆臣> ―臣 ─の�?

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

A vector V

## Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

•  $S = \overline{S}2^{t-3k/2} + \underline{S}$ •  $\overline{S} \leftarrow RED(\overline{S})$ •  $S \leftarrow \overline{S}2^{t-3k/2} + \underline{S}$ •  $t \leftarrow t - (k/2 - 1)$ 

## Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm

#### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

2 WHILE 
$$t > k + 1$$
 DO

$$5 = 52^{t-3k/2} + 5$$
  

$$\overline{S} \leftarrow RED(\overline{S})$$
  

$$S \leftarrow \overline{S}2^{t-3k/2} + 5$$
  

$$t \leftarrow t - (k/2 - 1)$$

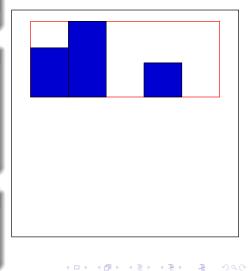
Cat 21/2

## Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

# The Algorithm RED



Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

## Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

$$2 WHILE  $t > k + 1 DO$$$

$$S = 52^{t-3k/2} + S$$
  

$$\overline{S} \leftarrow RED(\overline{S})$$
  

$$S \leftarrow \overline{S}2^{t-3k/2} + S$$
  

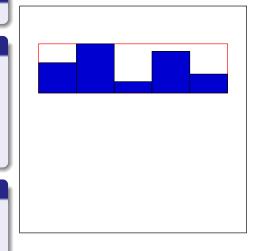
$$t \leftarrow t - (k/2 - 1)$$

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

#### Modular Number Systems: Beyond the Mersenne family



Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

WHILE 
$$t > k + 1$$
 DO  
 $S = \overline{S}2^{t-3k/2} + S$ 

$$\begin{array}{c} \overline{S} \leftarrow \overline{RED}(\overline{S}) \\ \overline{S} \leftarrow \overline{S}2^{t-3k/2} + \underline{S} \\ \overline{S} \leftarrow \overline{S}2^{t-3k/2} + \underline{S} \\ \overline{S} \leftarrow t - (k/2 - 1) \end{array}$$

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆圖> ◆臣> ◆臣> ―臣 ─の�?

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

## Algorithm

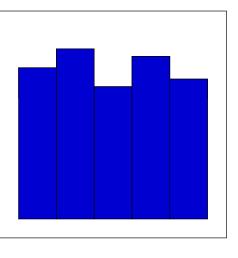
$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

• 
$$S = S2^{t-3k/2} + \underline{S}$$
  
•  $\overline{S} \leftarrow RED(\overline{S})$   
•  $S \leftarrow \overline{S}2^{t-3k/2} + \underline{S}$   
•  $t \leftarrow t - (k/2 - 1)$ 

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

(日) (图) (문) (문) (문)

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

## Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

$$5 = 52^{t-3k/2} + 5$$
  

$$\overline{S} \leftarrow RED(\overline{S})$$
  

$$S \leftarrow \overline{S}2^{t-3k/2} + 5$$
  

$$t \leftarrow t - (k/2 - 1)$$

01.10

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆圖> ◆臣> ◆臣> ―臣 ─の�?

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

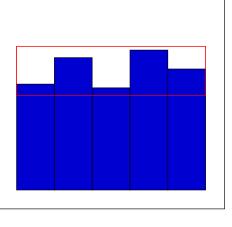
$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO  
**3**  $S = \overline{S}2^{t-3k/2} + S$ 

**2** 
$$\overline{S} \leftarrow \underline{RED}(\overline{S})$$
  
**3**  $S \leftarrow \overline{S}2^{t-3k/2} + \underline{S}$   
**4**  $t \leftarrow t - (k/2 - 1)$ 

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

$$S = S2^{t-3k/2} + S$$
  

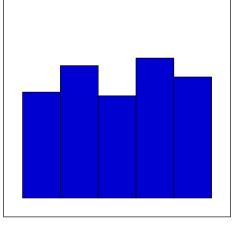
$$\overline{S} \leftarrow RED(\overline{S})$$
  

$$S \leftarrow \overline{S}2^{t-3k/2} + S$$
  

$$t \leftarrow t - (k/2 - 1)$$

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆圖> ◆臣> ◆臣> ―臣 ─の�?

