Brief Introduction to Number Theoretic Transform

From the Perspective of Ring Theory

Cesare Huang Cheng Wei

Academia Sinica

January 8, 2025

Table of Contents

Motivation and Goals

- **Core Problem**: Fast polynomial multiplication in $\mathbb{Z}_p[x]/(x^n - 1)$, where n is a power of 2.
  The problems we deal with include more general quotient rings, but in this slide, we firstly focus on such simple ring for the purpose of illustration.

Motivation and Goals

- **Core Problem**: Fast polynomial multiplication in $\mathbb{Z}_p[x]/(x^n - 1)$, where n is a power of 2. The problems we deal with include more general quotient rings, but in this slide, we firstly focus on such simple ring for the purpose of illustration.
- **Background**:
  - In many applications in cryptography, we have to multiply the elements in the ring of the kind $\mathbb{Z}_p[x]/(x^n - 1)$, which is a very time-consuming operation.
  - 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.

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

- Suppose we want to perform the multiplication $31 * 27 = 102$ in

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:
$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$
- Suppose we want to perform the multiplication $31 * 27 = 102$ in
- Suppose we want to perform the multiplication $31 * 27 = 102$ in the ring $\mathbb{Z}/105\mathbb{Z}$

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

- Suppose we want to perform the multiplication $31 * 27 = 102$ in
- Suppose we want to perform the multiplication $31 * 27 = 102$ in the ring $\mathbb{Z}/105\mathbb{Z}$
- We first project the operands (31, 27) to the three "coordinate"-rings:

$$31 \mapsto (1, 1, 3) \quad 27 \mapsto (0, 2, 6)$$

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:
$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$
- Suppose we want to perform the multiplication $31 * 27 = 102$ in
- Suppose we want to perform the multiplication $31 * 27 = 102$ in the ring $\mathbb{Z}/105\mathbb{Z}$
- We first project the operands (31, 27) to the three "coordinate"-rings:
$$31 \mapsto (1, 1, 3) \quad 27 \mapsto (0, 2, 6)$$
- Multiply the corresponding "coordinates" to get
$$(1, 1, 3) \cdot (0, 2, 6) = (0, 2, 4)$$

Residual Number System and Theory of Quotient Rings

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

- Suppose we want to perform the multiplication $31 * 27 = 102$ in
- Suppose we want to perform the multiplication $31 * 27 = 102$ in the ring $\mathbb{Z}/105\mathbb{Z}$
- We first project the operands (31, 27) to the three "coordinate"-rings:

$$31 \mapsto (1, 1, 3) \quad 27 \mapsto (0, 2, 6)$$

- Multiply the corresponding "coordinates" to get

$$(1, 1, 3) \cdot (0, 2, 6) = (0, 2, 4)$$

- Finally, we recombine the result to get the final answer: The process involves the so-called Chinese Remainder Theorem (CRT), that is, to find the solution to the system

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

  The solution is $x = 102$, which is the answer to the original multiplication.

Remarks on CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.

Remarks on CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.
- Another advantage of the RNS CRT approach is that, after decomposing the ring into several "coordinate"-rings, we can perform the multiplication in the "coordinate"-rings in parallel.

Remarks on CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.
- Another advantage of the RNS CRT approach is that, after decomposing the ring into several "coordinate"-rings, we can perform the multiplication in the "coordinate"-rings in parallel.
- If the whole process involves many times of multiplication, we can leave the big integers in the RNS coordinate representations, and after performing all required multiplications, recombine the results via the CRT once.

Remarks on CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.
- Another advantage of the RNS CRT approach is that, after decomposing the ring into several "coordinate"-rings, we can perform the multiplication in the "coordinate"-rings in parallel.
- If the whole process involves many times of multiplication, we can leave the big integers in the RNS coordinate representations, and after performing all required multiplications, recombine the results via the CRT once.
- Such technique is applicable in real-world, for example, to compute a discrete logarithm in the ring $\mathbb{Z}/n\mathbb{Z}$.

REMARKS ON CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.
- Another advantage of the RNS CRT approach is that, after decomposing the ring into several "coordinate"-rings, we can perform the multiplication in the "coordinate"-rings in parallel.
- If the whole process involves many times of multiplication, we can leave the big integers in the RNS coordinate representations, and after performing all required multiplications, recombine the results via the CRT once.
- Such technique is applicable in real-world, for example, to compute a discrete logarithm in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For more discussion on the RNS, see the paper: Modular exponentiation via the explicit Chinese remainder theorem by DJB.

