Euclidean lattice and PMNS: arithmetic, redundancy and equality test

Fangan Yssouf Dosso[1], Alexandre Berzati[2],
Nadia El Mrabet[1], Julien Proy[2]

[1]*École des mines de Saint-Étienne*, SAS Laboratory, Gardanne
[2]*Thales DIS*, Meyreuil

Séminaires Cryptographie de Rennes
Rennes, January 31 2025

Introduction

Context:

- Main goal: Efficient and secure modular arithmetic
- PMNS: Polynomial Modular Number System
- Main characteristic: Elements are polynomials in the PMNS
- Additional characteristic: PMNS is a redundant system

Introduction

Context:

- Main goal: Efficient and secure modular arithmetic
- PMNS: Polynomial Modular Number System
- Main characteristic: Elements are polynomials in the PMNS
- Additional characteristic: PMNS is a redundant system

Goals:

- Improve and extend PMNS generation
- Study and control the redundancy in the PMNS
- Perform equality test within the system

Presentation based on: https://eprint.iacr.org/2023/1231

Plan

PMNS: Polynomial Modular Number System

Let $p \geqslant 3$, be an odd integer. We want to represent elements of $\mathbb{Z}/p\mathbb{Z}$.

A PMNS is a subset of $\mathbb{Z}[X]$, defined by a tuple $\mathcal{B} = (p,\ n,\ \gamma,\ \rho, E)$.

- n: elements are represented with n coefficients.
- γ: a polynomial $T \in \mathcal{B}$ represents the integer $t = T(\gamma) \pmod{p}$
- ρ: $\|T\|_\infty < \rho$, $\forall T \in \mathcal{B}$
- E: a monic polynomial $\in \mathbb{Z}_n[X]$, such that $E(\gamma) \equiv 0 \pmod{p}$.

where $0 < \gamma < p$ and $\rho \approx \sqrt[n]{p}$.

Example: $\mathcal{B} = (p, n, \gamma, \rho, E) = (19, 3, 7, 2, X^3 - 1)$

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

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

10	11	12	13	14
$\boldsymbol{X^2 - 1}$	X^2	$X^2 + 1$	$-X + 1$	$-X^2 + X - 1$

15	16	17	18
$-X^2 + X$	$-X^2 + X + 1$	$X^2 + X - 1$	-1

$(X^2 - 1) \equiv 10_{\mathcal{B}}$, since $7^2 - 1 = 48 \equiv 10 \pmod{19}$.

A redundant system: $(-X - 1) \equiv 11_{\mathcal{B}}$.

$$(X^2 + X + 1) \equiv 0_{\mathcal{B}}.$$

Main operations and reductions

Let $A, B \in \mathcal{B}$. There are two main operations:

- Addition: $S = A + B$
- Multiplication: $C = A \times B$

We have:

- $\deg(S) < n$, but $\|S\|_\infty < 2\rho$
- $\deg(C) < 2n - 1$, and $\|C\|_\infty < n\rho^2$

So, we need to:

- reduce $\deg(C)$ $\Rightarrow$ **External reduction**
- reduce $\|C\|_\infty$ and $\|S\|_\infty$ $\Rightarrow$ **Internal reduction**

The external reduction

It is the computation:

$R = C \bmod E$

Result:

- $R \in \mathbb{Z}_{n-1}[X]$
- $E(\gamma) \equiv 0 \pmod{p} \quad \Rightarrow \quad R(\gamma) \equiv C(\gamma) \pmod{p}$

Essential:

E is chosen so that the reduction modulo it is very efficient.

For example: $X^n \pm 2,\ X^n \pm X \pm 1,\ \ldots$

Multiplication example for $\mathcal{B} = (19,\ 3,\ 7,\ 2,\ X^3 - 1)$

Remember that: $p = 19,\ n = 3,\ \gamma = 7,\ \rho = 2,\ E(X) = X^3 - 1.$

- Let $a = 8$; $A \equiv a_{\mathcal{B}}$, with $A(X) = X + 1$
- Let $b = 12$; $B \equiv b_{\mathcal{B}}$, with $B(X) = X^2 + 1$

Multiplication example for $\mathcal{B} = (19, 3, 7, 2, X^3 - 1)$

Remember that: $p = 19,\ n = 3,\ \gamma = 7,\ \rho = 2,\ E(X) = X^3 - 1.$

- Let $a = 8$; $A \equiv a_{\mathcal{B}}$, with $A(X) = X + 1$
- Let $b = 12$; $B \equiv b_{\mathcal{B}}$, with $B(X) = X^2 + 1$

- $C = AB = X^3 + X^2 + X + 1$
- $C(7) \bmod 19 = 1 = ab \pmod{19} = 1$, but $C \notin \mathcal{B}$

Multiplication example for $\mathcal{B} = (19, 3, 7, 2, X^3 - 1)$

Remember that: $p = 19,\ n = 3,\ \gamma = 7,\ \rho = 2,\ E(X) = X^3 - 1.$

- Let $a = 8$; $A \equiv a_{\mathcal{B}}$, with $A(X) = X + 1$
- Let $b = 12$; $B \equiv b_{\mathcal{B}}$, with $B(X) = X^2 + 1$

- $C = AB = X^3 + X^2 + X + 1$
- $C(7) \bmod 19 = 1 = ab \pmod{19} = 1$, but $C \notin \mathcal{B}$
- $R = C \bmod E = X^2 + X + 2$
- $R(7) \bmod 19 = 1$ and $\deg(R) < 3$, but $R \notin \mathcal{B}$.