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

$$5 = 52^{t} + 5$$
  

$$\overline{S} \leftarrow RED(\overline{S})$$
  

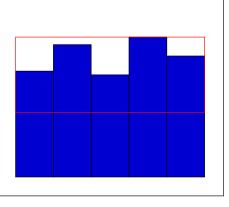
$$S \leftarrow \overline{S}2^{t-3k/2} + 5$$
  

$$F \leftarrow t = (k/2 - 1)$$

 $\overline{C}$  ot -3k/2 + C

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

◆□> ◆□> ◆豆> ◆豆> ・豆 ● のへの

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

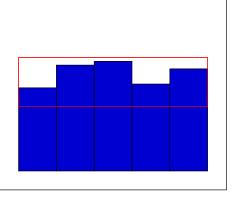
$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO  
**3**  $S = \overline{S}2^{t-3k/2} + S$ 

$$\begin{array}{l} \textcircled{0} \quad \begin{array}{l} S \leftarrow \underline{RED(S)} \\ \fbox{0} \quad \begin{array}{l} S \leftarrow \overline{S}2^{t-3k/2} + \underline{S} \\ \r{0} \quad t \leftarrow t - (k/2 - 1) \end{array} \end{array}$$

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm The Algorithm *RED* An example

### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

2 WHILE 
$$t > k + 1$$
 DO  

$$S = \overline{S}2^{t-3k/2} + S$$

$$\overline{S} \leftarrow RED(\overline{S})$$

$$\overline{S} \leftarrow \overline{S}2^{t-3k/2} + \underline{S}$$

$$\overline{S} \leftarrow \overline{S}2^{t-3k/2} + \underline{S}$$

$$t \leftarrow t - (k/2 - 1)$$

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm The Algorithm *RED* An example

#### Input

• A vector V

# Algorithm

$$S \leftarrow V, t \leftarrow |S|_2$$

**2** WHILE 
$$t > k + 1$$
 DO

$$S = S2^{t-3k/2} + S$$

$$S \leftarrow RED(\overline{S})$$

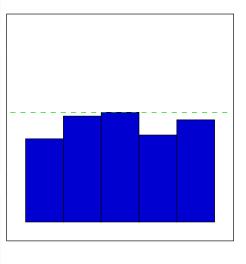
$$S \leftarrow \overline{S}2^{t-3k/2} + S$$

$$t \leftarrow t - (k/2 - 1)$$

Cat 21/2 . 0

### Output

- A vector  $S \equiv V$
- With coefficients  $S_i < \rho = 2^{k+1}$



Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

Coefficient Reduction Algorithm The Algorithm *RED* An example

## The Algorithm RED

#### Input

• A vector V with its coefficients  $V_i < 2^{3k/2}$ 

## Algorithm RED

• 
$$V = \overline{V}2^k + \underline{V}$$
  
•  $S \leftarrow \overline{V}M + V$ , where  $M \equiv 2^k Id$ 

### Output

- A vector  $S \equiv V$
- With its coefficients  $S_i < 2^{k+1}$

Coefficient Reduction Algorithm The Algorithm *RED* An example

イロン イヨン イヨン イヨン

3

# How find M with $M \equiv 2^k I$

### Condition

- A vector  $\xi$  which represent  $2^k$ :  $2^k \equiv \xi[\gamma] \pmod{P}$
- With small coefficients:  $\sum_{i=0}^{n-1} \xi_i < 2^{\lfloor k/2 \rfloor}/c$

Coefficient Reduction Algorithm The Algorithm *RED* An example

(1)

# How find M with $M \equiv 2^k I$

### Condition

- A vector  $\xi$  which represent  $2^k$ :  $2^k \equiv \xi[\gamma] \pmod{P}$
- With small coefficients:  $\sum_{i=0}^{n-1} \xi_i < 2^{\lfloor k/2 \rfloor}/c$

#### How to build M

$$\begin{pmatrix} 2^{k} & 0 & \cdots & 0 & 0\\ 0 & 2^{k} & \cdots & 0 & 0\\ \vdots & & & \vdots\\ 0 & 0 & \cdots & 2^{k} & 0\\ 0 & 0 & \cdots & 0 & 2^{k} \end{pmatrix} \equiv \left( \begin{array}{c} \end{array} \right)$$

