Efficient modular arithmetic in Adapted Modular Number System using Lagrange representation

Christophe Negre[1]
Thomas Plantard[2]

[1] Team DALI, University of Perpignan
[2] Centre for Information Security Research
University of Wollongong

christophe.negre@univ-perp.fr
thomaspl@uow.edu.au

Outcome

1. Modular Arithmetic
   - Modular Arithmetic needs for PKC
   - Modular Multiplication
2. Modular Number System
   - Number system
   - Adapted Modular Number System
   - Arithmetic on AMNS
3. A General Modular Multiplication for AMNS
   - AMNS Multiplication
   - Lattice Theory
   - Advantage
4. Conclusion

Modular Arithmetic

Modular Arithmetic needs for PKC

Diffie-Hellman

- An exponentiation over the prime field F_p
- Needs: Multiplication modulo p (prime)
- Length: $1024, 2048, \ldots$ bits

RSA

- An exponentiation on the ring $\mathbb{Z}/n\mathbb{Z}$
- Needs: Multiplication modulo n (composite, $n = p.q$)
- Length: $1024, 2048, \ldots$ bits

ECC

- Elliptic curve point multiplication
- Needs: Arithmetic operations (+,-,*,/) over the finite field F_q, where q is a power of a prime p
- Length: $160, 192, \ldots$ bits

Modular Multiplication

Modular Multiplication

- Input: a, b and a moduli p with $0 \leq a, b < p < 2^n$
- Output: $r = ab \bmod p$
  - r $0 \leq r < p$ (the rest)
  - $q = \lfloor \frac{ab}{p} \rfloor$ (the quotient)

Strategies

1. General Algorithms: for any type of moduli.
   Taylor , Blakley , Montgomery , Barrett , Takagi . . .
2. Specific Algorithms: for a class of moduli.
   Mersenne Number, Pseudo Mersenne, Generalized Mersenne , More generalized Mersenne. . .

Modular Number System

Number system

Positional number system with radix β

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

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

Modular number system **MNS**(p, n, γ, ρ)

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

How find a "good" Modular Number System?

What do we need?

1. A MNS where ρ is small (about $\rho \sim p^{1/n}$)
2. A "fast" arithmetic on the MNS

AMNS

A modular number system $\mathcal{B} = MNS(p, n, \gamma, \rho)$ is called Adapted Modular Number System (AMNS) if

$$\gamma^n \bmod P = c,$$

with c is a small integer.

Arithmetic on AMNS

Modular Multiplication in AMNS

1. Polynomial multiplication in $\mathbb{Z}[X]$: $C(X) \leftarrow A(X)\,B(X)$
2. Polynomial reduction: $U(X) \leftarrow C(X) \bmod X^n - c$
3. Coefficient reduction: $R \leftarrow CR(U)$, gives $R(\gamma) \equiv C'(\gamma) \pmod{p}$

Generalization

Operation on AMNS $\rightarrow$ polynomial operation + coefficient reduction

Example

AMNS

- $p = 247649$
- $n = 4$, $\rho = 16$
- $\gamma = 106581$ such $c = -1 = \gamma^4 \bmod p$

Input

- $A = 3 + 4X + 12X^2 + 14X^3 \Rightarrow A(\gamma) \bmod p = 41702$
- $B = 11 + 5X + X^2 + 15X^3 \Rightarrow B(\gamma) \bmod p = 219732$

Example

AMNS

- $p = 247649$
- $n = 4$, $\rho = 16$
- $\gamma = 106581$ such $c = -1 = \gamma^4 \bmod p$

Input

- $A = 3 + 4X + 12X^2 + 14X^3 \Rightarrow A(\gamma) \bmod p = 41702$
- $B = 11 + 5X + X^2 + 15X^3 \Rightarrow B(\gamma) \bmod p = 219732$

AMNS Modular Multiplication

1. $C(X) = A(X) \times B(X)$
   $C(X) = 33 + 59X + 155X^2 + 263X^3 + 142X^4 + 194X^5 + 210X^6$
2. $U(X) = C(X) \bmod (X^4 + 1) \leftarrow -109 - 135X - 55X^2 + 263X^3$
3. $R(X) = ?$

Example

AMNS

- $p = 247649$
- $n = 4$, $\rho = 16$
- $\gamma = 106581$ such $c = -1 = \gamma^4 \bmod p$

