# Polynomial Modular Number System for Large Integers

## Revisiting the Montgomery Internal Reduction

Nicolas Méloni, François Palma, Pascal Véron

Laboratoire IMATH
Université de Toulon

ALCOCRYPT, February 2023


# Definition

## What is a PMNS and why is it relevant?

- A Polynomial Modular Number System (PMNS) is a non-positional number system based on polynomial operations.
- Fast modular operations (ECC, RSA, etc.)
- Very adapted to parallel processing.
- Faster than GMP for integer sizes $\leqslant 512$ bits.[1]

[1] Dosso, Robert, and Veron. "PMNS for efficient Arithmetic and Small Memory Cost" (IEEE TETC July 2022).

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

# Definition

## What is a PMNS? (toy example)

We take the PMNS ($p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2$)

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$
- $b = 6 \to B(X) = X - 1 \to C(X) = A(X)B(X)$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$
- $b = 6 \to B(X) = X - 1 \to C(X) = A(X)B(X)$
- $C(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$
- $b = 6 \to B(X) = X - 1 \to C(X) = A(X)B(X)$
- $C(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $E(\gamma) \equiv E(7) \equiv 7^3 - 2 \equiv 341 \equiv 0 \pmod{11}$

# Definition

## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$
- $b = 6 \to B(X) = X - 1 \to C(X) = A(X)B(X)$
- $C(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $E(\gamma) \equiv E(7) \equiv 7^3 - 2 \equiv 341 \equiv 0 \pmod{11}$
- $C'(X) = C(X) \pmod{E(X)} = X^3 - 2X^2 + 1 - (X^3 - 2) = -2X^2 + 3$

# Definition

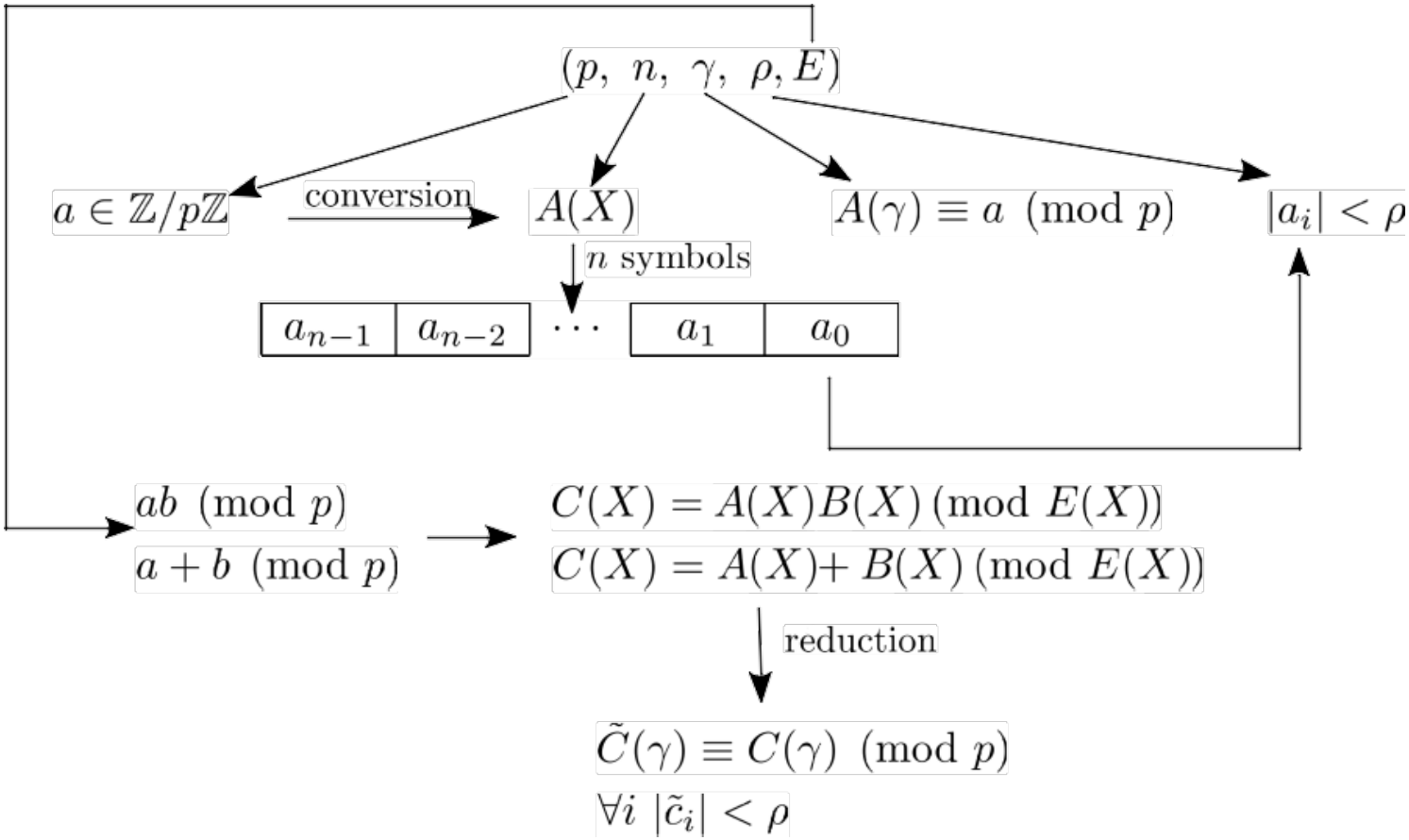
## What is a PMNS? (toy example)

