On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Jean Claude Bajard

joint work with Jérémy Marrez, Thomas Plantard and Pascal Véron

MACAO - Inria - University of Wollongong 2019

Mathematics and Algorithms for Cryptographic Advanced Objects

Outline

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Some Background on Pseudo-Mersenne Numbers

- **Classical Positional Number System** $\beta \in \mathbb{N}$ and $\beta \geq 2$, $a \in \mathbb{N}$ with $a < \beta^m$, there exists an unique sequence of integers $(a_i)_{i=0\ldots m-1}$, such that ,
  $a = \sum_{i=0}^{m-1} a_i \beta^i$, with $a_i \in \mathbb{N}$, $0 \leq a_i < \beta$.
- **Specific Modular Reduction**
  Let $p \in \mathbb{N}$, $\beta^{n-1} \leq p < \beta^n$, $\beta^n \equiv \delta \pmod{p}$, with $\delta < p$,

  do
  1. $a \rightarrow a_0 + \beta^n a_1$ with $a_0, a_1 < \beta^n$
  2. $a \leftarrow a_0 + \delta a_1$

  until $a < \beta^n$

  (if $\delta \leq \beta^{\frac{1}{2}\mathbf{n}}$ then two iterations give $a < 2\beta^n - \beta^{\frac{1}{2}n} - 1$, if necessary, a last subtraction of $(\beta^n - \delta)$ gives $a < \beta^n$)

Some Background on Pseudo-Mersenne Numbers

Polynomial approach

Since, $\beta^n - \delta \equiv 0 \pmod{p}$, then β is a root of the polynomial $E(X) = X^n - \Delta(X)$ modulo p,

where $\Delta(\beta) \equiv \delta \pmod{p}$, with $\deg \Delta(X) = d < n$ and $\|\Delta(X)\|_\infty < \beta$.

Reduction modulo p is computed in two steps:

1. **polynomial reduction** : $C(X) = A(X) \bmod E(X)$
2. **coefficients reduction** : $C'(\beta) \equiv C(\beta) \pmod{p}$ with $C'(X)$ of degree lower than n and coefficients smaller than β

The **polynomial reduction** looks like:

1. $C(X) \leftarrow A(X)$
2. **do** $C(X) \leftarrow \Delta(X) \times \sum_{i=n}^{m-1} c_i X^{i-n} + \sum_{i=0}^{n-1} c_i X^i$, degree decreases of $(n-d)$

   until $\deg C(X) \leq n-1$

Thus, if $\deg C(X) \leq 2n$ and $\deg \Delta(X) \leq n/2$, then $\deg C(X) \leq n-1$ in two steps.

Some Background on Pseudo-Mersenne Numbers

Polynomial approach

Let t be the smallest integer such that $\|C(X)\|_\infty < \beta^t$.

The **coefficient reduction** could look like:

Do

1. $C(X) \leftarrow \sum_{i=0}^{t-1} C_i(X)\beta^i$, with C_i's coefficients smaller than β
2. $C(X) \leftarrow \sum_{i=0}^{t-1} C_i(X)X^i$, with $\deg C(X) < t + n$ and $\|C(X)\|_\infty < t\beta$
3. Polynomial reduction of $C(X)$,

Until $t = 1$

This can be seen as a carry propagation.

Some Background on Pseudo-Mersenne Numbers

Lattices approach

The coefficient reduction can be seen as the subtraction of a close vector in the lattice defined by:

$$\mathbf{A} = \begin{pmatrix} p & 0 & \dots & \dots & 0 & 0 \\ -\beta & 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \dots & -\beta & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & -\beta & 1 \end{pmatrix} \text{ or } \begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ -\beta & 1 & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & & & \vdots \\ -\beta^i & \dots & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ -\beta^{n-1} & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

The first vector $(p, 0, \dots, 0, 0)$ represents the modulo p reduction. Vectors like $(0, \dots, -\beta, 1, \dots, 0)$ represent the carry propagation.

