Polynomial Modular Number Systems and the roots of their reduction polynomial in the field $\mathbb{Z}/p\mathbb{Z}$

Jérémy Marrez, Jean-Claude Bajard

UMR 7606
Laboratory of Computer Sciences, Paris 6 LIP6
Pierre and Marie Curie University

January 15th, 2019

Context

Modular operations occur in several of today's public key cryptography algorithms as RSA, Diffie-Hellman key exchange and ECC.

Polynomial Modular Number System (PMNS) is introduced in 2004, allowing

- The implementation of an effective modular arithmetic, involving only additions and multiplications.
- A fast polynomial arithmetic and easy parallelization for an arbitrary p.
- Algorithms more efficient than known methods such as Montgomery and Barrett, and without any division.

Number of PMNS

Construction of PMNS $B = (p, n, \gamma, \rho)_{E(X)}$ based on sparse polynomials $E(X)$, called *reduction polynomials* whose roots γ are the radices of this kind of positional representation.

The number of PMNS systems for an integer p

$=$

The number of suitable E(X) $\times$ The number of roots of each $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.

Problematic

- The existing theorem on PMNS only proves the existence of at least one PMNS from an integer p, for a polynomial $E(X)$ of the specific form $E(X) = X^n + aX + b$.
- Building such systems from a given p is not trivial : one has to seek a sparse polynomial $E(X)$ satisfying the conditions of the theorem.
- and find one of its roots in $\mathbb{Z}/p\mathbb{Z}$ in an exhaustive way,
- Reductions during calculations are performed using tables that contain a lot of data.

Idea

We want to provide as many PMNS bases as possible for a fixed prime number p,

- to choose the most efficient systems in terms of calculation and storage.
- to use the different representations produced to mask the computations (protection against attacks as DPA)
  - different coding of variables from one execution to another.

Our approach

- We propose a new theorem wich proves the existence of PMNS for any kind of reduction polynomial E.
  - ✓ Offers new possibilities in the choice of PMNS parameters.
- We improves the initial bound on the digits of the system.
  - ✓ Allows to create more compact PMNS with a lower redundancy that initially proved.
- We introduce classes of irreducible polynomials $E(X)$ with good reduction properties.
  - ✓ Eligible for the role of reduction polynomial, and allowing efficient reductions.
  - ✓ Allow to describe how many PMNS systems we can built from a prime p, by evaluating the number of their roots modulo p.
- We count the minimum number of PMNS we can reach
  - Two special cases where $E(X)$ has a specific form, then the case when $E(X)$ is irreducible, whatever its the form.

Summary

- Definitions and properties
- The new theorem of PMNS
- Classes of suitable reduction polynomials
- Number of PMNS from the roots of their reduction polynomial modulo p

Summary

- Definitions and properties
- The new theorem of PMNS
- Classes of suitable reduction polynomials
- Number of PMNS from the roots of their reduction polynomial modulo p

Classical positional number system

For β a fixed integer greater than 2 call the *radix*, an integer $x \in \mathbb{N}$ with $x < \beta^m$ is represented by a unique sequence of integers $(x_i)_{i=0\ldots m-1}$ such that

$$x = \sum_{i=0}^{m-1} x_i \beta^i$$

x_i's : digits, $x_i \in \mathbb{N}$, $0 \leq x_i < \beta$, m : max number of digits.

Polynomial representation

- An integer $a < \beta^m$ is represented by the polynomial $A(X) = \sum_{i=0}^{m-1} a_i X^i$,

  with $a_i \in \mathbb{N}$, $0 \leq a_i < \beta$, satisfying $A(\beta) = a$.

The coefficients of $A(X)$ are the digits of the representation.

Modular reduction a modulo p

Idea : compute $c \equiv a \mod p$, $c < \beta^n$, since $p < \beta^n$.

- An iterative approach with no division :

If $\beta^n \equiv \delta \pmod{p}$, with $\delta << p$, $\delta < \beta^t$, δ represented by $\Delta(X)$ on at most t digits, then

$$\begin{aligned} \beta^n &\equiv \delta \pmod{p} \\ \Leftrightarrow \beta^n - \delta &\equiv 0 \pmod{p} \\ \Leftrightarrow \beta^n - \Delta(\beta) &\equiv 0 \pmod{p}. \end{aligned}$$

➤ $E(X) = X^n - \Delta(X)$, satisfies $E(\beta) \equiv 0 \pmod{p}$
We put $c = a$, and replace β^n with δ modulo p in c until $c < \beta^n$.

  ➤ Equivalent to $A(X)$ modulo $E(X)$.

➤ The reduction modulo E returns a polynomial with at most $\deg(E(X))$ digits representing the same element modulo p.

The more sparse $E(X)$ is, the less computations are needed in the reduction.

Such polynomials will serve to ensure the stability of the system.

PMNS system

A Polynomial Modular Number System (PMNS) is defined by

- a quadruple (p, n, γ, ρ)
- a polynomial $E(X) \in \mathbb{Z}[X]$, called *reduction polynomial with respect to p*,

such that for each integer x in $[0, p]$, there exists $(x_{n-1}, \ldots, x_0)$ with

$$x \equiv \sum_{i=0}^{n-1} x_i \gamma^i \pmod{p},$$

where $x_i \in \mathbb{N}$, $0 \leq x_i < \rho$, $1 < \gamma < p$, $E(\gamma) \equiv 0 \pmod{p}$ and $\deg E = n$.

Representations of an integer

The set of representations of a in the PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_{E(X)}$, denoted $a_{\mathfrak{B}}$ is define as

$$A \in a_{\mathfrak{B}} \iff \begin{cases} A(\gamma) \equiv a \pmod{p}, \\ \deg A < n, \\ \|A\|_\infty < \rho, \end{cases}$$

with $\|.\|_\infty$ the infinity norm.

Example of PMNS

We condiser the PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_{E(X)}$ with $p = 31$, $n = 3$, $\gamma = 11$ and $\rho = 4$

- to represent the elements of $\mathbb{Z}_{31}$ as vectors with 3 digits and components in {0,1,2,3}.

Here $E(X) = X^3 + 2$ because we remark $\gamma^3 + 2 = 0 \bmod 31$.