Multiplication example for $\mathcal{B} = (19, 3, 7, 2, X^3 - 1)$

Remember that: $p = 19,\ n = 3,\ \gamma = 7,\ \rho = 2,\ E(X) = X^3 - 1.$

- Let $a = 8$; $A \equiv a_{\mathcal{B}}$, with $A(X) = X + 1$
- Let $b = 12$; $B \equiv b_{\mathcal{B}}$, with $B(X) = X^2 + 1$

- $C = AB = X^3 + X^2 + X + 1$
- $C(7) \bmod 19 = 1 = ab \pmod{19} = 1$, but $C \notin \mathcal{B}$
- $R = C \bmod E = X^2 + X + 2$
- $R(7) \bmod 19 = 1$ and $\deg(R) < 3$, but $R \notin \mathcal{B}$.

Internal reduction:

- Let $T(X) = X^2 + X + 1$.
  $T(7) \equiv 0 \pmod{19}$ and $S = R - T = 1 \in \mathcal{B}$
- How to find such a polynomial T?
  $\Rightarrow$ the **internal reduction** process

The internal reduction

Let $R \in \mathbb{Z}_{n-1}[X]$, with possibly $\|R\|_\infty \geqslant \rho$.

The Goal:

find $S \in \mathbb{Z}_{n-1}[X]$, such that: $\|S\|_\infty < \rho$ and $S(\gamma) \equiv R(\gamma) \pmod{p}$

Equivalent to compute:

$T \in \mathbb{Z}_{n-1}[X]$, such that: $T(\gamma) \equiv 0 \pmod{p}$ and $\|S\|_\infty = \|R - T\|_\infty < \rho$

The internal reduction

Let $R \in \mathbb{Z}_{n-1}[X]$, with possibly $\|R\|_\infty \geqslant \rho$.

The Goal:

find $S \in \mathbb{Z}_{n-1}[X]$, such that: $\|S\|_\infty < \rho$ and $S(\gamma) \equiv R(\gamma) \pmod{p}$

Equivalent to compute:

$T \in \mathbb{Z}_{n-1}[X]$, such that: $T(\gamma) \equiv 0 \pmod{p}$ and $\|S\|_\infty = \|R - T\|_\infty < \rho$

Many methods to do this reduction:

- **Montgomery-like method**
- Barrett-like method
- Babaï-based approaches
- 'Direct' approaches

Internal reduction: the Montgomery-like approach

By Christophe Negre and Thomas Plantard (2008).

Introduces an integer ϕ and two polynomials $M, M' \in \mathbb{Z}_{n-1}[X]$, such that:

- $\phi \geqslant 2$
- $M(\gamma) \equiv 0 \pmod{p}$
- $M' = -M^{-1} \bmod (E, \phi)$

Mont-like:

1: **Input :** $R \in \mathbb{Z}_{n-1}[X]$
2: **Output :** $S \in \mathbb{Z}_{n-1}[X]$, with $S(\gamma) \equiv R(\gamma)\phi^{-1} \pmod{p}$
3: $Q \leftarrow R \times M' \bmod (E, \phi)$
4: $T \leftarrow Q \times M \bmod E$
5: $S \leftarrow (R + T)/\phi$ # exact divisions
6: **return** S

Generation of M: a lattice of zeros

To a PMNS $\mathcal{B}$, one associates the following lattice:

$$\boldsymbol{\mathcal{L}_{\mathcal{B}} = \{A \in \mathbb{Z}_{n-1}[X] \mid A(\gamma) \equiv 0 \pmod{p}\}}$$

- $\mathcal{L}_{\mathcal{B}}$ is a n-dimensional full-rank Euclidean lattice;
- a basis of $\mathcal{L}_{\mathcal{B}}$ is:

$$\mathbf{B} = \begin{pmatrix} p & 0 & 0 & \ldots & 0 & 0 \\ t_1 & 1 & 0 & \ldots & 0 & 0 \\ t_2 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ t_{n-2} & 0 & 0 & \ldots & 1 & 0 \\ t_{n-1} & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow p \\ \leftarrow X + t_1 \\ \leftarrow X^2 + t_2 \\ \\ \leftarrow X^{n-2} + t_{n-2} \\ \leftarrow X^{n-1} + t_{n-1} \end{matrix}$$

where $t_i = (-\gamma)^i \bmod p$.

Note: each line i of $\mathbf{B}$ represents the polynomial $X^i + t_i$.

Generation of M: a lattice of zeros

- Let $\mathcal{W}$ be a reduced basis of $\mathcal{L}_{\mathcal{B}}$;
- i.e. $\mathcal{W} = LLL(\mathbf{B}) = BKZ(\mathbf{B}) = HKZ(\mathbf{B})$, ...

Let's assume that ϕ is a power of two (best choice for efficiency).

Fundamental result: (Didier, Dosso, Véron, JCEN-2020)

There always exists $(\alpha_0, \ldots, \alpha_{n-1}) \in \{0,1\}^n$, such that:

$$M = \sum_{i=0}^{n-1} \alpha_i \mathcal{W}_i \text{ and } M' = -M^{-1} \bmod (E, \phi) \text{ exists.}$$

Note:

- we need Resultant(E, M) to be odd for M' to exist.
- we take $\rho \approx \|M\|_\infty$, hence a reduced basis $\mathcal{W}$.

So, to find a suitable polynomial M, a search is done in a space of size 2^n.

Simplified example of PMNS generation

Let p be a 192-bits prime, such that:

$$p = 4519769796091041823898087646286620970503624228268900016911$$

Simplified example of PMNS generation

Let p be a 192-bits prime, such that:

$$p = 4519769796091041823898087646286620970503624228268900016911$$

Steps in order:

1. We choose $\phi = 2^{64}$, which leads to: $n = 4$.
2. We choose $E(X) = X^4 - 2$, which leads to:

$$\gamma = 2110166219506859592569288331390507089403470310341596434834$$

Simplified example of PMNS generation

Let p be a 192-bits prime, such that:

$$p = 4519769796091041823898087646286620970503624228268900016911$$

Steps in order:

1. We choose $\phi = 2^{64}$, which leads to: $n = 4$.
2. We choose $E(X) = X^4 - 2$, which leads to:

   $$\gamma = 2110166219506859592569288331390507089403470310341596434834$$

3. With the basis $\mathbf{B}$ and $\mathcal{W} = LLL(\mathbf{B})$, we obtain a suitable M, i.e. with Resultant(E, M) odd, such that: $M(X) = -158498747706969 + 167054566018957X - 98192163350595X^2 - 34173855083107X^3$.

