On Polynomial Modular Number Systems over Z/pZ

Jean-Claude Bajard, Jérémy Marrez, Thomas Plantard, Pascal Véron

Advances in Mathematics of Communications doi:10.3934/amc.2022018

ON POLYNOMIAL MODULAR NUMBER SYSTEMS OVER $\mathbb{Z}/p\mathbb{Z}$

Jean-Claude Bajard

Sorbonne Université, CNRS, Inria, Institut de Mathématiques de Jussieu
Paris Rive Gauche, France

Jérémy Marrez

Sorbonne Université, CNRS, Laboratoire d'informatique de Paris 6
Paris, France

Thomas Plantard

Paypal, Emerging Technology Research Group
San Jose, USA

Pascal Véron

Laboratoire IMath, Université de Toulon
La Garde, France

(Communicated by Sihem Mesnager)

Abstract. Since their introduction in 2004, Polynomial Modular Number Systems (PMNS) have become a very interesting tool for implementing cryptosystems relying on modular arithmetic in a secure and efficient way. However, while their implementation is simple, their parameterization is not trivial and relies on a suitable choice of the polynomial on which the PMNS operates. The initial proposals were based on particular binomials and trinomials. But these polynomials do not always provide systems with interesting characteristics such as small digits, fast reduction, etc.

In this work, we study a larger family of polynomials that can be exploited to design a safe and efficient PMNS. To do so, we first state a complete existence theorem for PMNS which provides bounds on the size of the digits for a generic polynomial, significantly improving previous bounds. Then, we present classes of suitable polynomials which provide numerous PMNS for safe and efficient arithmetic.

1. Introduction

Context of the modular arithmetic. Modular arithmetic is at the core of modern cryptography [56]. Modular operations (essentially multiplication and addition) appear in most of today's public key cryptography. Widely used cryptographic protocols such as RSA [53], DSA [47] and their counterparts based on elliptic curves [42, 36] are at the core of modern communication. The main cost of all these cryptosystems is due to modular arithmetic. Their potential successors, currently competing in the post-quantum cryptography standardization contest organized by the U.S. National Institute of Standards and Technology NIST [2], also rely heavily on modular arithmetic. As an example, lattice based proposals such

2020 *Mathematics Subject Classification:* Primary: 11T06, 11T71; Secondary: 11H06, 94A60, 68W99.

Key words and phrases: Polynomial Modular Number System, polynomial roots, finite field, modular arithmetic.

as Kiber [13], NTRU [34], Saber [21], Falcon [52], or isogeny based key exchange (SIKE [35]) rely all on fast modular arithmetic. Furthermore, pairing based cryptography offers revolutionary protocols [11] which rely as well on modular arithmetic on large moduli.

SPECIFIC MODULAR ARITHMETIC. As improving modular arithmetic has such a wide impact on the efficiency of modern cryptographic protocols, special classes of moduli have been investigated. These special moduli are generally inspired by Mersenne numbers (integers of the form $2^m - 1$) to perform a modular reduction as fast as possible, namely Pseudo Mersenne [20], Generalized Mersenne [55]. Other ones have been created to be particularly efficient when used with some specific algorithm. As an example, Montgomery-friendly primes [30, 12, 4] have been created to be operated with Montgomery reduction [45]. However, these classes are by definition limited and multiple cryptosystems require a free choice of the moduli on which they operate.

THE ORIGIN OF PMNS. To obtain efficient modular arithmetic for all moduli, and not only for a class of special moduli, the PMNS[50] were proposed as an effective representation system. They operate without carry propagation and offer both the advantages of fast polynomial arithmetic and easy parallelization for arbitrary moduli p. Specifically, a PMNS is a modular system, where any integer a modulo p (which is not necessarily a prime) is represented as a polynomial $A(X)$ of degree smaller than a fixed integer n. Modular multiplication and addition of two integers a and b in $\mathbb{Z}/p\mathbb{Z}$ are then computed using their representatives $A(X)$ and $B(X)$ in the PMNS. The coefficients of the polynomials are the digits and are bounded by an integer ρ, which is small relatively to p ($\rho \simeq p^{1/n}$). The construction of such systems is based on sparse polynomials whose roots γ are used as radices for this kind of positional representation, that is to say, $A(\gamma) \equiv a \pmod p$. The interest of these sparse polynomials lies in the efficiency of the spawned modular arithmetic. The operations in PMNS are done in two steps. First, the operations are carried out on polynomials modulo a sparse polynomial $E(X)$, called reduction polynomial, which is of degree n, and this reduction ensures that the degree of the result is smaller than n. In other words, to compute $a \odot b$ ($\odot$ representing an addition or a multiplication), one computes $C(X) = A(X) \odot B(X) \bmod E(X)$. Then, a coefficient reduction is performed involving a lattice associated with the system [31, 51, 28]; this operation guarantees that the coefficients of the result $C(X)$ are bounded by ρ.

A method for constructing a prime p which has an efficient PMNS, has been published in 2004 [6]. The system is built from two sparse polynomials with good reduction properties (one is the reduction polynomial $E(X)$, the other one is used for the coefficient reduction), in order to derive the corresponding integer p through the computation of a resultant, and also of one root γ. In order to be able to work with an arbitrary p, prime or not, another approach has been developed in [5] by constructing PMNS from an integer p, a number of digits n and an integer polynomial $E(X)$ of the form $E(X) = X^n + aX + b$ satisfying some assumptions. Moreover, this result guarantees the existence of a PMNS with a bound on the digit size ρ allowing the representation of all numbers modulo p. Nevertheless, building such systems for a given p is not trivial.

The structure of the reduction polynomial $E(X)$ gives the complexity of the polynomial reduction. Then, with p and a root γ of $E(X)$ modulo p, we can define an associated lattice which allows to define the bound ρ on the coefficients

of the representation and also provides the method of reduction of the coefficients. Therefore, it is interesting, for a given p, to find polynomials $E(X)$ giving efficient polynomial modular reductions and roots γ to define the associated lattice and the reduction of the coefficients.

PMNS in a cryptographic context. The efficiency of this system of representation was the subject of an in-depth study in [23] for binomials $E(X) = X^n - \lambda$. Such a representation system is called an AMNS (Adapted Modular Number System) [6]. It has been observed that, for primes p whose size fits the standard sizes used in elliptic curve cryptography (ECC), the AMNS representation allows to compute modular multiplications in a much more efficient way than the classical libraries OpenSSL and GnuMP (even if using for the latter the low level arithmetic functions and the undocumented Montgomery multiplication function). Later, this study has been confirmed in [18] which described a specific library for ECC, named MPHELL, and compared it with other dedicated cryptographic libraries. The results show that on a 64-bit architecture, the AMNS representation gives the best results inside MPHELL for ECDSA/EdDSA signatures (generation and verification). Moreover, it offers also competitive timings on an ARM v8 architecture or a STM32F4 board. In [14], the authors extend the AMNS representation system to $\mathbb{F}_{p^k}$ and show how it can be used in order to improve the performances of SIKE [35], one of the alternate KEM candidate of the NIST post-quantum standardization process [46]. A first hardware implementation of the AMNS is described in [17]. To end, it is shown in [22, 49] that some "random steps" can be injected in AMNS multiplication in order to resist to a side channel analysis.

Motivation and main results. The major motivation and result of this paper is an effective construction of efficient PMNS for any integer p. The efficiency is measured in particular by the minimality of the digit size ρ which depends on a reduced basis of the associated lattice that we explicitly construct. In Section 4, we give bounds and properties and used them in Sections 5 and 6 to define what is a suitable polynomial for PMNS. The main results can be summarised as follows :

1. Theorem 4.2 lays down critical result on PMNS existence. It relates the digit size ρ to the infinity norm of the transpose of a reduced basis (seen as a matrix) of the associated lattice. The reduction criterion consists, in this context of PMNS, in searching for a basis such that the infinity norm of its transpose is close to a minimal.
2. In Proposition 4.1, we first construct a reduced basis for a sublattice built from a short vector of the initial associated lattice. Proposition 4.2 specifies this point when $E(X)$ is an irreducible polynomial. In this case, we give a bound for the digit size ρ depending only on p and $E(X)$. Then, Corollaries 4.1 and 4.2 provide concrete construction methods for reduced lattice bases.
3. Then we introduce effective constructions of efficient PMNS introduced in Sections 5 and 6. We provide multiple classes of polynomial $E(X)$ over which PMNS can be efficiently used, with studies on both their irreducibility and the size of the set of their roots in $\mathbb{Z}/p\mathbb{Z}$, two key parameters for their usability.

Organization of the paper. This paper is organized as follows: Sections 2 and 3 recall the necessary background respectively on lattice theory and PMNS. Then Section 4 presents theorems, propositions and their corollaries, which provide criteria for constructing concrete efficient PMNS for any p. In Section 5, we specify what

is a suitable reduction polynomial $E(X)$, and propose main classes of suitable irreducible polynomials; they allow efficient reductions, and their roots can be clearly identified in a finite prime field $\mathbb{Z}/p\mathbb{Z}$. Section 6 studies the number of roots in a finite prime field $\mathbb{Z}/p\mathbb{Z}$ of the reduction polynomial $E(X)$.

2. Lattice basics

Lattice theory, also known as geometry of numbers, was introduced by H. Minkowski in 1896 [44].

A comprehensive discussion on the basics of lattice theory is presented in [16, 41, 19]. We present in this section only the different definitions and results useful for the comprehension of our paper.

Definition 2.1 (Lattice)**.** A *lattice* $\mathfrak{L}$ is a discrete subgroup of $\mathbb{R}^n$, that is, the set of all the integral combinations of $d \leqslant n$ linearly independent vectors over $\mathbb{R}$:

$$\mathfrak{L} = \mathbb{Z}\, b_1 + \cdots + \mathbb{Z}\, b_d, \quad b_i \in \mathbb{R}^n.$$

Here, $B = (b_1, ..., b_d)$ is called a basis of $\mathfrak{L}$ and d, the *dimension* of $\mathfrak{L}$. We note $\mathfrak{L}(B)$ a lattice of basis B. If $d = n$, the lattice is called *full-rank*.