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- These are examples of quotient rings.

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.
- We can extend the idea to polynomial operations:
  - the set $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients. Operations are performed as usual.
  - the set $\mathbb{Z}[x]/(x^n - 1)$ thus meanes that all operations are performed modulo $x^n - 1$.
  - For example, in the ring $\mathbb{Z}[x]/(x^2 - 1)$,

$$(x+1) \cdot (x+2) = x^2 + 3x + 2 \equiv 3x + 4 \pmod{x^2 - 1}$$

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.
- We can extend the idea to polynomial operations:
    - the set $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients. Operations are performed as usual.
    - the set $\mathbb{Z}[x]/(x^n - 1)$ thus meanes that all operations are performed modulo $x^n - 1$.
    - For example, in the ring $\mathbb{Z}[x]/(x^2 - 1)$,

$$(x + 1) \cdot (x + 2) = x^2 + 3x + 2 \equiv 3x + 4 \pmod{x^2 - 1}$$

- Generally, $\mathbb{Z}[x]/(f(x))$: Polynomial congruences where $f(x) \equiv 0$.

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n - 1), \quad \mathbb{Z}_p[x]/(x^n - 1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.
- We can extend the idea to polynomial operations:
  - the set $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients. Operations are performed as usual.
  - the set $\mathbb{Z}[x]/(x^n - 1)$ thus meanes that all operations are performed modulo $x^n - 1$.
  - For example, in the ring $\mathbb{Z}[x]/(x^2 - 1)$,

$$(x+1) \cdot (x+2) = x^2 + 3x + 2 \equiv 3x + 4 \pmod{x^2 - 1}$$

- Generally, $\mathbb{Z}[x]/(f(x))$: Polynomial congruences where $f(x) \equiv 0$.
- We also write the quotient integer rings $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}_n$

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n-1), \quad \mathbb{Z}_p[x]/(x^n-1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.
- We can extend the idea to polynomial operations:
  - the set $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients. Operations are performed as usual.
  - the set $\mathbb{Z}[x]/(x^n-1)$ thus meanes that all operations are performed modulo x^n-1.
  - For example, in the ring $\mathbb{Z}[x]/(x^2-1)$,

$$(x+1)\cdot(x+2) = x^2+3x+2 \equiv 3x+4 \pmod{x^2-1}$$

- Generally, $\mathbb{Z}[x]/(f(x))$: Polynomial congruences where $f(x) \equiv 0$.
- We also write the quotient integer rings $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}_n$
- Hence, the meaning of $\mathbb{Z}_p[x]/(x^n-1)$ is that the coefficients are reduced modulo p, and the polynomial is reduced modulo x^n-1.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2 - 1)$.
- Easy to see that $x^2 - 1 = (x - 1)(x + 1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 - 1) \cong \mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x + 1)$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2 - 1)$.
- Easy to see that $x^2 - 1 = (x - 1)(x + 1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 - 1) \cong \mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x + 1)$$

- Suppose we want to multiply $(3 + 1x) \cdot (2 + 7x) = 13 + 23x$ in the ring $\mathbb{Z}[x]/(x^2 - 1)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$.
- Easy to see that $x^2-1=(x-1)(x+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2-1) \cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1)$$

- Suppose we want to multiply $(3+1x)\cdot(2+7x)=13+23x$ in the ring $\mathbb{Z}[x]/(x^2-1)$.
- We first project the operands to the two "coordinate"-rings:

$$3+1x \mapsto (4,2), \quad 2+7x \mapsto (9,-5).$$

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2 - 1)$.
- Easy to see that $x^2 - 1 = (x - 1)(x + 1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 - 1) \cong \mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x + 1)$$

- Suppose we want to multiply $(3 + 1x) \cdot (2 + 7x) = 13 + 23x$ in the ring $\mathbb{Z}[x]/(x^2 - 1)$.
- We first project the operands to the two "coordinate"-rings:

$$3 + 1x \mapsto (4, 2), \quad 2 + 7x \mapsto (9, -5).$$

- Multiply the corresponding "coordinates" to get

$$(4, 2) \cdot (9, -5) = (36, -10).$$

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$.
- Easy to see that $x^2-1=(x-1)(x+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2-1) \cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1)$$