0	1	2	3	4	5	6	7
(0, 0, 0) (1, 3, 3) (3, 3, 2)	(0, 0, 1) (2, 0, 0) (3, 3, 3)	(0, 0, 2) (2, 0, 1)	(0, 0, 3) (2, 0, 2)	(0, 1, 0) (2, 0, 3)	(0, 1, 1) (2, 1, 0)	(0, 1, 2) (2, 1, 1)	(0, 1, 3) (2, 1, 2)

8	9	10	11	12	13	14	15
(0, 2, 0) (2, 1, 3)	(0, 2, 1) (2, 2, 0)	(0, 2, 2) (2, 2, 1)	(0, 2, 3) (2, 2, 2)	(0, 3, 0) (2, 2, 3)	(0, 3, 1) (2, 3, 0)	(0, 3, 2) (2, 3, 1)	(0, 3, 3) (2, 3, 2)

16	17	18	19	20	21	22	23
(1, 0, 0) (2, 3, 3)	(1, 0, 1) (3, 0, 0)	(1, 0, 2) (3, 0, 1)	(1, 0, 3) (3, 0, 2)	(1, 1, 0) (3, 0, 3)	(1, 1, 1) (3, 1, 0)	(1, 1, 2) (3, 1, 1)	(1, 1, 3) (3, 1, 2)

24	25	26	27	28	29	30
(1, 2, 0) (3, 1, 3)	(1, 2, 1) (3, 2, 0)	(1, 2, 2) (3, 2, 1)	(1, 2, 3) (3, 2, 2)	(1, 3, 0) (3, 2, 3)	(1, 3, 1) (3, 3, 0)	(1, 3, 2) (3, 3, 1)

FIGURE: The elements of $\mathbb{Z}_{31}$ in the PMNS $B = MNS(31, 3, 11, 4)$

Summary

- Definitions and properties
- The new theorem of PMNS
- Classes of suitable reduction polynomials
- Number of PMNS from the roots of their reduction polynomial modulo p

Notations

The induced norm for an $m \times n$ matrix $\mathbf{A}$, $\|\mathbf{A}\|_\infty = \max_{1 \le i \le m} \sum_{j=1}^{n} |a_{ij}|$, where $a_{i,j}$ are the coefficients of $\mathbf{A}$. The i-th power of a matrix $\mathbf{C}$ is denoted by $\mathbf{C}^{\mathbf{i}}$.

The new theorem of PMNS

Theorem 1 :
Let $p, n > 1$, $E(X)$ be an irreducible monic polynomial of degree n in $\mathbb{Z}[X]$, $\mathbf{C}$ its companion matrix and γ be a root of $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.

Then, the smallest integer $\rho_{\min}$ for which $\mathfrak{B} = (p, n, \gamma, \rho)_{E(X)}$ with $\rho \geq \rho_{\min}$ is a PMNS, is such that

$$\rho_{\min} \leq p^{1/n} s,$$

$$\text{where } s = \min\{ \, \|(\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})^T\|_\infty \, , \, \left(\det(\sum_{i=0}^{n-1} \mathbf{C}^i (\mathbf{C}^i)^T)\right)^{1/n} \, \}.$$

Proof

Step 1 : we consider the lattice $\mathfrak{L}$ composed of the PMNS representations of 0 in $\mathbb{Z}/p\mathbb{Z}$.

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & -\gamma^{n-1} \\ 0 & 1 & 0 & \dots & 0 & 0 & -\gamma^{n-2} \\ 0 & 0 & 1 & \dots & 0 & 0 & -\gamma^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & -\gamma^{2} \\ 0 & 0 & 0 & \dots & 0 & 1 & -\gamma \\ 0 & 0 & 0 & \dots & 0 & 0 & p \end{pmatrix}$$

$$A_0(X) = p \text{ and } A_i(X) = X^i - \gamma^i \text{ for } 1 \leq i \leq n-1$$

$\mathcal{L}$ has a dimension n :

n linearly independent vectors $\Rightarrow \mathcal{L}$ is a full-rank lattice and $\det(\mathcal{L}) = p$

Proof

All vectors representing in the PMNS the same element of $\mathbb{Z}/p\mathbb{Z}$ are equivalent modulo the lattice $\mathcal{L}$.

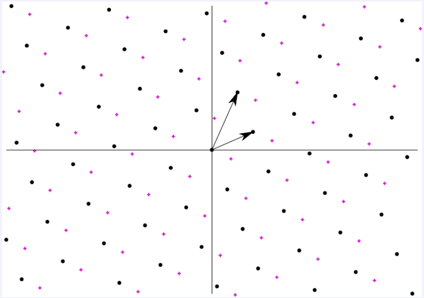


FIGURE: Elements of a PMNS representing the same integer modulo p.

Proof

Step 2 : Thanks to Minkowski's theorem ,

$$\exists V \in \mathcal{L} \text{ tel que } 0 < \|V\|_\infty \leq det(\mathcal{L})^{1/n} = p^{1/n}$$

Construction of a sub-lattice $\mathfrak{L}' \subseteq \mathfrak{L}$, of base B composed of the n vectors B_i with $B_i \in \mathbb{Z}[X]/(E)$ defined as follows

$$B_i(X) = X^i \times V(X) \mod E(X).$$

B is a base : the B_i are linearly independent. Otherwise, there exists $l \neq 0$ such that

$$\sum_{i=0}^{n-1} l_i B_i(X) = 0$$
$$\Leftrightarrow \sum_{i=0}^{n-1} l_i X^i V(X) = 0 \mod E$$
$$\Leftrightarrow L(X)V(X) = 0 \mod E$$

$\deg(E(X)) = n$, and $L(X)$, $V(X) \neq 0$ of degrees strictly between 0 and n : we have a factorization of $E(X)$. The irreducibility of $E(X)$ in $\mathbb{Z}[x]$ hypothesis makes this case impossible.

Proof

Étape 3 : The fundamental domain $\mathcal{H}$ of the sub-lattice $\mathfrak{L}'$ is defined as follows

$$\mathcal{H} = \{x \in \mathbb{R}^n \ : \ x = \sum_{i=0}^{n-1} x_i b_i, \ 0 \leq x_i < 1\}$$

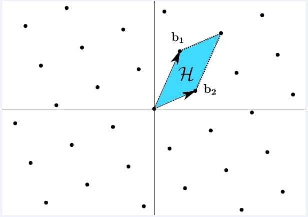


FIGURE: Fundamental domain $\mathcal{H}$ of $\mathfrak{L}'$

We consider $\mathcal{H}_0$ which intersects a half of $\mathcal{H}$ and another half of $-\mathcal{H}$.

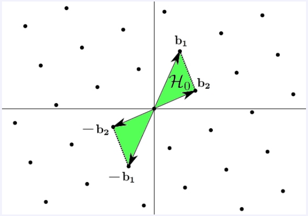


FIGURE: Domain $\mathcal{H}_0$ of $\mathfrak{L}'$

Proof

$$\text{To bound } \mathcal{H}_0 \Leftrightarrow \text{To bound } B$$

We use *the companion matrix* **C** of $E(X)$ to construct the base B.

For $E(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$,

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

$$XV(X) \mod E(X) \Leftrightarrow V \times \mathbf{C},$$

Then $B_i = V \times \mathbf{C}^i$.
For bounding **B**, i.e. the quantity $\max_{B_i(X) \in \mathbf{B}} ||B_i||_\infty$, we present two approaches that depend on how **B** is built.

Proof

First method : from Minkowski's theorem, $V \in \mathfrak{L}$ such that $\|V\|_\infty \leq p^{1/n}$.

We can recover the base **B** with the $n \times n^2$ matrix $\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1}$,

$$(\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})^T \times V^T = B.$$

B is a n^2 column vector containing the components of the n vectors of the base **B**.
To bound the $\max\limits_{B_i(X)\in\mathbf{B}} ||B_i||_\infty \Leftrightarrow$ to bound $||B||_\infty$.

