Brief Introduction to Number Theoretic Transform

From the Perspective of Ring Theory

Cesare Huang

Academia Sinica

Aug 28, 2025

About me

- Research Assistant @ Academia Sinica, Institute of Information Science — Post-Quantum Cryptography & High-Performance Software
- B.S. in Mathematics, NTU
- Research interests — cryptographic engineering:
  - Implement cryptographic primitives in AArch64 assembly
  - Design fast algorithms; harden against side-channel attacks
  - Formal verification of cryptographic software
- Selected work: AArch64 25519 modular inversion — sub-μs on Apple M1
- Tooling:
  - *qhasm* — high-performance assembly generator
  - SLOTHY — ILP-based instruction scheduling
  - Cryptoline — formal verification of crypto software
- Teaching & writing:
  - TA — “Post-Quantum Cryptography”, NTU
  - TA — “Quantum Information and Computation”, NTU
  - 30-day technical series (Introduction to Post-Quantum Cryptography) @ ithome https://ithelp.ithome.com.tw/m/users/20168745/ironman/7741
  - TA (coming semester) - "Cryptographic Engineering", NTU
- Github: https://github.com/cheng-wei-huang0612

TABLE OF CONTENTS

1 Preliminaries 4

1.1 Modular Arithmetic 4

1.2 Background 7

2 Theory of Number Theoretic Transform 8

2.1 Start from Residue Number System and Chinese Remainder Theorem 8

2.2 Decomposition of $\mathbb{Z}_p[x]/\langle x^2 - 1\rangle$ 10

2.3 Decomposition of $\mathbb{Z}_p[x]/\langle x^4 - 1\rangle$ 15

2.4 Decomposition of $\mathbb{Z}_p[x]/\langle x^8 - 1\rangle$ 27

2.5 Decomposition of $\mathbb{Z}_p[x]/\langle x^n - 1\rangle$ 32

3 The Implementation of Algorithms 33

3.1 Example of $\mathbb{Z}_{17}[x]/(x^8 - 1)$ 33

Table of Contents

4 Advanced Topics 42

4.1 Shapeless Modular Reduction and Multiplication 42
4.2 NTT-unfriendly rings 44
4.3 Incomplete NTT 45
4.4 Good's Trick 47
4.5 NTT-based Integer Multiplication 50
4.6 Multi-moduli NTT 51

PRELIMINARIES: MODULAR ARITHMETIC

- We are already familiar with modular arithmetic such as

$$4 \times 5 \mod 17 = 3.$$

- Modular arithmetic can be extended to polynomials

$$\begin{aligned}
&(x-1) \times (x-2) \mod (x^2-1) \\
&= x^2 - 3x + 2 \mod (x^2-1) \\
&= (x^2 - 1) + 1 - 3x + 2 \mod (x^2-1) \\
&= -3x + 3.
\end{aligned}$$

Effectively, you can do modular reduction (i.e., taking remainders) by simply replacing x^2 by 1.

PRELIMINARIES: QUOTIENT RING

- Collecting all remainders modulo 17 gives a set

$$\mathbb{Z}/\langle 17\rangle = \{a \bmod 17 : a \in \mathbb{Z}\} = \{0, 1, 2, \ldots, 16\} = \mathbb{Z}/17\mathbb{Z} = \mathbb{Z}_{17}.$$

  the last two notations (symbols) are common in the literature. This is also known as Integer Quotient Ring.
- We denote the set of polynomials by

$$\mathbb{Z}[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{Z}, n < \infty \right\}.$$

  This is also known as Polynomial Ring.
- Then collecting all reminders modulo $x^2 - 1$ gives a set

$$\mathbb{Z}[x]/\langle x^2 - 1\rangle = \{f(x) \bmod (x^2 - 1) : f(x) \in \mathbb{Z}[x]\} = \{ax + b : a, b \in \mathbb{Z}\}.$$

  Effectively, it just collects all integer-coefficient polynomials with degree lower than 2.

PRELIMINARIES: QUOTIENT RING

- Exercise: Describe the set
$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle$$
- This set contains polynomials taken modulo $x^4 - 1$, where their coefficients are taken modulo 17.
- Example of arithmetic in this set:
$$\begin{aligned}
&(3 + x + 4x^2 + x^3)\,(2 + 7x + x^2 + 7x^3) \\
&= 6 + 23x + 18x^2 + 52x^3 + 18x^4 + 29x^5 + 7x^6 \\
&= 6 + 23x + 18x^2 + 52x^3 + 18{\cdot}1 + 29{\cdot}x + 7{\cdot}x^2 \\
&= 24 + 52x + 25x^2 + 52x^3 \\
&= 7 + x + 8x^2 + x^3.
\end{aligned}$$
- Multiplication in such structured quotient ring is also known as the Cyclic Convolution.

WHY WE NEED THIS

- **Background**:
  - In many applications in cryptography, we have to multiply the integer-coefficient polynomials, which is a very time-consuming operation.
    - In Groth16, PLONK, STARK(FRI), one have to compute a lot of polynomial multiplication.
    - In NTRU, one have to compute the multiplication of the rings

$$\mathbb{Z}_{2048}[x]/\langle x^{677}-1\rangle, \quad \mathbb{Z}_{4096}[x]/\langle x^{821}-1\rangle, \text{etc.}$$

  - Suppose we can perform such operation more efficiently, then in the same cost of computational resource (i.e., time), we can perform such multiplication for larger n, and thus improve the security level of the cryptographic scheme.
- **Problem**: Fast polynomial multiplication in $\mathbb{Z}_p[x]/\langle x^n-1\rangle$, where n is a power of 2.

Theory of Number Theoretic Transform

Start from Residue Number System and Chinese Remainder Theorem

- Goal: compute $31 \cdot 27 \pmod{105}$.
- We can do

$$\begin{cases} 31 \times 27 \bmod 3 \\ 31 \times 27 \bmod 5 \\ 31 \times 27 \bmod 7 \end{cases}$$

  we get

$$\begin{cases} 31 \times 27 = 1 \times 0 = 0 \pmod 3 \\ 31 \times 27 = 1 \times 2 = 2 \pmod 5 \\ 31 \times 27 = 3 \times 6 = 4 \pmod 7 \end{cases}$$

- This is an instance of Chinese Remainder Theorem. We can recover the answer by solving the system in x

$$x \equiv 0 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 4 \pmod 7$$

- The formula of CRT immediately gives

$$0 \times \underbrace{70}_{\text{precomputed}} + 2 \times \underbrace{21}_{\text{precomputed}} + 4 \times \underbrace{15}_{\text{precomputed}} = 102.$$

- Quick check: $31 \cdot 27 = 837 \equiv 102 \pmod{105}$.

- The above computation of $31 \times 27 \bmod 105$ can be summarized into:
  1. Map to quotient integer ring:

$$\begin{aligned} \mathbb{Z}/\langle 105\rangle &\cong \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 5\rangle \times \mathbb{Z}/\langle 7\rangle \\ 31 &\mapsto (1,1,3) \\ 27 &\mapsto (0,2,6) \end{aligned}$$

  2. Multiply parallelly in each coordinate

$$(1,1,3) \odot (0,2,6) = (0 \bmod 3, 2 \bmod 5, 4 \bmod 7)$$

  3. Reconstruct the big integer

$$\begin{aligned} \mathbb{Z}/\langle 105\rangle &\cong \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 5\rangle \times \mathbb{Z}/\langle 7\rangle \\ 102 &\mapsfrom (0,2,4) \end{aligned}$$

- Takeaway: We can use Chinese Remainder Theorem to craft a divide-and-conquer algorithm for big number multiplication. And things can be extended to Multiplication of Polynomial Rings.