Some Background on Pseudo-Mersenne Numbers

Lattices approach

When we consider $\beta^n - \delta \equiv 0 \pmod{p}$, we can replace $(p, 0, \ldots, 0, 0)$ is replaced by $(\delta_0, \delta_1, \ldots, \delta_{n-2}, \delta_{n-1} - \beta)$ thus we obtain a sub-lattice with a reduced base.

$$\mathbf{A}' = \begin{pmatrix} \delta_0 & \delta_1 & \ldots & \ldots & \delta_{n-2} & \delta_{n-1} - \beta \\ -\beta & 1 & \ldots & \ldots & 0 & 0 \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \ldots & -\beta & 1 & \ldots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & -\beta & 1 \end{pmatrix}$$

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Polynomial Modular Number System

Definition

A **Polynomial Modular Number System** (PMNS) is defined by

- a quadruple (p, n, γ, ρ) and
- a monic polynomial of degree n, $E(X) \in \mathbb{Z}[X]$, such that $E(\gamma) \equiv 0 \pmod{p}$
- for each integer x in $\{0, \ldots p-1\}$, there exists $(x_0, \ldots, x_{n-1})$ with $x \equiv \sum_{i=0}^{n-1} x_i \gamma^i \pmod{p}$, $x_i \in \mathbb{N}$, $-\rho < x_i < \rho$, and $0 < \gamma < p$,

Proposition

If $\mathfrak{B} = (p, n, \gamma, \rho)_E$ *is a PMNS, then* $p \leq (2\rho - 1)^n$.

Polynomial Modular Number System

Example: $p = 31$, $n = 4$, $\gamma = 15$, $\gamma^4 \equiv 2 \pmod{p}$, and $\rho = 2$

0	1	2	3	4	5
(0, 0, 0, 0)	(1, 0, 0, 0)	(-1, 1, -1, 1)	(-1, -1, -1, 1) (-1, 0, 0, -1) (-1, 0, 1, 1) (0, 1, -1, 1)	(0, -1, -1, 1) (0, 0, 0, -1) (0, 0, 1, 1) (1, 1, -1, 1)	(1, -1, -1, 1) (1, 0, 0, -1) (1, 0, 1, 1)
6	7	8	9	10	11
(-1, 1, -1, 0)	(-1, -1, -1, 0) (-1, 0, 1, 0) (0, 1, -1, 0)	(0, -1, -1, 0) (0, 0, 1, 0) (1, 1, -1, 0)	(1, -1, -1, 0) (1, 0, 1, 0)	(-1, 1, -1, -1) (-1, 1, 0, 1)	(-1, -1, -1, -1) (-1, -1, 0, 1) (-1, 0, 1, -1) (0, 1, -1, -1) (0, 1, 0, 1)
12	13	14	15	16	17
(0, -1, -1, -1) (0, -1, 0, 1) (0, 0, 1, -1) (1, 1, -1, -1) (1, 1, 0, 1)	(1, -1, -1, -1) (1, -1, 0, 1) (1, 0, 1, -1)	(-1, 1, 0, 0)	(-1, -1, 0, 0) (0, 1, 0, 0)	(0, -1, 0, 0) (1, 1, 0, 0)	(1, -1, 0, 0)
18	19	20	21	22	23
(-1, 0, -1, 1) (-1, 1, 0, -1) (-1, 1, 1, 1)	(-1, -1, 0, -1) (-1, -1, 1, 1) (0, 0, -1, 1) (0, 1, 0, -1) (0, 1, 1, 1)	(0, -1, 0, -1) (0, -1, 1, 1) (1, 0, -1, 1) (1, 1, 0, -1) (1, 1, 1, 1)	(1, -1, 0, -1) (1, -1, 1, 1)	(-1, 0, -1, 0) (-1, 1, 1, 0)	(-1, -1, 1, 0) (0, 0, -1, 0) (0, 1, 1, 0)
24	25	26	27	28	29
(0, -1, 1, 0) (1, 0, -1, 0) (1, 1, 1, 0)	(1, -1, 1, 0)	(-1, 0, -1, -1) (-1, 0, 0, 1) (-1, 1, 1, -1)	(-1, -1, 1, -1) (0, 0, -1, -1) (0, 0, 0, 1) (0, 1, 1, -1)	(0, -1, 1, -1) (1, 0, -1, -1) (1, 0, 0, 1) (1, 1, 1, -1)	(1, -1, 1, -1)
30					
(-1, 0, 0, 0)					

Polynomial Modular Number System

Remarks

1. PMNS looks like a positional system, but is not.
   $(\gamma^i \bmod p) < (\gamma^{i+1} \bmod p)$ is not always true anymore.
2. For every quadruple (p, n, γ, ρ), there exists a polynomial $E(X) \in \mathbb{Z}[X]$ satisfying $E(\gamma) \equiv 0 \mod p$ and $\deg E(X) = n$: for example $E(X) = X^n - (\gamma^n \mod p)$.
3. If $p < (2\rho - 1)^n$, then the representation is redundant (i.e., some values can have more than one representation).
4. If $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a PMNS, so is $\mathfrak{B}' = (p, n, \gamma, \rho + 1)_E$.
5. Given p, n, γ, E, there exists a minimal ρ which defines a PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$.