- Suppose we want to multiply $(3+1x)\cdot(2+7x)=13+23x$ in the ring $\mathbb{Z}[x]/(x^2-1)$.
- We first project the operands to the two "coordinate"-rings:

$$3+1x \mapsto (4,2), \quad 2+7x \mapsto (9,-5).$$

- Multiply the corresponding "coordinates" to get

$$(4,2)\cdot(9,-5)=(36,-10).$$

- Finally, we recombine the result to the final asnwer: that is, to find the solution to the system

$$f(x)\equiv 36 \pmod{x-1}, \quad f(x)\equiv -10 \pmod{x+1}.$$

  The solution is $f(x)=13+23x$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$.
- Easy to see that $x^2-1=(x-1)(x+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2-1) \cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1)$$

- Suppose we want to multiply $(3+1x)\cdot(2+7x)=13+23x$ in the ring $\mathbb{Z}[x]/(x^2-1)$.
- We first project the operands to the two "coordinate"-rings:

$$3+1x \mapsto (4,2), \quad 2+7x \mapsto (9,-5).$$

- Multiply the corresponding "coordinates" to get

$$(4,2)\cdot(9,-5)=(36,-10).$$

- Finally, we recombine the result to the final asnwer: that is, to find the solution to the system

$$f(x) \equiv 36 \pmod{x-1}, \quad f(x) \equiv -10 \pmod{x+1}.$$

  The solution is $f(x)=13+23x$.
- It seems that the recombination is very hard to solve. But, no, see the next slide.

DECOMPOSITION OF $\mathbb{Z}[x]/(x^2 - 1)$

- A saying goes that "How to go forward then how to go back" (Cesare Huang, 2024)

- A saying goes that "How to go forward then how to go back" (Cesare Huang, 2024)
- Let $a+bx$ be one of the operand in the ring $\mathbb{Z}[x]/(x^2-1)$, then we have the following projection:

$$\begin{aligned}\mathbb{Z}[x]/(x^2-1) &\cong \mathbb{Z}[x]/(x-1)\times\mathbb{Z}[x]/(x+1)\\ a+bx &\mapsto (a+b, a-b)\\ \frac{A+B}{2}+\frac{A-B}{2}x &\mapsto (A, B).\end{aligned}$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- A saying goes that "How to go forward then how to go back" (Cesare Huang, 2024)
- Let $a+bx$ be one of the operand in the ring $\mathbb{Z}[x]/(x^2-1)$, then we have the following projection:

$$\mathbb{Z}[x]/(x^2-1) \cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1)$$
$$a+bx \mapsto (a+b, a-b)$$
$$\frac{A+B}{2} + \frac{A-B}{2}x \mapsto (A, B).$$

- Hence, the recombination is easy, once receive the A, B from the component-wise multiplication, the solution in $\mathbb{Z}[x]/(x^2-1)$ is simply

$$\frac{A+B}{2} + \frac{A-B}{2}x$$

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- A saying goes that "How to go forward then how to go back" (Cesare Huang, 2024)
- Let $a+bx$ be one of the operand in the ring $\mathbb{Z}[x]/(x^2-1)$, then we have the following projection:

$$\begin{aligned} \mathbb{Z}[x]/(x^2-1) &\cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1) \\ a+bx &\mapsto (a+b, a-b) \\ \frac{A+B}{2} + \frac{A-B}{2}x &\mapsto (A, B). \end{aligned}$$

- Hence, the recombination is easy, once receive the A, B from the component-wise multiplication, the solution in $\mathbb{Z}[x]/(x^2-1)$ is simply

$$\frac{A+B}{2} + \frac{A-B}{2}x$$

- Check:

$$f(x) \equiv 36 \pmod{x-1}, \quad f(x) \equiv -10 \pmod{x+1}.$$

The solution is $f(x) = 13 + 23x$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2 - 1)$ just invented.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2 - 1)$ just invented.
- Let $a + bx$ and $c + dx$ be the two operands, out algorithm goes as follows:

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$ just invented.
- Let $a+bx$ and $c+dx$ be the two operands, out algorithm goes as follows:
  1. Project the ring elements into two "coordinate"-rings:

$$a+bx \mapsto (a+b, a-b), \quad c+dx \mapsto (c+d, c-d).$$

     It takes four add/sub operations in this step.