The *determinant* of $\mathfrak{L}$ defined by $\det \mathfrak{L} = \sqrt{\det(BB^T)}$ is invariant for any basis B of $\mathfrak{L}$.

Lattice theory problems are based on minimising the distance between vectors. The natural norm used in lattice theory is the euclidean norm. The *euclidean norm* of a vector v is computed by

$$\|v\|_2 = \sqrt{\sum_{i=1}^{n} v_i^2}.$$

Other l_p-norm, $\|v\|_p = \left(\sum_{i=1}^{n} |v_i|^p\right)^{1/p}$, can also be used. If $p = \infty$, then the norm is called the max-norm $\|v\|_\infty = max_{i=1}^{n}|v_i|$.

One of the most studied lattice problems is the Shortest Vector Problem (SVP).

Definition 2.2 (SVP)**.** Given a lattice $\mathfrak{L}$, solving the Shortest Vector Problem, amounts to finding a vector $u \in \mathfrak{L}$ such that $\forall v \in \mathfrak{L} \setminus \{0\}, 0 < \|u\| \leqslant \|v\|$ for a given norm $\|.\|$.

The norm $\|u\|$ of such vector u is called the *first minimum* and is denoted as λ_1. Moreover, λ_i will represent the norm of the i^{th} minimum (the minimum norm of i linearly independent vectors).
If the norm is not specified, one will assume λ_i to be the i^{th} minimum of $\mathfrak{L}$ for the Euclidean norm, $\lambda_{i,p}$ will represent the i^{th} minimum of $\mathfrak{L}$ for the l_p norm.

In 1998, M. Ajtai [1] proved that SVP is NP-hard under a randomized reduction. Therefore, the best algorithm to compute SVP in polynomial space uses exponential time. It was proposed by R. Kannan in 1983 and relies on strongly reducing each vector of a basis by recursion. It is often referenced as HKZ for Hermite-Korkin-Zolotareff. Its current best time estimation is at $2^{O(d)}d^{\frac{d}{2e}}$ [32]. Furthermore, some polynomial solutions exist as well such as LLL [39] or BKZ [54]. However, these solutions return vectors whose norm is equal to the size of the shortest vector times an exponential factor.

Nevertheless, certain bounds do exist on the first minimum and were given by Minkowski's initial work:

Theorem 2.3 (Minkowski)**.** *Let $\mathfrak{L}$ a lattice of dimension d, then*

$$\lambda_{1,\infty} \leqslant (\det \mathfrak{L})^{\frac{1}{d}}.$$

This bound is tight in max-norm. However, it is still an open problem for the Euclidean Norm. A second key problem of lattice theory is the Closest Vector Problem (CVP).

Definition 2.4 (CVP)**.** Given a lattice $\mathfrak{L}$ and a vector w, to solve CVP is to find a vector $u \in \mathfrak{L}$ such that $\forall v \in \mathfrak{L}, \|w-u\| \leqslant \|w-v\|$. The quantity $\|w-u\|$ is noted $dist(w, \mathfrak{L})$.

The problem CVP is NP-Hard as well [8]. Finally, a key invariant has been studied to try to evaluate the orthogonality of a lattice, i.e., the *Covering Radius*.

Definition 2.5 (Covering Radius)**.** Let $\mathfrak{L}$ be a full rank lattice. The covering radius of $\mathfrak{L}$, noted $\mu(\mathfrak{L})$, is the supremum of distances between any vector of $\mathbb{R}^d$ and $\mathfrak{L}$, i.e.,

$$\mu(\mathfrak{L}) = \max_{v \in \mathbb{R}^d} dist(v, \mathfrak{L})\,.$$

No polynomial algorithm exists to find the covering radius [29]. However, we know that for any l_p-norm [29], we have

$$\mu_p(\mathfrak{L}) \geqslant \frac{\lambda_{d,p}}{2}.$$

For the Euclidean norm, we know that $\mu_2(\mathfrak{L}) \leqslant \sqrt{d}\lambda_d(\mathfrak{L})$ [29]. By simple norm relation, we obtain that $\mu_\infty(\mathfrak{L}) \leqslant \sqrt{d}\lambda_d(\mathfrak{L})$.

3. Polynomial Modular Number System

In this section, we recall basic definitions and results on PMNS.

Definition 3.1 (Polynomial Modular Number System)**.** Let $p \geqslant 3$, $n \geqslant 2$, $\gamma \in [1, p-1]$ and $\rho \in [1, p-1]$ be integers. Let $E(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree n that satisfies $E(\gamma) \equiv 0 \pmod p$. A Polynomial Modular Number System (PMNS) is a set $\mathfrak{B} \subset \mathbb{Z}[X]$ such that:

1. $\forall A(X) \in \mathfrak{B}$, $\deg(A(X)) < n$,
2. $\forall A(X) = \sum_{i=0}^{n-1} a_i X^i \in \mathfrak{B}$, $-\rho < a_i < \rho$ for all i,
3. $\forall a \in \{0, \dots p-1\}$, $\exists A(X) \in \mathfrak{B}$ such that $A(\gamma) \equiv a \pmod p$.

The polynomial $E(X)$ is called *reduction polynomial* with respect to p.

A PMNS is thus a system of representation for elements in $\mathbb{Z}/p\mathbb{Z}$ where

$$a \in \mathbb{Z}/p\mathbb{Z} \text{ with } a \equiv \sum_{i=0}^{n-1} a_i \gamma^i \pmod p = A(\gamma) \bmod p \text{ and } -\rho < a_i < \rho \text{ for all }.$$

It looks a priori like the classic γ-ary positional system but since the $\gamma^i \bmod p$ are not ordered, there is no obvious way to compare two representatives $A(X)$ and $B(X)$ without computing $A(\gamma) \bmod p$ and $B(\gamma) \bmod p$. This is clearly shown in Example 1.

Throughout this paper, we use the notation $\mathfrak{B} = (p, n, \gamma, \rho)_E$ to recall that the PMNS $\mathfrak{B}$ is determined by these five parameters. Also, with a polynomial $A(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$ we associate the vector $A = (a_0, a_1, \dots, a_{n-1})$. We will switch between both notation when it is best suited for comprehension.

Operations in $\mathfrak{B}$ are first done modulo $E(X)$, and then a coefficient reduction process is performed, by subtracting an appropriate polynomial having γ as root modulo p, to guarantee that all the coefficients are bounded by ρ in absolute value [51, 23].

Example 1. Table 1 shows how to represent elements of $\mathbb{Z}/31\mathbb{Z}$ as polynomials of degree lower or equal to 3 and coefficients belonging to $\{-1, 0, 1\}$.

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)					

TABLE 1. Elements of $\mathbb{Z}/31\mathbb{Z}$ are represented as polynomials in γ, noted as vectors with lowest degree first. The reduction polynomial is $E(X) = X^4 - 2$ and $\gamma = 15$ is a root of $E(X)$. The digit set is $\{-1, 0, 1\}$ (i.e., $\rho = 2$)

We note that some values have more than one representation. This redundancy is not studied here, but it is useful in some applications [22]. Since all the elements of $\mathbb{Z}/p\mathbb{Z}$ are represented, the value of ρ satisfies $\sqrt[n]{p} \leq 2\rho - 1$, and redundancy starts when $\frac{\sqrt[n]{p}+1}{2} < \rho$.

Remark 1. In [48], the authors proved that for every quadruple (p, n, γ, ρ), there always exists a polynomial $E(X) \in \mathbb{Z}[X]$ satisfying $E(\gamma) \equiv 0 \mod p$, $\deg E(X) = n$ and $E(X) = X^n - c$ with $|c| \leqslant 2^{\frac{n}{2}}$. However, one cannot hope to obtain fast primitives for modular arithmetic using a polynomial $E(X)$ with such a coefficient c exponential in n. Indeed, it is important to understand that modular operations are replaced in a PMNS by polynomial operations modulo $E(X)$, so that the degree of the result be still less than or equal to n. The small size of the coefficients and the low density of the reduction polynomial $E(X)$ play a key role in the efficiency of modular reductions and in maintaining concise arithmetic.

Moreover, from a cryptographic point of view in the context of Side Channel Resistance, it could be of interest to build a PMNS from a polynomial $E(X)$ which

has numerous roots modulo p, since distinct roots yield distinct associated PMNS. In other words, from one execution to another one, for a fixed polynomial $E(X)$, a same secret value k could be represented by a polynomial $K(X)$ which depends on the root used to build the PMNS.

Consequently, once the parameters p and n are given, or in other words, once it has been held that the integers modulo p will be encoded on n symbols, the key question that arises is then which polynomials $E(X)$

1. allow one to find a parameter ρ as small as possible,
2. offer a good modular reduction,
3. have a large number of roots γ in $\mathbb{Z}/p\mathbb{Z}$.

Next sections of this paper are devoted to these questions.

4. Construction and specifications of PMNS

In this section, we give conditions to ensure the existence of a PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ for a generic $E(X)$.

Theorem 4.1. *Let $p \geqslant 2$ and $n \geqslant 2$ be two integers, $E(X)$ be a monic polynomial of degree n in $\mathbb{Z}[X]$ and γ an integer which is a root of $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.*
Let $\mathfrak{L}$ be the n-dimensional lattice generated by the polynomials in $\mathbb{Z}[X]$ of degree at most $n-1$ for which γ is a root modulo p. This lattice $\mathfrak{L}$ is generated by the following $n \times n$ matrix $\mathbf{A}$ (with respect to the canonical monomial basis, with polynomials represented in lines)

$$\mathbf{A} = \begin{pmatrix} p & 0 & \dots & \dots & 0 & 0 \\ -\gamma & 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \dots & -\gamma & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & -\gamma & 1 \end{pmatrix}. \tag{1}$$

Then,
for any $\rho > \mu_\infty(\mathfrak{L})$ (the covering radius for the max-norm),
the system $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a Polynomial Modular Number System.