Polynomial Modular Number System

Question

The question, for p and n given, Which polynomials $E(X)$

-i) offer an efficient modular reduction?

-ii) have a large number of roots γ in $\mathbb{Z}/p\mathbb{Z}$?

-iii) allow to have ρ as small as possible?

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Existence and bounds of PMNS

PMNS and lattices

We consider the lattice $\mathfrak{L}$ over $\mathbb{Z}^n$ of the polynomials of degree at most $n-1$, for which, γ is a root modulo p.

$$\mathbf{A} = \begin{pmatrix} p & 0 & \dots & \dots & 0 & 0 \\ -\gamma & 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \dots & -\gamma & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & -\gamma & 1 \end{pmatrix} \text{ or } \begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ -\gamma & 1 & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & & & \vdots \\ -\gamma^i & \dots & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ -\gamma^{n-1} & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

The fundamental volume of $\mathfrak{L}$ is $\det \mathbf{A} = p$.

Existence and bounds of PMNS

PMNS and lattices

Theorem

Let $p \geq 2$ and $n \geq 2$ two integers, $E(X)$ a polynomial of degree n in $\mathbb{Z}[X]$ and γ be a root of $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.
Let r be the covering radius of the lattice $\mathfrak{L}$, if $\rho > r$, then $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a Polynomial Modular Number System.

Proof.

The covering radius r of $\mathfrak{L}$ is the smallest number, such that the balls $\mathcal{B}_V = \{T \in \mathbb{R}^n, \|T - V\|_2 \leq r\}$ centered on any point $V \in \mathfrak{L}$, cover the space $\mathbb{R}^n$. In other words, for any $T \in \mathbb{R}^n$ there exists $V \in \mathfrak{L}$ such that $\|T - V\|_\infty \leq \|T - V\|_2 \leq r$. Thus for any $T \in \mathbb{R}^n$ there exists $V \in \mathfrak{L}$, such that $T - V \in \mathcal{C}_O$, $\mathcal{C}_O = \{T \in \mathbb{R}^n, \|T\|_\infty \leq r\}$. □

Existence and bounds of PMNS

Lattice's bases and PMNS

Theorem

Let $\mathrm{B} = \{B_0, \ldots, B_{n-1}\}$ *a base of* $\mathfrak{L}$*, and* $\mathbf{B}$ *the matrix associated such that,* B_i *represents the* i^{th} *row., with* $B_i = (b_{i,0}, \ldots, b_{i,n-1})$*, thus* $b_{i,j}$ *represents the coefficient of the* i *th row,* j^{th} *column.*

If $\rho > \frac{1}{2} \|\mathbf{B}\|_1$, $\left(\|\mathbf{B}\|_1 = \max_j \left\{ \sum_{i=0}^{n-1} |b_{i,j}| \right\}\right)$*, then* $\mathfrak{B} = (p, n, \gamma, \rho)_E$ *is a Polynomial Modular Number System.*

Proof.

Let $S \in \mathbb{R}^n$, we search a close vector $T \in \mathfrak{L}$ using a Babaï round-off approach.We have, $T = \mathbf{B}^T . \lfloor (\mathbf{B}^T)^{-1} . S \rceil$.

$S = \mathbf{B}^T . (\mathbf{B}^T)^{-1} . S = T + \mathbf{B}^T . \mathrm{frac}\left((\mathbf{B}^T)^{-1} . S\right)$ with $\left\|\mathrm{frac}\left((\mathbf{B}^T)^{-1} . S\right)\right\|_\infty \leq \frac{1}{2}$

Then

$\|S - T\|_\infty = \left\|\mathbf{B}^T . \mathrm{frac}\left((\mathbf{B}^T)^{-1} . S\right)\right\|_\infty \leq \frac{1}{2} \left\|\mathbf{B}^T\right\|_\infty = \frac{1}{2} \|\mathbf{B}\|_1 .$ □

Existence and bounds of PMNS

Irreducible polynomials and PMNS

Let $E(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, and let $\mathbf{C}$ be the companion matrix of $E(X)$:

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Let $V = (v_0, \dots, v_{n-1})$ the vector representing the coefficient of the polynomial $V(X) = \sum_{i=0}^{n-1} v_i X^i$, then $V.\mathbf{C}$ is the vector whose coordinates are the coefficients of the polynomial $X.V(X) \bmod E(X)$.