We take the PMNS $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}$
- $a \to A(X) = X^2 - X - 1 : A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$
- $deg(A) < 3$ and $\forall i, |a_i| < 2$
- $b = 6 \to B(X) = X - 1 \to C(X) = A(X)B(X)$
- $C(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $E(\gamma) \equiv E(7) \equiv 7^3 - 2 \equiv 341 \equiv 0 \pmod{11}$
- $C'(X) = C(X) \pmod{E(X)} = X^3 - 2X^2 + 1 - (X^3 - 2) = -2X^2 + 3$
- $ab \equiv 8 \times 6 \equiv 48 \equiv 4 \pmod{11}$
- $C'(\gamma) \equiv C'(7) \equiv -2 \times 7^2 + 3 \equiv -95 \equiv 4 \pmod{11}$

# Definition

## What is a PMNS?




$E \in \mathbb{Z}[X]$ a monic polynomial with $deg(E) = n$ and $E(\gamma) \equiv 0 \pmod p$.

# Coefficient reduction

First idea: find a polynomial that vanishes in $\gamma$.

# Coefficient reduction

Going back to $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$. As a reminder we had $ab \equiv 4 \pmod{11}$ and $C(X) = -2X^2 + 3$.

# Coefficient reduction

Going back to $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$. As a reminder we had $ab \equiv 4 \pmod{11}$ and $C(X) = -2X^2 + 3$.

$T(X) = -2X^2 + X + 3$. $T(7) \equiv -2 \times 49 + 7 + 3 \equiv -88 \equiv 0 \pmod{11}$

# Coefficient reduction

Going back to $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$. As a reminder we had $ab \equiv 4 \pmod{11}$ and $C(X) = -2X^2 + 3$.

$T(X) = -2X^2 + X + 3$. $T(7) \equiv -2 \times 49 + 7 + 3 \equiv -88 \equiv 0 \pmod{11}$

$$C'(X) = C(X) - T(X) = -2X^2 + 3 - (-2X^2 + X + 3) = -X$$

# Coefficient reduction

Going back to $(p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$. As a reminder we had $ab \equiv 4 \pmod{11}$ and $C(X) = -2X^2 + 3$.

$T(X) = -2X^2 + X + 3$. $T(7) \equiv -2 \times 49 + 7 + 3 \equiv -88 \equiv 0 \pmod{11}$

$$C'(X) = C(X) - T(X) = -2X^2 + 3 - (-2X^2 + X + 3) = -X$$

$C'(7) \equiv -7 \equiv 4 \pmod{11}$ and $|c'_i| < 2$

# Problems with this method

## Taking a real example PMNS

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E = X^5 - 2$)

- $A(X) = -16418323151436339X^4 + 276252764540687X^3 + 743784201893843 2X^2 + 1547027964108875 3X - 287287559924033 1$
- $B(X) = 84153449096529 60X^4 + 116184205860341 14X^3 + 48780491573144 45X^2 - 12466769851259518X + 13065840613549045$

# Problems with this method

## Taking a real example PMNS

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E = X^5 - 2$)