Proof. Let $a \in [0, p-1]$ and let $T_a(X) = a$. We know that for any vector $T \in \mathbb{R}^n$ there exists $V \in \mathfrak{L}$ such that $\|T - V\|_\infty \leqslant \mu_\infty(\mathfrak{L})$. Hence, there exists $V_a \in \mathfrak{L}$ such that $\|T_a - V_a\|_\infty \leqslant \mu_\infty(\mathfrak{L}) < \rho$, and $(T_a - V_a)(\gamma) \equiv T_a(\gamma) - V_a(\gamma) \equiv a \bmod p$ (since $V_a \in \mathfrak{L}$). In consequence, for any $a \in [0, p-1]$, $T_a - V_a$ is a polynomial which fulfills the condition of Theorem 3.1. We conclude that $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a PMNS. □

Currently, there is no efficient algorithm to compute the covering radius of a lattice. In the next two sections, we describe how to obtain an effective calculation of the bound on ρ.

4.1. Relation between the lattice's basis and the PMNS.

Theorem 4.2. *Let $p \geqslant 2$ and $n \geqslant 2$ be two integers, $E(X)$ be a monic polynomial of degree n in $\mathbb{Z}[X]$ and γ be a root of $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.*

Let $\mathfrak{L}$ be the lattice of polynomials in $\mathbb{Z}[X]$ of degree at most $n-1$, for which γ is a root modulo p , B a basis of $\mathfrak{L}$ and $\mathbf{B}$ the matrix associated to this basis (each

row is an element of B).
Then,

$$\text{for any } \rho > \frac{1}{2}\left\|\mathbf{B^T}\right\|_\infty = \max_j \left\{\sum_{i=0}^{n-1} |b_{i,j}|\right\},$$

$$\mathfrak{B} = (p, n, \gamma, \rho)_E \text{ is a Polynomial Modular Number System.}$$

Proof. Following the proof of Theorem 4.1, we only have to show that for any polynomial $S(X)$, one can find a polynomial $T(X) \in \mathfrak{L}$ such that $\|S - T\|_\infty \leqslant \frac{1}{2}\|\mathbf{B}^T\|_\infty$. Let $S \in \mathbb{R}^n$. We define:

- $\lfloor S \rceil$ as the vector whose coordinates are integers equal to the rounding to nearest integer of those of S;
- $\mathrm{frac}(S)$ as the vector $(S) = S - \lfloor S \rceil$; notice that $\|\mathrm{frac}(S)\|_\infty \leqslant \frac{1}{2}$.

Let $S \in \mathbb{R}^n$. We search a close vector $T \in \mathfrak{L}$ using a Babaï round-off approach [3]. We have, $T = \mathbf{B}^T \cdot \lfloor (\mathbf{B}^T)^{-1} \cdot S \rceil$, thus

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

Then

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

□

In order to minimize ρ, a natural strategy is to choose a basis B so that $\|\mathbf{B^T}\|_\infty$ is small. Such a basis can be computed from A (Theorem 4.1, Eq. (1)) using algorithms like LLL, BKZ or HKZ.

The next strategies can be applied when the polynomial $E(X)$ is irreducible.

4.2. THE CASE OF IRREDUCIBLE REDUCTION POLYNOMIALS. Notice that Theorem 4.2 states that for any vector $S \in \mathbb{R}^n$, one can compute a vector T in a lattice $\mathfrak{L}$ such that $\|S - T\|_\infty$ be smaller than $\frac{1}{2}\|\mathbf{B}^T\|_\infty$, where B is a basis of $\mathfrak{L}$ and $\mathbf{B}$ its matrix form. The result holds for any lattice $\mathfrak{L}$ and any basis B of this lattice. As a consequence, it can be applied to any basis B' of a sublattice $\mathfrak{L}'$ of the lattice $\mathfrak{L}$ linked to the PMNS. The strategies described in this section are based on this remark.

Let $E(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, and let $\mathbf{C}$ be the companion matrix of $E(X)$:

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

Let $V = (v_0, \dots, v_{n-1})$ be the vector representing the coefficients 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 4.1. *Let V be a non-zero vector of $\mathfrak{L}$, the lattice of rank n defined by $\mathbf{A}$ (Theorem 4.1, Eq. (1)). Let $B_i = V \cdot \mathbf{C}^i$ be the row vector whose coordinates are the coefficients of the polynomial $B_i(X) = X^i \cdot V(X) \bmod E(X)$. Let $\mathbf{B}$ be the $n \times n$ matrix whose i^{th} row is the vector B_i.*

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., $B = (B_0, \ldots, B_{n-1})$ is a basis of $\mathfrak{L}'$),*
- *and $V \in \mathfrak{L}'$.*

Proof. The B_i are linearly independent. Indeed, let us suppose that there exists a non-zero vector $(t_0, t_1, \ldots, t_{n-1}) \in \mathbb{Z}^n$ 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 basis of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$ (which corresponds to the first row of B). □

Corollary 4.1. *Let V be a non-zero vector of $\mathfrak{L}$, the lattice of rank n defined by $\mathbf{A}$ (Theorem 4.1, eq. (Eq. (1))).*

If $E(X)$ is irreducible, then

- *V defines a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, (i.e., $\mathrm{B} = (B_0, \ldots, B_{n-1})$, defined in Proposition 4.1 is a basis of $\mathfrak{L}'$),*
- *moreover $V \in \mathfrak{L}'$.*

Proof. If $E(X)$ is irreducible, then $V(X)$ is inversible and Proposition 4.1 gives $B = (B_0, \ldots, B_{n-1})$, a basis of $\mathfrak{L}'$, $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$. □

A possible strategy to lower the bound on ρ is then to take a short vector $V \in \mathfrak{L}$, that is, a vector which satisfies the Minkowski bound $\|V\|_\infty \leqslant \alpha p^{1/n}$ with $\alpha \in]0, 1]$. From this vector V, we build the basis B of the sublattice $\mathfrak{L}'$ to compute the lower bound on ρ.

In this context, we can provide a bound such that if ρ is greater than this, then we are guaranteed to have a PMNS. Let us consider the $(2n-1) \times n$ matrix M whose rows are the coefficients of $X^i \bmod E(X)$ for $0 \leqslant i \leqslant 2n-2$. For any polynomial $T(X)$ of degree at most $2n-2$, the coefficients of $T(X) \bmod E(X)$ are computed as the vector-matrix product TM.

Proposition 4.2. *Let $E(X)$ be an irreducible polynomial, let M be the $(2n-1) \times n$ matrix whose rows are the coefficients of $X^i \bmod E(X)$, for $0 \leqslant i \leqslant 2n-2$, and $s = \|M^T\|_\infty$.*

$$\text{If } \rho > \frac{1}{2} p^{1/n} (1 + (n-1)s) \ (\geqslant \frac{1}{2} \|\mathbf{B}^T\|_\infty),$$

then $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a Polynomial Modular Number System.

Proof. Let V be a short vector of the lattice $\mathfrak{L}$, hence $\|V\|_\infty \leqslant p^{1/n}$. From Proposition 4.1, the matrix $\mathbf{B}$ is a basis of a sublattice $\mathfrak{L}'$. Each row B_i contains the coefficients of $X^i V(X) \bmod E(X)$. These coefficients are computed as the vector-matrix product $T^{(i)}M$ where $T^{(i)}(X) = X^i V(X)$. Hence $\|B_i\|_\infty \leqslant s\|V\|_\infty$ for $i \geqslant 1$, and $\|B_0\|_\infty \leqslant p^{1/n}$. Therefore $\|\mathbf{B}^T\|_\infty \leqslant p^{1/n}(1 + (n-1)s)$. We conclude using Theorem 4.2. □

A second strategy is to use the companion matrix $\mathbf{C}$ of $E(X)$ for computing a basis B of $\mathfrak{L}'$.

Corollary 4.2. *Let $\mathfrak{L}$ be the lattice of rank n given by $\mathbf{A}$ (Theorem 4.1, eq. Eq. (1)), let $\mathbf{C}$ be the companion matrix of $E(X)$, and let $\mathfrak{L}_D$ be the lattice of rank n in $\mathbb{Z}^{n^2}$ defined by $\mathbf{D} = (\mathbf{A}|\mathbf{A} \cdot \mathbf{C}^1| \cdots |\mathbf{A} \cdot \mathbf{C}^{n-1})$.*

For any $\overline{V} = (V_0, V_1, \cdots, V_{n-1}) \in \mathfrak{L}_D$ *such that* $\overline{V} \neq (0)^{n^2}$, *if* $E(X)$ *is irreducible then:*

1. $V_0 \in \mathfrak{L}$,
2. $(V_0, V_1, \cdots, V_{n-1})$ *is a basis 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 $V_i = V_0 \cdot \mathbf{C}^i$, for all $i \geqslant 1$, then, due to Corollary 4.1, the vector $(V_0, V_1, ..., V_{n-1})$ is a basis of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$. □

Hence, the last strategy is to choose a short vector $(V_0, V_1, \cdots, V_{n-1})$ of $\mathfrak{L}_D$ and to build the basis B of $\mathfrak{L}'$ from V.

4.3. SOME EXAMPLES OF PMNS. In these examples we give the value of the norm $\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty$ for each reduced basis approach: LLL [39]or BKZ [54] or HKZ reduction [37, 38] of $\mathbf{A}$, or the one of Corollary 4.1, or Corollary 4.2. We remark that the last two approaches offer the best results for polynomials $E(X)$ with small coefficients. In Section 6.4, we give experimental results with exhaustive searches.