- Let's do multiplication in a simple ring: $\mathbb{Z}_p[x]/\langle x^2-1\rangle$.
- The schoolbook multiplication (namely, traditional one) do

$$\begin{aligned}&(a_0+a_1x)\times(b_0+b_1x)\\&=a_0b_0+(a_0b_1+a_1b_0)x+a_1b_1x^2\\&=a_0b_0+a_1b_1+(a_0b_1+a_1b_0)x\end{aligned}$$

  This requires four multiplication operations.
- By the previous experience working with CRT, we firstly observe the co-prime factorization:

$$(x^2-1)=(x-1)\times(x+1)$$

  Then we can write down the Chinese Remainder Theorem

$$\mathbb{Z}_p[x]/\langle x^2-1\rangle\cong\mathbb{Z}_p[x]/\langle x-1\rangle\times\mathbb{Z}_p[x]/\langle x+1\rangle.$$

- Concretely, we first do

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^2 - 1\rangle &\cong \mathbb{Z}_p[x]/\langle x - 1\rangle \times \mathbb{Z}_p[x]/\langle x + 1\rangle \\ (a_0 + a_1 x) &\mapsto (a_0 + a_1, a_0 - a_1) \\ (b_0 + b_1 x) &\mapsto (b_0 + b_1, b_0 - b_1)\end{aligned}$$

- Then multiply parallelly in each coordinate

$$(a_0 + a_1, a_0 - a_1) \odot (b_0 + b_1, b_0 - b_1) := (C_0, C_1).$$

- Finally we try to Reconstruct the big polynomial

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^2 - 1\rangle &\cong \mathbb{Z}_p[x]/\langle x - 1\rangle \times \mathbb{Z}_p[x]/\langle x + 1\rangle \\ c_0 + c_1 x &\leftarrow\!\shortmid (C_0, C_1)\end{aligned}$$

- Finally we try to Reconstruct the big polynomial

$$\mathbb{Z}_p[x]/\langle x^2-1\rangle \cong \mathbb{Z}_p[x]/\langle x-1\rangle \times \mathbb{Z}_p[x]/\langle x+1\rangle$$
$$c_0 + c_1 x \leftrightarrow (C_0, C_1)$$

- How to reconstruct it?
- Interpretation via Remainder Theorem from your high school: taking the remainder of $(x-1)$ is equivalent to evaluate the polynomial at $x=1$. So the above reconstruct problem turn into

$$\begin{cases} [c_0 + c_1 x]_{x=1} = C0 \\ [c_0 + c_1 x]_{x=-1} = C1 \end{cases}$$

That is,

$$\begin{cases} c_0 + c_1 = C_0 \\ c_0 - c_1 = C_1 \end{cases}$$

and hence

$$c_0 = \frac{C_0 + C_1}{2}, \quad c_1 = \frac{C_0 - C_1}{2}$$

- Concretely, we first do

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^2-1\rangle &\cong \mathbb{Z}_p[x]/\langle x-1\rangle \times \mathbb{Z}_p[x]/\langle x+1\rangle \\ (a_0+a_1x) &\mapsto (a_0+a_1, a_0-a_1) \\ (b_0+b_1x) &\mapsto (b_0+b_1, b_0-b_1)\end{aligned}$$

- Then multiply parallelly in each coordinate

$$(a_0+a_1, a_0-a_1)\odot(b_0+b_1, b_0-b_1) := (C_0, C_1).$$

- Finally we try to Reconstruct the big polynomial

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^2-1\rangle &\cong \mathbb{Z}_p[x]/\langle x-1\rangle \times \mathbb{Z}_p[x]/\langle x+1\rangle \\ c_0+c_1x &\leftarrow\!\shortmid (C_0, C_1)\end{aligned}$$

  where, from the above page, the answer is

$$c_0+c_1x = \left(\frac{C_0+C_1}{2}\right) + \left(\frac{C_0-C_1}{2}\right)x$$

- Recall that school book requires four multiplications and several additions.
- This divide-and-conquer strategy requires two multiplications, namely the step:

$$(a_0 + a_1, a_0 - a_1) \odot (b_0 + b_1, b_0 - b_1) := (C_0, C_1).$$

  and two multiplication by constant, namely, the divided by two (multiplication by $2^{-1} \bmod p$ in the final step:

$$c_0 + c_1 x = \left(\frac{C_0 + C_1}{2}\right) + \left(\frac{C_0 - C_1}{2}\right) x$$

- So far, the divide-and-conquer does not save the number of operations so much? Let's slightly increase the problem size.

- Let's do multiplication in the ring $\mathbb{Z}_p[x]/\langle x^4 - 1\rangle$.
- If you proceed by schoolbook method, a brief computation in mind returns to you that it requires 16 multiplications and several additions.
- From the experience in previous slides, a coprime factorization immediately come to your mind:

$$(x^4 - 1) = (x^2 - 1)(x^2 + 1).$$

and then we can write down the CRT

$$\mathbb{Z}_p[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_p[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_p[x]/\langle x^2 + 1\rangle$$
$$(a_0 + a_1 x + a_2 x^2 + a_3 x^3) \mapsto (a_0 + a_2 + (a_1 + a_3)x, a_0 - a_2 + (a_1 - a_3)x)$$

- But the component $\mathbb{Z}_p[x]/\langle x^2 - 1\rangle$ seems to be able to be further decomposed into

$$\mathbb{Z}_p[x]/\langle x^2 - 1\rangle \cong \mathbb{Z}_p[x]/\langle x - 1\rangle \times \mathbb{Z}_p[x]/\langle x + 1\rangle.$$

- So we try

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^4 - 1\rangle &\cong \mathbb{Z}_p[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_p[x]/\langle x^2 + 1\rangle \\ &\cong \mathbb{Z}_p[x]/\langle x - 1\rangle \times \mathbb{Z}_p[x]/\langle x + 1\rangle \times ????_0 \times ????_1\end{aligned}$$

- In order to find out $????_0$ and $????_1$, we need a factorization of

$$(x^2 + 1)$$

  under $\mathbb{Z}_p[x]$.
- Such decomposition must be in the form (degree 1 poly) $\times$ (degree 1 poly). So, effectively, to factor $(x^2 + 1)$ is to find the root of it, and, is to find an x such that $x^2 = -1$.
- From your memory in high school, using $i = \sqrt{-1} \in \mathbb{C}$ in complex number serves our need:

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^4 - 1\rangle &\cong \mathbb{Z}_p[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_p[x]/\langle x^2 + 1\rangle \\ &\subseteq \mathbb{Z}_p[x]/\langle x - 1\rangle \times \mathbb{Z}_p[x]/\langle x + 1\rangle \times \mathbb{C}[x]/\langle x - i\rangle \times \mathbb{C}[x]/\langle x + i\rangle\end{aligned}$$

  However, as you see, this increases another variable for us, and hence, more multiplication operations are needed.