- $A(X) = -1641832315143633 9X^4 + 276252764540687X^3 + 743784201893843 2X^2 + 154702796410887 53X - 287287559924033 1$
- $B(X) = 841534490965296 0X^4 + 116184205860341 14X^3 + 487804915731444 5X^2 - 124667698512595 18X + 130658406135490 45$
- $C(X) = A(X)B(X) \pmod{E} = -2611703767839511242980444531479 9X^4 - 3233615868012433854401492460433 90X^3 - 4865572286777221668630406660551 61X^2 + 2093721656764958620763939504877 09X + 8077329583075397655290038034189 95$

# Problems with this method

## Taking a real example PMNS

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E = X^5 - 2$)

- $A(X) = -1641832315143633 9X^4 + 276252764540687X^3 + 743784201893843 2X^2 + 1547027964108875 3X - 287287559924033 1$
- $B(X) = 841534490965296 0X^4 + 116184205860341 14X^3 + 487804915731444 5X^2 - 124667698512595 18X + 130658406135490 45$
- $C(X) = A(X)B(X) \pmod{E} = -2611703767839511242980444531479 9X^4 - 3233615868012433854401492460433 90X^3 - 4865572286777221668630406605516 1X^2 + 2093721656764958620763939504877 09X + 8077329583075397655290038034189 95$
- $T(X) = -2611703767839511370287526888552 7X^4 - 3233615868012433863531023688911 63X^3 - 4865572286777221665968479066956 02X^2 + 2093721656764958622175562186624 21X + 8077329583075397643128743351041 00$

# Montgomery Reduction

Second idea: we get inspired by the Montgomery Integer Reduction to adapt it to polynomials.[2]

[2] Negre and Plantard. "Efficient Modular Arithmetic in Adapted Modular Number System Using Lagrange Representation" (ACISP 2008).

# Montgomery Integer Reduction

Let $\phi = 2^{64}$

# Montgomery Integer Reduction

Let $\phi = 2^{64}$

We want $c = ab \pmod{m}$ with $m \in \mathbb{N}$ odd and such that $\frac{\phi}{2} \leqslant m < \phi$

# Montgomery Integer Reduction

Let $\phi = 2^{64}$

We want $c = ab \pmod{m}$ with $m \in \mathbb{N}$ odd and such that $\frac{\phi}{2} \leqslant m < \phi$

We want to find $q \in \mathbb{Z}$ such that $c + qm \equiv 0 \pmod{\phi}$

# Montgomery Integer Reduction

Let $\phi = 2^{64}$

We want $c = ab \pmod{m}$ with $m \in \mathbb{N}$ odd and such that $\frac{\phi}{2} \leqslant m < \phi$

We want to find $q \in \mathbb{Z}$ such that $c + qm \equiv 0 \pmod{\phi}$

We get $q = -cm^{-1} \pmod{\phi}$

# Montgomery Integer Reduction

Let $\phi = 2^{64}$

We want $c = ab \pmod{m}$ with $m \in \mathbb{N}$ odd and such that $\frac{\phi}{2} \leqslant m < \phi$

We want to find $q \in \mathbb{Z}$ such that $c + qm \equiv 0 \pmod{\phi}$

We get $q = -cm^{-1} \pmod{\phi}$

$c' = c - (cm^{-1} \pmod{\phi})m$ is a multiple of $\phi$

$\frac{c'}{\phi}$ represents $c\phi^{-1}$ in $\mathbb{Z}/m\mathbb{Z}$

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

Let $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$ and $M$ admits an inverse $M^{-1} \pmod{E, \phi}$.

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

Let $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$ and $M$ admits an inverse $M^{-1} \pmod{E, \phi}$.

$$((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv C \pmod{\phi}$$

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

Let $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$ and $M$ admits an inverse $M^{-1} \pmod{E, \phi}$.

$$((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv C \pmod{\phi}$$

$$C' = C - ((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv 0 \pmod{\phi}$$

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

Let $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$ and $M$ admits an inverse $M^{-1} \pmod{E, \phi}$.

$$((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv C \pmod{\phi}$$

$$C' = C - ((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv 0 \pmod{\phi}$$

$C'(\gamma) = C(\gamma)$ and if $|c'_i| < \rho\phi$, $|\frac{c'_i}{\phi}| < \rho$.

# Montgomery Polynomial Reduction

Let $C$ be a polynomial for which we want to reduce the coefficients.

Let $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$ and $M$ admits an inverse $M^{-1} \pmod{E, \phi}$.

$$((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv C \pmod{\phi}$$

$$C' = C - ((C \times M^{-1}) \pmod{E, \phi}) \times M \pmod{E}) \equiv 0 \pmod{\phi}$$

$C'(\gamma) = C(\gamma)$ and if $|c'_i| < \rho\phi$, $|\frac{c'_i}{\phi}| < \rho$.