Example 2.

$p = 112848483075082590657416923680536930196574208889254960005437791530871071177777$
$n = 8,\ E(X) = X^8 + X^2 + X + 1,$
$\gamma = 14916364465236885841418726559687117741451144740538862548429866622655455887 74$

LLL:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 16940155314$	BKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 15289909984$
HKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 15289909984$		
Cor. 4.1:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 13881325101$	Cor. 4.2:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12883199915$

Example 3.

$p = 96777329138546418411606037850670691916278980249035796845487391462163262877831$
$n = 8,\ E(X) = X^8 - X^4 - 1,$
$\gamma = 66378119609141043317728290217053385256449145407556727004132373270146455575461$

LLL:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 17955608045$	BKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 17955608045$
HKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 17955608045$		
Cor. 4.1:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 11628752571$	Cor. 4.2:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 10489321362$

Example 4.

$p = 94234089378179148303661339351342500658910595299680545500602453424882978290351$
$n = 8,\ E(X) = X^8 + X^4 - X^3 + 1,$
$\gamma = 55857489577292751855009098551500852039618350925837275620376166398325678525151$

LLL:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12305954812$	BKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12305954812$
HKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12305954812$		
Cor. 4.1:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 15570303402$	Cor. 4.2:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 14857375293$

Example 5.

$p = 96777329138546418411606037850670691916278980249035796845487391462163262877831$
$n = 8,\ E(X) = X^8 + 6,$
$\gamma = 55382746543295148021817266189065902379362952375536660625428080706764845726 74$

LLL:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12509178620$	BKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12509178620$
HKZ:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 12509178620$		
Cor. 4.1:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 47611052126$	Cor. 4.2:	$\left\|\mathbf{B}^{\mathbf{T}}\right\|_\infty = 40733847267$

5. SUITABLE IRREDUCIBLE POLYNOMIALS FOR PMNS

In Theorem 4.1, we proved that if $E(X)$ is an irreducible polynomial, then we can define a PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ depending of $E(X)$. For efficiency reason on

reducing modulo $E(X)$, $E(X)$ must respect some criteria, in particular with respect to the size of the digits in $\mathfrak{B} = (p, n, \gamma, \rho)_E$. We thus define what can be a suitable PMNS irreducible reduction polynomial.

5.1. Suitable PMNS reduction polynomial.

Definition 5.1. A 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 $n \geqslant 2$ and $k \leqslant \frac{n}{2}$,
3. most of the coefficients a_i are zero, other ones are very small (if possible equal to ± 1) compare to $p^{1/n}$.

The second item ensures that the polynomial reduction modulo $E(X)$ of a polynomial $T(X)$ of degree lower than $2n$ is done in two steps, i.e., by two times, we split $T(X) = T_1(X)X^n + T_0(X)$ with $T_1(X)$ and $T_0(X)$ of degree lower than n, and we substitute $X^n \bmod E(X) = -(\sum_{i=0}^{k} a_i X^i) \bmod E(X)$.

The third item allows one to give a bound on the coefficients of $T(X) \bmod E(X)$, namely $\|T(X) \bmod E(X)\|_\infty < s\|T(X)\|_\infty$, where s is the $l1-$norm of the $(2n-1) \times n$ matrix S whose row i represents the coefficients of $X^i \pmod{E(X)}$ for $i = 0 \ldots 2n-1$ (see Prop. 2.3 of [22]). As a consequence, if $G(X)$ and $F(X)$ are two elements of the PMNS, i.e., $\|F(X)\|_\infty < \rho$ and $\|G(X)\|_\infty < \rho$, then $\|F(X) \times G(X)\|_\infty < n\rho^2$ and $\|F(X) \times G(X) \pmod{E(X)}\|_\infty < sn\rho^2$.

Why consider alternatives for $E(X)$

Since the definition of the PMNS representation system, all the research focused on the polynomial $E(X) = X^n - \lambda$ because the external reduction can be efficiently performed when λ is "small" (often a power of 2 to use logical operator) [6, 48, 26, 25, 22, 23, 14, 18, 49]. Now, from proposition 4.2, we know that the size of the coefficients used in the PMNS representation system depends on the parameter s which in turn depends on the coefficients of the polynomial $E(X)$ since $s = \|M^T\|_\infty$ where M is the $(2n-1) \times n$ matrix whose rows are the coefficients of $X^i \bmod E(X)$. Hence the smaller s is, the smaller ρ is. As a toy example, let us consider $n = 6$ and the irreducible polynomial $E(X) = X^6 + 4$, then it is easy to see that $s = 5$ since each column of M contains only two elements (1 and -4), except the last one which contains only one element equal to 1. Now let us consider $E(X) = X^6 - X - 1$, then it is irreducible (see proposition 5.5) and a simple computation gives $s = 3$. This value for s can also be obtained considering the polynomial $E(X) = X^6 - 2$ which corresponds to the AMNS case. In fact, for the AMNS case, one can see that $s = |\lambda| + 1$, hence s is proportional to λ. So, the only way to minimize s is to take $\lambda = \pm 2$ (a simple argument shows that $\lambda = \pm 1$ does not allow to build an AMNS). Notice that the reduction modulo $X^6 - X - 1$ is very efficient and competitive with the one computed with $X^6 - 2$. Our goal to study suitable PMNS reduction polynomial is thus to enlarge the set of polynomials which can be used to define a PMNS without being restricted to the exclusive choise of the AMNS subset taking $\lambda = \pm 2$. We propose to developpers a set of polynomials for which the value s can easily be computed so that depending on the context (software or hardware), they can select the better choice which fits their constraints.

Another point of view concerns countermeasure to side channel attack. In the spirit of what has been proposed in [7], one may consider to build for a fixed prime p numerous PMNS representations. Let us consider the ECC context. Once kP

must be computed, first we choose the PMNS system to use, than we compute kP. This approach complements other countermeasures described in [22, 49]. Now, from a practical point of view, if we focus on the polynomials $E(X) = X^n - \lambda$ with λ a power of 2, this will drastically reduce the choice of possible PMNS. Hence our goal is to enlarge the possible choice of PMNS for a prime p by considering other polynomials $E(X)$ with small coefficients so that the external reduction can be efficiently performed and so that ρ be small.

According to the first item of Theorem 5.1, a suitable polynomial is irreducible. In the sequel, we adapt some classical irreducibility criteria and give examples of irreducible polynomials with few non-zero coefficients satisfying the two other items.

5.2. CLASSICAL POLYNOMIAL IRREDUCIBILITY CRITERIA. To verify the first item of Theorem 5.1, we can use general criteria such as the Schönemann-Eisenstein criterion, Dumas' criterion [24] or the generalization given by N. C. Bonciocat in [10]. We adapt these criteria to our purpose, namely to a monic polynomial $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$, with $k \leqslant \frac{n}{2}$.

Proposition 5.1 (from Dumas' criterion [24])**.** *If there exists a prime μ and an integer α such that, $\mu^\alpha \mid a_0$, $\mu^{\alpha+1} \nmid a_0$, $\mu^{\lceil \alpha(n-i)/n \rceil} \mid a_i$, 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 according to this criterion. If $k < n/2$ and $\mu << p^{1/n}$, then $E(X)$ is a suitable PMNS reduction polynomial.

Proposition 5.2 (from Corollary 1.2 [10])**.** *Let $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$, $a_0 \neq 0$, let $t \geqslant 2$ and let $\mu_1, \ldots, \mu_t$ be pairwise distinct numbers, and $\alpha_1, \ldots, \alpha_t$ positive integers. If, for $j = 1, \ldots, t$, and $i = 0, \ldots, k$, $\mu_j^{\alpha_j} \mid a_i$, $\mu_j^{\alpha_j+1} \nmid a_0$, 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.

5.3. SUITABLE CYCLOTOMIC POLYNOMIALS FOR PMNS. A well-known set of irreducible polynomials in $\mathbb{Z}[X]$ is the set of cyclotomic polynomials. Let us denote by `ClassCyclo(n)` the class of suitable cyclotomic polynomials for PMNS, whose degree is n.

Proposition 5.3. *For $n > 1$, $\Phi_m(X)$ the m-th cyclotomic polynomial is a suitable polynomial if and only if $\varphi(m) = n = 2^i 3^j$ with $i \geqslant 1, j \geqslant 0$.*

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

Proof. For $m > 1$ $\Phi_m(X)$ the m-th cyclotomic polynomial, is self-reciprocal, $\Phi_m(X) = X^n \Phi_m(\frac{1}{X})$ with $n = \varphi(m)$ the degree of $\Phi_m(X)$, (i.e.,the coefficients a_i of the term X^i are equal to those a_{n-i} of the terms X^{n-i} for all i). Thus, suitable cyclotomic polynomials will be of the form $X^{2n'} + aX^{n'} + 1$ with $n = 2n'$.

If X_0 is a root of a cyclotomic $X^{2n'} + aX^{n'} + 1$, then $X_0^{n'}$ is a root of unity and a root of $X^2 + aX + 1$, as its conjugate too, hence we have $a = 2 \cdot cos\theta$. Since a is an integer, we have $a = \pm 2, \pm 1, 0$. But, for $a = \pm 2$ the polynomial $X^{2n'} \pm 2X^{n'} + 1 = (X^{n'} \pm 1)^2$ is not irreducible. Therefore $a = \pm 1, 0$.

- a $= 0$, we consider $X^n + 1$. If $n = 2^i \cdot t$ with $t > 1$ odd then $X^n + 1 = (X^{2^i} + 1)(X^{2^i \cdot (t-1)} + X^{2^i \cdot (t-2)} + \cdots + 1)$. Thus $n = 2^i$ and the cyclotomic polynomials are $\Phi_{2^{i+1}}(X) = X^{2^i} + 1$.