The induced norm for the matrices is consistent with the infinity norm,

$$\|B\|_\infty \leq \|V\|_\infty \times \|(\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})^T\|_\infty$$

$$\|\mathbf{B}\|_\infty \leq p^{1/n} \times \|(\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})^T\|_\infty.$$

Proof

Second method : we can extract directly the base $\mathbf{B}$ as a n^2 vector of the extended lattice $\mathfrak{D}$ with base $\mathbf{D} = \mathbf{A} \times (\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})$, where $\mathbf{A}$ is the base of $\mathfrak{L}$.

$\mathbf{D}$ is an $n \times n^2$ matrix,and determinant of $\det(\mathfrak{D}) = \sqrt{\det(\mathbf{D} \times \mathbf{D}^T)}$.
From Minkowski's theorem,

$$\|\mathbf{B}\|_\infty \leq \left(\sqrt{\det(\mathbf{D} \times \mathbf{D}^T)}\right)^{1/n}.$$

We note, $\mathbf{K} = (\mathbf{C}^0|\mathbf{C}^1|\cdots|\mathbf{C}^{n-1})$.
Thus $\mathbf{D} = \mathbf{A} \times \mathbf{K}$ and

$$\det(\mathbf{D} \times \mathbf{D}^T) = \det(\mathbf{A}) \times \det(\mathbf{K} \times \mathbf{K}^T).$$

and

$$\|\mathbf{B}\|_\infty \leq \left(p \times \sqrt{\det(\mathbf{K} \times \mathbf{K}^T)}\right)^{1/n}.$$

We remark that, $\mathbf{K} \times \mathbf{K}^T = \sum_{i=0}^{n-1} \mathbf{C}^{\mathbf{i}}(\mathbf{C}^{\mathbf{i}})^T$.

Proof

Step 4 : $\mathcal{H}_0$ that we have bounded contains all the vectors representing in $\mathfrak{B}$ an element of $\mathbb{Z}/p\mathbb{Z}$ $\square$

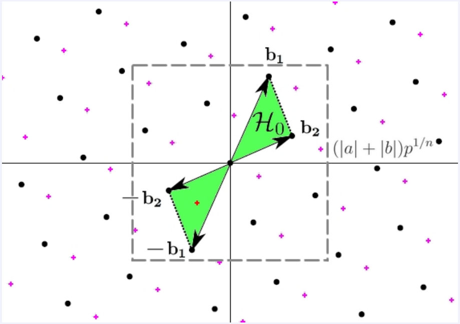


FIGURE: Bounding of $\mathcal{H}_0$.

Système PMNS

Un système AMNS vérifiant les conditions de ce théorème d'existence est appelé *Système de représentation modulaire polynomial* (PMNS).

Summary

- Definitions and properties
- The new theorem of PMNS
- Classes of suitable reduction polynomials
- Number of PMNS from the roots of their reduction polynomial modulo p

Suitable reduction polynomials for PMNS

To build compact systems with an efficient arithmetic on representations, we need polynomials $E(X)$ with good reduction properties, which ensure

- a reduction with a limited number of steps,
- a low bound on $\rho_{\min}$ for the digits.

For these reasons, a polynomial is said *suitable for reduction* if

- $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, with $n \geq 2$ and $k \leq \frac{n}{2}$
  - ✓ to garantee a reduction in only two steps.
- E(X) is sparse, with few non-zero coefficients, small, if possible equal to 1.
  - ✓ to ensure a small bound on $\rho_{\min}$ which depends on $E(X)$

ClassCyclo(n)

For a fixed $n \geq 2$, the first class of polynomials eligible for the role of reduction polynomial, called `ClassCyclo(n)`, is the set composed of the three cyclotomics of degree n,

- $\Phi_{2n}(X) = X^n + 1$, if n is a power of 2
- $\Phi_{\frac{3n}{2}}(X) = X^n + X^{\frac{n}{2}} + 1$, if n is even and $\frac{n}{2} = 3^k$ for $k \in \mathbb{N}$
- $\Phi_{3n}(X) = X^n - X^{\frac{n}{2}} + 1$, if n is even $\frac{n}{2} = 2^i \,.\, 3^j$ for $i, j \in \mathbb{N}$

Proof

Let $m \in \mathbb{N} \backslash \{0\}$.

The roots of $\Phi_m(X)$ are exactly the primitive roots $m - th$ of unity

$$\Phi_m(X) = \prod_{\substack{k=1 \\ k \wedge m = 1}}^{m} (X - \zeta^k).$$

For all m, the polynomial $\Phi_m(X)$ is irreducible in $\mathbb{Z}[X]$.

To satisfy the reduction properties : a polynomial of degree n must have its second non-zero term of degree lower than $n/2$.

- $\Phi_m(X)$ of degree $n = \varphi(m)$ is self-reciprocal for $m \geq 2$,

$$\text{i.e. } a_i = a_{n-i}, \text{ for } 0 \leq i \leq n.$$

➤ for $n \geq 2$, the only ones possible have two terms, one of degree n and one constant, or three, with the middle term of degree $n/2$.

Bound of rho for *ClassCyclo*(n) : determinant vs norm

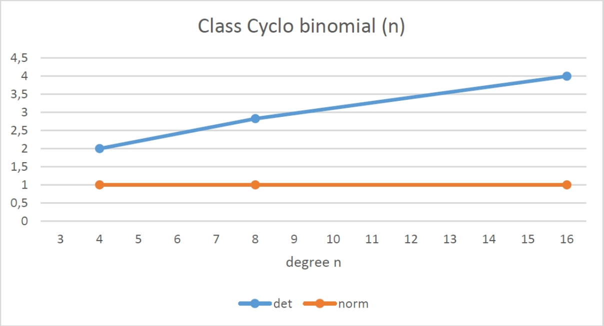


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassCyclo*(n)

Number of PMNS with a cyclotomic reduction polynomial

Let p prime, $m \geq 3$ such that $\varphi(m)$ is even and $p \equiv 1 \mod m$.

Then there exists $\varphi(m)$ PMNS $(p, n, \gamma_i, \rho)_{E(X)}$ with

- $\rightarrow$ $n = \varphi(m)$,
- $\rightarrow$ $E(X) = \Phi_m(X)$,
- $\rightarrow$ $\rho \leq \lceil 2p^{1/\varphi(m)} \rceil$
- $\rightarrow$ and γ_i one of the $\varphi(m)$ distinct roots of $E(X)$ modulo p, $0 \leq i < \varphi(m)$.

Proof

The roots ζ of a cyclotomic polynomial $\Phi_m(X)$ are of order m.

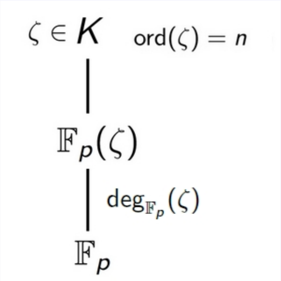
We write $\deg_{\mathbb{F}_p}(\zeta)$ the degree of a root ζ on the field of p elements with p prime.