Problem: Our result won't be $ab \pmod{p}$ but $ab\phi^{-1} \pmod{p}$. Also we need to guarantee $M$ exists and is invertible.

# Generating $M$

Let $\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$

This is a sublattice of $\mathbb{Z}[X]$ of rank $n$ and we can constitute the following basis matrix:

$$\mathcal{B} = \begin{pmatrix} p & 0 & \dots & \dots & \dots & 0 \\ -\gamma & 1 & 0 & \dots & \dots & 0 \\ -\gamma^2 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -\gamma^{n-1} & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

We then apply the LLL algorithm to it to find a short vector.

# Montgomery Polynomial Reduction

We then obtain an internal reduction matrix as follows.

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

$A \cdot \mathcal{M}$ is equivalent to $A \times M \pmod{E}$

Similar process for $M^{-1}$.

# Generation algorithm

**Algorithm 1** [3] Generation of parameters $M$ and $\mathcal{M}$

**Require:** : $n, E \in \mathbb{Z}[X]$ a monic polynomial of degree $n$ having $\gamma$ as a root modulo $p$ and $G$ a reduced basis computed from $\mathcal{B}$
**Ensure:** $M \in \mathbb{Z}[X]$ such that: $deg(M) < n$, $M(\gamma) \equiv 0 \pmod{p}$ and $M' = -M^{-1} \pmod{E, \phi}$ exists.

```
for i = 1 ... 2^n − 1 do
    t ← (t_0, ..., t_{n−1}) # binary decomposition of i
    M ← (t_0, ..., t_{n−1})G
    Compute M
    if det(M = 1) then
        return (M, M)
    end if
end for
```

**Problems:**

Finding $M$ may involve a $O(2^n)$ step of binary linear combination of the basis's vectors.

$2^n$ is not a big issue for 512-bit primes, not so much for 8192-bit primes.

[3] Dosso, Robert, and Veron. "PMNS for efficient Arithmetic and Small Memory Cost" (IEEE TETC July 2022).

# Novel Montgomery Lattice Reduction

Adaptation of the second idea: why not use the reduced basis immediately?

# Montgomery Reduction Principles

For Montgomery Integer Reduction we want to add an integer representative of 0 in $\mathbb{Z}/m\mathbb{Z}$ which is a multiple $qm$ of $m$ such that $c + qm \equiv 0 \pmod{\phi}$.

# Montgomery Reduction Principles

For Montgomery Integer Reduction we want to add an integer representative of 0 in $\mathbb{Z}/m\mathbb{Z}$ which is a multiple $qm$ of $m$ such that $c + qm \equiv 0 \pmod{\phi}$.

For Negre and Plantard's adaptation to Polynomials, they multiply $M$, a polynomial representative of 0 in $\mathbb{Z}/p\mathbb{Z}$, by a polynomial $Q$ such that $C + QM \equiv 0 \pmod{\phi}$

# Montgomery Reduction Principles

For Montgomery Integer Reduction we want to add an integer representative of 0 in $\mathbb{Z}/m\mathbb{Z}$ which is a multiple $qm$ of $m$ such that $c + qm \equiv 0 \pmod{\phi}$.

For Negre and Plantard's adaptation to Polynomials, they multiply $M$, a polynomial representative of 0 in $\mathbb{Z}/p\mathbb{Z}$, by a polynomial $Q$ such that $C + QM \equiv 0 \pmod{\phi}$

Instead of specifying $M$, any representative of 0 in $\mathbb{Z}/p\mathbb{Z}$ would do and this is obtainable with any linear combination of the reduced basis.

# Montgomery Lattice Reduction

Let $\mathcal{L}$ be a reduced basis of
$\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$.

# Montgomery Lattice Reduction

Let $\mathcal{L}$ be a reduced basis of
$\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$.

For any $Q \in \mathbb{Z}[X]$, $T = Q \cdot \mathcal{L}$ is such that $T(\gamma) \equiv 0 \pmod p$ as $T \in \mathfrak{L}$.

# Montgomery Lattice Reduction

Let $\mathcal{L}$ be a reduced basis of
$\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$.

For any $Q \in \mathbb{Z}[X]$, $T = Q \cdot \mathcal{L}$ is such that $T(\gamma) \equiv 0 \pmod p$ as $T \in \mathfrak{L}$.