Proposition

Let V a non-null vector of $\mathfrak{L}$, the lattice of rank n defined by $\mathbf{A}$. Let $\mathbf{B}$ the $n \times n$ matrix whose i^{th} row is the vector B_i such that $B_i = V.\mathbf{C}^i$ (with polynomial $B_i(X) = X^i.V(X) \bmod E(X)$). If $V(X)$ is inversible modulo $E(X)$ then:

- *the matrix $\mathbf{B}$ defines a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n (i.e. $\mathrm{B} = (B_0, \dots, B_{n-1})$ is a base of $\mathfrak{L}'$),*
- *and $V \in \mathfrak{L}'$.*

Proof.

The B_i are linearly independent. Indeed, let us suppose that there exists a non nul vector $(t_0, t_1, \dots, t_{n-1}) \in \mathbb{Z}^n$ such that $\sum_{i=0}^{n-1} t_i B_i = 0$. It means that $\sum_{i=0}^{n-1} t_i X^i V(X) = 0 \bmod E(X)$, or equivalently $T(X)V(X) = 0 \bmod E(X)$, with $T(X) = \sum_{i=0}^{n-1} t_i X^i$. Then $T(X)V(X)V^{-1}(X) \bmod E(X) = T(X) = 0$, since $V(X)$ is inversible modulo $E(X)$ and degree of $T(X)$ is at most $n-1$. Hence the rows of $\mathbf{B}$ are a base of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$.

Existence and bounds of PMNS

Irreducible polynomials and PMNS

Corollary

Let V a non-null vector of $\mathfrak{L}$, the lattice of rank n defined by $\mathbf{A}$.
If $E(X)$ is irreducible, then

- *V can define a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n,*
- *and $V \in \mathfrak{L}'$.*

Proof.

If $E(X)$ is irreducible, then $V(X)$ is inversible and Proposition 5 gives $\mathrm{B} = (B_0, \ldots, B_{n-1})$ a base of $\mathfrak{L}'$, $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$. □

Existence and bounds of PMNS

Irreducible polynomials and PMNS

Corollary

Let $\mathfrak{L}$, the lattice of rank n given by $\mathbf{A}$,and let the lattice $\mathfrak{L}_D$ of rank n in $\mathbb{Z}^{n^2}$ defined by $\mathbf{D} = (\mathbf{A}|\mathbf{A}.\mathbf{C}^1|\cdots|\mathbf{A}.\mathbf{C}^{n-1})$, then for any $\overline{V} = (V_0, V_1, \ldots, V_{n-1}) \in \mathfrak{L}_D$ such that $\overline{V} \neq (0)^{n^2}$:

If $E(X)$ is irreducible then:

1. $V_0 \in \mathfrak{L}$,
2. $(V_0, V_1, \ldots, V_{n-1})$ *is a base of* $\mathfrak{L}' \subseteq \mathfrak{L}$.

Proof.

V_0 is a linear combination of rows of $\mathbf{A}$, hence it belongs to $\mathfrak{L}$. Next, since $V_i = V_0.\mathbf{C}^i$, for all $i \geq 1$, then, due to Corollary 6, the vector $(V_0, V_1, \ldots, V_{n-1})$ is a base of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$. $\square$

Hence, a strategy is to choose a vector $(V_0, V_1, \ldots, V_{n-1})$ of $\mathfrak{L}_D$ and to build the base B of $\mathfrak{L}$ from V_0 with $\|\mathbf{B}\|_1$ as small as possible.

Existence and bounds of PMNS

Remarks

- For any p and n there exist $E(X)$ monic of degree n, with γ as root, and ρ such that $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a PMNS.
  (for example $E(X) = X^n - (\gamma^n \mod p)$)
- Then, a $\mathfrak{L}$ the lattice of rank n can be defined by $\mathbf{A}$ depending of p, n and γ.
- If $E(X)$ is irreducible and $V \in \mathfrak{L}$ then we can construct easily a "reduced" base B of $\mathfrak{L}$.
- Thus, one goal is to find a base B of $\mathfrak{L}$ with $\|\mathbf{B}\|_1$ as small as possible, to give interesting bounds of ρ.