For every ζ,

$$\deg_{\mathbb{F}_p}(\zeta) = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(p).$$

As we want

$$\zeta \in \mathbb{Z}/p\mathbb{Z}$$
$$\Leftrightarrow \deg_{\mathbb{F}_p}(\zeta) = 1$$
$$\Leftrightarrow ord_{(\mathbb{Z}/n\mathbb{Z})^\times}(p) = 1$$



The only element of order 1 of a multiplicative group is the neutral element 1.

- $p \equiv 1 \mod m$.

All roots ζ have the same order, they all have the same degree on $\mathbb{F}_p$.

The roots of $\Phi_m(X)$ are the roots of $P(X) = X^m - 1$, and $P(X)$ and $P'(X) = mX^{m-1}$ have no common root, then all the roots of $\Phi_m(X)$ are distinct.

- the $\varphi(m)$ distincts roots of $\Phi_m(X)$ are in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \mod m$.

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
Φ_{2n} $\Phi_{\frac{3n}{2}}$ Φ_{3n}	if n is a power of 2 if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 3^k$ if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 2^i \,.\, 3^j$	all iff $p \equiv 1 \mod n'$ where n' is the order of the roots

Number of PMNS from *ClassCyclo*(n)

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

- If $\nu_2(n) > 0$, $\nu_3(n) = 0$, and $2\,n$ divides $p-1$, then there exist n PMNS $(p, n, \gamma_i, \rho)_{E(X)}$ with $E(X) = \Phi_{2n}(X) = X^n + 1$ and γ_i one of its n distinct roots modulo p.

- If $\nu_2(n) = 1$, $\nu_3(n) \geq 0$, and $3\,n\,/\,2$ divides $p-1$, then there exist n PMNS $(p, n, \gamma_i, \rho)_{E(X)}$ with $E(X) = \Phi_{\frac{3n}{2}}(X) = X^n + X^{\frac{n}{2}} + 1$ and γ_i one of its n distinct roots modulo p.

- If $\nu_2(n) \geq 1$, $\nu_3(n) \geq 0$, and $3\,n$ divides $p-1$, then there exist n PMNS $(p, n, \gamma_i, \rho)_{E(X)}$ with $E(X) = \Phi_{3n}(X) = X^n - X^{\frac{n}{2}} + 1$ and γ_i one of its n distinct roots modulo p.

Example

Construction of 8 PMNS with a cyclotomic reduction polynomial for $p = 22273$ and $n = 4$

$E(X)$	γ	$\rho_{\min}$
$X^4 + 1$	1254	9
	4991	9
	17282	9
	21019	9
$X^4 - X^2 + 1$	1355	9
	7512	9
	14761	9
	20918	9

ClassBinomial(n, c)

For a fixed $n \geq 2$, and $c \in \mathbb{Z}$ such that there exists μ prime satisfying

$$c = q\mu^k, \text{ with } \gcd(q, \mu) = 1 \text{ and } \gcd(k, n) = 1,$$

the fourth class of polynomials eligible for the role of reduction polynomial, and call `ClassBinomial(n, c)`, is the singleton $\{X^n + c\}$.

Proof

Dumas's criterion :

For $P(X) = a_nX^n + \cdots + a_1X + a_0 \in Z[X]$, if $\exists\, \mu$ prime such that

1) $\frac{\nu_\mu(a_i)}{i} > \frac{\nu_\mu(a_n)}{n}$ for $1 \leq i \leq n-1$,
2) $\nu_\mu(a_0) = 0$,
3) $\gcd(\nu_\mu(a_n)\ ,\ n) = 1$,

then $P(X)$ irreducible in $Q[X]$.

We divide $P(X)$ by its leading coefficient a_n,

- $\nu_\mu(a_n/a_n) = 0$ and $\nu_\mu(a_0/a_n) = -\nu_\mu(a_n)$.

A binomial $P(X) = X^n + a_0$ respects Dumas's criterion as soon as there exists μ prime such that

$$\gcd(\nu_\mu(a_0)\ ,\ n) = 1,$$

i.e. $P(X) = X^n + c\mu^k$, $c \in \mathbb{Z}$, μ prime, $\gcd(c, \mu) = 1$ and $\gcd(k, n) = 1$, where $k = \nu_\mu(c\mu^k)$.

Gauss's lemma : $P(X)$ is irreducible over $\mathbb{Z}$.

Bound of rho for *ClassBinomial*(n, c), $c = 3$: determinant vs norm

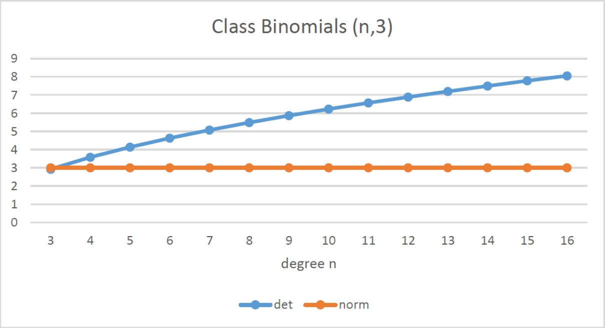


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassBinomial*$(n, 3)$

Number of PMNS from *ClassBinomial*(n, c)

Let p prime, $n \geq 2$, $c \in \mathbb{Z}$, $|c| \geq 2$, such that there exists a prime μ satisfying

$$\gcd(\nu_\mu(c)\ ,\ n) = 1.$$

Let g a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, and y such that $g^y \equiv c \mod p$ and

$$\gcd(n, p-1) | y.$$

Then there exist $\gcd(n, p-1)$ PMNS $(p, n, \gamma_i, \rho)_{E(X)}$, with

- → $E(X) = X^n - c$,
- → $\rho = \lceil cp^{1/n} \rceil$
- → and γ_i one of the $\gcd(n, p-1)$ distinct roots of $E(X)$ modulo p, $0 \leq i < \gcd(n, p-1)$.

Existence

p prime $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ is a field and $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic ;

$\exists$g $\in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\forall x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\exists\, y$ such that $g^y \equiv x \mod p$.

Let $c \in \mathbb{Z}$, $|c| \geq 2$ for wich $\exists\, \mu$ prime satisfying $\gcd(\nu_\mu(c)\ ,\ n) = 1$.

In particular, $\exists y$ tel que

$$g^y \equiv c \mod p. \tag{1}$$

We denote $d = \mathrm{pgcd}(n, p-1)$

Extended Euclidean Theorem : $\exists\, u$ and v such that :

$$un + v(p-1) = d$$

We assume $d \mid y$, i.e. $\exists\, m$ such that $y = dm$.

$$unm + v(p-1)m = dm = y \tag{2}$$

Existence

We replace (2) in (1)

$$g^{unm+v(p-1)m} \equiv c \mod p$$
$$(g^{um})^n (g^{(p-1)})^{vm} \equiv c \mod p$$

Fermat's little theorem : if p is prime, $g^{(p-1)} \equiv 1 \mod p$, then

$$(g^{um})^n \equiv c \mod p$$

$\gamma = g^{um}$ is a root of $X^n - c \mod p$.