Theory of Number Theoretic Transform

Decomposition of $\mathbb{Z}_p[x]/\langle x^4 - 1\rangle$

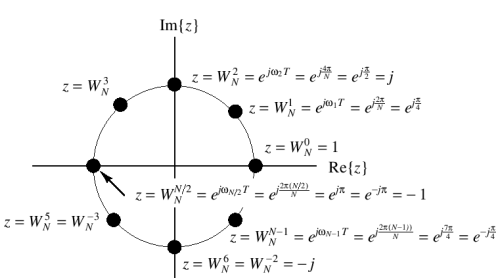
- In order to find out $????_0$ and $????_1$, we need a factorization of

$$(x^2 + 1)$$

under $\mathbb{Z}_p$.

- Such decomposition must be in the form (degree 1 poly) $\times$ (degree 1 poly). So, effectively, to factor $(x^2 + 1)$ is to find the root of it, and, is to find an x such that $x^2 = -1$.
- Another way to resolve this, is to utilize the structure of $\mathrm{mod}\, p$ of coefficients,
- **Theorem.** Let p be a odd prime, if $p - 1$ is divisible by k, then there exists kth primitive root, denoted ω_k such that

$$(\omega_k)^k \bmod p = 1 \text{ and } (\omega_k)^i \bmod p \neq 1 \text{ if } i < k.$$

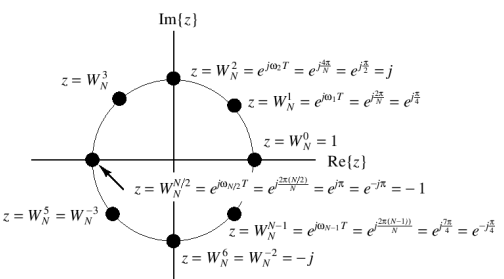


Theory of Number Theoretic Transform

Decomposition of $\mathbb{Z}_p[x]/\langle x^4 - 1\rangle$

- Another way to resolve this, is to utilize the structure of $\bmod p$ of coefficients,
- **Theorem.** Let p be a odd prime, if $p-1$ is divisible by k, then there exists kth primitive root, denoted ω_k such that

$$(\omega_k)^k \bmod p = 1 \text{ and } (\omega_k)^i \bmod p \neq 1 \text{ if } i < k.$$



- For example, let $p = 17$, then 16 divides $p-1$, so there exists 16th primitive root ω_{16}:

$$\omega_{16} = 3, \quad \omega_8 = 9, \quad \omega_4 = 13, \quad \omega_2 = 16 = -1$$

- For example, let $p = 17$, then 16 divides $p-1$, so there exists 16th primitive root ω_{16}:

$$\omega_{16} = 3, \quad \omega_8 = 9, \quad \omega_4 = 13, \quad \omega_2 = 16 = -1$$

- Hence, lets investigate the multiplication in the ring $\mathbb{Z}_{17}[x]/\langle x^4-1\rangle$.
- By, previous experience, and the existence of $\omega_4 = 13$, we can now write sown

$$\begin{aligned}
\mathbb{Z}_{17}[x]/\langle x^4-1\rangle &\cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2+1\rangle \\
&\cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2-(-1)\rangle \\
&\cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2-\omega_4^2\rangle \\
&\cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-\omega_4\rangle \times \mathbb{Z}_{17}[x]/\langle x+\omega_4\rangle \\
&\cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle
\end{aligned}$$

- **Example.**

$$\begin{aligned}
\mathbb{Z}_{17}[x]/\langle x^4-1\rangle &\cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2+1\rangle \\
(1+2x+3x^2+4x^3) &\mapsto (4+6x, -2-2x)
\end{aligned}$$

$$\begin{aligned}
&\cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle \\
&\mapsto (10, -2, -28, 24) = (10, 15, 6, 7).
\end{aligned}$$

- With the following CRT decomposition in mind

$$\begin{aligned}\mathbb{Z}_{17}[x]/\langle x^4-1\rangle &\cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2+1\rangle \\ &\cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle\end{aligned}$$

  we can use this to craft a fast algorithm of multiplication in $\mathbb{Z}_{17}[x]/\langle x^4-1\rangle$.
- Say, we want to multiply $3+x+4x^2+2x^3$ and $2+7x+x^2+7x^3$ in $\mathbb{Z}_{17}[x]/\langle x^4-1\rangle$. We proceed by
  1. Project the operands into the coordinate ring:

$$\mathbb{Z}_{17}[x]/\langle x^4-1\rangle \cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle$$

$$(3+x+4x^2+2x^3) \mapsto (10,4,3,12)$$

$$(2+7x+x^2+7x^3) \mapsto (0,6,1,1)$$

  2. Multiply the coordinates parallelly

$$(10,4,3,12) \odot (0,6,1,1) = (0,7,3,12).$$

  3. Reconstruct the big polynomial:

$$\mathbb{Z}_{17}[x]/\langle x^4-1\rangle \cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle$$

$$(c_0+c_1x+c_2x^2+c_3x^3) \leftarrow\!\shortmid (0,7,3,12).$$

- Reconstruct the big polynomial

$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle$$
$$(c_0 + c_1 x + c_2 x^2 + c_3 x^3) \leftarrow\!\shortmid (????_0 + ????_1 x, ????_2 + ????_3 x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle$$
$$\leftarrow\!\shortmid (0, 7, 3, 12).$$

- Note that we can split the decomposition into two parts:

$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle$$
$$(c_0 + c_1 x + c_2 x^2 + c_3 x^3) \leftarrow\!\shortmid (????_0 + ????_1 x, ????_2 + ????_3 x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle$$
$$\leftarrow\!\shortmid (0, 7, 3, 12).$$

blue parts and red parts are independent.

- Note that we can split the decomposition into two parts:

$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle$$
$$(c_0 + c_1 x + c_2 x^2 + c_3 x^3) \leftrightarrow (????_0 + ????_1 x, ????_2 + ????_3 x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle$$
$$\leftrightarrow (0, 7, 3, 12).$$

blue parts and red parts are independent.

- Blue parts solves to

$$\begin{cases} ????_0 + ????_1 = 0 \\ ????_0 - ????_1 = 7 \end{cases}$$

and the solution is

$$????_0 = (0 + 7)/2 \pmod{17} = 12$$
$$????_1 = (0 - 7)/2 \pmod{17} = 5$$

- Note that we can split the decomposition into two parts:

$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle$$
$$(c_0 + c_1 x + c_2 x^2 + c_3 x^3) \leftrightarrow (12 + 5x, ????_2 + ????_3 x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle$$
$$\leftrightarrow (0, 7, 3, 12).$$

  blue parts and red parts are independent.

- Red parts solves to

$$\begin{cases} ????_2 + 13 \cdot ????_3 = 3 \\ ????_2 - 13 \cdot ????_3 = 12 \end{cases}$$

  and the solution is

$$????_2 = (3 + 12)/2 \pmod{17} = 16$$
$$????_3 = (3 - 12)/(2 \cdot 13) \pmod{17} = 16$$

- So far, we have

$$\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle$$
$$(c_0 + c_1 x + c_2 x^2 + c_3 x^3) \leftrightarrow (12 + 5x, 16 + 16x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle$$
$$\leftrightarrow (0, 7, 3, 12).$$

  Now we solve for c_0, c_1, c_2, c_3.
- This is in fact an easy job. We can write down the equations:

$$\begin{cases} c_0 + c_2 = 12 \\ c_0 - c_2 = 16 \\ c_1 + c_3 = 5 \\ c_1 - c_3 = 16 \end{cases}$$

  which solves to $c_0 = (12 + 16)/2 \pmod{17} = 14$, $c_2 = (12 - 16)/2 = 15$,
  $c_1 = (5 + 16)/2 \pmod{17} = 2$, $c_3 = (5 - 16)/2 \pmod{17} = 3$.