- $a = 1$, then we look for $\Phi_m(X) = X^{2n'} + X^{n'} + 1$, and $e^{\frac{2i\pi}{3n'}}$ is a root of this polynomial. $e^{\frac{2i\pi}{3n'}}$ is also a root of $X^{3n'} - 1$. We know that $X^{3n'} - 1$ is the product of the cyclotomic $\Phi_d(X)$ with $d|3n'$ and $e^{\frac{2i\pi}{3}}$ is one of its roots, thus $e^{\frac{2i\pi}{3}}$ is a root of $\frac{X^{3n'}-1}{X^{2n'}+X^{n'}+1} = X^{n'} - 1$. Hence n' is a multiple of 3 and by induction $n' = 3^j$ and $\Phi_m(X) = \Phi_{3^{j+1}}(X) = X^{2\cdot 3^j} + X^{3^j} + 1$ with $j \geq 0$.
- $a = -1$, then we look for $\Phi_m(X) = X^{2n'} - X^{n'} + 1$. Let $n' = 2^{i-1} \cdot \alpha$, with α odd and $i \geq 1$, then $X^{2^i\alpha} - X^{2^{i-1}\alpha} + 1 = (-X^{2^{i-1}})^{2\alpha} + (-X^{2^{i-1}})^{\alpha} + 1$, we can refer to the previous case to deduce that $\alpha = 3^j$. Thus $\Phi_m(X) = \Phi_{2^i 3^{j+1}}(X) = X^{2^i\cdot 3^j} - X^{2^{i-1}3^j} + 1$ with $i \geq 1$ and $j \geq 0$.

We have proved that for $n > 1$, if `ClassCyclo(n)` $\neq \emptyset$ then $n = 2^i 3^j$ with $i \geqslant 1, j \geqslant 0$.

Reciprocally, for $n = 2^i 3^j$, $i \geqslant 1$, $j \geqslant 0$, we have to show that there exists a suitable cyclotomic polynomial whose degree is n.

Let $n = 2^i$ $(i \geqslant 1)$, since $n = \varphi(m)$, then $m = 2^{i+1}$ and $\Phi_{2^{i+1}}(X) = X^{2^i} + 1$ is a suitable cyclotomic polynomial.

Let $n = 2.3^j$ $(j \geqslant 1)$, since $n = \varphi(m)$, then $m = 3^{j+1}$ and $\Phi_{3^{j+1}}(X) = X^{2.3^j} + X^{3^j} + 1$ is a suitable cyclotomic polynomial.

Let $n = 2^i 3^j$ $(i \geqslant 2, j \geqslant 1)$, since $n = \varphi(m)$, then $m = 2^i 3^{j+1}$ and $\Phi_{2^i 3^{j+1}}(X) = X^{2^i 3^j} - X^{2^{i-1}3^j} + 1$ is a suitable cyclotomic polynomial. □

5.4. Suitable reduction $\{-1, 1\}$-quadrinomials. In [27], Finch and Jones give criteria of irreducibility for polynomials $X^a + \beta X^b + \gamma X^c + \delta$ with $\beta, \gamma, \delta \in \{-1, 1\}$ and $a > b > c > 0$.

Proposition 5.4 (Theorem 2 in [27])**.** *The quadrinomial $X^a + \beta X^b + \gamma X^c + \delta$ with $\beta, \gamma, \delta \in \{-1, 1\}$ and $a > b > c > 0$, is irreducible over $\mathbb{Z}[X]$ if and only if $\gcd(a, b, c) = 2^t m$ with m odd, and it 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* $a' - b' \not\equiv 0 \pmod{2\overline{c}}$.

Where $a' = a/2^t$, $b' = b/2^t$, $c' = c/2^t$ and $\overline{a} = \gcd(a', b' - c')$, $\overline{b} = \gcd(b', a' - c')$, $\overline{c} = \gcd(c', a' - b')$.

We call this class of suitable reduction quadrinomials `ClassQuadrinomials`*, and* `ClassQuadrinomials(n)` *is the set of such quadrinomials of degree n.*

For example, $E(X) = X^{2^t 7m} + X^{2^t 3m} + X^{2^t m} + 1$, with m odd, is a suitable PMNS reduction quadrinomial verifying the first condition.

5.5. Suitable reduction $\{-1, 1\}$trinomials. In this part we refer to a paper of W.H. Mills [43] and one of W. Ljunggren [40]. The first one gives a criterion on quadrinomials and roots of unity, the second one gives an application to trinomials.

Proposition 5.5. *We note $\gcd(n, m) = d$ and $n = d\cdot n_1$, $m = d\cdot m_1$. 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 $\mathbb{Z}[X]$.*

The class of the suitable reduction trinomials verifying these criteria is named `ClassTrinomials`*, and* `ClassTrinomials(n)` *represents the set of the trinomials of degree* n*.*

Proof. Let us transform, like in [40], $E(X) = X^n + \beta X^m + \delta$ in quadrinomial:

$$(X^n + \beta X^m + \delta)(X^n - \delta) = X^{2n} + \beta X^{n+m} - \beta\delta X^m - 1 = F(X).$$

Theorem 2 of [43] states that if $F(X) = A(X)E(X)$, where every root of $A(X)$ and no root of $E(X)$ is a root of unity, then $E(X)$ is irreducible except if there exists r such that:

- $(2n, n+m, m) = (8r, 7r, r)$ and $(\beta, \delta) = (1, -1)$ or $(-1, -1)$,
- or $(2n, n+m, m) = (8r, 4r, 2r)$ and $(\beta, \delta) = (1, -1)$,
- or $(2n, n+m, m) = (8r, 6r, 4r)$ and $(\beta, \delta) = (-1, -1)$.

It is easy to check that there is no integer r which satisfies any of these 3 constraints, hence we only have to verify that no root of $E(X)$ is a root of unity. First notice that, because $n = dn_1$ and $m = dm_1$ with $\gcd(n_1, m_1) = 1$, if λ is a root of $E(X)$, then λ^d is root of $X^{n_1} + \beta X^{m_1} + \delta$. Hence, if the roots of $X^{n_1} + \beta X^{m_1} + \delta$ are not roots of unity, then no root of $E(X) = X^n + \beta X^m + \delta$ is a root of unity.

Let us assume that λ is a root of $X^{n_1} + \beta X^{m_1} + \delta$, which is also a root of unity. Then there exit $t > 1$ and k with $\gcd(k, t) = 1$, such that:

$$\lambda = e^{\frac{2ik\pi}{t}} = \cos\frac{2k\pi}{t} + i\sin\frac{2k\pi}{t}.$$

Assume that $\beta = 1$. Then

$$\begin{cases} \cos(\frac{2n_1k\pi}{t}) + \cos(\frac{2m_1k\pi}{t}) = 2\cos(\frac{k\pi(n_1+m_1)}{t})\cos(\frac{k\pi(n_1-m_1)}{t}) = -\delta \\ \sin(\frac{2n_1k\pi}{t}) + \sin(\frac{2m_1k\pi}{t}) = 2\sin(\frac{k\pi(n_1+m_1)}{t})\cos(\frac{k\pi(n_1-m_1)}{t}) = 0. \end{cases}$$

Last equality implies that $\sin(\frac{k\pi(n_1+m_1)}{t}) = 0$ or $\cos(\frac{k\pi(n_1-m_1)}{t}) = 0$. Since $\delta \neq 0$, the first equation implies that $\cos(\frac{k\pi(n_1-m_1)}{t}) \neq 0$, hence $\frac{k(n_1+m_1)}{t}$ is an integer. Since $\gcd(k, t) = 1$, $t \mid (n_1 + m_1)$. This last result implies that the first equation can be reduced to

$$\cos\left(\frac{k\pi(n_1 - m_1)}{t}\right) = \pm\frac{1}{2}$$

because $\delta = \pm 1$.

It means that

$$\frac{k\pi(n_1 - m_1)}{t} = j\frac{\pi}{3}, \quad j = 1, 2, 4, 5 \pmod 6.$$

Hence, $t \mid 3(n_1 - m_1)$, since $\gcd(k, t) = 1$.

Assume that $\beta = -1$. The system becomes:

$$\begin{cases} \cos(\frac{2n_1k\pi}{t}) - \cos(\frac{2m_1k\pi}{t}) = -2\sin(\frac{k\pi(n_1+m_1)}{t})\sin(\frac{k\pi(n_1-m_1)}{t}) = -\delta \\ \sin(\frac{2n_1k\pi}{t}) - \sin(\frac{2m_1k\pi}{t}) = 2\cos(\frac{k\pi(n_1+m_1)}{t})\sin(\frac{k\pi(n_1-m_1)}{t}) = 0. \end{cases}$$

The first equation implies that $\sin(\frac{k\pi(n_1-m_1)}{t}) \neq 0$, hence the second equation gives $\frac{k\pi(n_1+m_1)}{t} = j\frac{\pi}{2}$ for j odd, which implies $t \mid 2(n_1+m_1)$. Since $\frac{k\pi(n_1+m_1)}{t} = j\frac{\pi}{2}$ for j odd, then the first equation can be reduced to $\sin(\frac{k\pi(n_1-m_1)}{t}) = \pm\frac{1}{2}$, which means that

$$\frac{k\pi(n_1 - m_1)}{t} = j\frac{\pi}{6}, \quad j = 1, 5, 7, 11 \pmod{12}.$$

Hence $t \mid 6(n_1 - m_1)$.

To sum up, if λ is a t^{th} root of unity of $X^{n_1} + \beta X^{m_1} + \delta$ with $\delta, \beta \in \{-1, 1\}$, then:

(a) if $\beta = 1$, $t \mid (n_1 + m_1)$ and $t \mid 3(n_1 - m_1)$,
(b) if $\beta = -1$, $t \mid 2(n_1 + m_1)$ and $t \mid 6(n_1 - m_1)$.