Roots d-th of unity

$d \mid p-1 \Rightarrow p \equiv 1 \mod d$.
ω_i for $1 \leq i \leq d$, the d roots d-th of unity, of order d_i dividing d verify

$$\begin{aligned} \deg_{\mathbb{F}_p}(\omega_i) &= \mathrm{ord}_{(\mathbb{Z}/d_i\mathbb{Z})^\times}(p) \\ &= 1 \end{aligned}$$

Then for $1 \leq i \leq d$, $\omega_i \in \mathbb{F}_p$.

Number of roots

γ une racine de $X^n - c \mod p$
For $1 \leq i \leq d$,

$$(w_i\gamma)^n = w_i^n\gamma^n \mod p$$

Since $d \mid n$, we obtain

$$\begin{aligned} w_i^n\gamma^n &= (w_i^d)^{\frac{n}{d}}\gamma^n \mod p \\ &= c \mod p \end{aligned}$$

$\Rightarrow d$ distinct roots $w_i\gamma$, $1 \leq i \leq d$, of $X^n - c$ in $\mathbb{F}_p$. $\square$

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
Φ_{2n} $\Phi_{\frac{3n}{2}}$ Φ_{3n}	if n is a power of 2 if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 3^k$ if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 2^i . 3^j$	all iff $p \equiv 1 \mod n'$ where n' is the order of the roots
$X^n + c\mu^k$, $c \in \mathbb{Z}$	μ prime, $\gcd(c, \mu) = 1$ and $\gcd(k, n) = 1$	1 if $\gcd(n, p-1) = 1$ or $\gcd(n, p-1)$ if $\gcd(n, p-1) \mid y$ with $g^y \equiv c \mod p$ where g generates $(\mathbb{Z}/p\mathbb{Z})^\times$

Proposition 1

Let $E(X) = X^n - c$, $c \in \mathbb{Z}$, $|c| \geq 2$, satisfying the Theorem 1 for a prime p, with $\gcd(n, p-1) \mid \frac{p-1}{2}$.

Then $E'(X) = X^n + c$ is also a reduction binomial with respect to p and allows to construct the same number of PMNS.

Proposition 2

Let p prime, $n \geq 2$, $c \in \mathbb{Z}$, $|c| \geq 2$, such that there exists a prime μ satisfying $\gcd(\nu_\mu(c)\ ,\ n) = 1$, and g a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ relatively prime to μ.

Then there exist $\gcd(n, p-1)$ PMNS $(p, n, \gamma_i, \rho)_{E(X)}$, where

→ $E(X) = X^n - cg^t$ is the unique reduction binomial with respect to p for t in $[|0, \gcd(n, p-1) - 1|]$,

→ $\rho = \lceil cg^t p^{1/n} \rceil$

→ and γ_i one of the $\gcd(n, p-1)$ distinct roots of $E(X)$ modulo p, $0 \leq i < \gcd(n, p-1)$.

Proposition 3

Let p prime, $n \geq 2$ and two reduction polynomials with respect to p, $E(X) = X^n - c$ and $E'(X) = X^n - c'$, satisfying $\gcd(\nu_\mu(a_0)\ ,\ n) = 1$, and such that at least one prime μ satisfying $\gcd(\nu_\mu(c)\ ,\ n) = 1$ is relatively prime to c'.

Then there exist $\gcd(n, p-1)$ PMNS $(p, n, \gamma_i^{''}, \rho)_{E''}$, with $E^{''}(X) = X^n - (cc')$, $\rho = \lceil cc'p^{1/n} \rceil$ and γ_i one of the $\gcd(n, p-1)$ distinct roots of $E^{''}(X)$ modulo p, $0 \leq i < \gcd(n, p-1)$.

Example

For the prime $p = 317$, $n = 4$. Here $\gcd(n, p-1) = 4$.

We set $c = 5$, and pick 2 as a generator of $(\mathbb{Z}/317\mathbb{Z})^\times$ and $\gcd(2,5) = 1$.
From Proposition 2, there exists a unique reduction binomial $E(X) = X^n - 5 \cdot 2^t$ for t in $[|0, 3|]$.

The following Tables show the roots of the four polynomials considered for $c = 5$, and for $c = -5$.

P(X) for $c = 5$	roots in $\mathbb{Z}/317\mathbb{Z}$
$X^4 - 5$	/
$X^4 - 5 \cdot 2$	71 148 169 246
$X^4 - 5 \cdot 2^2$	/
$X^4 - 5 \cdot 2^3$	/

P(X) for $c = -5$	roots in $\mathbb{Z}/317\mathbb{Z}$
$X^4 + 5$	/
$X^4 + 5 \cdot 2$	/
$X^4 + 5 \cdot 2^2$	/
$X^4 + 5 \cdot 2^3$	77 98 219 240

ClassTrinomials(n)

For a fixed $n \geq 2$, the second class of polynomials eligible for the role of reduction polynomial, and call `ClassTrinomials(n)`, is the set of trinomials of degree n satisfying the criteria of the Theorem of Ljunggren, described as follow,

if $n = n_1 d, m = m_1 d$, with $d = \gcd(n, m)$, $n \leq 2m$, then the polynomial $X^n + \delta X^m + \epsilon$, with δ and ϵ equal to ± 1, is irreducible in $\mathbb{Q}[X]$, apart from the three cases :

- n_1 and m_1 are both odd
- n_1 is even and $\epsilon = 1$
- m_1 is even and $\delta = \epsilon$

where $P(X)$ is a product of the polynomial $X^{2d} + \delta^m \epsilon^n X^d + 1$ and a second irreducible polynomial.

Bound of rho for *ClassTrinomials*(n) : determinant vs norm

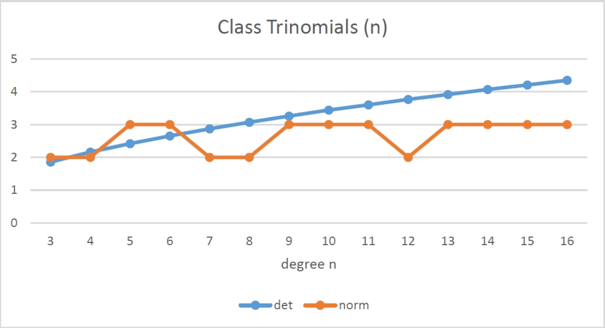


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassTrinomials*(n)

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
Φ_{2n} $\Phi_{\frac{3n}{2}}$ Φ_{3n}	if n is a power of 2 if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 3^k$ if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 2^i . 3^j$	all iff $p \equiv 1 \mod n'$ where n' is the order of the roots
$X^n + c\mu^k$, $c \in \mathbb{Z}$	μ prime, $\gcd(c, \mu) = 1$ and $\gcd(k, n) = 1$	1 if $\gcd(n, p-1) = 1$ or $\gcd(n, p-1)$ if $\gcd(n, p-1) \mid y$ with $g^y \equiv c \mod p$ where g generates $(\mathbb{Z}/p\mathbb{Z})^\times$
$X^n + \delta X^m + \epsilon$, with $n \leq 2m$ $\delta = \pm 1$, $\epsilon = \pm 1$ $X^n + 2X - 1$ $X^{2m+1} + 2X + 1$ $X^{2m} - 2X - 1$	yes, apart from the three cases : $\frac{n}{\gcd(n,m)}$ and $\frac{m}{\gcd(n,m)}$ are both odd, $\frac{n}{\gcd(n,m)}$ is even and $\epsilon = 1$, $\frac{m}{\gcd(n,m)}$ is even and $\delta = \epsilon$. yes	