Input

- $A = 3 + 4X + 12X^2 + 14X^3 \Rightarrow A(\gamma) \bmod p = 41702$
- $B = 11 + 5X + X^2 + 15X^3 \Rightarrow B(\gamma) \bmod p = 219732$

AMNS Modular Multiplication

1. $C(X) = A(X) \times B(X)$
   $C(X) = 33 + 59X + 155X^2 + 263X^3 + 142X^4 + 194X^5 + 210X^6$
2. $U(X) = C(X) \bmod (X^4 + 1) \leftarrow -109 - 135X - 55X^2 + 263X^3$
3. $R(X) = ?$

A General Modular Multiplication for AMNS

AMNS Multiplication

Rewrite of classic method

1. Change modulo p by modulo $M[X]$.
2. $M(\gamma) = 0 \bmod p$
3. $\|M\|_\infty$ small

Modular Multiplication in AMNS

1. $C \leftarrow A \times B \bmod X^n - c$
2. $Q \leftarrow C \times (-M^{-1}) \bmod (X^n - c, 2^r)$
3. $R \leftarrow (C + Q \times M \bmod X^n - c)/2^r$

Lattice Theory

Definition of a Lattice

- All the integral combinations of $d \leq n$ linearly independent vectors over $\mathbb{R}$

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

- d dimension.
- $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a *basis*.

"SVP" : Shortest Vector Problem

- Find a vector $m \in \mathcal{L}$ such that $\|m\|$ minimal.