The case (a) implies that if $3 \nmid t$, then $t \mid (n_1 - m_1)$, thus $t \mid 2n_1$ and $t \mid 2m_1$, as $\gcd(n_1, m_1) = 1$. We conclude that $t = 2$ and $\lambda = 1$ or -1 is a root of $E(X)$ which is impossible.

The case (b) implies that if $3 \nmid t$, then $t \mid 2(n_1 - m_1)$, thus $t = 4$, and $\lambda = i$, $-i$, 1 or -1 is a root of $E(X)$, which is impossible.

Hence, if one root of $E(X)$ is a root of unity, then 3 divides t, and $n_1 + m_1 \equiv 0 \mod 3$.

In conclusion, if $\gcd(n_1, m_1) = 1$ and $n_1 + m_1 \not\equiv 0 \mod 3$, then $X^{n_1} + \beta X^{m_1} + \delta$ and $X^n + \beta X^m + \delta$ are irreducible. □

5.6. Case of irreducibility of binomials $X^n + c$, $c \in \mathbb{Z}$, $|c| \geqslant 2$, over $\mathbb{Z}$.

Proposition 5.6. *Let $|c| = \prod_{j=1}^{k} p_j^{m_j}$ with p_j pairwise distinct prime numbers, and m_j positive integers. If $gcd(m_1, \ldots, m_k, n) = 1$, then the polynomial $X^n + c$, with $c \in \mathbb{Z}$, $|c| \geqslant 2$, is irreducible over $\mathbb{Z}[X]$.*

We call this class of suitable polynomials `ClassBinomial`*, and, for n and c satisfying this proposition,* `ClassBinomial(n, c)` *is the singleton $\{X^n + c\}$.*

Proof. It is a direct application of Corollary 1.2 of a paper due to Nicolae Ciprian Bonciocat [10]. □

5.7. Polynomials with bounds on the modules of their complex roots. The two propositions given in this section are inspired by the Perron irreducibility criterium, which is proved thanks to Rouché's theorem [9].

Proposition 5.7. *For a fixed $n \geqslant 2$ and a prime μ, let $P(X) = X^n + \sum_{i=1}^{n/2} \varepsilon_i X^i \pm \mu$ 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 $\mathbb{Z}[X]$.

They represent the fifth class of suitable reduction polynomials. We call this class `ClassPrimeCst`*, and* `ClassPrimeCst(n, μ)` *represents all the polynomials of this class with $n \geqslant 2$ and μ a prime number.*

Proof. Since $\mu > 1 + \sum_{i=1}^{n/2} |\varepsilon_i|$, there exists $\delta > 1$ such that $\mu > \delta^n \left(1 + \sum_{i=1}^{n/2} |\varepsilon_i|\right)$.

Let us consider $\mathcal{C} = \{z \in \mathbb{C} \ / \ |z| = \delta\}$, $P(X) = X^n + \sum_{i=1}^{n/2} \varepsilon_i X^i + \varepsilon\mu$ ($\varepsilon_i \in \{-1, 0, 1\}$, $\varepsilon \in \{-1, 1\}$), $F(X) = \varepsilon\mu$ and $G(X) = P(X) - F(X)$.

For any $z \in \mathcal{C}$, we have $|G(z)| \leqslant \delta^n \left(1 + \sum_{i=1}^{n/2} |\varepsilon_i|\right) < \mu = |F(z)|$.

Since $F(z)$ and $G(z)$ are holomorphic functions, Rouché's theorem states that $F(z)$ and $P(z) = F(z) + G(z)$ have the same number of roots inside $\mathcal{C}$. Hence $P(z)$

has no root inside $\mathcal{C}$ since $F(z)$ is constant. In other words, any root α of $P(z)$ satisfies $|\alpha| \geqslant \delta > 1$.

Assume now that $P(X)$ is reducible over $\mathbb{Z}[X]$. Hence, $P(X) = H(X)Q(X)$ with $H(X)$ and $Q(X)$ two monic polynomials. Since $|P(0)| = \mu$ (a prime number), we can assume that $|H(0)| = \mu$ and $|Q(0)| = 1$. Now $\prod |z_i| = 1$, where z_i are all the roots of $Q(X)$. But the roots of $Q(X)$ are also roots of $P(X)$ which is not possible since any root α of $P(X)$ is such that $|\alpha| \geqslant \delta > 1$. Hence, $P(X)$ is irreducible over $\mathbb{Z}[X]$. □

Remark 2. If $\mu > n/2 + 1$, then $\texttt{ClassPrimeCst}(\texttt{n}, \mu)$ contains $3^{n/2}$ elements (for each ε_i three possibilities), else $\displaystyle\sum_{i=0}^{\mu-2} \binom{n/2}{i} 2^{i+1}$ elements.

Proposition 5.8. *For a fixed $n \geqslant 2$, let $P(X) = X^n + \displaystyle\sum_{i=2}^{n/2} \varepsilon_i X^i + a_1 X \pm 1$ with $\varepsilon_i \in \{-1, 0, 1\}$ and $a_1 \in \mathbb{Z}^*$.*

If $|a_1| > 2 + \displaystyle\sum_{i=2}^{n/2} |\varepsilon_i|$, then the polynomial $P(X)$ is irreducible over $\mathbb{Z}[X]$.

We call this class $\texttt{ClassPerron}$*, and* $\texttt{ClassPerron}(\texttt{n}, \texttt{a}_1)$ *represents all the polynomials of this class with $n \geqslant 2$, $a_1 \in \mathbb{Z}^*$.*

Proof. The proof is similar to the previous one. From $|a_1| > 2 + \sum_{i=2}^{n/2} |\varepsilon_i|$, we can deduce that there exists $\delta > 1$ such that $|a_1| > \delta^n \left(2 + \sum_{i=2}^{n/2} |\varepsilon_i|\right)$. Then, from Rouché's theorem, $P(z)$ and $F(z) = a_1 z$ have the same number of roots inside $\mathcal{C} = \{z \in \mathbb{C} \,/\, |z| = \delta\}$. Hence $P(z)$ has only one root whose module is strictly less than δ.

Now, if $P(X)$ is reducible over $\mathbb{Z}[X]$, then $P(X) = H(X)Q(X)$, with $H(X)$ and $Q(X)$ two monic polynomials and $|H(0)| = |G(0)| = 1$. Hence, $H(z)$ has at least one root z_H such that $|z_H| \leqslant 1$ and $G(z)$ has at least one root z_G such that $|z_G| \leqslant 1$. It means that $P(z)$ has at least two roots inside $\mathcal{C}$, which is not possible. Hence, $P(X)$ is irreducible over $\mathbb{Z}[X]$. □

Remark 3. If $|a_1| > n/2+1$, then $\texttt{ClassPerron}(\texttt{n}, \texttt{a}_1)$ contains $2 \times 3^{n/2-1}$ elements, else $\displaystyle\sum_{i=0}^{|a_1|-3} \binom{n/2-1}{i} 2^{i+1}$ elements.

6. Number of PMNS in function of their reduction polynomial in $\mathbb{Z}/p\mathbb{Z}$ with p prime

In this section, we determine for each class, the reduction polynomials which have one or more roots γ in $\mathbb{Z}/p\mathbb{Z}$. The number of roots in $\mathbb{Z}/p\mathbb{Z}$ defines the number of possible PMNS.

As we have to build, for a given prime p and a given number of digits n, many PMNS with an efficient arithmetic, finding relevant reduction polynomials is crucial. Now that we have described classes of irreducible polynomials with specific reduction properties, we need to identify for a prime p which polynomials have at least one root in $\mathbb{Z}/p\mathbb{Z}$, and if possible, how many. We begin with a presentation of two special cases where the reduction polynomials are cyclotomics or binomials, then

we propose a method in the general case that works for any irreducible integer polynomial.

6.1. Number of PMNS with a cyclotomic reduction polynomial.

Proposition 6.1. *Let p be a prime number, $p > 2$, and an integer $m \geqslant 3$ such that $m \mid (p-1)$. Then the cyclotomic polynomial $\Phi_m(X)$ satisfies $\Phi_m(X) \mid (X^{p-1}-1)$ and $\Phi_m(X)$ has $\varphi(m)$ roots over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. We have $(X^{p-1}-1) = \prod_{\xi_i \in (\mathbb{Z}/p\mathbb{Z})^*} (X-\xi_i) = \prod_{d|(p-1)} \Phi_d(X)$.

Thus $\Phi_m(X) \mid (X^{p-1}-1)$, and $\Phi_m(X)$ has $\varphi(m)$ (its degree) roots over $\mathbb{Z}/p\mathbb{Z}$. □

We apply Proposition 6.1 to the different cyclotomic polynomials of the class `ClassCyclo(n)` introduced in Proposition 5.3.

Corollary 6.1. *Let p be a prime number, $n \geqslant 2$ such that $n = 2^i 3^j$, with $i, j \in \mathbb{N}$. If either one of these conditions folds, i.e.;*

a) $i > 0$, $j = 0$, $(2\,n)$ divides $(p-1)$, and $E(X) = \Phi_{2n}(X) = X^n + 1$;
b) $i = 1$, $j \geqslant 0$, $(3\,n\,/\,2)$ divides $(p-1)$, and $E(X) = \Phi_{\frac{3n}{2}}(X) = X^n + X^{\frac{n}{2}} + 1$;
c) $i \geqslant 1$, $j \geqslant 0$, $(3\,n)$ 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 $E(X)$.

Example 6. Construction of PMNS from a cyclotomic reduction polynomial for $p = 2^{256} \cdot 3^{157} \cdot 115 + 1$ coded on 512 bits.