DECOMPOSITION OF $\mathbb{Z}[x]/(x^2-1)$

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$ just invented.
- Let $a+bx$ and $c+dx$ be the two operands, out algorithm goes as follows:
  1. Project the ring elements into two "coordinate"-rings:

     $$a+bx \mapsto (a+b, a-b), \quad c+dx \mapsto (c+d, c-d).$$

     It takes four add/sub operations in this step.
  2. Multiply the "coordinates" to get

     $$(a+b, a-b)\cdot(c+d, c-d) = ((a+b)(c+d), (a-b)(c-d)) := (A, B).$$

     It takes two multiplications in this step.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$ just invented.
- Let $a+bx$ and $c+dx$ be the two operands, out algorithm goes as follows:
  1. Project the ring elements into two "coordinate"-rings:

     $$a+bx \mapsto (a+b, a-b), \quad c+dx \mapsto (c+d, c-d).$$

     It takes four add/sub operations in this step.
  2. Multiply the "coordinates" to get

     $$(a+b, a-b)\cdot(c+d, c-d) = ((a+b)(c+d), (a-b)(c-d)) := (A, B).$$

     It takes two multiplications in this step.
  3. Recombine the result to get the final answer:

     $$\frac{A+B}{2} + \frac{A-B}{2}x.$$

     It takes two add/sub operations and two divided by 2 operations in this step. Note that divided by 2 is a shift operation, which is very fast.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- The algorithm we just invented takes:
  - 6 add/sub operations
  - 2 multiplications
  - 2 shift operation

- The algorithm we just invented takes:
  - 6 add/sub operations
  - 2 multiplications
  - 2 shift operation
- The naive algorithm (schoolbook multiplication) takes:
  - 4 multiplications
  - 2 additions

Decomposition of $\mathbb{Z}[x]/(x^2 - 1)$

- The algorithm we just invented takes:
  - 6 add/sub operations
  - 2 multiplications
  - 2 shift operation
- The naive algorithm (schoolbook multiplication) takes:
  - 4 multiplications
  - 2 additions
- The analysis we just made are based on number of mathematic operations. This is illustrative, but not the whole story. In practice, please benchmark the performance by the actual cycle-count.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2 - 1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4 - 1)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2 - 1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4 - 1)$.
- Easy to see that $x^4 - 1 = (x^2 - 1)(x^2 + 1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^4 - 1) \cong \mathbb{Z}[x]/(x^2 - 1) \times \mathbb{Z}[x]/(x^2 + 1)$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2-1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4-1)$.
- Easy to see that $x^4-1=(x^2-1)(x^2+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^4-1) \cong \mathbb{Z}[x]/(x^2-1) \times \mathbb{Z}[x]/(x^2+1)$$

- Until here, we can already develop a fast multiplication algorithm by such decomposition. But it the first coordinate-ring can be further decomposed, and it seems that decomposing then one more time can bring more speedup.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2-1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4-1)$.
- Easy to see that $x^4-1=(x^2-1)(x^2+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^4-1) \cong \mathbb{Z}[x]/(x^2-1) \times \mathbb{Z}[x]/(x^2+1)$$

- Until here, we can already develop a fast multiplication algorithm by such decomposition. But it the first coordinate-ring can be further decomposed, and it seems that decomposing then one more time can bring more speedup.
- The first ring can be decomposed as we just did. However, for the second one,

$$\mathbb{Z}[x]/(x^2+1)$$

there is no obvious factorization of x^2+1.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2-1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4-1)$.
- Easy to see that $x^4-1=(x^2-1)(x^2+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^4-1) \cong \mathbb{Z}[x]/(x^2-1) \times \mathbb{Z}[x]/(x^2+1)$$

- Until here, we can already develop a fast multiplication algorithm by such decomposition. But it the first coordinate-ring can be further decomposed, and it seems that decomposing then one more time can bring more speedup.
- The first ring can be decomposed as we just did. However, for the second one,

$$\mathbb{Z}[x]/(x^2+1)$$

  there is no obvious factorization of x^2+1.
- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[x]/(x-i) \times \mathbb{Z}[x]/(x+i)$$

  The same trick as above can be applied in the cost of introducing complex numbers. Such trick is called the Discrete Fourier Transform (DFT).