- Finally, we have

$$\mathbb{Z}_{17}[x]/\langle x^4-1\rangle \cong \mathbb{Z}_{17}[x]/\langle x^2-1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2+1\rangle$$
$$(14+2x+15x^2+3x^3) \hookleftarrow (12+5x, 16+16x)$$

$$\cong \mathbb{Z}_{17}[x]/\langle x-1\rangle \times \mathbb{Z}_{17}[x]/\langle x+1\rangle \times \mathbb{Z}_{17}[x]/\langle x-13\rangle \times \mathbb{Z}_{17}[x]/\langle x+13\rangle$$
$$\hookleftarrow (0,7,3,12).$$

- We can check that

$$\begin{aligned}
&(3+x+4x^2+2x^3)(2+7x+x^2+7x^3)\\
&= 6+23x+18x^2+54x^3+25x^4+30x^5+14x^6\\
&= 6+23x+18x^2+54x^3+25\cdot 1+30\cdot x+14\cdot x^2\\
&= 31+53x+32x^2+54x^3\\
&= 14+2x+15x^2+3x^3.
\end{aligned}$$

- Let's give a complexity analysis of the algorithm just crafted:
  1. Project two polynomials into the coordinate rings:

$$\begin{aligned}\mathbb{Z}_{17}[x]/\langle x^4 - 1\rangle &\cong \mathbb{Z}_{17}[x]/\langle x^2 - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x^2 + 1\rangle \\ &\cong \mathbb{Z}_{17}[x]/\langle x - 1\rangle \times \mathbb{Z}_{17}[x]/\langle x + 1\rangle \times \mathbb{Z}_{17}[x]/\langle x - 13\rangle \times \mathbb{Z}_{17}[x]/\langle x + 13\rangle\end{aligned}$$

     The first $\cong$ requires subtractions and additions only. The blue part also requires subtractions and additions. The red part then requires 1 multiplication by $\omega_4 = 13$ for each operand.
  2. Multiply coordinate rings parallelly requires 4 multiplications.
  3. Reconstruct the big polynomial. The blue part requires 2 multiplication by $2^{-1} \pmod p$ The red part requires 1 multiplication by $2^{-1} \pmod p$ and 1 multiplication by $(2 \cdot \omega_4)^{-1} \pmod p$. After that, one requires 4 multiplication by $2^{-1} \pmod p$ to fully reconstruct the big polynomial.
- In total, 2 + 4 + 4 + 4 = 14 multiplications are required. Compare with the school book method which requires 16 multiplications.
- Furthermore, in the reconstruction part, one can collect all multiplication by $2^{-1} \pmod p$ and deal with it finally, this saves 3 more multiplications.

- Now we describe the same strategy applied to $\mathbb{Z}_p[x]/\langle x^8-1\rangle$, where we assume $p-1$ is divisible by 8 and hence ω_8 exists.
- Then one have the following factorization:

$$\begin{aligned}(x^8-1) &= (x^4-1)(x^4+1) = (x^4-1)(x^4-\omega_4^2)\\ &= (x^2-1)(x^2+1)(x^2-\omega_4)(x^2+\omega_4)\\ &= (x^2-1)(x^2-\omega_4^2)(x^2-\omega_8^2)(x^2-\omega_8^6)\\ &= (x-1)(x+1)(x-\omega_4)(x+\omega_4)(x-\omega_8)(x+\omega_8)(x-\omega_8^3)(x+\omega_8^3).\end{aligned}$$

- Hence we have the decomposition:

$$\begin{aligned}\mathbb{Z}_p[x]/(x^8-1) &\cong (\mathbb{Z}_p[x]/(x^4-1)) \times (\mathbb{Z}_p[x]/(x^4+1))\\ &\cong (\mathbb{Z}_p[x]/(x^2-1)) \times (\mathbb{Z}_p[x]/(x^2+1)) \times (\mathbb{Z}_p[x]/(x^2-\omega_4)) \times (\mathbb{Z}_p[x]/(x^2+\omega_4))\\ &\cong (\mathbb{Z}_p[x]/(x-1)) \times (\mathbb{Z}_p[x]/(x+1)) \times (\mathbb{Z}_p[x]/(x-\omega_4)) \times (\mathbb{Z}_p[x]/(x+\omega_4))\\ &\quad \times (\mathbb{Z}_p[x]/(x-\omega_8)) \times (\mathbb{Z}_p[x]/(x+\omega_8)) \times (\mathbb{Z}_p[x]/(x-\omega_8^3)) \times (\mathbb{Z}_p[x]/(x+\omega_8^3)).\end{aligned}$$

- We can rewrite the decomposition so as to see the pattern:

$$\begin{aligned}
\mathbb{Z}_p[x]/(x^8-1) &\cong (\mathbb{Z}_p[x]/(x^4-1)) \times (\mathbb{Z}_p[x]/(x^4+1)) = (\mathbb{Z}_p[x]/(x-\omega_2^0)) \times (\mathbb{Z}_p[x]/(x-\omega_2^1)) \\
&\cong (\mathbb{Z}_p[x]/(x^2-1)) \times (\mathbb{Z}_p[x]/(x^2+1)) \times (\mathbb{Z}_p[x]/(x^2-\omega_4)) \times (\mathbb{Z}_p[x]/(x^2+\omega_4)) \\
&= (\mathbb{Z}_p[x]/(x^2-\omega_4^0)) \times (\mathbb{Z}_p[x]/(x^2-\omega_4^2)) \times (\mathbb{Z}_p[x]/(x^2-\omega_4)) \times (\mathbb{Z}_p[x]/(x^2-\omega_4^3)) \\
&\cong (\mathbb{Z}_p[x]/(x-1)) \times (\mathbb{Z}_p[x]/(x+1)) \times (\mathbb{Z}_p[x]/(x-\omega_4)) \times (\mathbb{Z}_p[x]/(x+\omega_4)) \\
&\quad \times (\mathbb{Z}_p[x]/(x-\omega_8)) \times (\mathbb{Z}_p[x]/(x+\omega_8)) \times (\mathbb{Z}_p[x]/(x-\omega_8^3)) \times (\mathbb{Z}_p[x]/(x+\omega_8^3)) \\
&= (\mathbb{Z}_p[x]/(x-\omega_8^0)) \times (\mathbb{Z}_p[x]/(x-\omega_8^4)) \times (\mathbb{Z}_p[x]/(x-\omega_8^2)) \times (\mathbb{Z}_p[x]/(x-\omega_8^6)) \\
&\quad \times (\mathbb{Z}_p[x]/(x-\omega_8)) \times (\mathbb{Z}_p[x]/(x-\omega_8^5)) \times (\mathbb{Z}_p[x]/(x-\omega_8^3)) \times (\mathbb{Z}_p[x]/(x-\omega_8^7)).
\end{aligned}$$

- The exponent of ω_8 is 0, 4, 2, 6, 1, 5, 3, 7, which is the bit-reverse-order:

$$\begin{aligned}
0 = 000_{(2)} &\xmapsto{\text{brv}_3} 000_{(2)} = 0, \quad 1 = 001_{(2)} \xmapsto{\text{brv}_3} 100_{(2)} = 4, \\
2 = 010_{(2)} &\xmapsto{\text{brv}_3} 010_{(2)} = 2, \quad 3 = 011_{(2)} \xmapsto{\text{brv}_3} 110_{(2)} = 6, \\
4 = 100_{(2)} &\xmapsto{\text{brv}_3} 001_{(2)} = 1, \quad 5 = 101_{(2)} \xmapsto{\text{brv}_3} 101_{(2)} = 5, \\
6 = 110_{(2)} &\xmapsto{\text{brv}_3} 011_{(2)} = 3, \quad 7 = 111_{(2)} \xmapsto{\text{brv}_3} 111_{(2)} = 7
\end{aligned}$$