- $E(X) = X^8 + 1$: from its eight roots, the best ρ is obtained with Corollary 4.1 and Corollary 4.2., and it is 66 bits number.
- $E(X) = X^6 + X^3 + 1$: from its six roots, the best ρ is obtained twice with LLL, else with Corollary 4.1 and Corollary 4.2, and it is 87 bits number.
- $E(X) = X^6 - X^3 + 1$: from its six roots, the best ρ is obtained with Corollary 4.1 and Corollary 4.2, and it is 87 bits number.

6.2. Number of PMNS with reduction binomials $X^n + c$, $c \in \mathbb{Z}$, $|c| \geqslant 2$.

Proposition 6.2. *Let $E(X) = X^n + c$ be an element of* `ClassBinomial(n,c)` *(Proposition 5.6). Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and y such that $g^y \equiv -c \mod p$.*

If $\gcd(n, p-1)$ divides y, then $E(X) = X^n + c$ has $\gcd(n, p-1)$ different roots.

Proof. Let X_0 be a solution of $E(X) = 0 \pmod p$. Then there exists x_0 such that $X_0 \equiv g^{x_0} \pmod p$ and $g^{n \cdot x_0} \equiv -c \equiv g^y \pmod p$. In other words, $n \cdot x_0 \equiv y \pmod{p-1}$.

Now, let $\delta = \gcd(n, p-1)$. A classical result in modular arithmetic states that this linear equation admits δ solutions if and only if δ divides y, each solution being equal to $x_0 + jp'$, where $j \in \{0, \ldots, \delta - 1\}$ and $(p-1) = \delta p'$. □

Remark 4. If $\gcd(n, p-1) = 1$, then $E(X) = X^n + c$ is guaranted to have one root.

Example 7. For $p = 40993$, 5 is a generator of $(\mathbb{Z}/40993\mathbb{Z})^*$. Let $n = 4$ and $E(X) = X^4 + c$. For $c = 2$, we can find $y = 33788$ such that $-c = 5^y \mod p$. Since $\gcd(1, n) = 1$, from Proposition 6.2, $E(X)$ is irreducible. Moreover, $\gcd(n, p-1) = 4$ divides y, hence four PMNS can be generated from $E(X)$. For $c' = -2$, we can find $y' = 13292$ and $\gcd(n, p-1) = 4$ divides y', giving once again four possible PMNS.

6.3. NUMBER OF PMNS IN THE GENERAL CASE. In this part, we propose a general method to count the minimum number of PMNS we can reach from a prime p and any irreducible polynomial $E(X)$ in $\mathbb{Z}[X]$.

Proposition 6.3. *Let p be a prime number, $n > 2$, $E(X)$ a polynomial of degree n and irreducible in $\mathbb{Z}[X]$, and $D(X) = \gcd(X^p - X, E(X)) \mod p$.*

There exist $\deg(D(X))$ Polynomial Modular Number Systems $(p, n, \gamma_i, \rho)_{E(X)}$.

Proof. The proof is immediate considering, when p is prime, that the roots of $X^p - X \mod p$ are the p elements of $\mathbb{Z}/p\mathbb{Z}$. □

Remark 5. Proposition 6.1 can be considered as a corollary of Proposition 6.3.

The computation of $\gcd(X^p - X, E(X)) \mod p = \gcd(X^{p-1} - 1, E(X)) \mod p$ ($E(X)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$) can be done, in a reasonable time, in two steps:

1. we compute $X^{p-1} \bmod E(X) \bmod p$ with a square and multiply exponentiation algorithm, and we compute $F(X) = X^{p-1} - 1 \bmod E(X) \bmod p$,
2. then, we compute $D(X) = \gcd(F(X), E(X)) \bmod p$ with polynomials of degrees lower than or equal to n.

The first step represents $O(\log_2(p))$ squares and additions of polynomials of degree lower than n in $\mathbb{Z}/p\mathbb{Z}[X]$, and the second step represents at most n iterations of the Euclidean algorithm.

The roots can be found using the method of Cantor-Zassenhaus[15] for separating the roots of $D(X) = \gcd(X^p - X, E(X)) \bmod p$.

As $X^p - X = \prod_{z \in \mathbb{Z}/p\mathbb{Z}}(X - z)$, then $D(X) = \prod_{i=1}^{k}(X - e_i)$ with $k = \deg(D(X))$ and $e_i \in \mathbb{Z}/p\mathbb{Z}$ all distinct.

Due to the Chinese Remainder Theorem, any polynomial $A(X)$ of degree strictly lower than k, can be represented by its values modulo the $(X - e_i)$:

$$a_i = A(X) \bmod (X - e_i) \text{ in } \mathbb{Z}/p\mathbb{Z} \text{ for } i = 1, \ldots, k\,.$$

Let us consider a polynomial $A(x)$ such that $a_i \in \{0, 1, -1\}$ and $A(X) \neq 0, 1, -1 \bmod D(X)$ (i.e., a_i are not all equal). We note $T = \{i, a_i = 1\}$ and $S = \{i, a_i = 0\}$. As $A(X) \neq 0, 1, -1 \bmod D(X)$, at least one of this two sets is not empty with a cardinal strictly lower than k. We can obtain a proper factor of $D(X)$ by computing;

$$\gcd(D(X), A(X) - 1) = \prod_{i \in T}(X - e_i) \text{ or } \gcd(D(X), A(X)) = \prod_{i \in S}(X - e_i)\,.$$

To find such a polynomial $A(X)$, we consider a random polynomial $B(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ of degree lower than k. We note $b_i = B(X) \bmod (X - e_i)$ in $\mathbb{Z}/p\mathbb{Z}$. Then,

$$b_i^{p-1} = 0, 1 \text{ and } b_i^{\frac{p-1}{2}} = 0, 1, -1 \text{ in } \mathbb{Z}/p\mathbb{Z}\,.$$

If $B(X)^{\frac{p-1}{2}} \neq 0, 1, -1 \bmod D(X)$, then we choose $A(X) = B(X)^{\frac{p-1}{2}} \bmod D(X)$. If $\gcd(D(X), A(X) - 1)$ and $\gcd(D(X), A(X))$ are trivial factors, then we draw randomly another polynomial $B(X)$, else we iterate this method with the found non trivial factors $\gcd(D(X), A(X) - 1)$, $\gcd(D(X), A(X))$ and $D(X)$ divided by these factors, until all the factors are of degree 1.

Example 8. We consider $p = 78264746924694600393874000999999297$ and the reduction polynomial $E(X) = X^5 + X^2 + 1$. First, we compute

$$\begin{aligned} R(X) &= X^{p-1} - 1 \bmod E(X) \text{ in } (\mathbb{Z}/p\mathbb{Z})[X] \\ &= 365918908630093001420710658331842 1\ X^4 \\ &+732212625942009817709398509909462 4\ X^3 \\ &+172782621530124334904222246113526 2\ X^2 \\ &+709803098390905698521163009018283 1\ X \\ &+737295850362666465909672848502029 4 \end{aligned}$$

Then we obtain

$$\begin{aligned} D(X) &= \gcd(R(X), E(X)) \text{ in } (\mathbb{Z}/p\mathbb{Z})[X] \\ &= X^2 + 13058499984190672910003378977052 58\ X \\ &+179307300095420454603419406809882 6 \end{aligned}$$

Next, we randomly draw $B(X) \bmod D(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$,

$$\begin{aligned} B(X) = \quad & 709063421374141469660625428978185 9\ X \\ &+489618407023729458501454482212065 1 \end{aligned}$$

We compute $A(X) = B(X)^{\frac{p-1}{2}} \bmod D(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$

$$\begin{aligned} &= 663061205116446120492511318858289 5\ X \\ &+709960240140096624747842855508736 5 \end{aligned}$$

We obtain a first factor in $(\mathbb{Z}/p\mathbb{Z})[X]$,

$$T(X) = gcd(A(X) - 1, D(X)) = X + 29746256513307180597166691026336 43.$$

By division we find the second factor,

$$D(X)/T(X) = X - 16687756529116507687163312049283 85$$

6.4. Example giving all the possible PMNS for a given p. This example was produced with SageMath subroutines for the 256-bits prime p: $p = 57896044618658097711785492504343953926634992332820282019728792003956566811073$, and $n = 9$. We consider the PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ such that:

- $E(X) = X^9 + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, where $k \leqslant 4$,
- the coefficients a_i satisfy $|a_i| \leqslant 1$ for $1 \leqslant i \leqslant k$ and $|a_0| \leqslant 3$,
- $\rho \leqslant 2^{31}$.

The number of PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ that can be built for different polynomials verifying the criteria is equal to 354.

Most of the time, the best ρ is obtained 266 times by LLL but BKZ or HKZ are 46 times better than LLL , then 42 are better than the previous ones with Corollary 4.1 or Corollary 4.2 or Proposition 4.1 with a short vector.

7. Conclusion

In this paper, we have shown with Theorem 4.1 the link between the existence of a PMNS and the lattice generated by its reduction polynomial and its modulo. We thus set a bound on the size of the PMNS digits depending on the covering radius of this lattice. Then, Theorem 4.2 provides a bound which can easily be computed from the infinity norm of a basis of the lattice. This second theorem has led us to consider PMNS defined by an irreducible polynomial. In this case, it is easy to define a basis of the lattice that can be associated with the PMNS (Proposition 4.1, Corollary 4.1 and Corollary 4.2). These results allowed us to produce PMNS with

specific reduction polynomials allowing efficient reductions and whose roots give the bases (γ) of these systems. Now, we have the opportunity to offer for a given modulo p a wide variety of PMNS with small digits and reduced associated lattices.

Very recently, the use of PMNS to perform modular multiplications was reintroduced in [33], where some interesting complexity theoretical bounds are given.

ACKNOWLEDGMENT

We thank Mrs. Valérie Berthé for her attentive proofreading and her judicious suggestions.