The remaining parameters are easy to compute.

A summary: the good news

- High parallelization capability (no carry propagation nor conditional branching)
- It is always possible to generate efficient PMNS given any prime: Efficient modular operations using the adapted modular number system (JCEN-2020)
- PMNS has been proven competitive for both hardware and software implementations:
  - PMNS for Efficient Arithmetic and Small Memory Cost (TETC-2022)
  - Modular Multiplication in the AMNS representation: Hardware Implementation (SAC-2024)
- PMNS is redundant: it allows easy and efficient randomisation. See: Randomization of Arithmetic over Polynomial Modular Number System (ARITH-26/2019).

A summary: the bad news

When n becomes big:

- The generation of the parameter M could be very long;
  the search is done in a space of size 2^n.
- It could have a significant impact on the infinite norm of M.
  Thus, increasing memory requirement to represent elements, since $\rho \approx \|M\|_\infty$.

A summary: the bad news

When n becomes big:

- The generation of the parameter M could be very long; the search is done in a space of size 2^n.
- It could have a significant impact on the infinite norm of M. Thus, increasing memory requirement to represent elements, since $\rho \approx \|M\|_\infty$.

PMNS is redundant:

- More memory is needed to represent elements (compared to a non-redundant system).
- **Trivial equality test is not possible.**

Our goals in the remaining:

- Simplify and generalise the parameter generation process.
- Define and control redundancy in the PMNS.
- Make equality test possible within the PMNS
  (even when the system is chosen very redundant).

Rewriting the Montgomery-like approach

From PMNS for Efficient Arithmetic and Small Memory Cost
(**Dosso**, Robert, Véron, TETC-2022).

Let $\mathcal{M}$ be the $n \times n$ matrix such that:

$$\mathcal{M} = \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ \dots & \dots & \dots & \dots \\ \vdots & \vdots & & \vdots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{matrix} \leftarrow M \\ \leftarrow X.M \bmod E \\ \\ \leftarrow X^{n-1}.M \bmod E \end{matrix}$$

Let $\mathcal{M}'$ be the $n \times n$ matrix such that:

$$\mathcal{M}' = \begin{pmatrix} m'_0 & m'_1 & \dots & m'_{n-1} \\ \dots & \dots & \dots & \dots \\ \vdots & \vdots & & \vdots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{matrix} \leftarrow M' \\ \leftarrow X.M' \bmod (E, \phi) \\ \\ \leftarrow X^{n-1}.M' \bmod (E, \phi) \end{matrix}$$

Rewriting the Montgomery-like approach

Mont-like:

1: **Input :** $R \in \mathbb{Z}_{n-1}[X]$

2: **Output :** $S \in \mathbb{Z}_{n-1}[X]$, such that $S(\gamma) \equiv R(\gamma)\phi^{-1} \pmod{p}$

3: $Q \leftarrow (r_0, \ldots, r_{n-1})\mathcal{M}' \pmod{\phi}$

4: $T \leftarrow (q_0, \ldots, q_{n-1})\mathcal{M}$

5: $S \leftarrow (R + T)/\phi$

6: **return** S

Rewriting the Montgomery-like approach

Mont-like:

1: **Input :** $R \in \mathbb{Z}_{n-1}[X]$

2: **Output :** $S \in \mathbb{Z}_{n-1}[X]$, such that $S(\gamma) \equiv R(\gamma)\phi^{-1} \pmod{p}$

3: $Q \leftarrow (r_0, \ldots, r_{n-1})\mathcal{M}' \pmod{\phi}$

4: $T \leftarrow (q_0, \ldots, q_{n-1})\mathcal{M}$

5: $S \leftarrow (R + T)/\phi$

6: **return** S

Remember that: $\boldsymbol{\mathcal{L}_{\mathcal{B}} = \{A \in \mathbb{Z}_{n-1}[X] \mid A(\gamma) \equiv 0 \pmod{p}\}}$

- $\mathcal{M}$ is a basis of a sub-lattice $\mathcal{L}(\mathcal{M})$ of $\mathcal{L}_{\mathcal{B}}$
- $\mathcal{L}(\mathcal{M}) = \{AM \bmod E \mid A \in \mathbb{Z}_{n-1}[X]\}$
- $T \in \mathcal{L}(\mathcal{M})$ (see line 4 in **Mont-like**)

Question: Is it possible to use another sub-lattice of $\mathcal{L}_{\mathcal{B}}$?

Sub-lattice $\mathcal{L}$ of zeros

Let's assume that p is an odd prime.

$$\mathbf{B} = \begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ t_1 & 1 & 0 & \dots & 0 & 0 \\ t_2 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ t_{n-2} & 0 & 0 & \dots & 1 & 0 \\ t_{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

- $\mathbf{B}$ is a basis of $\mathcal{L}_{\mathcal{B}}$
- $\det(\mathbf{B}) = p$

Let $\mathcal{L}$ be a **sub-lattice** of $\mathcal{L}_{\mathcal{B}}$.

If a matrix $\mathcal{G}$ is a basis of $\mathcal{L}$, then:

- $\det(\mathcal{G}) = kp$, with $k \in \mathbb{Z} \setminus \{0\}$,
- $\mathcal{L} = \mathcal{L}_{\mathcal{B}} \iff \det(\mathcal{G}) = \pm p$

Sub-lattice $\mathcal{L}$ of zeros: some fundamental regions

Let $\mathcal{G}$ be a basis of $\mathcal{L}$.