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- After experience the fast multiplication brought by the decomposition of $\mathbb{Z}[x]/(x^2-1)$, we now try to decompose the ring $\mathbb{Z}[x]/(x^4-1)$.
- Easy to see that $x^4-1=(x^2-1)(x^2+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^4-1) \cong \mathbb{Z}[x]/(x^2-1) \times \mathbb{Z}[x]/(x^2+1)$$

- Until here, we can already develop a fast multiplication algorithm by such decomposition. But it the first coordinate-ring can be further decomposed, and it seems that decomposing then one more time can bring more speedup.
- The first ring can be decomposed as we just did. However, for the second one,

$$\mathbb{Z}[x]/(x^2+1)$$

  there is no obvious factorization of x^2+1.
- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[x]/(x-i) \times \mathbb{Z}[x]/(x+i)$$

  The same trick as above can be applied in the cost of introducing complex numbers. Such trick is called the Discrete Fourier Transform (DFT).
- The concept of the Number Theoretic Transform (NTT) is similar to DFT, but required more well-strucutred ring.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[x]/(x - i) \times \mathbb{Z}[x]/(x + i)$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[x]/(x - i) \times \mathbb{Z}[x]/(x + i)$$

- The concept of the Number Theoretic Transform (NTT) is similar to DFT, but required more well-strucutred ring.

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[x]/(x-i) \times \mathbb{Z}[x]/(x+i)$$

- The concept of the Number Theoretic Transform (NTT) is similar to DFT, but required more well-strucutred ring.
- Recall that our core problem is to deal with the multiplication of the ring $\mathbb{Z}_p[x]/(x^n - 1)$. Here, we in particular consider the ring $\mathbb{Z}_p[x]/(x^4 - 1)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[x]/(x - i) \times \mathbb{Z}[x]/(x + i)$$

- The concept of the Number Theoretic Transform (NTT) is similar to DFT, but required more well-strucutred ring.
- Recall that our core problem is to deal with the multiplication of the ring $\mathbb{Z}_p[x]/(x^n - 1)$. Here, we in particular consider the ring $\mathbb{Z}_p[x]/(x^4 - 1)$.
- The important observation is that, there may be some element in $\mathbb{Z}_p$, denoted as ω, such that $\omega^2 = -1$, which, serves as the imaginary unit as in the DFT.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- One way is to employ the complex number field, and we have the following decomposition:

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[x]/(x - i) \times \mathbb{Z}[x]/(x + i)$$

- The concept of the Number Theoretic Transform (NTT) is similar to DFT, but required more well-strucutred ring.
- Recall that our core problem is to deal with the multiplication of the ring $\mathbb{Z}_p[x]/(x^n - 1)$. Here, we in particular consider the ring $\mathbb{Z}_p[x]/(x^4 - 1)$.
- The important observation is that, there may be some element in $\mathbb{Z}_p$, denoted as ω, such that $\omega^2 = -1$, which, serves as the imaginary unit as in the DFT.
- Take, for example, the ring $\mathbb{Z}_{17}[x]/(x^4 - 1)$ for example. In this ring,

$$4^2 = 16 \equiv -1 \pmod{17}.$$

We thus have the following decomposition:

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

- Take, for example, the ring $\mathbb{Z}_{17}[x]/(x^4 - 1)$ for example. In this ring,

  $$4^2 = 16 \equiv -1 \pmod{17}.$$

  We thus have the following decomposition:

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

- Take, for example, the ring $\mathbb{Z}_{17}[x]/(x^4-1)$ for example. In this ring,

$$4^2 = 16 \equiv -1 \pmod{17}.$$

  We thus have the following decomposition:

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

- Hence we have the full decomposition:

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

- Take, for example, the ring $\mathbb{Z}_{17}[x]/(x^4-1)$ for example. In this ring,

$$4^2 = 16 \equiv -1 \pmod{17}.$$

  We thus have the following decomposition:

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

- Hence we have the full decomposition:

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

- We can analogously develop a fast multiplication algorithm for the ring $\mathbb{Z}_{17}[x]/(x^4-1)$: projection to coordinate-ring, coordinate-wise multiplication, recombination.