- With the brv_3 in mind, we can rewrite the decomposition as:

$$\begin{aligned}\mathbb{Z}_p[x]/\langle x^8 - 1\rangle &\cong \prod_{i=0}^{1} \mathbb{Z}_p[x]/\langle x^4 - \omega_2^{\mathrm{brv}_1(i)}\rangle \\ &\cong \prod_{i=0}^{3} \mathbb{Z}_p[x]/\langle x^2 - \omega_4^{\mathrm{brv}_2(i)}\rangle \\ &\cong \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle.\end{aligned}$$

- We can now finally define the term Number Theoretic Transform: Number Theoretic Transform is in fact just the natural projections:

$$\mathrm{NTT}_8 : \mathbb{Z}_p[x]/\langle x^8 - 1\rangle \to \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle$$

and the Inverse Number Theoretic Transform is just the inversion of it:

$$\mathrm{INTT}_8 : \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle \to \mathbb{Z}_p[x]/\langle x^8 - 1\rangle$$

- Our fast algorithm of multiplying $f(x)$ and $g(x)$ in the ring
  1. Do NTT:

$$\begin{aligned}\mathrm{NTT}_8 : \mathbb{Z}_p[x]/\langle x^8 - 1\rangle &\to \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle \\ f(x) &\mapsto (\hat{f}[0], \hat{f}[1], ..., \hat{f}[7]) \\ g(x) &\mapsto (\hat{g}[0], \hat{g}[1], ..., \hat{g}[7])\end{aligned}$$

  2. Then multiply the coordinates parallelly:

$$(\hat{f}[0], \hat{f}[1], ..., \hat{f}[7]) \odot (\hat{g}[0], \hat{g}[1], ..., \hat{g}[7]) = (\hat{h}[0], \hat{h}[1], ..., \hat{h}[7])$$

  3. Then do INTT:

$$\begin{aligned}\mathrm{INTT}_8 : \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle &\to \mathbb{Z}_p[x]/\langle x^8 - 1\rangle \\ (\hat{h}[0], \hat{h}[1], ..., \hat{h}[7]) &\mapsto h(x)\end{aligned}$$

- Some papers summarize the fast algorithm as:

$$h(x) = \mathrm{INTT}(\mathrm{NTT}(f(x)) \odot \mathrm{NTT}(g(x))).$$

- Here, we also make another remark that, NTT is effectively doing

$$\begin{aligned}\mathrm{NTT}_8 : \mathbb{Z}_p[x]/\langle x^8 - 1\rangle &\to \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x - \omega_8^{\mathrm{brv}_3(i)}\rangle \\ f(x) &\mapsto (\hat{f}[0], \hat{f}[1], \hat{f}[2], \hat{f}[3], \hat{f}[4], \hat{f}[5], \hat{f}[6], \hat{f}[7]) \\ &= (f(\omega_8^0), f(\omega_8^4), f(\omega_8^2), f(\omega_8^6), f(\omega_8), f(\omega_8^5), f(\omega_8^3), f(\omega_8^7))\end{aligned}$$

  which is the bit-reverse-order of

$$(f(\omega_8^0), f(\omega_8^1), f(\omega_8^2), f(\omega_8^3), f(\omega_8^4), f(\omega_8^5), f(\omega_8^6), f(\omega_8^7))$$

  Hence, in some paper, definition of NTT may written as (note slightly difference on bit-reverse-order)

$$\mathrm{NTT}(f)[i] = f(\omega_8^i) = \sum_{j=0}^{7} f_j \omega_8^{ij}$$

  This is just the Fourier Transform with primitive roots, ω, in complex number replaced by the primitive in "modulo p" ring. This explains the name Number Theoretic "Transform".

- Let's conclude the theory part with the general decomposition formula:
- Suppose p is a prime and $p - 1$ is divisible by $n = 2^k$, then the nth primitive root ω_n exists in $\mathbb{Z}_p$.
- Decomposition of $\mathbb{Z}_p[x]/\langle x^n - 1\rangle$ is then

$$
\begin{aligned}
&\mathbb{Z}_p[x]/\langle x^{2^k} - 1\rangle \\
&\cong \prod_{i=0}^{1} \mathbb{Z}_p[x]/\langle x^{2^{k-1}} - \omega_2^{\mathrm{brv_1(i)}}\rangle \\
&\cong \prod_{i=0}^{3} \mathbb{Z}_p[x]/\langle x^{2^{k-2}} - \omega_4^{\mathrm{brv_2(i)}}\rangle \\
&\cong \prod_{i=0}^{7} \mathbb{Z}_p[x]/\langle x^{2^{k-3}} - \omega_8^{\mathrm{brv_3(i)}}\rangle \\
&\dots \\
&\cong \prod_{i=0}^{2^k-1} \mathbb{Z}_p[x]/\langle x - \omega_n^{\mathrm{brv_k(i)}}\rangle
\end{aligned}
$$

- We now demonstrate the actual implementations of the fast algorithm of

$$\mathbb{Z}_{17}[x]/(x^8-1).$$

  We note that $\omega_4 = 4$ and $\omega_8 = 2$.
- The first step is the projection:

$$\begin{aligned}\mathbb{Z}_{17}[x]/(x^8-1) &\underbrace{\cong}_{(1)} \mathbb{Z}_{17}[x]/(x^4-1) \times \mathbb{Z}_{17}[x]/(x^4+1)\\ &\underbrace{\cong}_{(2)} \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1) \times \mathbb{Z}_{17}[x]/(x^2-4) \times \mathbb{Z}_{17}[x]/(x^2+4)\\ &\underbrace{\cong}_{(3)} \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4)\\ &\quad \times \mathbb{Z}_{17}[x]/(x-2) \times \mathbb{Z}_{17}[x]/(x+2) \times \mathbb{Z}_{17}[x]/(x-8) \times \mathbb{Z}_{17}[x]/(x+8).\end{aligned}$$

- The input of the algorithm are two polynomials, and we will perform the projection on both of them. Let's denote a generic polynomial by $a(x)$, and see how to implement it.