Let $\mathcal{H}$ be the fundamental domain of $\mathcal{L}$:

$$\mathcal{H} = \{t \in \mathbb{R}^n \mid t = \sum_{i=0}^{n-1} \mu_i \mathcal{G}_i \text{ and } 0 \leqslant \mu_i < 1\}$$

And $\mathcal{H}'$ be the fundamental region:

$$\mathcal{H}' = \{t \in \mathbb{R}^n \mid t = \sum_{i=0}^{n-1} \mu_i \mathcal{G}_i \text{ and } -\frac{1}{2} \leqslant \mu_i < \frac{1}{2}\}$$

Remarks:

- If $V \in \mathcal{H}$, then $\|V\|_\infty < \|\mathcal{G}\|_1$.
- If $V \in \mathcal{H}'$, then $\|V\|_\infty \leqslant \frac{1}{2}\|\mathcal{G}\|_1$.

A representation of $\mathcal{H}$ and $\mathcal{H}'$, for $n = 2$

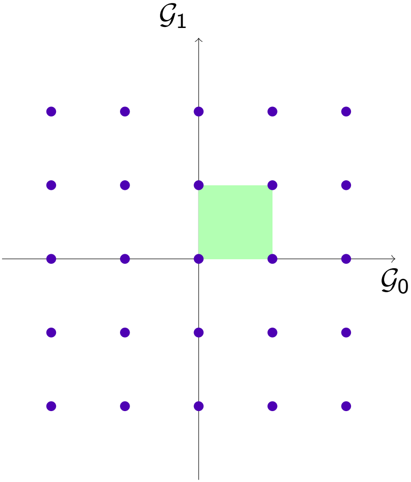


Figure: $\mathcal{H}$

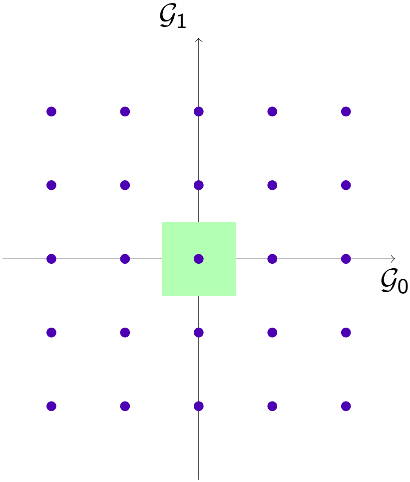


Figure: $\mathcal{H}'$

Some fundamental properties

Let $d = |\det(\mathcal{G})| = |kp|$.

Let us assume that:

$$\gcd(d, \phi) = 1$$

Then:

- $\mathcal{G}' = -\mathcal{G}^{-1} \pmod{\phi}$ exists.
- Let $C \in \mathbb{Z}_{n-1}[X]$, such that: $C = \alpha \mathcal{G}$.
  For each α_i, there exists $k_i \in \mathbb{Z}$, such that:

$$\alpha_i = \frac{k_i}{d}$$

So, $(\alpha_i \bmod \phi)$ exists.

GMont-like: Generalised Montgomery-like method

GMont-like:

1: **Input :** $C \in \mathbb{Z}_{n-1}[X]$

2: **Output :** $S \in \mathbb{Z}_{n-1}[X]$, such that $S(\gamma) \equiv C(\gamma)\phi^{-1} \pmod{p}$

3: $Q \leftarrow (c_0, \ldots, c_{n-1})\mathcal{G}' \pmod{\phi}$

4: $T \leftarrow (q_0, \ldots, q_{n-1})\mathcal{G}$

5: $S \leftarrow (C + T)/\phi$

6: **return** S

Essential: Output coordinates with respect to the basis $\mathcal{G}$

If $C = \alpha\mathcal{G}$, then:

$$S = \frac{\alpha + (-\alpha \bmod \phi)}{\phi}\mathcal{G}$$

*$(-\alpha \bmod \phi) = ((-\alpha_0) \bmod \phi,\ (-\alpha_1) \bmod \phi,\ \ldots\ ,(-\alpha_{n-1}) \bmod \phi)$

GMont-like: Generalised Montgomery-like method

To sum up:

- **Any basis $\mathcal{G}$ of any sub-lattice** of $\mathcal{L}_{\mathcal{B}}$, provided that $\gcd(\det(\mathcal{G}), \phi) = 1$, can be used for internal reduction.
- In particular, any (reduced) basis of $\mathcal{L}_{\mathcal{B}}$ can be used.
- So, no need to search a polynomial M.
- Thus, leading to a **faster**, **simpler** and **generalised** parameters generation process.

Redundancy in the PMNS

Limitations:

- It is not precisely defined.
- We can only choose the **minimum** number of distinct representations for $\mathbb{Z}/p\mathbb{Z}$ elements in the PMNS.
  See: Randomization of Arithmetic over PMNS (ARITH-26).

Motivations:

Precisely control the redundancy for:

- smaller memory requirement to represent element,
- a more reliable randomisation.

A new tool: the set $\mathcal{D}_j$

$\mathcal{D}_j$: the Domain j

Let $j \geqslant 1$ be an integer.