- The projection goes like:

$$
\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1) \\
&\cong \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4). \\
3+1x+4x^2+2x^3 &\mapsto (7+3x, -1-1x) \cong (7+3x, 16+16x), \\
&\mapsto (10, -4, -5, 3) \cong (10, 13, 12, 3) \\
2+7x+1x^2+2x^3 &\mapsto (3+9x, 1+5x) \\
&\mapsto (12, -6, 21, -19) \cong (12, 11, 4, 15).
\end{aligned}
$$

- The projection goes like:

$$\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1)\times\mathbb{Z}_{17}[x]/(x^2+1)\\
&\cong \mathbb{Z}_{17}[x]/(x-1)\times\mathbb{Z}_{17}[x]/(x+1)\times\mathbb{Z}_{17}[x]/(x-4)\times\mathbb{Z}_{17}[x]/(x+4).\\
3+1x+4x^2+2x^3 &\mapsto (7+3x,-1-1x)\cong(7+3x,16+16x),\\
&\mapsto (10,-4,-5,3)\cong(10,13,12,3)\\
2+7x+1x^2+2x^3 &\mapsto (3+9x,1+5x)\\
&\mapsto (12,-6,21,-19)\cong(12,11,4,15).
\end{aligned}$$

- The projection goes like:

$$\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1) \\
&\cong \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4). \\
3+1x+4x^2+2x^3 &\mapsto (7+3x, -1-1x) \cong (7+3x, 16+16x), \\
&\mapsto (10, -4, -5, 3) \cong (10, 13, 12, 3) \\
2+7x+1x^2+2x^3 &\mapsto (3+9x, 1+5x) \\
&\mapsto (12, -6, 21, -19) \cong (12, 11, 4, 15).
\end{aligned}$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- Suppose we want to multiply two polynomials in the ring $\mathbb{Z}_{17}[x]/(x^4-1)$:

$$3 + 1x + 4x^2 + 2x^3, \quad 2 + 7x + 1x^2 + 2x^3.$$

- The projection goes like:

$$\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1) \\
&\cong \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4). \\
3 + 1x + 4x^2 + 2x^3 &\mapsto (7+3x, -1-1x) \cong (7+3x, 16+16x), \\
&\mapsto (10, -4, -5, 3) \cong (10, 13, 12, 3) \\
2 + 7x + 1x^2 + 2x^3 &\mapsto (3+9x, 1+5x) \\
&\mapsto (12, -6, 21, -19) \cong (12, 11, 4, 15).
\end{aligned}$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- Suppose we want to multiply two polynomials in the ring $\mathbb{Z}_{17}[x]/(x^4-1)$:

$$3+1x+4x^2+2x^3, \quad 2+7x+1x^2+2x^3.$$

- The projection goes like:

$$\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1)\times\mathbb{Z}_{17}[x]/(x^2+1)\\
&\cong \mathbb{Z}_{17}[x]/(x-1)\times\mathbb{Z}_{17}[x]/(x+1)\times\mathbb{Z}_{17}[x]/(x-4)\times\mathbb{Z}_{17}[x]/(x+4).\\
3+1x+4x^2+2x^3 &\mapsto (7+3x,-1-1x)\cong(7+3x,16+16x),\\
&\mapsto (10,-4,-5,3)\cong(10,13,12,3)\\
2+7x+1x^2+2x^3 &\mapsto (3+9x,1+5x)\\
&\mapsto (12,-6,21,-19)\cong(12,11,4,15).
\end{aligned}$$

- Coordinate-wise multiplication is straightforward:

$$(10,13,12,3)\cdot(12,11,4,15)=(120,143,48,45)\cong(1,7,14,11).$$

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- Suppose we want to multiply two polynomials in the ring $\mathbb{Z}_{17}[x]/(x^4-1)$:

$$3+1x+4x^2+2x^3, \quad 2+7x+1x^2+2x^3.$$

- The projection goes like:

$$\begin{aligned}
\mathbb{Z}_{17}[x]/(x^4-1) &\cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1) \\
&\cong \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4). \\
3+1x+4x^2+2x^3 &\mapsto (7+3x, -1-1x) \cong (7+3x, 16+16x), \\
&\mapsto (10, -4, -5, 3) \cong (10, 13, 12, 3) \\
2+7x+1x^2+2x^3 &\mapsto (3+9x, 1+5x) \\
&\mapsto (12, -6, 21, -19) \cong (12, 11, 4, 15).
\end{aligned}$$

- Coordinate-wise multiplication is straightforward:

$$(10, 13, 12, 3) \cdot (12, 11, 4, 15) = (120, 143, 48, 45) \cong (1, 7, 14, 11).$$

- Recombination is not obvious, see the next slide.