- Usually, we use *array* to represent a polynomial. If the input polynomial is $a(x) = a_0 + a_1 x + \cdots + a_7 x^7$, then the initial array representation (or memory layout) is

$$[a_0, a_1, \ldots, a_7].$$

- The first layer projection is

$$\mathbb{Z}_{17}[x]/(x^8-1) \underbrace{\cong}_{(1)} \mathbb{Z}_{17}[x]/(x^4-1) \times \mathbb{Z}_{17}[x]/(x^4+1)$$

- It will project the polynomial $a(x)$ to two polynomials:

$$a_0 + a_4 + (a_1 + a_5)x + (a_2 + a_6)x^2 + (a_3 + a_7)x^3 \in \mathbb{Z}_{17}[x]/(x^4-1)$$

and

$$a_0 - a_4 + (a_1 - a_5)x + (a_2 - a_6)x^2 + (a_3 - a_7)x^3 \in \mathbb{Z}_{17}[x]/(x^4+1)$$

- In our array representation, the projection is simply the addition and subtraction of the corresponding elements:

$$[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7] \mapsto [a_0 + a_4, a_1 + a_5, a_2 + a_6, a_3 + a_7, a_0 - a_4, a_1 - a_5, a_2 - a_6, a_3 - a_7].$$

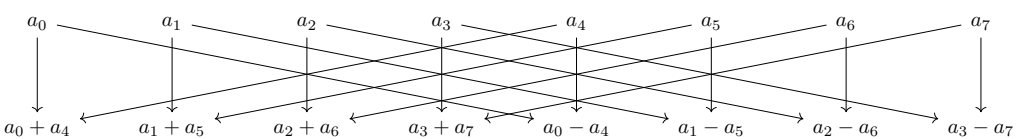
The Implementation of Algorithms

Example of $\mathbb{Z}_{17}[x]/(x^8 - 1)$

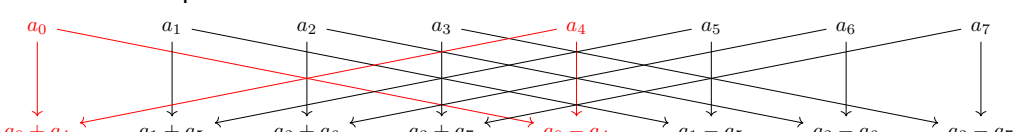
- In our array representation, the projection is simply the addition and subtraction of the corresponding elements:

$$[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7] \mapsto [a_0 + a_4, a_1 + a_5, a_2 + a_6, a_3 + a_7, a_0 - a_4, a_1 - a_5, a_2 - a_6, a_3 - a_7].$$

- Let's make a graph to see the pattern:



- There are in fact four repetitions of the same butterflies:



- After implementing the first layer, we now focus on the second layer:

$$\begin{aligned}&\mathbb{Z}_{17}[x]/(x^4-1)\times\mathbb{Z}_{17}[x]/(x^4+1)\\ &\underbrace{\cong}_{(2)}\mathbb{Z}_{17}[x]/(x^2-1)\times\mathbb{Z}_{17}[x]/(x^2+1)\times\mathbb{Z}_{17}[x]/(x^2-4)\times\mathbb{Z}_{17}[x]/(x^2+4).\end{aligned}$$

- Our array is now the output of the above layer (layer 1), we reset the symbols:

$$[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7]$$

  which denotes $a_0+a_1x+a_2x^2+a_3x^3$ and $a_4+a_5x+a_6x^2+a_7x^3$ in the respective space.
- It will project two polynomials to four polynomials:

$$\begin{aligned}a_0+a_2+(a_1+a_3)x&\in\mathbb{Z}_{17}[x]/(x^2-1),\\ a_0-a_2+(a_1-a_3)x&\in\mathbb{Z}_{17}[x]/(x^2+1),\\ a_4+4a_6+(a_5+4a_7)x&\in\mathbb{Z}_{17}[x]/(x^2-4),\\ a_4-4a_6+(a_5-4a_7)x&\in\mathbb{Z}_{17}[x]/(x^2+4).\end{aligned}$$

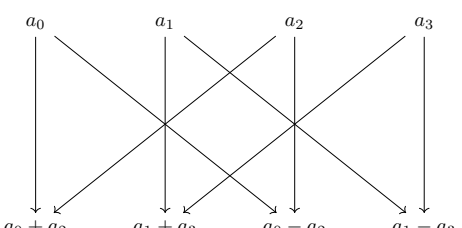
- In our array representation, the projection is to perform:

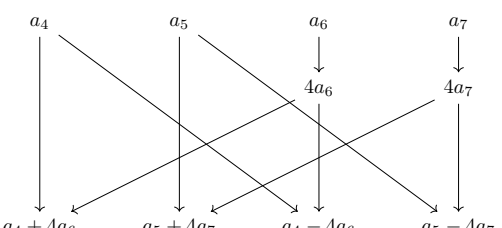
$$[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7]\mapsto[a_0+a_2,a_1+a_3,a_0-a_2,a_1-a_3,a_4+4a_6,a_5+4a_7,a_4-4a_6,a_5-4a_7].$$

- In our array representation, the projection is to perform:

  $$[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7] \mapsto [a_0 + a_2, a_1 + a_3, a_0 - a_2, a_1 - a_3, a_4 + 4a_6, a_5 + 4a_7, a_4 - 4a_6, a_5 - 4a_7].$$

  The pattern is not obvious, lets make a graph:





- After implementing the second layer, we now focus on the last layer:

$$\begin{aligned}&\mathbb{Z}_{17}[x]/(x^2-1)\times\mathbb{Z}_{17}[x]/(x^2+1)\times\mathbb{Z}_{17}[x]/(x^2-4)\times\mathbb{Z}_{17}[x]/(x^2+4)\\ &\underbrace{\cong}_{(3)}\mathbb{Z}_{17}[x]/(x-1)\times\mathbb{Z}_{17}[x]/(x+1)\times\mathbb{Z}_{17}[x]/(x-4)\times\mathbb{Z}_{17}[x]/(x+4)\\ &\qquad\times\mathbb{Z}_{17}[x]/(x-2)\times\mathbb{Z}_{17}[x]/(x+2)\times\mathbb{Z}_{17}[x]/(x-8)\times\mathbb{Z}_{17}[x]/(x+8).\end{aligned}$$

- Our array is now the output of the above layer (layer 2), we reset the symbols:

$$[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7]$$

- It will project four polynomials to eight scalars:

$$\begin{aligned}a_0+a_1&\in\mathbb{Z}_{17}[x]/(x-1), & a_0-a_1&\in\mathbb{Z}_{17}[x]/(x+1),\\ a_2+4a_3&\in\mathbb{Z}_{17}[x]/(x-4), & a_2-4a_3&\in\mathbb{Z}_{17}[x]/(x+4),\\ a_4+2a_5&\in\mathbb{Z}_{17}[x]/(x-2), & a_4-2a_5&\in\mathbb{Z}_{17}[x]/(x+2),\\ a_6+8a_7&\in\mathbb{Z}_{17}[x]/(x-8), & a_6-8a_7&\in\mathbb{Z}_{17}[x]/(x+8).\end{aligned}$$

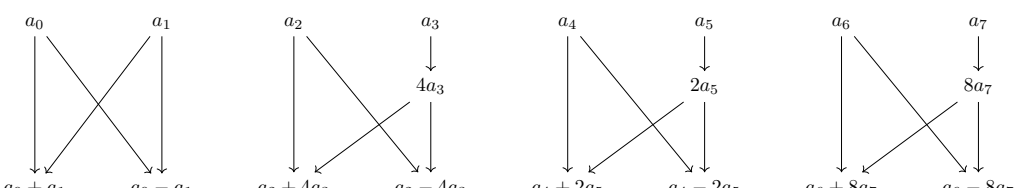
- In our array representation, the projection is to perform:

$$[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7]\mapsto[a_0+a_1,a_0-a_1,a_2+4a_3,a_2-4a_3,a_4+2a_5,a_4-2a_5,a_6+8a_7,a_6-8a_7].$$