We define the set $\mathcal{D}_j$ as:

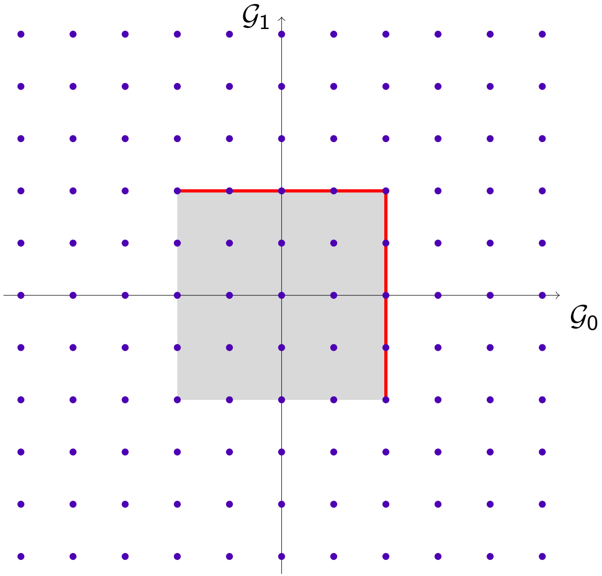
$$\mathcal{D}_j = \{t \in \mathbb{R}^n \mid t = \sum_{i=0}^{n-1} \mu_i \mathcal{G}_i \text{ and } -j \leqslant \mu_i < j\}$$

This can be seen as an extension of the fundamental region $\mathcal{H}'$.

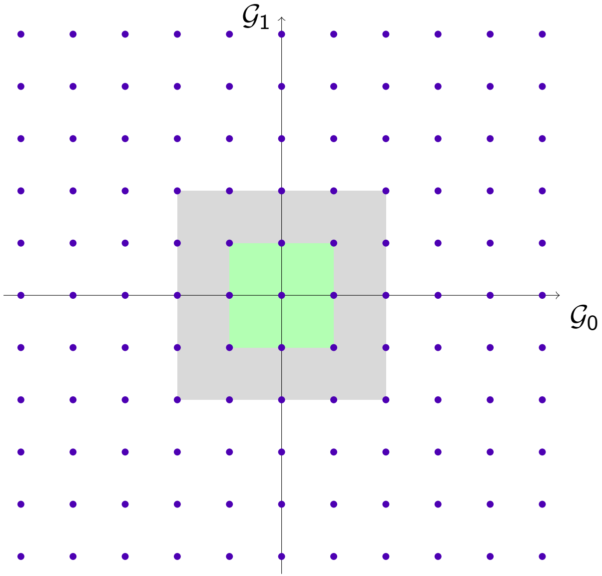
Remark

If $A \in \mathcal{D}_j$, then: $\|A\|_\infty \leqslant j\|\mathcal{G}\|_1$.

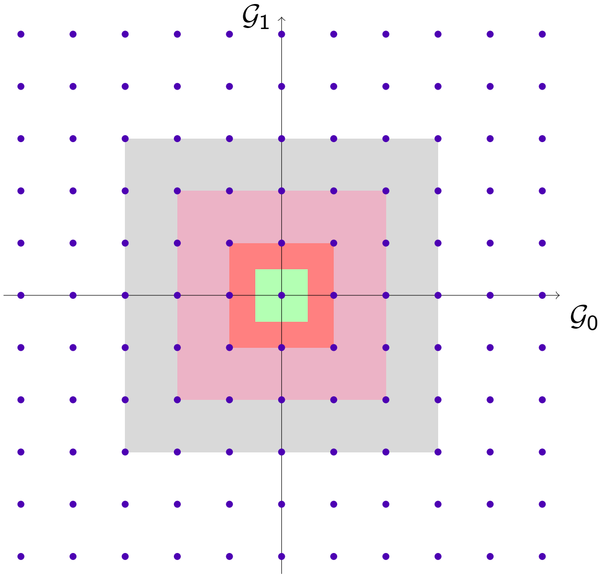
A representation of $\mathcal{D}_2$, for $n = 2$



Domain $\mathcal{D}_1$ vs $\mathcal{D}_2$, for $n = 2$



A representation of $\mathcal{H}'$, $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$, for $n = 2$



Redundancy in the PMNS

Fundamental result:

The set $\mathcal{D}_j$ contains exactly $(2j)^n$ times the set $\mathcal{H}$.

Property:

If $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$, then each $a \in \mathbb{Z}/p\mathbb{Z}$ has **exactly one representation** in $\mathcal{H}$.

Open question: what if $\mathcal{L} \neq \mathcal{L}_{\mathcal{B}}$?

Redundancy in the PMNS

Fundamental result:

The set $\mathcal{D}_j$ contains exactly $(2j)^n$ times the set $\mathcal{H}$.

Property:

If $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$, then each $a \in \mathbb{Z}/p\mathbb{Z}$ has **exactly one representation** in $\mathcal{H}$.

Open question: what if $\mathcal{L} \neq \mathcal{L}_{\mathcal{B}}$?

Consequence:

If $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$, then:

each $a \in \mathbb{Z}/p\mathbb{Z}$ has **exactly** $(2j)^n$ **representation** in $\mathcal{D}_j$.

Redundancy in the PMNS

Let $a \in \mathbb{Z}/p\mathbb{Z}$.

The set of representations

Let's define the set $\mathcal{R}_j(a)$ as:

$$\mathcal{R}_j(a) = \{A \in \mathcal{D}_j \cap \mathbb{Z}^n \mid a = A(\gamma) \pmod p\}$$

Redundancy in the PMNS

Let $a \in \mathbb{Z}/p\mathbb{Z}$.

The set of representations

Let's define the set $\mathcal{R}_j(a)$ as:

$$\mathcal{R}_j(a) = \{A \in \mathcal{D}_j \cap \mathbb{Z}^n \mid a = A(\gamma) \pmod{p}\}$$

Property:

If $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$, then:

$$\#\mathcal{R}_j(a) = (2j)^n$$

In particular, $\#\mathcal{R}_1(a) = 2^n$.