Existence and bounds of PMNS

Example with $p \sim 2^{256}$ and $\rho < 2^{33}$

$p = 112848483075082590657416923680536930196574208889254960005437791530871071177777$

$n = 8,\ E(X) = X^8 + X^2 + X + 1,$

$\gamma = 14916364465236885841418726559687117741451144740538386254842986662265545588774$

LLL:	$\|\mathbf{B}\|_1 = 16940155314$	BKZ:	$\|\mathbf{B}\|_1 = 15289909984$
Cor. 6 :	$\|\mathbf{B}\|_1 = 13881325101$	Cor. 7, :	$\|\mathbf{B}\|_1 = 12883199915$

$p = 96777329138546418411606037850670691916278980249035796845487391462163262877831$

$n = 8,\ E(X) = X^8 + 6,$

$\gamma = 55382746543295148021817266189065902379362952375536660625428080706764845726 74$

LLL:	$\|\mathbf{B}\|_1 = 12509178620$	BKZ:	$\|\mathbf{B}\|_1 = 12509178620$
Cor. 6:	$\|\mathbf{B}\|_1 = 47611052126$	Cor. 7:	$\|\mathbf{B}\|_1 = 40733847267$

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Suitable irreducible polynomials for PMNS

Definition

A monic polynomial $E(X)$ is a suitable PMNS reduction polynomial, if:

1. $E(X)$ is irreducible in $\mathbb{Z}[X]$,
2. $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, with $n \geq 2$ and $k \leq \frac{n}{2}$,
3. most of coefficients a_i are zero, and others are very small (if possible equal to ± 1) compare to $p^{1/n}$.

Suitable irreducible polynomials for PMNS

Classical criteria of irreducibility

Proposition (from Dumas' criterion 1906)

We assume that if there exists a prime μ and an integer α, such that, $\mu^\alpha \mid a_0$, $\mu^{\alpha+1} \nmid a_0$ and, $\mu^{\lceil \alpha(n-i)/n \rceil} \mid a_i$, and $\gcd(\alpha, n) = 1$, then $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$ is irreducible over $\mathbb{Z}[X]$.

For example, $E(X) = X^n + \mu X^k + \mu$ is irreducible with this criterion. If $k < n/2$ and $\mu << p^{1/n}$, then $E(X)$ is a suitable PMNS reduction polynomial.

Suitable irreducible polynomials for PMNS

Classical criteria of irreducibility

Proposition (from N. C. Bonciocat 2015)

Let $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$, $a_0 \neq 0$, let $t \geq 2$ and let $\mu_1, \ldots, \mu_t$ be pair-wise distinct prime numbers, and $\alpha_1, \ldots, \alpha_t$ positive integers. If, for $j = 1, \ldots, t$, and $i = 0, \ldots, k$, $\mu_j^{\alpha_j} \mid a_i$ and $\mu_j^{\alpha_j+1} \nmid a_0$, and $\gcd(\alpha_1, \ldots, \alpha_t, n) = 1$ then $E(X)$ is irreducible over $\mathbb{Z}[X]$.

For example, $E(X) = X^n + \mu_1^{\alpha_1}\mu_2^{\alpha_2}X^k + \mu_1^{\alpha_1}\mu_2^{\alpha_2}$ with $\gcd(\alpha_1, \alpha_2, n) = 1$, is irreducible with this criterion. If $k < n/2$ and $\mu_1^{\alpha_1}\mu_2^{\alpha_2} << p^{1/n}$, then $E(X)$ is a suitable PMNS reduction polynomial.

Suitable irreducible polynomials for PMNS

Cyclotomic Polynomials

`ClassCyclo(n)` the class of suitable cyclotomic polynomials for PMNS, whose degree is n.

Proposition

`ClassCyclo(n)` $\neq \emptyset$ if and only if, $n = 2^i 3^j$ with $i \geq 1, j \geq 0$.

Hence, suitable cyclotomic polynomials are:

- $\Phi_{2^i}(X) = X^{2^{i-1}} + 1$, thus $n = 2^{i-1}$ with $i \geq 2$,
- $\Phi_{3^j}(X) = X^{2.3^{j-1}} + X^{3^{j-1}} + 1$, thus $n = 2.3^{j-1}$ with $j \in \mathbb{N}^*$,
- $\Phi_{2^i.3^j}(X) = X^{2^i.3^{j-1}} - X^{2^{i-1}.3^{j-1}} + 1$, thus $n = 2^i.3^{j-1}$ for $i, j \in \mathbb{N}^*$.