FUNDING. This work was partially supported by the ANR project ARRAND 15-CE39-0002-01 and the INRIA international associated team MACAO. All examples were coded with SageMath https://www.sagemath.org

REFERENCES

[1] M. Ajtai, The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract), *Thirtieth Annual ACM Symposium on the Theory of Computing (STOC 1998)*, (1998), 10–19.

[2] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson and D. Smith-Tone, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, Tech. Report NIST IR 8309, National Institute of Standards and Technology, July 2020.

[3] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem, *Combinatorica*, **6** (1986), 1–13.

[4] J. C. Bajard and S. Duquesne, Montgomery-friendly primes and applications to cryptography, *Journal of Cryptographic Engineering*, **11** (2021), 399–415.

[5] J.-C. Bajard, L. Imbert and T. Plantard, Arithmetic operations in the polynomial modular number system, *17th IEEE Symposium on Computer Arithmetic (ARITH'05), IEEE*, (2005), 206–213.

[6] ———, Modular number systems: Beyond the Mersenne family, *Selected Areas in Cryptography, Springer*, (2005), 159–169.

[7] J.-C. Bajard, L. Imbert, P.-Y. Liardet and Y. Teglia, Leak resistant arithmetic, *Cryptographic Hardware and Embedded Systems - CHES 2004 (Berlin, Heidelberg) (Marc Joye and Jean-Jacques Quisquater, eds.), Springer Berlin Heidelberg*, (2004), 62–75.

[8] P. Van Emde Boas, *Another NP-Complete Problem and the Complexity of Computing Short Vectors in Lattices*, Tech. Report 81-04, Mathematics Department, University of Amsterdam, 1981.

[9] N. C. Bonciocat, On an irreducibility criterion of Perron for multivariate polynomials, *Bull. Math. Soc. Sci. Math. Roumanie*, **53** (2010), 213–217.

[10] ———, Schönemann–Eisenstein–Dumas-type irreducibility conditions that use arbitrarily many prime numbers, *Journal Communications in Algebra*, **43** (2015).

[11] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology—CRYPTO 2001 (Santa Barbara, CA), Lecture Notes in Comput. Sci., Springer, Berlin*, **2139** (2001), 213–229.

[12] J. W. Bos, C. Costello, H. Hisil and K. E. Lauter, Fast cryptography in genus 2, *Advances in cryptology—EUROCRYPT 2013, Lecture Notes in Comput. Sci., Springer, Heidelberg*, **7881** (2013), 194–210.

[13] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler and D. Stehle, Crystals–kyber: A CCA-secure module-lattice-based KEM, *3rd IEEE European Symposium on Security and Privacy*, (2018), 353–367.

[14] C. Bouvier and L. Imbert, An alternative approach for SIDH arithmetic, *Public-key cryptography—PKC 2021, Part I, Lecture Notes in Comput. Sci., Springer, Cham*, **12710** (2021), 27–44.

[15] D. G. Cantor and H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, *Mathematics of Computation*, **36** (1981), 587–592.

[16] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997.
[17] A. Chaouch, L.-S. Didier, F. Y. Dosso, N. El Mrabet, B. Bouallegue and B. Ouni, Two hardware implementations for modular multiplication in the AMNS: Sequential and semi-parallel, *J. Inf. Secur. Appl.*, **58** (2021), 102770.
[18] T. Coladon, P. Elbaz-Vincent and C. Hugounenq, Mphell: A fast and robust library with unified and versatile arithmetics for elliptic curves cryptography, *2021 IEEE 28th Symposium on Computer Arithmetic (ARITH)*, (2021), 78–85.
[19] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der mathematischen Wissenschaften, 290. Springer-Verlag, New York, 1988.
[20] R. Crandall, *Method and Apparatus for Public Key Exchange in a Cryptographic System*, U.S. Patent number 5159632, 1992.
[21] J.-P. D'Anvers, A. Karmakar, S. Sinha Roy and F. Vercauteren, Saber: Module-lwr based key exchange, CPA-secure encryption and CCA-secure KEM, *Progress in cryptology—AFRICACRYPT 2018, Lecture Notes in Comput. Sci., Springer, Cham*, **10831** (2018), 282–305.
[22] L.-S. Didier, F.-Y. Dosso, N. El Mrabet, J. Marrez and P. Véron, Randomization of arithmetic over polynomial modular number system, *26th IEEE International Symposium on Computer Arithmetic, IEEE Computer Society*, **1** (2019), 199–206.
[23] L.-S. Didier, F.-Y. Dosso and P. Véron, Efficient modular operations using the adapted modular number system, *Journal of Cryptographic Engineering*, **10** (2020), 111–133.
[24] G. Dumas, Sur quelques cas d'irreductibilité des polynômes à coefficients rationnels, *Journal de Mathématique Pure et Appliquée*, **2** (1906).
[25] N. El Mrabet and N. Gama, Efficient multiplication over extension fields, *Arithmetic of Finite Fields, Lecture Notes in Comput. Sci., Springer, Heidelberg*, **7369** (2012), 136–151.
[26] N. El Mrabet and C. Nègre, Finite field multiplication combining AMNS and DFT approach for pairing cryptography, *ACISP, Lecture Notes in Computer Science, Springer*, **5594** (2009), 422–436.
[27] C. Finch and L. Jones, On the irreducibility of $\{-1, 0, 1\}$-quadrinomials, *INTEGERS: Electronic Journal of Combinatorial Number Theory*, **6** (2006), A16, 4 pp.
[28] S. D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, Cambridge, 2012.
[29] V. Guruswami, D. Micciancio and O. Regev, The complexity of the covering radius problem on lattices and codes, *IEEE Conference on Computational Complexity*, (2004), 161–173.
[30] M. Hamburg, Fast and compact elliptic-curve cryptography, *IACR Cryptol. ePrint Arch.*, **2012** (2012), 309.
[31] G. Hanrot, X. Pujol and D. Stehlé, Algorithms for the shortest and closest lattice vector problems, *Coding and Cryptology, Lecture Notes in Comput. Sci., Springer, Heidelberg*, **6639** (2011), 159–190.
[32] G. Hanrot and D. Stehle, Improved analysis of Kannan's shortest lattice vector algorithm, *Advances in Cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., Springer, Berlin*, **4622** (2007), 170–186.
[33] D. Harvey and J. van der Hoeven, Faster integer multiplication using short lattice vectors, *Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., Math. Sci. Publ., Berkeley, CA*, **2** 2019, 293–310.
[34] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: A ring-based public key cryptosystem, *Algorithmic Number Theory (ANTS 1998), LNCS, Springer*, **1423** (1998), 267–288.
[35] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev and D. Urbanik, *SIKE: Supersingular Isogeny Key Encapsulation*, Submission to the NIST's Post-Quantum Cryptography Standardization Process, 2019.
[36] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987), 203–209.
[37] A. Korkine and G. Zolotareff, Sur les formes quadratiques, *Mathematische Annalen*, **6** (1873), 366–389.
[38] J. C. Lagarias, H. W. Lenstra and C.-P. Schnorr, Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica*, **10** (1990), 333–348.
[39] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, **261** (1982), 513–534.

[40] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Mathematica Scandinavica*, **8** (1960), 65–70.
[41] L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, CBMS-NSF Regional Conference Series in Applied Mathematics, 50, SIAM Publications, 1986.
[42] V. S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., Springer, Berlin*, 218 (1986), 417–426.
[43] W. H. Mills, The factorization of certain quadrinomials, *Mathematica Scandinavica*, **57** (1985), 44–50.
[44] H. Minkowski, *Geometrie der Zahlen*, B. G. Teubner, Leipzig, 1896.
[45] P. L. Montgomery, Modular multiplication without trial division, *Mathematics of Computation*, **44** (1985), 519–521.
[46] D. Moody, G. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, R. Peralta, Ra. Perlner, A. Robinson, D. Smith-Tone and J. Alperin-Sheriff, *Status Report on the Second Round of the Nist Post-Quantum Cryptography Standardization Process*, 2020-07-22 2020.
[47] *National Institute for Standards and Technology*, Digital Signature Standard (DSS), Jun 2009.
[48] C. Negre and T. Plantard, Efficient modular arithmetic in adapted modular number system using lagrange representation, *ACISP 2008: Information Security and Privacy*, 463–477.
[49] C. Negre, *Side Channel Counter-Measures Based on Randomized AMNS Modular Multiplication*, Proceedings of the 18th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, 2021.
[50] T. Plantard, *Arithmétique Modulaire Pour la Cryptographie*, Theses, Université Montpellier II - Sciences et Techniques du Languedoc, 2005.
[51] T. Plantard, W. Susilo and Z. Zhang, LLL for ideal lattices: Re-evaluation of the security of gentry–halevi's fhe scheme, *Designs, Codes and Cryptography*, **76** (2015), 325–344.
[52] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang, *Falcon: Fast-Fourier Lattice-Based Compact Signatures Over NTRU*, Submission to the NIST's post-quantum cryptography standardization process, 2017.
[53] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21** (1978), 120–126.
[54] C.-P. Schnorr, Block reduced lattice bases and successive minima, *Combin. Probab. Comput.*, **3** (1994), 507–522.
[55] J. A. Solinas, *Generalized Mersenne Numbers*, Research Report CORR-99-39, Center for Applied Cryptographic Research, University of Waterloo, Waterloo, ON, Canada, 1999.
[56] D. R. Stinson and M. Paterson, *Cryptography Theory and Practice*, Fourth edition ed., Chapman and Hall/CRC, 2018.

Received September 2021; revised February 2022; early access March 2022.

E-mail address: jean-claude.bajard@sorbonne-universite.fr
E-mail address: jeremy.marrez@sorbonne-universite.fr
E-mail address: tplantard@paypal.com
E-mail address: pascal.veron@univ-tln.fr