Easy to compute: the representations of zeros in $\mathcal{D}_j$

It corresponds to the lattice points in $\mathcal{D}_j$.

$$\mathcal{R}_j(0) = \{(\alpha_0, \ldots, \alpha_{n-1})\mathcal{G}, \text{ with } \alpha_i \in \mathbb{Z} \cap [-j, j[\,\}.$$

Redundancy in the PMNS

Property:

Let us assume that $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$.
Let $a \in \mathbb{Z}/p\mathbb{Z}$. If A is its unique representation in $\mathcal{H}$, then:

$$\mathcal{R}_j(a) = \{A + J \mid J \in \mathcal{R}_j(0)\}\,.$$

Questions:

- How to compute a representation in $\mathcal{H}$?
- How to make PMNS elements live in a set $\mathcal{D}_j$?

Let us first focus on $\mathcal{D}_1$.

An interesting comparison: $\mathcal{D}_1$ vs $\mathcal{H}$

Comparison 1:

If $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$, then:

- each $a \in \mathbb{Z}/p\mathbb{Z}$ has **exactly one representation** in $\mathcal{H}$.
- each $a \in \mathbb{Z}/p\mathbb{Z}$ has **exactly** 2^n **representation** in $\mathcal{D}_1$.

Comparison 2:

- If $A \in \mathcal{H}$, then $\|A\|_\infty < \|\mathcal{G}\|_1$.
- If $A \in \mathcal{D}_1$, then $\|A\|_\infty \leqslant \|\mathcal{G}\|_1$.

So, same memory requirement to represent their elements.
But, different redundancies.

Internal reduction to $\mathcal{D}_1$

Let $A \in \mathbb{Z}_{n-1}[X]$, with $A = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})\mathcal{G}$.

Fundamental property:

If $\forall i \in \{0, ..., n-1\},\ -\phi \leqslant \alpha_i \leqslant 0$, then:

$$\textbf{GMont-like}(A) \in \mathcal{D}_1.$$

Question:

How to make all the coordinates of an element negative?

Answer:

Using **the translation vector**.

The translation vector (a simplified version)

Let $A, B \in \mathcal{B}$ and $C = A \times B \bmod E$.

Property:

$C = \alpha\mathcal{G}$, with $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{R}^n$ such that:

$$\|\alpha\|_\infty \leqslant w(\rho - 1)^2 \|\mathcal{G}^{-1}\|_1 \,.$$

- Let $u = \lceil w(\rho - 1)^2 \|\mathcal{G}^{-1}\|_1 \rceil$.
- The **translation vector** $\mathcal{T}$ is defined as follows:

$$\mathcal{T} = (-u, \ldots, -u)\mathcal{G} \,.$$

Important: note that $\mathcal{T} \in \mathcal{L}$.

The translation vector (a simplified version)

Let $A, B \in \mathcal{B}$ and $C = A \times B \bmod E$.

Property:

$C = \alpha\mathcal{G}$, with $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{R}^n$ such that:

$$\|\alpha\|_\infty \leqslant w(\rho - 1)^2 \|\mathcal{G}^{-1}\|_1 \,.$$

- Let $u = \lceil w(\rho - 1)^2 \|\mathcal{G}^{-1}\|_1 \rceil$.
- The **translation vector** $\mathcal{T}$ is defined as follows:

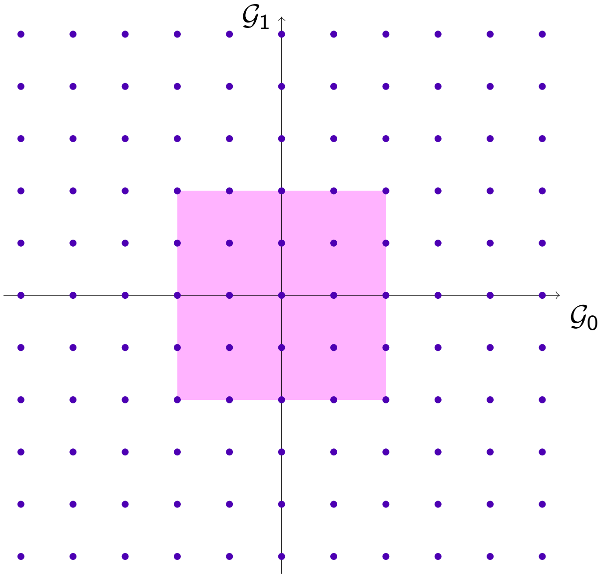
$$\mathcal{T} = (-u, \ldots, -u)\mathcal{G} \,.$$

Important: note that $\mathcal{T} \in \mathcal{L}$.

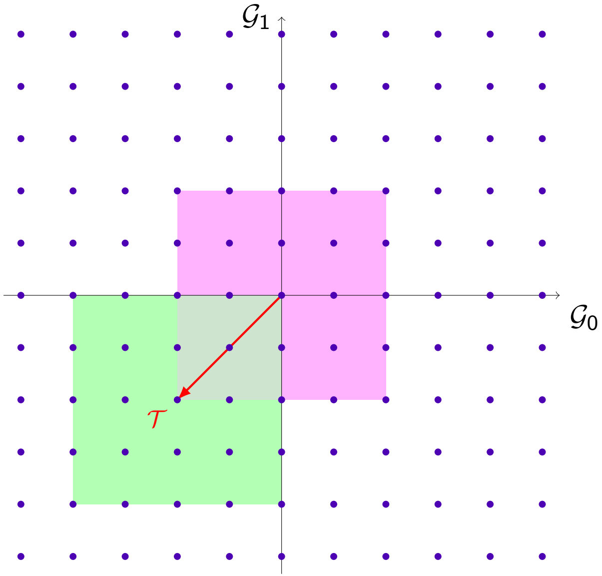
Consequence:

- $C + \mathcal{T} = \beta\mathcal{G}$, with $-2u \leqslant \beta_i \leqslant 0$.
- Thus, if $\phi \geqslant \mathbf{2u}$, then **GMont-like**$(C + \mathcal{T}) \in \mathcal{D}_1$.

The translation vector: example for $\phi = 4$, with $u = 2$



The translation vector: example for $\phi = 4$, with $u = 2$



About the bounds

Note: For simplicity, the parameter δ for 'free' additions is not included. See https://eprint.iacr.org/2023/1231 for full formulas and details.