Suitable irreducible polynomials for PMNS

$\{-1, 1\}$-quadrinomials

Proposition (Finch and Jones 2006)

The quadrinomial $X^a + \beta X^b + \gamma X^c + \delta$ is irreducible over $\mathbb{Z}[X]$, (with $\beta, \gamma, \delta \in \{-1, 1\}$ and $a > b > c > 0$ with $\gcd(a, b, c) = 2^t m$, with m odd and they note $a' = a/2^t$, $b' = b/2^t$ and $c' = c/2^t$. They define $\overline{a} = \gcd(a', b' - c')$, $\overline{b} = \gcd(b', a' - c')$ and $\overline{c} = \gcd(c', a' - b')$) if and only if, its satisfies one of the following conditions:

1. $(\beta, \gamma, \delta) = (1, 1, 1)$ *and* $\overline{a}\overline{b}\overline{c} \equiv 1 \pmod 2$
2. $(\beta, \gamma, \delta) = (-1, 1, 1)$, $b' - c' \not\equiv 0 \pmod{2\overline{a}}$, $b' \not\equiv 0 \pmod{2\overline{b}}$ *and* $a' - b' \not\equiv 0 \pmod{2\overline{c}}$
3. $(\beta, \gamma, \delta) = (1, -1, 1)$, $b' - c' \not\equiv 0 \pmod{2\overline{a}}$, $a' - c' \not\equiv 0 \pmod{2\overline{b}}$ *and* $c' \not\equiv 0 \pmod{2\overline{c}}$
4. $(\beta, \gamma, \delta) = (1, 1, -1)$, $a' \not\equiv 0 \pmod{2\overline{a}}$, $b' \not\equiv 0 \pmod{2\overline{b}}$ *and* $c' \not\equiv 0 \pmod{2\overline{c}}$
5. $(\beta, \gamma, \delta) = (-1, -1, -1)$, $a' \not\equiv 0 \pmod{2\overline{a}}$, $a' - c' \not\equiv 0 \pmod{2\overline{b}}$ *and* $a' - b' \not\equiv 0 \pmod{2\overline{c}}$

For example, $E(X) = X^{2^t 7m} + X^{2^t 5m} + X^{2^t 3m} + 1$ is a suitable PMNS reduction quadrinomial.

Suitable irreducible polynomials for PMNS

$\{-1, 1\}$-trinomials and binomials

Proposition (W. Ljunggren1960, W.H. Mills 1985)

We note $\gcd(n, m) = d$ *and* $n = d.n_1$, $m = d.m_1$. *If* $n_1 + m_1 \not\equiv 0 \mod 3$ *then the polynomial* $X^n + \beta X^m + \delta$ *with* $\delta, \beta \in \{-1, 1\}$ *and* $n > 2m > 0$, *is irreducible over* $\mathbb{Z}[X]$.

Proposition (N. C. Bonciocat 2015)

We note, $c = \prod_{j=1}^{k} p_j^{m_j}$ *with* p_j *pair-wise distinct prime numbers, and* m_j *positive integers.*
If $gcd(m_1, \ldots, m_k, n) = 1$ *then the polynomial* $X^n + c$ *with* $c \in \mathbb{Z}$, $|c| \geq 2$, *is irreducible over* $\mathbb{Z}[X]$.

Suitable irreducible polynomials for PMNS

From Perron irreducibility (N. C. Bonciocat 2010)

Proposition

For a fixed $n \geq 2$, *a prime* μ, *and* $P(X) = X^n + \sum_{i=1}^{n/2} \varepsilon_i X^i \pm \mu$ *with* $\varepsilon_i \in \{-1, 0, 1\}$,
if $\mu > 1 + \sum_{i=1}^{n/2} |\varepsilon_i|$ *then the polynomial* $P(X)$ *is irreducible over* $\mathbb{Z}[X]$.

Proposition

For a fixed $n \geq 2$, *and* $P(X) = X^n + \sum_{i=2}^{n/2} \varepsilon_i X^i + a_1 X \pm 1$ *with* $\varepsilon_i \in \{-1, 0, 1\}$ *and* $a_1 \in \mathbb{Z}^*$.
If $|a_1| > 2 + \sum_{i=2}^{n/2} |\varepsilon_i|$ *then the polynomial* $P(X)$ *is irreducible over* $\mathbb{Z}[X]$.

Number of PMNS for a given p

General case

Proposition

Let p prime, $n > 2$, $E(X)$ a polynomial of degree n and irreducible in $\mathbb{Z}[X]$, and $D(X) = \gcd(X^p - X, E(X)) \mod p$, there exists $\deg(D(X))$ Polynomial Modular Number Systems $(p, n, \gamma_i, \rho)_{E(X)}$.