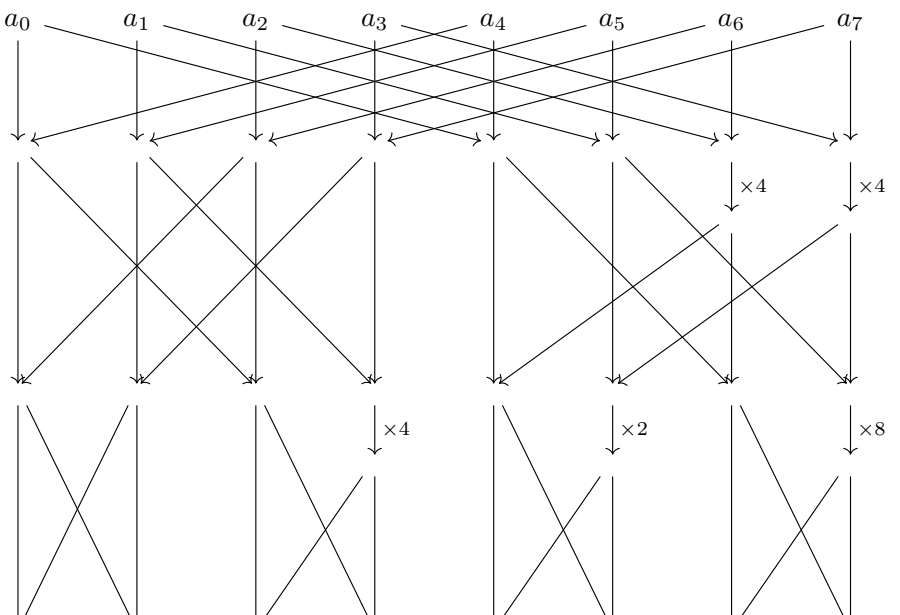
- In our array representation, the projection is to perform:

  $[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7] \mapsto [a_0+a_1, a_0-a_1, a_2+4a_3, a_2-4a_3, a_4+2a_5, a_4-2a_5, a_6+8a_7, a_6-8a_7]$.

  The pattern is not obvious, lets make a graph:



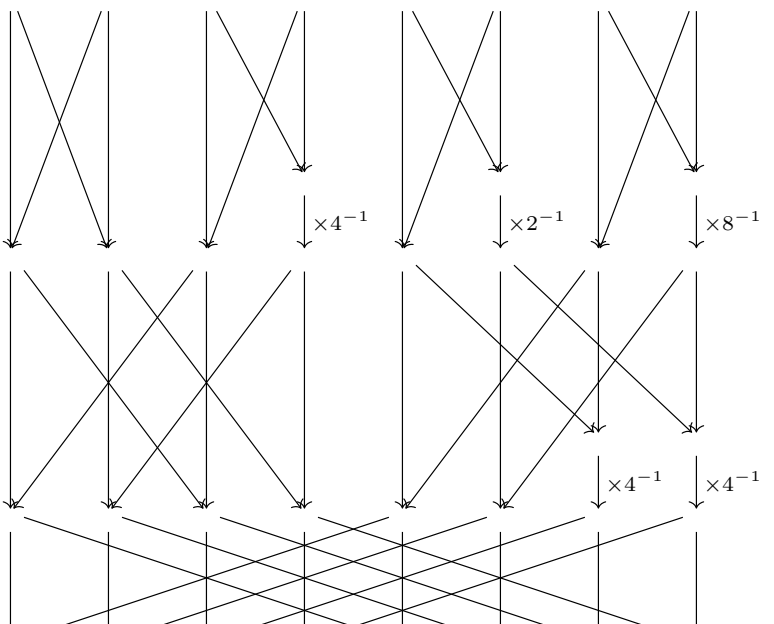
In total, the projection can be represented by the following graph:



The Implementation of Algorithms

Example of $\mathbb{Z}_{17}[x]/(x^8 - 1)$

- After the projection, the point-wise multiplication is simple.
- The inverse NTT is the reverse of the above circuits:



- During the NTT, the multiplication operations are in fact "modular" multiplication:

$$a \times b \bmod p.$$

- A traditional way is to use Division Algorithm, that is, to find q and r such that

$$ab = q \cdot p + r$$

- Such operation is most likely compiled into the instruction UDIV or SDIV, and they have the following parameters on Raspberry Pi 5:

Instruction	Latency	Throughput
$\mathrm{UDIV}/\mathrm{SDIV}$(W-form)	5 - 12	1/12 - 1/5
$\mathrm{UDIV}/\mathrm{SDIV}$(X-form)	5 - 20	1/20 - 1/5

Table. Latency and throughput of division instructions on Raspberry Pi 5

- The variable-time algorithm is not acceptable for cryptographic implementation.
- Hence scientists invented several method to compute the remainder, such as Barrett Reduction, Montgomery Reduction, Plantard Reduction...

- The idea of Barrett reduction is simple. It tries to approximate the quotient q and then we can compute r.
- Note that if we want the signed representation of $ab \bmod p$, i.e.,

$$-\frac{p}{2} \leq ab \bmod p < \frac{p}{2}.$$

  It is equivalent to compute r in the following equation

$$r = ab - qp = ab - \left\lfloor \frac{ab}{p} \right\rceil q$$

- We can approximate the above number by

$$r = ab - \left\lfloor \frac{ab}{p} \right\rceil q = ab - \left\lfloor \frac{ab\frac{R}{p}}{R} \right\rceil q$$
$$= ab - \left\lfloor \frac{ab\left\lfloor \frac{R}{p} \right\rceil}{R} \right\rceil q$$

  where R is taken to be some constant related to computer arithmetic, say, $R = 2^{32}$, $R = 2^{64}$.
- Note that $\left\lfloor \frac{R}{p} \right\rceil$ can be precomputed. And division by R is a shifting operation in computer.

- We have investigated the decomposition, for $n = 2^k$

$$\mathbb{Z}_p[x]/\langle x^n - 1\rangle \cong \prod_{i=0}^{n-1} \mathbb{Z}_p[x]/\langle x - \omega_n^{\mathrm{brv}(i)}\rangle$$

- However, this decomposition requires the primitive nth root of unity, that is, it requires the condition that $p - 1$ is divisible by n.
- When n is not a power of 2, or the primitive root does not exists, we can that these rings are NTT-unfriendly.
- We can take the ring

$$\mathbb{Z}_{13}[x]/\langle x^8 - 1\rangle.$$

  for example. Since $p - 1 = 12$ is not divisible by 8 (and divisible by 4), so ω_8 does not exist and ω_4 exists.
- If we want to perform the NTT decomposition, then we try

$$\mathbb{Z}_{13}[x]/\langle x^8-1\rangle \cong \prod_{i=0}^{1} \mathbb{Z}_{13}[x]/\langle x^4-\omega_2^{\mathrm{brv}_1(i)}\rangle \cong \prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2-\omega_4^{\mathrm{brv}_2(i)}\rangle \cong \prod_{i=0}^{7} \mathbb{Z}_{13}[x]/\langle x-\underbrace{\omega_8}_{\text{does not exists}}^{\mathrm{brv}_3(i)}\rangle$$

- If we want to perform the NTT decomposition, then we try

$$\mathbb{Z}_{13}[x]/\langle x^8-1\rangle \cong \prod_{i=0}^{1} \mathbb{Z}_{13}[x]/\langle x^4-\omega_2^{\mathrm{brv}_1(i)}\rangle \cong \prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2-\omega_4^{\mathrm{brv}_2(i)}\rangle \cong \prod_{i=0}^{7} \mathbb{Z}_{13}[x]/\langle x-\underbrace{\omega_8}_{\text{does not exists}}^{\mathrm{brv}_3(i)}\rangle$$