Example

Construction of 8 PMNS with a reduction trinomial and $\pi = 2$

(p, n)	$E(X)$	γ	$\rho_{\min}$
$(22273, 3)$	$X^3 + X + 1$	18048	19
	$X^3 - X + 1$	1105	18
		3912	20
		17256	16
	$X^3 + X - 1$	4225	19
	$X^3 - X - 1$	5017	16
		18361	20
		21168	18

ClassQuadrinomials(n)

For a fixed $n \geq 2$, the third class of polynomials eligible for the role of reduction polynomial, and call `ClassQuadrinomials(n)`, is the set of quadrinomials of degree n satisfying the criteria of the Theorem of Ljunggren, described as follow,

let $P(X) = X^n + X^m + X^q \pm 1$, where $n \geq m + \mu$. We set $n = n_1 d, m = m_1 d, q = q_1 d$ and $(n_1, m_1, q_1) = 1$.
If n_1, m_1 and q_1 are odd integers then $P(X)$ is irreducible over $\mathbb{Z}$.

Bound of rho for *ClassQuadrinomials*(n) : determinant vs norm

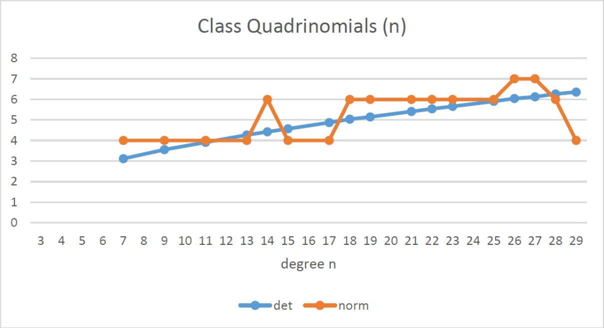


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassQuadrinomials*(n)

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
$X^n + X^m + X^p \pm 1$ with $n \geq m + p$	$n/\gcd(n, m, p)$, $m/\gcd(n, m, p)$ and $p/\gcd(n, m, p)$ are odd integers	

Lemma 1

Let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$, if

$$|a_k| > 1 + |a_{n-1}| + \cdots + |a_{k+1}| + |a_{k-1}| + \cdots + |a_0|,$$

then exactly k roots of P(X) lie strictly inside the unit circle, i.e. are such that $|r| < 1$,

and the $n-k$ other roots lie strictly outside the unit circle, i.e. are such that $|r| > 1$.

ClassPrimeCst(n, μ)

For a fixed $n \geq 2$, and a prime μ, the fifth class of polynomials eligible for the role of reduction polynomial, and call `ClassPrimeCst`$(\mathtt{n}, \mu)$, is the set composed of the polynomials $X^n + \sum_{i=1}^{n/2} \epsilon_i X^i \pm \mu$, with $\epsilon_i \in \{-1, 0, 1\}$.

Proof

We find a contradiction in the case $k = 0$, assuming a_0 is prime.

If $P(X)$ is reducible in $\mathbb{Z}[X]$, it admits a decomposition of the form

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 = G(X)H(X)$$

Since $|a_0|$ is prime, $|G(0)|$ or $|H(0)|$ is equal to 1, hence we assume $|G(0)| = 1$.

As the complex zeros of $G(X)$ satisfy $\prod_{z|G(z)=0} |z| = \frac{1}{lc(G)} \leq 1$,

- at least one root, suppose z_0, is such that $|z_0| \leq 1$.

But $P(X)$ also verifies Lemma 1 for $k = 0$,

- all its roots z satisfy $|z| > 1$,

which leads to the expected contradiction, then P is irreducible over $\mathbb{Z}$.

Bound of rho for *ClassPrimeCst*(n, μ), $\mu = 3$: determinant vs norm

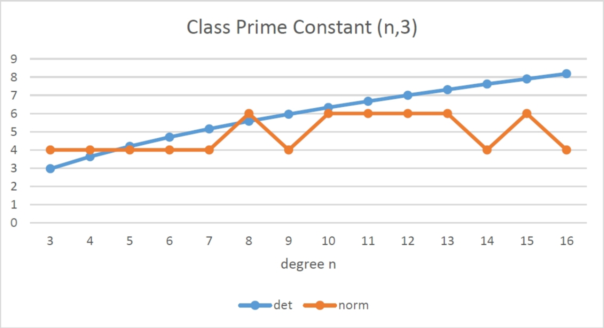


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassPrimeCst*$(n, 3)$

$ClassPerron(n, a_1)$

For a fixed $n \geq 2$, and an integer $a_1 \in \mathbb{N}$, the sixth class of polynomials eligible for the role of reduction polynomial, and call $\mathtt{ClassPerron(n, a_1)}$, is the set composed of the polynomials $X^n + \sum_{i=2}^{n/2} \epsilon_i X^i \pm a_1 X \pm 1$, with $\epsilon_i \in \{-1, 0, 1\}$.

Proof

We find a contradiction in the case $k = 1$, assuming $|a_0| = 1$.

If $P(X)$ is reducible in $\mathbb{Z}[X]$, it admits a decomposition of the form

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 = G(X)H(X)$$

Here $|G(0)| = |H(0)| = |a_0| = 1$.

As the complex zeros of $G(X)$ satisfy $\prod_{z|G(z)=0} |z| = \frac{1}{lc(G)} \leq 1$ (same with $H(X)$),

- at least one root of $G(X)$ and one root of $H(X)$, suppose $z_{G(X)}$ and $z_{H(X)}$, are such that $|z_{G(X)}| \leq 1$ and $|z_{H(X)}| \leq 1$.

But $P(X)$ also verifies Lemma 1 for $k = 1$,

- only one of its roots z satisfies $|z| \leq 1$,

which leads to the expected contradiction, then P is irreducible over $\mathbb{Z}$.