Thus $C' = C - (C \cdot \mathcal{L}^{-1} \pmod \phi) \cdot \mathcal{L}$ is such that $C'(\gamma) = C(\gamma)$.

# Montgomery Lattice Reduction

Let $\mathcal{L}$ be a reduced basis of
$\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$.

For any $Q \in \mathbb{Z}[X]$, $T = Q \cdot \mathcal{L}$ is such that $T(\gamma) \equiv 0 \pmod p$ as $T \in \mathfrak{L}$.

Thus $C' = C - (C \cdot \mathcal{L}^{-1} \pmod \phi) \cdot \mathcal{L}$ is such that $C'(\gamma) = C(\gamma)$.

Since $(C \cdot \mathcal{L}^{-1} \pmod \phi) \equiv C \pmod \phi$ we get $C' \equiv 0 \pmod \phi$.

# Montgomery Lattice Reduction

Let $\mathcal{L}$ be a reduced basis of
$\mathfrak{L} = \{A(X) \text{ such that } \deg A(X) \leqslant n-1 \text{ and } A(\gamma) \equiv 0 \bmod p\}$.

For any $Q \in \mathbb{Z}[X]$, $T = Q \cdot \mathcal{L}$ is such that $T(\gamma) \equiv 0 \pmod p$ as $T \in \mathfrak{L}$.

Thus $C' = C - (C \cdot \mathcal{L}^{-1} \pmod \phi) \cdot \mathcal{L}$ is such that $C'(\gamma) = C(\gamma)$.

Since $(C \cdot \mathcal{L}^{-1} \pmod \phi) \equiv C \pmod \phi$ we get $C' \equiv 0 \pmod \phi$.

If $|c'_i| < \rho\phi$, $|\frac{c'_i}{\phi}| < \rho$.

# Reduction Algorithm

**Algorithm 2** Coefficients reduction, new version

**Require:** $\mathcal{B} = (p, n, \gamma, \rho, E)$ a PMNS, $C \in \mathbb{Z}_{n-1}[X]$, $\mathcal{L}$ a reduced basis of $\mathfrak{L}$, $\phi \in \mathbb{N} \setminus \{0\}$ and $\mathcal{L}^{-1} \bmod \phi$.

**Ensure:** $S(\gamma) \equiv C(\gamma)\phi^{-1} \bmod p$, with $S \in \mathbb{Z}_{n-1}[X]$

1: $q \leftarrow C(\mathcal{L}^{-1}) \bmod \phi$
2: $S \leftarrow (C - q\mathcal{L})/\phi$
3: return $S$

# Conclusions

New reduction method with faster generation with similar performances.

The new method allows for better bounds and lower degrees (marginal gains for 2436 bits, 2844 bits, 3251 bits).

# Problems still present

Time complexity is mostly dependent on $n$.

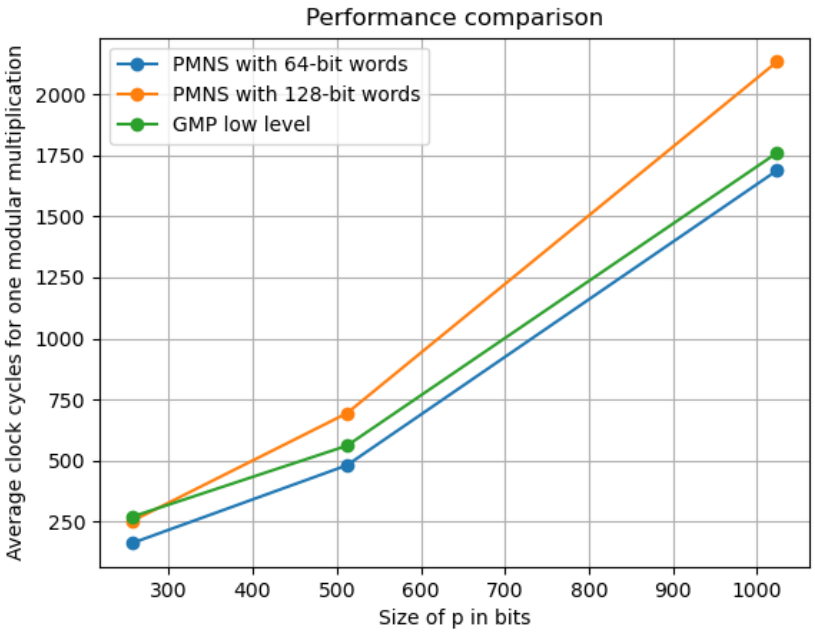
Bounds on $n$ depend on $\phi$ among other things.