- This leads us to a technique called incomplete NTT, that is, we perform decomposition until

$$\mathbb{Z}_{13}[x]/\langle x^8-1\rangle \cong \prod_{i=0}^{1} \mathbb{Z}_{13}[x]/\langle x^4-\omega_2^{\mathrm{brv}_1(i)}\rangle \cong \prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2-\omega_4^{\mathrm{brv}_2(i)}\rangle$$

  and then do the multiplication parallelly in the coordinate ring:

$$\prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2-\omega_4^{\mathrm{brv}_2(i)}\rangle$$

- If we denote the incomplete NTT transform by

$$\mathrm{NTT}_{8\to 2} : \mathbb{Z}_{13}[x]/\langle x^8 - 1\rangle \to \prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2 - \omega_4^{\mathrm{brv}_2(i)}\rangle$$

- and the inverse NTT by

$$\mathrm{INTT}_{8\to 2} : \prod_{i=0}^{3} \mathbb{Z}_{13}[x]/\langle x^2 - \omega_4^{\mathrm{brv}_2(i)}\rangle \to \mathbb{Z}_{13}[x]/\langle x^8 - 1\rangle.$$

- Our fast multiplication is then:

$$\mathrm{INTT}_{8\to 2}(\mathrm{NTT}_{8\to 2}(f) \odot \mathrm{NTT}_{8\to 2}(g)).$$

- Lets take a real-world example of another NTT-unfriendly ring:

$$\mathbb{Z}_{2048}/\langle x^{677} - 1\rangle$$

  This is the ring occurred in NTRU2048677.
- The exponent of x is not a power of two, and the coefficient modulo, 2048 is not a prime number. Then how to deal with multiplications in such ring?
- An solution is to enlarge the ring so that the original product is not destroyed, namely

$$\pi : \mathbb{Z}_{2048}/\langle x^{677} - 1\rangle \to \mathbb{Z}_p/\langle x^{2048} - 1\rangle.$$

  where p is a NTT-friendly prime number such that

$$p \geq 2048 \times 2048 \times 677.$$

- In the real-world implementation, one uses the projection

$$\pi : \mathbb{Z}_{2048}/\langle x^{677} - 1\rangle \to \mathbb{Z}_p/\langle x^{1536} - 1\rangle.$$

  where $p \geq 2048 \times 2048 \times 677$ and $p - 1$ is divisible by 1536. Since we have another technique called "Good's Trick".

- In the real-world implementation, one uses the projection

$$\pi : \mathbb{Z}_{2048}/\langle x^{677} - 1\rangle \to \mathbb{Z}_p/\langle x^{1536} - 1\rangle.$$

  where $p \geq 2048 \times 2048 \times 677$ and $p - 1$ is divisible by 1536.
- So, how to do multiplication in the ring $\mathbb{Z}_p/\langle x^{1536} - 1\rangle$?
- Note that $1536 = 3 \cdot 512 = 3 \cdot 2^9$.
- Good's trick is essentially an isomorphism:

$$\mathbb{Z}_p/\langle x^{1536} - 1\rangle \cong \mathbb{Z}_p/\langle y^3 - 1, z^{512} - 1, x - yz\rangle$$
$$x \mapsto yz$$

- The ring

$$\mathbb{Z}_p/\langle y^3 - 1, z^{512} - 1, x - yz\rangle$$

  can then be seen as two directions: y-direction and z-direction.

- The ring
$$\mathbb{Z}_p/\langle y^3 - 1, z^{512} - 1, x - yz\rangle$$
can then be seen as two directions: y-direction and z-direction.
- By the existence of ω_{1536}, the existence of ω_3 and ω_{512} follows immediately.
- We can then first do 3-NTT:
$$\mathbb{Z}_p/\langle y^3 - 1, z^{512} - 1, x - yz\rangle \to \prod_{i=0}^{2} \mathbb{Z}_p/\langle y - \omega_3^i, z^{512} - 1, x - yz\rangle$$
- and then do 512-NTT:
$$\prod_{i=0}^{2} \mathbb{Z}_p/\langle y - \omega_3^i, z^{512} - 1, x - yz\rangle \to \prod_{i=0}^{2}\prod_{j=0}^{511} \mathbb{Z}_p/\langle y - \omega_3^i, z - \omega_{512}^{\mathrm{brv}(j)}, x - yz\rangle.$$
- Here, each coordinate ring consists of remainders of degree-one polynomials, that is, consists of (zero-degree) constants.

- NTT is a very good technique to do polynomial multiplication.
- Integers can be expressed in polynomials:

$$3124 = 4 + 2 \cdot 10 + 1 \cdot 10^2 + 3 \cdot 10^3.$$

  Hence, we can invent fast multiplication algorithm for big integers.
- A paper that doing this on microprocessors: https://eprint.iacr.org/2022/439.
- My summer intern is currently working on small CPU (of raspberry pi 5, Cortex-A76) to find the crossover point of NTT-based multiplication algorithm.
- The idea is, given two $8448 = 22 \cdot 384$ bits big integer.
- Chunk the big number into the polynomial form

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{383} x^{383}.$$

- View them as polynomials in the ring

$$\mathbb{Z}_p[x]/\langle x^{768} - 1 \rangle,$$

  where $p \geq 2^{22} \cdot 2^{22} \cdot 384$ is NTT-friendly. Then proceed by using Good's Trick and NTT.

- As mentioned, the ring
$$\mathbb{Z}_p[x]/\langle x^{768} - 1\rangle,$$
has coefficient $p \geq 2^{22} \cdot 2^{22} \cdot 384 \geq 2^3 2$, so we expect that intermediate data should be opedated by 64-bits register.
- For some old processors (or old CPU), the register has size 32-bits, not large enough for single-word operation.
- Our (me and my interns) scheme is then: Let's not do the $\bmod p$ NTT, we do RNS + NTT.
- Chunking the big number into the polynomial form
$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{383} x^{383}.$$
and view them as polynomials in the ring
$$\mathbb{Z}_{q_1 q_2}[x]/\langle x^{768} - 1\rangle,$$
where $q_1 q_2 \geq 2^{22} \cdot 2^{22} \cdot 384$ and q_1 and q_2 are NTT-friendly.

- Chunking the big number into the polynomial form

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{383} x^{383}.$$

  and view them as polynomials in the ring

$$\mathbb{Z}_{q_1 q_2}[x]/\langle x^{768} - 1\rangle,$$

  where $q_1 q_2 \geq 2^{22} \cdot 2^{22} \cdot 384$ and q_1 and q_2 are NTT-friendly.
- Then we first do RNS-decomposition (the basic integer CRT):

$$\mathbb{Z}_{q_1 q_2}[x]/\langle x^{768} - 1\rangle \cong \mathbb{Z}_{q_1}[x]/\langle x^{768} - 1\rangle \times \mathbb{Z}_{q_2}[x]/\langle x^{768} - 1\rangle$$

- then we perform NTT + Good's Trick in individual rings.
- Here, $q_1 q_2 \geq 2^{22} \cdot 2^{22} \cdot 384 \approx 2^{53}$. So we can select $q_1, q_2 \approx 2^{27}$. This fits into 32 bits-register.
- Importantly, the Neon vector instruction extension of ARM profile-A CPU provides 128-bits vector registers. However, the instruction set does not support 64-bits NTT. So, using 32-bits NTT is very good choice for the today's modern processors.

Any Questions?