Old bounds on ρ and ϕ:

$$\rho \geqslant 2\|\mathcal{G}\|_1 \,,$$

$$\phi \geqslant 2w\rho \,.$$

New bounds for reduction in $\mathcal{D}_1$, using $\mathcal{T}$:

$$\rho = \|\mathcal{G}\|_1 + 1 \,,$$

$$\phi \geqslant 2u \,,$$

with $u = \lceil w\|\mathcal{G}\|_1^2\|\mathcal{G}^{-1}\|_1\rceil$.

Reduction to the fundamental regions $\mathcal{H}$ and $\mathcal{H}'$

SMont-like: a Signed GMont-like

Let us assume that ϕ is an even integer.

SMont-like:

1: **Input :** $C \in \mathbb{Z}_{n-1}[X]$

2: **Output :** $S \in \mathbb{Z}_{n-1}[X]$, such that $S(\gamma) \equiv C(\gamma)\phi^{\mathbf{-1}} \pmod{p}$

3: $Q \leftarrow (c_0, \ldots, c_{n-1})\mathcal{G}' \pmod{\phi}^c$ # Q coeffs are reduced in $[-\frac{\phi}{2}, \frac{\phi}{2}[$

4: $T \leftarrow (q_0, \ldots, q_{n-1})\mathcal{G}$

5: $S \leftarrow (C + T)/\phi$

6: **return** S

Reduction to $\mathcal{H}$ and $\mathcal{H}'$

Let $A \in \mathbb{Z}_{n-1}[X]$ be a polynomial.

Property 1

If $A \in \mathcal{D}_1$, then:

$$\textbf{GMont-like}^n(A) \in \mathcal{H}\,.$$

Property 2

If $A \in \mathcal{H}$, then $\textbf{SMont-like}(A) \in \mathcal{H}'$.

Consequence

If $A \in \mathcal{D}_1$, then:

$$\textbf{SMont-like}(\textbf{GMont-like}^n(A)) \in \mathcal{H}'\,.$$

Note that $\mathcal{H}'$ and $\mathcal{H}$ have the same redundancy, while $\mathcal{H}'$ requires less memory to represent its elements.

Example: Let $p = 291791$, a 19-bit prime integer

Let $\mathcal{B} = (p, n, \gamma, \rho, E) = (p,\ 2,\ 11810,\ 841,\ X^2 - 2)$ be a PMNS, with:

$$\mathcal{G} = \begin{pmatrix} 247 & 420 \\ -593 & 173 \end{pmatrix}.$$

We have $\det(\mathcal{G}) = p$, so $\mathcal{L} = \mathcal{L}_{\mathcal{B}}$.

$$\mathcal{R}_1(0) = \{-593X + 346, -173X + 593, -420X - 247, 0\}$$

The unique representation of $a = 122706$ in $\mathcal{H}$ is $A(X) = 381X - 39$, with:

$$(-39, 381) = (\frac{219186}{291791}, \frac{110487}{291791})\mathcal{G}.$$

So, $\mathcal{R}_1(a) = \{-212X + 307,\ 208X + 554,\ -39X - 286,\ 381X - 39\}$.

Its unique representation in $\mathcal{H}'$ is $-39X - 286$, with:

$$(-286, -39) = (\frac{-72605}{291791}, \frac{110487}{291791})\mathcal{G}.$$

Equality test in the PMNS

Let $A, B \in \mathcal{B}$.

Goal:

Check if $A(\gamma) \equiv B(\gamma) \pmod{p}$, **without** conversion out of the PMNS.

Fundamental property:

Let $\boldsymbol{A} \in \boldsymbol{\mathcal{L}}$, such that: $A = \alpha\mathcal{G}$. So $\alpha \in \mathbb{Z}^n$.

If $\forall i \in \{0, ..., n-1\}$, $-\phi < \alpha_i \leqslant 0$, then:

$$\textbf{GMont-like}(A) = 0$$

Equality test in the PMNS

We assume that $\phi \geqslant 2u \geqslant 4$, with $u = \lceil w(\rho - 1)^2 \|\mathcal{G}^{-1}\|_1 \rceil$.

A fact:

If $A, B \in \mathcal{B}$, then: $A - B = \nu \mathcal{G}$, with $\|\nu\|_\infty \leqslant 2 < \phi$.

So, the previous property applies.

The check:

$$A \equiv B \iff \textbf{GMont-like}((A - B) + \mathcal{T}) = 0$$

Remark:

- Works regardless of PMNS redundancy.
- Does not require that $\mathcal{L} = \mathcal{L}_\mathcal{B}$.

Implementations

Codes to generate PMNS, study its redundancy, perform equality test (with examples) and much more are available at:

https://github.com/arithPMNS/PMNS-and-redundancy

The associated GitHub account also contains repositories that provide C code generators from PMNS parameters.

GMont-like and lattice points

Let $A \in \mathcal{L}$, such that: $A = \alpha\mathcal{G}$. So, $\alpha \in \mathbb{Z}^n$.