- We now try to recombine the result by the information of coordinates

$$(1, 7, 14, 11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- We now try to recombine the result by the information of coordinates

$$(1, 7, 14, 11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- For the first two coordinate, we can partially recombine them into the ring $\mathbb{Z}_{17}[x]/(x^2 - 1)$, since they came from the colored projection as shown:

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

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- We now try to recombine the result by the information of coordinates

$$(1, 7, 14, 11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- For the first two coordinate, we can partially recombine them into the ring $\mathbb{Z}_{17}[x]/(x^2 - 1)$, since they came from the colored projection as shown:

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

- Such partial recombination is easy, as we done before:

$$4 - 3x = \frac{1+7}{2} + \frac{1-7}{2}x.$$

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- We now try to recombine the result, denoted $f(x)$, by the information of coordinates

$$(1, 7, 14, 11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- Check that $4 + 11x$ projects to $(14, 11)$.

- We now try to recombine the result, denoted $f(x)$, by the information of coordinates

$$(1,7,14,11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- For the last two coordinate, we can partially recombine them into the ring $\mathbb{Z}_{17}[x]/(x^2-1)$, since they came from the colored projection as shown:

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

- Check that $4+11x$ projects to $(14,11)$.

- We now try to recombine the result, denoted $f(x)$, by the information of coordinates

$$(1,7,14,11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- For the last two coordinate, we can partially recombine them into the ring $\mathbb{Z}_{17}[x]/(x^2-1)$, since they came from the colored projection as shown:

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

- But such partial recombination is a little bit tricky,

$$\mathbb{Z}_{17}[x]/(x^2+1) \cong \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4)$$

$$a+bx \mapsto (a+4b, a-4b) = (A,B).$$

$$\frac{1}{2}(A+B) + \frac{1}{2}\frac{A-B}{4}x \mapsto (A,B).$$

- Check that $4+11x$ projects to $(14,11)$.

- We now try to recombine the result, denoted $f(x)$, by the information of coordinates

$$(1,7,14,11) \in \mathbb{Z}_{17}[x]/(x-1) \times \mathbb{Z}_{17}[x]/(x+1) \times \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4).$$

- For the last two coordinate, we can partially recombine them into the ring $\mathbb{Z}_{17}[x]/(x^2-1)$, since they came from the colored projection as shown:

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

- But such partial recombination is a little bit tricky,

$$\begin{aligned}\mathbb{Z}_{17}[x]/(x^2+1) &\cong \mathbb{Z}_{17}[x]/(x-4) \times \mathbb{Z}_{17}[x]/(x+4) \\ a+bx &\mapsto (a+4b, a-4b) = (A,B).\end{aligned}$$

$$\frac{1}{2}(A+B) + \frac{1}{2}\frac{A-B}{4}x \mapsto (A,B).$$

- In this case, the recombination goes:

$$\frac{1}{2}(14+11) + \frac{1}{2}\frac{14-11}{4}x = 4+11x.$$

  Note that the division are performed in the ring $\mathbb{Z}_{17}$.
- Check that $4+11x$ projects to $(14,11)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- So far, we know that the answer of the multiplication, denoted $f(x)$, represented in the first layer of decomposition is:

$$\mathbb{Z}_{17}[x]/(x^4-1) \cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1)$$
$$f(x) \mapsto (4-3x, 4+11x)$$

We have to do one more layer of recombination to get the final answer.

- Check that $f(x) = 4 + 4x + 0x^2 - 7x^3$ projects to $(1, 7, 14, 11)$.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4-1)$

- So far, we know that the answer of the multiplication, denoted $f(x)$, represented in the first layer of decomposition is:

$$\mathbb{Z}_{17}[x]/(x^4-1) \cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1)$$
$$f(x) \mapsto (4-3x, 4+11x)$$

  We have to do one more layer of recombination to get the final answer.
- Take a look at the first layer of decomposition:

$$\mathbb{Z}_{17}[x]/(x^4-1) \cong \mathbb{Z}_{17}[x]/(x^2-1) \times \mathbb{Z}_{17}[x]/(x^2+1)$$
$$(a_0 + a_1x + a_2x^2 + a_3x^3) \mapsto (a_0 + a_2 + (a_1 + a_3)x, a_0 - a_2 + (a_1 - a_3)x) := (A_0 + A_1x, A_2 + A_3x).$$

  Hence

$$\frac{1}{2}(A_0 + A_2) + \frac{1}{2}(A_1 + A_3)x + \frac{1}{2}(A_0 - A_2)x^2 + \frac{1}{2}(A_1 - A_3)x^3 \mapsto (A_0 + A_1x, A_2 + A_3x).$$

- Check that $f(x) = 4 + 4x + 0x^2 - 7x^3$ projects to $(1, 7, 14, 11)$.