Bound of rho for *ClassPerron*(n, a_1), $a_1 = 3$: determinant vs norm

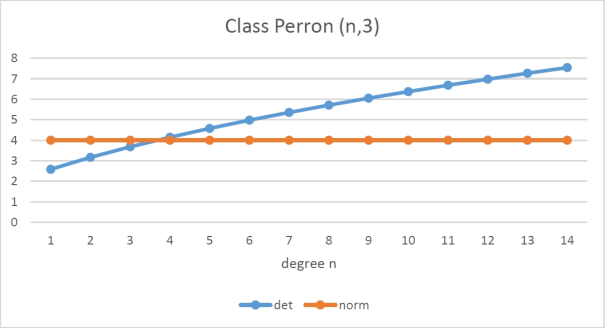


FIGURE: Graph of the average bound of rho depending on the degree n of $E(X)$ in *ClassPerron*$(n, 3)$

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
$X^n + X^m + X^p \pm 1$ with $n \geq m + p$	$n/\gcd(n,m,p)$, $m/\gcd(n,m,p)$ and $p/\gcd(n,m,p)$ are odd integers	
$X^n + a_k X^k + \cdots + a_0$ with $a_i \in \mathbb{Z}$, $0 \leq i \leq k$ and $k \leq \frac{n}{2}$	$\lvert a_0\rvert > 1 + \lvert a_{n-1}\rvert + \cdots + \lvert a_1\rvert$ and $\lvert a_o\rvert$ prime or $\lvert a_1\rvert > 1 + \lvert a_{n-1}\rvert + \cdots + \lvert a_2\rvert + \lvert a_0\rvert$ and $\lvert a_o\rvert = 1$	

Summary

- Definitions and properties
- The new theorem of PMNS
- Classes of suitable reduction polynomials
- Number of PMNS from the roots of their reduction polynomial modulo p

Number of systems when $E(X)$ is irreducible

Theorem 2 :

Let p prime, n $>$ 2, E a polynomial of degree n and irreducible in $\mathbb{Z}[X]$, and $D(X) = \gcd(X^p - X, E(X)) \mod p$.

If $D(X)$ is non constant, then $E(X)$ is a reduction polynomial with respect to p and :

- If the discriminant of $D(X)$ is not null, there exists $\deg(D(X))$ PMNS $(p, n, \gamma_i, \rho \leq \lceil p^{1/n} s \rceil)_{E(X)}$, where C is the companion matrix of $E(X)$, and $s = \min\{ \, \|(C^0 C^1 \cdots C^{n-1})^T\|_\infty \, , \, \det(\sum_{i=0}^{n-1} C^i (C^i)^T) \, \}$.
- If the discrimiant of $D(X)$ is null, there exists at least one PMNS with the same property.

Proof

Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.
A root γ of $P(X)$ belongs to $\mathbb{Z}/p\mathbb{Z}$ is also a root $X^p - X \mod p$.

$$\text{The number of roots of } P(X) \text{ in } \mathbb{Z}/p\mathbb{Z}$$
$$=$$
$$\deg(D(X)) \text{ with } D(X) = \gcd(X^p - X, P(X)) \mod p,\ D(X) \text{ non constant.}$$

We denote NrP_p the number of roots of $P(X)$ modulo p.

Two cases :

- → The discriminant of $D(X)$ is not null, $D(X)$ is separable, i.e. it has no multiple root.
  - ➤ $NrP_p = \deg(D(X))$.
- → The discriminant of $D(X)$ is null, $D(X)$ has at least one multiple root
  - ➤ $1 \leq NrP_p < \deg(D(X))$.

If $P(X)$ is irreducible in $\mathbb{Z}[X]$, from Theorem 1 the result is proved.

Example

We choose a prime $p = 57896044618658097711785492504343953926634992332820282019728792003956566811073$ on 256 bits,

$n = 8$, and we fix $\|E(X)\|_\infty \leq 7$.

Classes are given with the corresponding minimum number of PMNS we can reach from them.

$\texttt{ClassCyclo(n)}$: at least 8 systems	$\texttt{ClassTrinomials(n)}$: at least 24 systems
$\texttt{ClassQuadrinomials(n)}$: no system	$\texttt{ClassBinomials(n, 3)}$: no system
$\texttt{ClassBinomials(n, 4)}$: no system	$\texttt{ClassBinomials(n, 5)}$: no system
$\texttt{ClassBinomials(n, 6)}$: at least 16 systems	$\texttt{ClassBinomials(n, 7)}$: no system
$\texttt{ClassPrimeCst(n, 3)}$: at least 6 systems	$\texttt{ClassPrimeCst(n, 5)}$: at least 158 systems
$\texttt{ClassPrimeCst(n, 7)}$: at least 190 systems	$\texttt{ClassPerron(n, 3)}$: at least 8 systems
$\texttt{ClassPerron(n, 4)}$: at least 38 systems	$\texttt{ClassPerron(n, 5)}$: at least 78 systems
$\texttt{ClassPerron(n, 6)}$: at least 104 systems	$\texttt{ClassPerron(n, 7)}$: at least 112 systems

- There are at least 742 systems in total.

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
Φ_{2n} $\Phi_{\frac{3n}{2}}$ Φ_{3n}	if n is a power of 2 if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 3^k$ if $n \equiv 0 \mod 2$ and $\frac{n}{2} = 2^i . 3^j$	all iff $p \equiv 1 \mod n'$ where n' is the order of the roots
$X^n + c\mu^k$, $c \in \mathbb{Z}$	μ prime, $\gcd(c, \mu) = 1$ and $\gcd(k, n) = 1$	1 if $\gcd(n, p-1) = 1$ or $\gcd(n, p-1)$ if $\gcd(n, p-1) \mid y$ with $g^y \equiv c \mod p$ where g generates $(\mathbb{Z}/p\mathbb{Z})^\times$
$X^n + \delta X^m + \epsilon$, with $n \leq 2m$ $\delta = \pm 1$, $\epsilon = \pm 1$ $X^n + 2X - 1$ $X^{2m+1} + 2X + 1$ $X^{2m} - 2X - 1$	yes, apart from the three cases : $\frac{n}{\gcd(n,m)}$ and $\frac{m}{\gcd(n,m)}$ are both odd, $\frac{n}{\gcd(n,m)}$ is even and $\epsilon = 1$, $\frac{m}{\gcd(n,m)}$ is even and $\delta = \epsilon$. yes	$\leq \deg(\gcd(X^p - X, E(X)) \mod p)$ $O(\frac{\log p}{\log \log p})$ when $p \to +\infty$

Table of the reduction polynomials from which we can generate PMNS bases

$E(X)$	$E(X)$ irreducible in $\mathbb{Z}[x]$	roots of $E(X) \in \mathbb{Z}/p\mathbb{Z}[x]$
$X^n + X^m + X^p \pm 1$ with $n \geq m + p$	$n/\gcd(n, m, p)$, $m/\gcd(n, m, p)$ and $p/\gcd(n, m, p)$ are odd integers	$\leq \deg(\gcd(X^p - X, E(X)) \mod p)$
$X^n + a_k X^k + \cdots + a_0$ with $a_i \in \mathbb{Z}$, $0 \leq i \leq k$ and $k \leq \frac{n}{2}$	$\lvert a_0 \rvert > 1 + \lvert a_{n-1} \rvert + \cdots + \lvert a_1 \rvert$ and $\lvert a_o \rvert$ prime or $\lvert a_1 \rvert > 1 + \lvert a_{n-1} \rvert + \cdots + \lvert a_2 \rvert + \lvert a_0 \rvert$ and $\lvert a_o \rvert = 1$	