If $S =$ **GMont-like**(C), then $S = \beta\mathcal{G}$, with:

$$\beta_i = \lceil \frac{\alpha_i}{\phi} \rceil$$

Invariant for GMont-like

$$A = \textbf{GMont-like}(A) \iff \alpha_i \in \{0, 1\}, \forall i \in \{0, ..., n-1\}$$

Def: Canonical representations set

Let's define the canonical representation set $\mathcal{O}$ of $\mathcal{L}$ as:

$$\mathcal{O} = \{(\alpha_0, \ldots, \alpha_{n-1})\mathcal{G} \mid \alpha_i \in \{0, 1\}\}$$

Canonical representations set, for $n = 2$

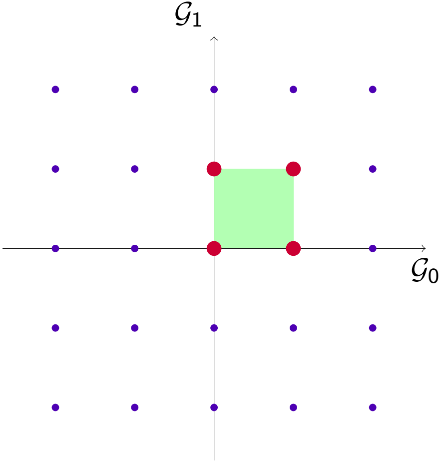


Figure: $\mathcal{O} = \mathcal{H}$ edges'

Canonical representation

Let $A \in \mathcal{L}$, such that: $A = \alpha\mathcal{G}$.

Property: Canonical representation of A

There exists $k \geqslant 0$ an integer and $\dot{A} \in \mathcal{O}$, such that:

$$\dot{A} = \textbf{GMont-like}^k(A)$$

Definition:

$\dot{A}$ is called **the canonical representation** of A.

Computation of the canonical representation

Let $A \in \mathcal{L}$, such that: $A = \alpha\mathcal{G}$.

Property: One step to the canonical representation

If $\forall i \in \{0, ..., n-1\}$, $-\phi < \alpha_i \leqslant \phi$. Then:

$$\dot{A} = \textbf{GMont-like}(A)$$

Computation of the canonical representation

Let $A \in \mathcal{L}$, such that: $A = \alpha\mathcal{G}$.

Property: One step to the canonical representation

If $\forall i \in \{0, ..., n-1\}$, $-\phi < \alpha_i \leqslant \phi$. Then:

$$\dot{A} = \textbf{GMont-like}(A)$$

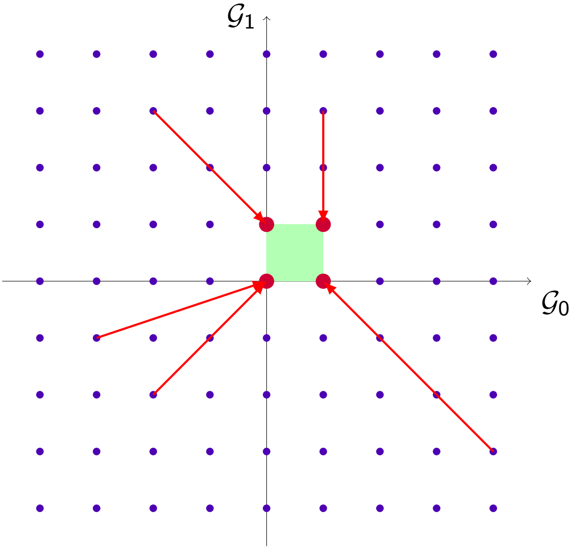
Property: a very simple case, when (the sign of) α_i is known

$$\dot{A} = \beta\mathcal{G},$$

with:

$$\beta_i = \begin{cases} 1 \text{ if } \alpha_i > 0, \\ 0 \text{ if not} \end{cases}$$

Computation of the canonical representation



Conclusion

A summary

- We have highlighted some limitations of the Mont-like (based on the polynomial M).
- We have simplified and generalised parameters generation process.
- We have provided tools and results to define and control the redundancy in the PMNS.
- We presented a simple way to perform equality test within the PMNS (even when the system is redundant).

Perspectives/questions

- How to express the redundancy in $\mathcal{H}$ when $\mathcal{L} \neq \mathcal{L}_{\mathcal{B}}$?
- Friendly bases for more security and/or efficiency?
  See: https://eprint.iacr.org/2025/090 (efficiency)

Thank you for your attention.

The external reduction matrix $\mathcal{E}$

Let's assume $E(X) = X^n + e_{n-1}X^{n-1} + \cdots + e_1 X + e_0$.

$$\mathcal{E} = \begin{pmatrix} -e_0 & -e_1 & \dots & -e_{n-1} \\ \dots & \dots & \dots & \dots \\ \vdots & \vdots & & \vdots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{matrix} \leftarrow X^n \bmod E \\ \leftarrow X^{n+1} \bmod E \\ \\ \leftarrow X^{2n-2} \bmod E \end{matrix}$$

$$R = (c_0, \dots, c_{n-1}) + (c_n, \dots, c_{2n-2})\mathcal{E}$$

Let $\mathcal{E}'$ be the $(n-1) \times n$ matrix such that $\mathcal{E}'_{ij} = |\mathcal{E}_{ij}|$. Then,

$$\|R\|_\infty \leqslant w\|A\|_\infty \|B\|_\infty ,$$

where $w = \|(1, 2, \dots, n) + (n-1, n-2, \dots, 1)\mathcal{E}'\|_\infty$.

Conversion operations

ConvToPMNS: conversion from $\mathbb{Z}/p\mathbb{Z}$ to $\mathcal{B}$

1: **Inputs:** $a \in \mathbb{Z}/p\mathbb{Z}$ and $P_i(X) \equiv (\beta^i \phi^2)_{\mathcal{B}}$, for $i = 0 \ldots (n-1)$

2: **Ensure:** $A \equiv (a.\phi)_{\mathcal{B}}$

3: $t = (a_{n-1}, ..., a_0)_\beta$ # radix-β decomposition of a

4: $U \leftarrow \sum_{i=0}^{n-1} t_i \, P_i$

5: $A \leftarrow$ **GMont-like**(U)

6: **return** A

with $\beta = 2^k$.

Conversion from $\mathcal{B}$ to $\mathbb{Z}/p\mathbb{Z}$

Let $A \in \mathbb{Z}_{n-1}[X]$. We compute: $a = A(\gamma)\phi^{-1} \pmod{p}$.
Can be optimised using precomputation or Horner polynomial evaluation method.