Computation of $\gcd(X^p - X, E(X)) \bmod p$, in two steps :

1. evaluation of $X^p \bmod E(X) \bmod p$ (square/multiply exponentiation), then of $F(X) = X^p - 1 \bmod E(X) \bmod p$,
2. evaluation of $\gcd(F(X), E(X)) \bmod p$ with $\deg F(X) < n$.

The roots are found by factorising the polynomial $\gcd(F(X), E(X)) \bmod p$.

Number of PMNS for a given p

Example of a General case

We consider $p = 78264746924694600393874000999999297$ and $E(X) = X^5 + X^2 + 1$.

Then, $X^p \bmod E(X) =$

$$\begin{aligned} & 73221262594200981770939850990094624\, X^4 \\ & +17278262153012433490422224611135262\, X^3 \\ & +34388418976081269710045235068644410\, X^2 \\ & +73729585036266646590967284850202950\, X \\ & +41672856061685300251802935166808760 \end{aligned}$$

Thus,

$$\begin{aligned} & \gcd(X^p \bmod E(X) - X, E(X)) \bmod p \\ & = X^2 + 13058499984190672910003378977052580\, X \\ & +17930730009542045460341940680988260 \\ & = (X + 61576990395578092706710688950709120) \\ & (X + 29746256513307180597166691026336430) \end{aligned}$$

Hence, we obtain two roots of $E(X) \bmod p$:

$$\gamma_1 = 16687756529116507687163312049283850$$
$$\gamma_2 = 48518490411387419796707309973656540$$

Number of PMNS for a given p

Cyclotomic case

Proposition

Let $p > 2$ a prime number, and an integer $m \geq 3$. If $m \mid (p-1)$, then the cyclotomic polynomial $\Phi_m(X)$ has $\varphi(m)$ roots over $\mathbb{Z}/p\mathbb{Z}$.
$(\Phi_m(X) \mid (X^{p-1} - 1) = \prod_{\xi_i \in (\mathbb{Z}/p\mathbb{Z})^*} (X - \xi_i)$)

Corollary

Let p prime, $n \geq 2$ such that $n = 2^i 3^j$, with $i, j \in \mathbb{N}$.

- *If $i > 0$, $j = 0$, and $(2\,n)$ divides $(p-1)$, and $E(X) = \Phi_{2n}(X) = X^n + 1$,*
- *If $i = 1$, $j \geq 0$, and $(3\,n\,/\,2)$ divides $(p-1)$, and $E(X) = \Phi_{\frac{3n}{2}}(X) = X^n + X^{\frac{n}{2}} + 1$,*
- *If $i \geq 1$, $j \geq 0$, and $(3\,n)$ divides $(p-1)$, and $E(X) = \Phi_{3n}(X) = X^n - X^{\frac{n}{2}} + 1$,*

then, there exist n PMNS $(p, n, \gamma_i, \rho)_{E(X)}$, with γ_i one of the n distinct roots modulo p of $E(X)$.

Number of PMNS for a given p

Example of Cyclotomic cases

Construction PMNS from a cyclotomic reduction polynomial for $p = 2^{256}.3^{157}.115 + 1$ coded on 512 bits.

- $E(X) = X^8 + 1$, from the 8 roots, the best ρ is obtained with our approach (with Corollary-6 and Corollary-7) and is 66 bits long.
- $E(X) = X^6 + X^3 + 1$, from the six roots, the best ρ is obtained two times with LLL, else with Corollary-6 and Corollary-7, and is 87 bits long.
- $E(X) = X^6 - X^3 + 1$, from the six roots, the best ρ is obtained with Corollary 6 and Corollary 7, and is 87 bits long.

Number of PMNS for a given p

Example of a General case

$p =$57896044618658097711785492504343953926634992332820282019728792003956566811073 a 256-bits prime, and $n = 9$.

We consider PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ such that:

- $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, with $n \geq 2$ and $k \leq \frac{n}{2}$,
- coefficients $|a_i| \leq 1$ for $1 \leq i \leq k$ and $|a_0| \leq 3$
- $\rho \leq 2^{31}$

The number of PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is equal to 354.

Most of the time, the best ρ is obtained first by LLL (266 times) or BKZ (46), some are due to Corollary-6 (10) or with Corollary-7 (28), or Proposition-5 (4) with a short vector.

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

PMNS Coefficient Reduction

Montgomery approach

$\mathfrak{B} = (p, n, \gamma, \rho)_E$ a PMNS, and α_E such that, with $\deg(A(X)) < 2n$, $\|A(X) \bmod E(X)\|_\infty < \alpha_E \|A(X)\|_\infty$. Let V a non-null vector of $\mathfrak{L}$.