Example

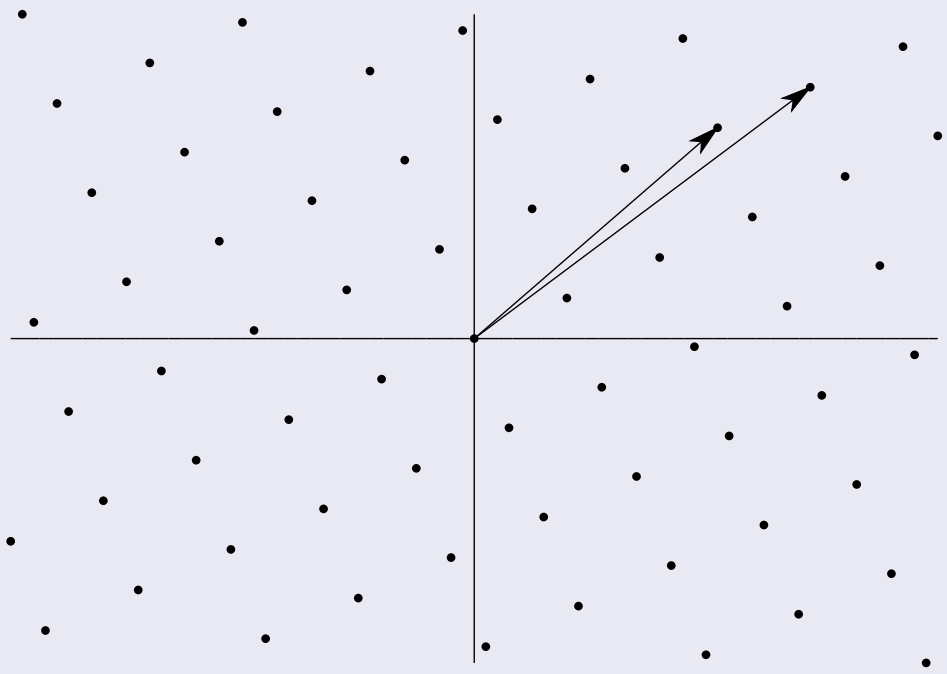
A lattice $\mathcal{L}$

Example

A lattice $\mathcal{L}$

$$\mathcal{B} = \begin{pmatrix} 29 & 31 \\ 21 & 26 \end{pmatrix} \tag{1}$$

"SVP": Shortest Vector Problem

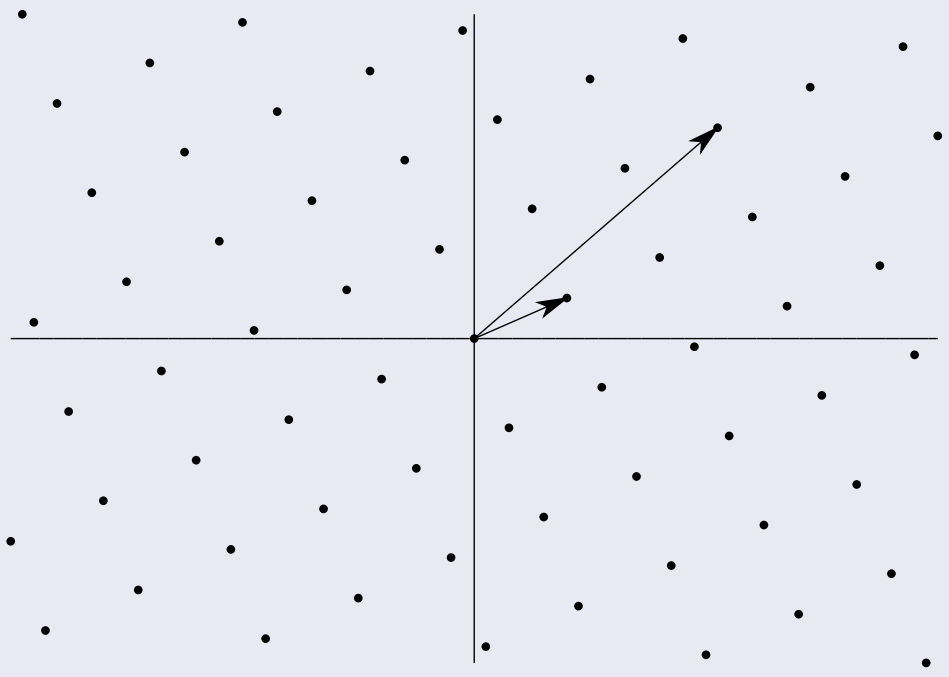


Example

A lattice $\mathcal{L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 21 & 26 \end{pmatrix} \tag{2}$$

"SVP": Shortest Vector Problem

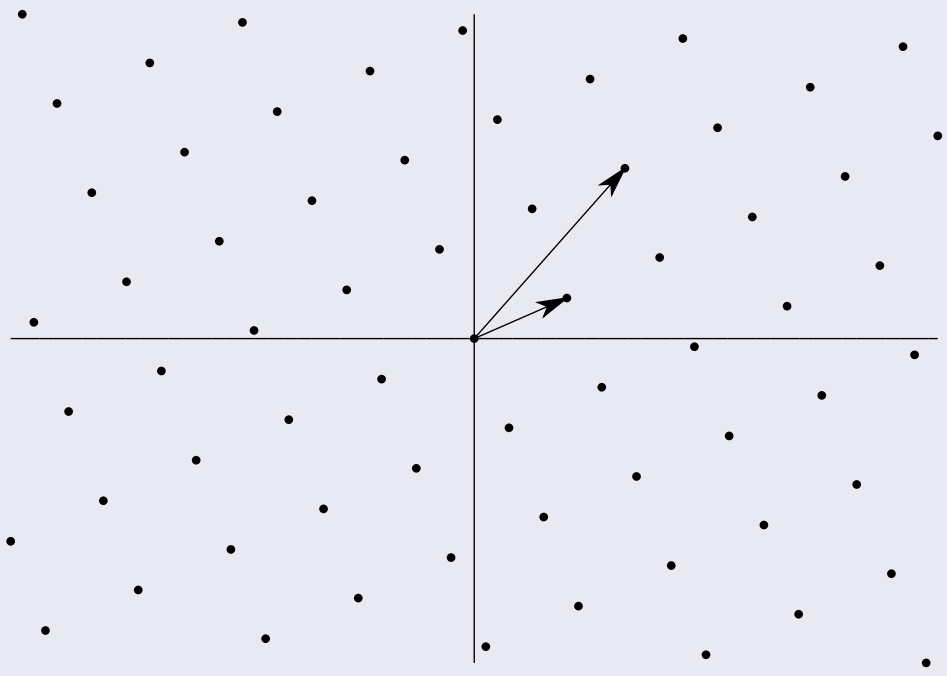


Example

A lattice $\mathcal{L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 13 & 21 \end{pmatrix} \tag{3}$$