Change of the radix γ

- $\mathfrak{B}_1 = (p = 31, n = 3, \gamma = 3, \rho = 4)$

0	1	2	3	4	5	6	7	8	9
(0, 0, 0) (3, 1, 1)	(0, 0, 1) (3, 1, 2)	(0, 0, 2) (3, 1, 3) (3, 2, 0)	(0, 0, 3) (0, 1, 0) (3, 2, 1)	(0, 1, 1) (3, 2, 2)	(0, 1, 2) (3, 2, 3) (3, 3, 0)	(0, 1, 3) (0, 2, 0) (3, 3, 1)	(0, 2, 1) (3, 3, 2)	(0, 2, 2) (3, 3, 3)	(0, 2, 3) (0, 3, 0) (1, 0, 0)

10	11	12	13	14	15	16	17	18	19
(0, 3, 1) (1, 0, 1)	(0, 3, 2) (1, 0, 2)	(0, 3, 3) (1, 0, 3) (1, 1, 0)	(1, 1, 1)	(1, 1, 2)	(1, 1, 3) (1, 2, 0)	(1, 2, 1)	(1, 2, 2)	(1, 2, 3) (1, 3, 0) (2, 0, 0)	(1, 3, 1) (2, 0, 1)

20	21	22	23	24	25	26	27	28	29
(1, 3, 2) (2, 0, 2)	(1, 3, 3) (2, 0, 3) (2, 1, 0)	(2, 1, 1)	(2, 1, 2)	(2, 1, 3) (2, 2, 0)	(2, 2, 1)	(2, 2, 2)	(2, 2, 3) (2, 3, 0) (3, 0, 0)	(2, 3, 1) (3, 0, 1)	(2, 3, 2) (3, 0, 2)

30
(2, 3, 3) (3, 0, 3) (3, 1, 0)

- $\mathfrak{B}_2 = (p = 31, n = 3, \gamma = 4, \rho = 4)$

0	1	2	3	4	5	6	7	8	9
(0, 0, 0) (1, 3, 3) (3, 3, 2)	(0, 0, 1) (2, 0, 0) (3, 3, 3)	(0, 0, 2) (2, 0, 1)	(0, 0, 3) (2, 0, 2)	(0, 1, 0) (2, 0, 3)	(0, 1, 1) (2, 1, 0)	(0, 1, 2) (2, 1, 1)	(0, 1, 3) (2, 1, 2)	(0, 2, 0) (2, 1, 3)	(0, 2, 1) (2, 2, 0)

10	11	12	13	14	15	16	17	18	19
(0, 2, 2) (2, 2, 1)	(0, 2, 3) (2, 2, 2)	(0, 3, 0) (2, 2, 3)	(0, 3, 1) (2, 3, 0)	(0, 3, 2) (2, 3, 1)	(0, 3, 3) (2, 3, 2)	(1, 0, 0) (2, 3, 3)	(1, 0, 1) (3, 0, 0)	(1, 0, 2) (3, 0, 1)	(1, 0, 3) (3, 0, 2)

20	21	22	23	24	25	26	27	28	29
(1, 1, 0) (3, 0, 3)	(1, 1, 1) (3, 1, 0)	(1, 1, 2) (3, 1, 1)	(1, 1, 3) (3, 1, 2)	(1, 2, 0) (3, 1, 3)	(1, 2, 1) (3, 2, 0)	(1, 2, 2) (3, 2, 1)	(1, 2, 3) (3, 2, 2)	(1, 3, 0) (3, 2, 3)	(1, 3, 1) (3, 3, 0)

30
(1, 3, 2) (3, 3, 1)

Change of the radix γ

- $\mathfrak{B}_3 = (p = 31, n = 3, \gamma = 11, \rho = 4)$

0	1	2	3	4	5	6	7	8	9
(0, 0, 0) (1, 0, 3) (1, 3, 1)	(0, 0, 1) (1, 3, 2)	(0, 0, 2) (0, 3, 0) (1, 3, 3) (3, 1, 0)	(0, 0, 3) (0, 3, 1) (3, 1, 1)	(0, 3, 2) (3, 1, 2)	(0, 3, 3) (2, 1, 0) (3, 1, 3)	(2, 1, 1)	(2, 1, 2)	(1, 1, 0) (2, 1, 3)	(1, 1, 1)

10	11	12	13	14	15	16	17	18	19
(1, 1, 2)	(0, 1, 0) (1, 1, 3)	(0, 1, 1)	(0, 1, 2) (3, 2, 0)	(0, 1, 3) (3, 2, 1)	(3, 2, 2)	(2, 2, 0) (3, 2, 3)	(2, 2, 1)	(2, 2, 2)	(1, 2, 0) (2, 2, 3)

20	21	22	23	24	25	26	27	28	29
(1, 2, 1)	(1, 2, 2)	(0, 2, 0) (1, 2, 3) (3, 0, 0)	(0, 2, 1) (3, 0, 1)	(0, 2, 2) (3, 0, 2) (3, 3, 0)	(0, 2, 3) (2, 0, 0) (3, 0, 3) (3, 3, 1)	(2, 0, 1) (3, 3, 2)	(2, 0, 2) (2, 3, 0) (3, 3, 3)	(1, 0, 0) (2, 0, 3) (2, 3, 1)	(1, 0, 1) (2, 3, 2)

30
(1, 0, 2) (1, 3, 0) (2, 3, 3)

- $\mathfrak{B}_4 = (p = 31, n = 3, \gamma = 17, \rho = 4)$

0	1	2	3	4	5	6	7	8	9
(0, 0, 0) (1, 3, 1) (3, 0, 1)	(0, 0, 1) (1, 3, 2) (3, 0, 2)	(0, 0, 2) (1, 3, 3) (3, 0, 3) (3, 2, 0)	(0, 0, 3) (0, 2, 0) (3, 2, 1)	(0, 2, 1) (3, 2, 2)	(0, 2, 2) (3, 2, 3)	(0, 2, 3) (2, 1, 0)	(2, 1, 1)	(2, 1, 2)	(2, 1, 3) (2, 3, 0)

10	11	12	13	14	15	16	17	18	19
(1, 0, 0) (2, 3, 1)	(1, 0, 1) (2, 3, 2)	(1, 0, 2) (2, 3, 3)	(1, 0, 3) (1, 2, 0)	(1, 2, 1)	(1, 2, 2)	(1, 2, 3) (3, 1, 0)	(0, 1, 0) (3, 1, 1)	(0, 1, 1) (3, 1, 2)	(0, 1, 2) (3, 1, 3) (3, 3, 0)

20	21	22	23	24	25	26	27	28	29
(0, 1, 3) (0, 3, 0) (2, 0, 0) (3, 3, 1)	(0, 3, 1) (2, 0, 1) (3, 3, 2)	(0, 3, 2) (2, 0, 2) (3, 3, 3)	(0, 3, 3) (2, 0, 3) (2, 2, 0)	(2, 2, 1)	(2, 2, 2)	(2, 2, 3)	(1, 1, 0)	(1, 1, 1)	(1, 1, 2)

30
(1, 1, 3) (1, 3, 0) (3, 0, 0)