If $\|V\|_\infty < \frac{1}{2n\alpha_E}\rho$ and there exists $V'(X) = \left(-V^{-1}(X) \bmod E(X)\right) \bmod 2^l$, then, for $A(X)$ with coefficients smaller than $2^{l-1}\rho$:

1. $Q(X) \leftarrow ((A(X)V'(X)) \bmod E(X)) \bmod 2^l$
2. $T(X) \leftarrow Q(X)V(X) \bmod E(X)$ (thus $T \in \mathfrak{L}$ and $\|T\|_\infty < 2^{l-1}\rho$)
3. $R(X) = A(X) + T(X)$ (thus $R(X)$ multiple of 2^l)
4. $S(X) = R(X)/2^l$ (thus $\|S\|_\infty < \rho$)

with $S(\gamma) \equiv A(\gamma)2^{-l} \pmod p$

If $n\rho < 2^l$ there exists $G(X)$ such that $G(\gamma) \equiv 2^{2l} \pmod p$ and $\|G\|_\infty < \rho$, then $G(\gamma)S(\gamma) \equiv 2^l A(\gamma) \pmod p$ and $F(X) = G(X)S(X) \bmod E(X)$ is such that $\|F\|_\infty < 2^{l-1}\rho$.

PMNS Coefficient Reduction

With $2^k = F(\gamma) \bmod p$

Find a $\mathfrak{B} = (p, n, \gamma, \rho)_E$ such that $2^k = F(\gamma) \bmod p$ with $\|F\|_\infty < 2^{\epsilon_F}$ and $\#$(non-null coeff of F) $< 2^\beta$

We note ϵ_E, the integer such that $\|C(X) \bmod E(x)\|_\infty < 2^{\epsilon_E} \|C(X)\|_\infty$

We consider $A(X)$ with $\|A(X)\|_\infty < 2^{k+t}$

do

1. We split $A(X) \to A_1(X)2^k + A_0(X)$
   with $\|A_1(X)\|_\infty < 2^t$ and $\|A_0(X)\|_\infty < 2^k$
2. $A(X) \leftarrow (A_1(X)F(X) \bmod E(X)) + A_0(X)$
   with $\|A(X)\|_\infty < 2^{t+\beta+\epsilon_F+\epsilon_E}$

until $\|A(X)\|_\infty < 2^k$

If $(\beta + \epsilon_F + \epsilon_E) < k$ then the algorithm converges.

PMNS Coefficient Reduction

Example of a pecific case approach (Plantard's PhD)

Find a $\mathfrak{B} = (p, n, \gamma, \rho)_E$ such that $2^k = F(\gamma) \bmod p$ with $\|F\|_\infty < \epsilon$

- The construction of the system giving some features: $n = 8$, and $\rho = 2^{32}$ with $p < \rho^n$ determine the size of the problem.
- The property $\gamma^8 \equiv 2 \pmod{p}$ for the polynomial reduction.
- The coefficient reduction is given by $2^{32} \equiv \gamma^5 + 1 \pmod{p}$

Thus $V = 2^{32} V_1 + V_0 = 2^{32} Id.V_1 + V_0 \equiv M.V_1 + V_0 \pmod{p}$ with

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{32} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2^{32} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2^{32} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2^{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2^{32} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2^{32} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2^{32} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2^{32} \end{pmatrix} \pmod{p}$$

PMNS Coefficient Reduction

Specific case approach

Remarks and construction

- $2^{32} Id - M = 0 \bmod p$ defines a lattice.
- p divides $\det(2^{32} Id - M)$, a factorization gives:

  $p = 115792089021636622262124715160334756877804245386980633020041035952359812890593$

  which corresponds to the expected size.
- The value of γ is deduced as a solution of $\gcd(X^8 - 2, 2^{32} - X^5 - 1)$ modulo p:

  $\gamma = 14474011127704577782765589395224532314179217058921488395049827733759590399996$
- Generally, M is found with coefficients lower than $2^{k/2} (\sim \sqrt{\rho})$, which means that three rounds are sufficient.

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Conclusions

- We observe that irreducible polynomials give better PMNS than non-irreducible ones.
- Coefficient reduction is equivalent to the research of a close vector.
- Is it possible to find an efficient algorithm for these specific lattices??
- Is a round-off Babai sufficient ?? Could we adapt the nearest plan approach?
- Find an ad hoc method like when a power of two has a "good" PMNS representation??
- How construct easily reduced bases for the norm-1 without the help of LLL family algorithms ??