We tried for $\phi = 2^{128}$ which adds multiprecision operations.

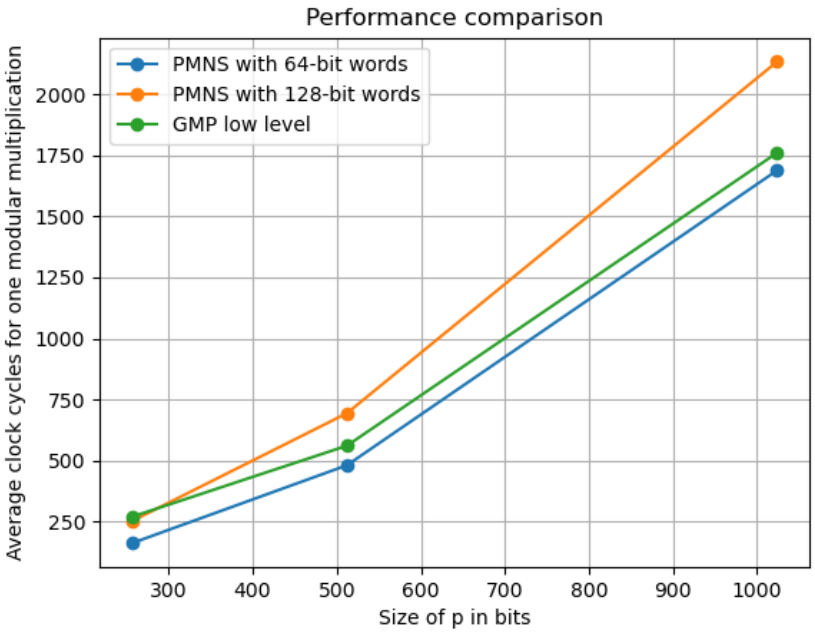
| size of $p$ in bits | 256 | 512 | 1024 | 2048 | 4096 | 8192 |
|---|---|---|---|---|---|---|
| number of GMP limbs | 4 | 8 | 16 | 32 | 64 | 128 |
| $n$ for $\phi = 2^{64}$ | 5 | 9 | 19 | 40 | 83 | 188 |
| $n$ for $\phi = 2^{128}$ | 3 | 5 | 9 | 18 | 36 | 73 |
| 64-bit words for $\phi = 2^{128}$ | 6 | 10 | 18 | 36 | 72 | 146 |

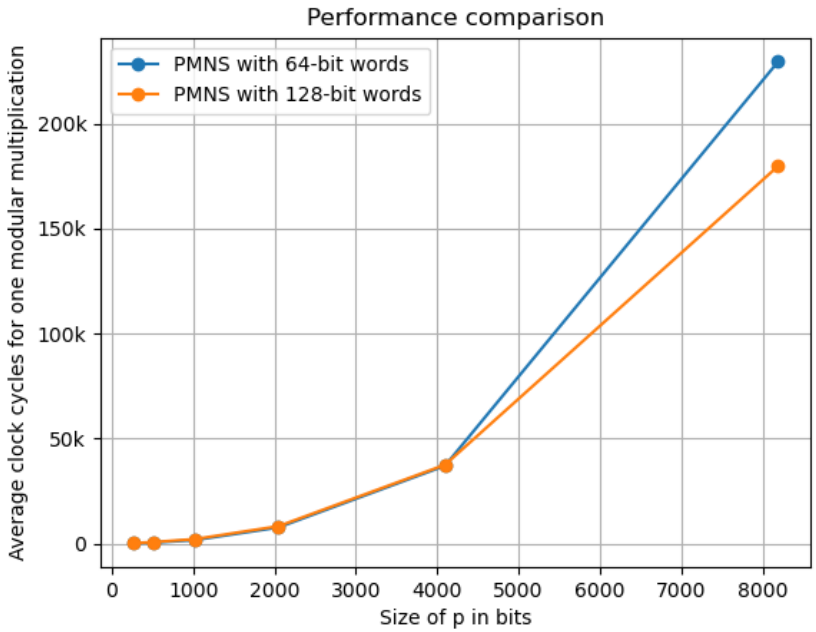
Table: Optimal polynomial degrees found in practice for different $\phi$ and comparison with GMP.

# Current Results



# Current Results




GMP uses subquadratic algorithms for large integer sizes.