Coefficient Reduction Algorithm The Algorithm *RED* An example

# How find M with $M \equiv 2^k I$

### Condition

- A vector  $\xi$  which represent  $2^k$ :  $2^k \equiv \xi[\gamma] \pmod{P}$
- With small coefficients:  $\sum_{i=0}^{n-1} \xi_i < 2^{\lfloor k/2 \rfloor}/c$

### How to build M

$$\begin{pmatrix} 2^{k} & 0 & \cdots & 0 & 0 \\ & & & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \\ & &$$

Coefficient Reduction Algorithm The Algorithm *RED* An example

# How find M with $M \equiv 2^k I$

### Condition

- A vector  $\xi$  which represent  $2^k$ :  $2^k \equiv \xi[\gamma] \pmod{P}$
- With small coefficients:  $\sum_{i=0}^{n-1} \xi_i < 2^{\lfloor k/2 \rfloor}/c$

### How to build M

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

Coefficient Reduction Algorithm The Algorithm *RED* An example

# How find M with $M \equiv 2^k I$

### Condition

- A vector  $\xi$  which represent  $2^k$ :  $2^k \equiv \xi[\gamma] \pmod{P}$
- With small coefficients:  $\sum_{i=0}^{n-1} \xi_i < 2^{\lfloor k/2 \rfloor}/c$

### How to build M

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

Coefficient Reduction Algorithm The Algorithm *RED* An example

## Input

•  $AMNS(\gamma = 127006, \rho = 128, n = 3, P = 250043)$  with  $\gamma^n \equiv 2$ •  $\gamma^3 = 2 \mod P$  and  $2^6 = 1 + \gamma^2 \mod P$ 

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

• A vector V = [120, 444, 22] with  $V_i < 2^{3k/2} = 2^9$ 

### RED

**1** 
$$V = [1, 6, 0]2^6 + [56, 60, 22]$$

**2** *S* ← 
$$[1, 6, 0]M + [56, 60, 22] = [1, 8, 12] + [56, 60, 22]$$

### Output

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

Jean-Claude Bajard Laurent Imbert Thomas Plantard - SAC 2004

Modular Number Systems: Beyond the Mersenne family

(2)

Coefficient Reduction Algorithm The Algorithm *RED* An example

<ロ> (四) (四) (三) (三) (三)

3

## An Example of Coefficient Reduction

#### Input

- $AMNS(\gamma = 127006, \rho = 128, n = 3, P = 250043)$  with  $\gamma^n \equiv 2$
- V = [5373, 16984, 6492]

### Step

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

### Output

$$S = [121, 56, 32]$$
 with  $S_i < 128$ 

## How to find convenient P?

#### How to make a AMNS?

- Choose  $\rho = 2^{k+1}$  with k = 15, 31, 63.
- **2** Define *n* such that  $|P| \sim kn$
- Select an integer *c* and a vector  $\xi$  with  $\xi_i \in \{0, 1, 2\}$
- Find *P*: *P* divides  $det(2^kI M)$

## How to find convenient P?

#### How to make a AMNS?

**1** Choose 
$$\rho = 2^{k+1}$$
 with  $k = 15, 31, 63$ .

- 2 Define *n* such that  $|P| \sim kn$
- Select an integer *c* and a vector  $\xi$  with  $\xi_i \in \{0, 1, 2\}$
- Find *P*: *P* divides  $det(2^kI M)$

#### Example

**1** 
$$\rho = 2^{16} \rightarrow k = 15$$

$$\bigcirc |P| \sim 160 \rightarrow n = 11$$

$${f 0}\ \ c=3$$
 and  $2^k=[1,1,1,0,0,1,0,0,0,0,1]_{\cal B}$ 

(日) (四) (三) (三) (三)

## Conclusions and future directions

#### What we proposed

- A new modular number system which is adapted to modular arithmetic
- A way to find interesting AMNS
- Fast algorithm for make operations on this AMNS

イロト イポト イヨト イヨト

## Conclusions and future directions

#### What we proposed

- A new modular number system which is adapted to modular arithmetic
- A way to find interesting AMNS
- Fast algorithm for make operations on this AMNS

#### Perspective

- Find a method to determine  $\gamma,\rho$  for a given  ${\it P}$
- Try to generalize this algorithm for all moduli

イロト イヨト イヨト イヨト