"SVP" : Shortest Vector Problem

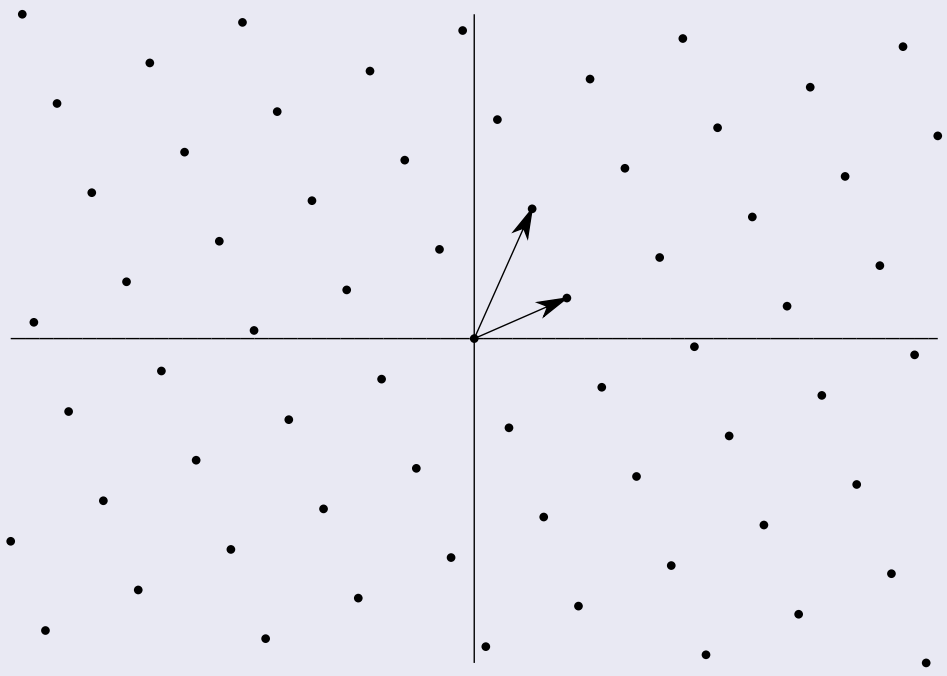


Example

A lattice $\mathcal{L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{4}$$

"SVP" : Shortest Vector Problem



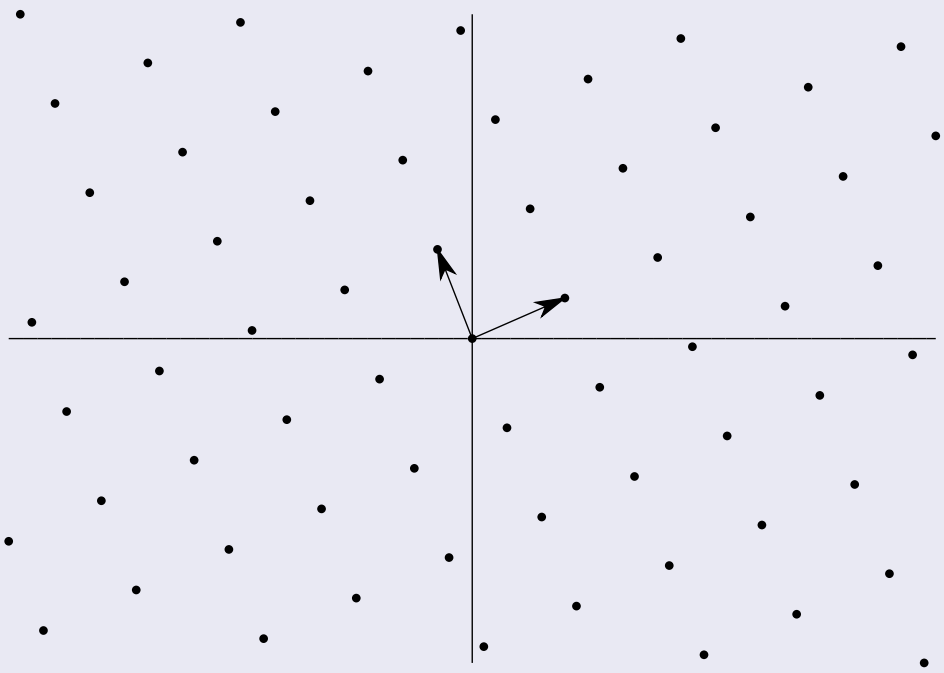
Example

A lattice $\mathcal{L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{5}$$

Shortest Vector : $(8, 5)$.

"SVP" : Shortest Vector Problem



Lattice

Minkowski Theorem, 1896

- There exist a shortest vector $m \in \mathcal{L}$ such that

$$\|m\|_\infty \leq \det \mathcal{L}^{1/n}$$

LLL (Lenstra Lenstra Lovasz) 1982

- Find a short vector.
- Practically, if $n < 50$ find the shortest vector.

Lattice for AMNS

A Lattice $\mathcal{L}$

$$\mathbf{B} = \begin{pmatrix} p & 0 & 0 & 0 & \dots & 0 \\ -\gamma & 1 & 0 & 0 & \dots & 0 \\ -\gamma^2 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ -\gamma^{n-2} & 0 & 0 & \dots & 1 & 0 \\ -\gamma^{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow p \\ \leftarrow X - \gamma \\ \leftarrow X^2 - \gamma^2 \\ \vdots \\ \leftarrow X^{n-2} - \gamma^{n-2} \\ \leftarrow X^{n-1} - \gamma^{n-1} \end{matrix} .$$

Lattice for AMNS

A Lattice $\mathcal{L}$

$$\mathbf{B} = \begin{pmatrix} p & 0 & 0 & 0 & \dots & 0 \\ -\gamma & 1 & 0 & 0 & \dots & 0 \\ -\gamma^2 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ -\gamma^{n-2} & 0 & 0 & \dots & 1 & 0 \\ -\gamma^{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow p \\ \leftarrow X - \gamma \\ \leftarrow X^2 - \gamma^2 \\ \vdots \\ \leftarrow X^{n-2} - \gamma^{n-2} \\ \leftarrow X^{n-1} - \gamma^{n-1} \end{matrix} .$$

Analysis of $\mathcal{L}$

- Determinant $Det(\mathcal{L}) = p$ and Dimension $d = n$
- Minkowski Theorem $\Rightarrow \exists \mathbf{m} \in \mathcal{L}$ such that $\|\mathbf{m}\|_\infty \leq p^{1/n}$
- A polynomial $M(X) = m_0 + m_1 X + \cdots + m_{n-1} X^{n-1}$ such that $M(\gamma) = 0 \bmod p$

Example

AMNS

- $p = 247649$
- $n = 4$, $\rho = 16$
- $\gamma = 106581$ such $c = -1 = \gamma^4 \bmod p$

AMNS Lattice

$$\mathbf{B} = \begin{pmatrix} p & 0 & 0 & 0 \\ -\gamma & 1 & 0 & 0 \\ -\gamma^2 & 0 & 1 & 0 \\ -\gamma^3 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 247649 & 0 & 0 & 0 \\ -106581 & 1 & 0 & 0 \\ -11359509561 & 0 & 1 & 0 \\ -1210707888520941 & 0 & 0 & 1 \end{pmatrix}$$

SVP

- $m = (-8, -5, -17, 11)$
- $M = -8 - 5X - 17X^2 + 11X^3$ with $M(\gamma) = 0 \bmod p$
- $\|M\|_\infty = 17 \cong p^{1/n} \simeq 22.3$

Example

Modular Multiplication in AMNS

1. $C \leftarrow A \times B \bmod X^n - c$
2. $Q \leftarrow C \times (-M^{-1}) \bmod (X^n - c, 2^r)$
3. $R \leftarrow (C + Q \times M \bmod X^n - c)/2^r$

Example

1. $C = -109 - 135X - 55X^2 + 263X^3$
2. $Q = 15 + 15X + X^2 + 5X^3$
3. $R = -11 - 8X - 14X^2 + 4X^3$

Advantage

Multiplication (Karatsuba, Tom-Cook, Schonhage-Strassen)

1. Integer $\longrightarrow$ Polynomial $\longrightarrow$ Points
2. Points multiplication
3. Points $\longrightarrow$ Polynomial $\longrightarrow$ Integer

Modular Multiplication

1. Modular Multiplication : between 2 and 3 Multiplication
2. AMNS Multiplication: between 2 and 3 Polynomial Multiplication

Lagrange Modular Multiplication

1. Montgomery FFT Multiplication: $15n \log n$
2. Mersenne FFT Multiplication: $6n \log n$
3. AMNS FFT Multiplication: $6n \log n$

Conclusion

Conclusion

What we proposed

- A Polynomial Version of Modular Multiplication method
- A General Modular Multiplication as efficient as Specific Method

Future works

- A complete library.