- So far, we know that the answer of the multiplication, denoted $f(x)$, represented in the first layer of decomposition is:

$$\mathbb{Z}_{17}[x]/(x^4 - 1) \cong \mathbb{Z}_{17}[x]/(x^2 - 1) \times \mathbb{Z}_{17}[x]/(x^2 + 1)$$
$$f(x) \mapsto (4 - 3x, 4 + 11x)$$

  We have to do one more layer of recombination to get the final answer.

- Take a look at the first layer of decomposition:

$$\mathbb{Z}_{17}[x]/(x^4 - 1) \cong \mathbb{Z}_{17}[x]/(x^2 - 1) \times \mathbb{Z}_{17}[x]/(x^2 + 1)$$
$$(a_0 + a_1 x + a_2 x^2 + a_3 x^3) \mapsto (a_0 + a_2 + (a_1 + a_3)x, a_0 - a_2 + (a_1 - a_3)x) := (A_0 + A_1 x, A_2 + A_3 x).$$

  Hence

$$\frac{1}{2}(A_0 + A_2) + \frac{1}{2}(A_1 + A_3)x + \frac{1}{2}(A_0 - A_2)x^2 + \frac{1}{2}(A_1 - A_3)x^3 \mapsto (A_0 + A_1 x, A_2 + A_3 x).$$

- Apply to our case, the final answer is:

$$\frac{1}{2}(4 + 4) + \frac{1}{2}(-3 + 11)x + \frac{1}{2}(4 - 4)x^2 + \frac{1}{2}(-3 - 11)x^3 = 4 + 4x + 0x^2 - 7x^3.$$

- Check that $f(x) = 4 + 4x + 0x^2 - 7x^3$ projects to $(1, 7, 14, 11)$.

- Let's now give a summary of the fast multiplication algorithm just invented:

- Let's now give a summary of the fast multiplication algorithm just invented:
  1. Project the operands $a(x), b(x)$ into the coordinate-rings

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

- Let's now give a summary of the fast multiplication algorithm just invented:
  1. Project the operands $a(x), b(x)$ into the coordinate-rings

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

  2. Perform the Coordinate-wise multiplication

- Let's now give a summary of the fast multiplication algorithm just invented:
  1. Project the operands $a(x), b(x)$ into the coordinate-rings

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

  2. Perform the Coordinate-wise multiplication
  3. Recombine the result to get the final answer As we have seen, the recombination is not trivial, however, there is a concept of butterfly algorithm, we will introduce it later.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- Let's now give a summary of the fast multiplication algorithm just invented:
  1. Project the operands $a(x), b(x)$ into the coordinate-rings

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

  2. Perform the Coordinate-wise multiplication
  3. Recombine the result to get the final answer As we have seen, the recombination is not trivial, however, there is a concept of butterfly algorithm, we will introduce it later.
- We left as an exercise that: The schoolbook of the same calculation requies 16 multiplications and some additions, make an estimation of the number of operations in the fast multiplication algorithm we just invented.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^4 - 1)$

- Let's now give a summary of the fast multiplication algorithm just invented:
  1. Project the operands $a(x), b(x)$ into the coordinate-rings

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

  2. Perform the Coordinate-wise multiplication
  3. Recombine the result to get the final answer As we have seen, the recombination is not trivial, however, there is a concept of butterfly algorithm, we will introduce it later.
- We left as an exercise that: The schoolbook of the same calculation requies 16 multiplications and some additions, make an estimation of the number of operations in the fast multiplication algorithm we just invented.
- Another issue is, here we picked a particular modular number 17, how to generalize the algorithm to arbitrary p? What conditions should the number p satisfy in order to have such decomposition (i.e., existence of the element ω such that $\omega^2 = -1$)? We will discuss this in the final part.

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^n - 1)$

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^8 - 1)$

- Proceeding from the previous example, we now try to decompose the ring $\mathbb{Z}_p[x]/(x^8 - 1)$.

- Proceeding from the previous example, we now try to decompose the ring $\mathbb{Z}_p[x]/(x^8 - 1)$.
- We assume that the modulus number p will make the existence of 8-th primitive root ω_8, that is, $\omega_8^8 = 1$ and $\omega_8^4 = -1$. Existence of ω_4 follows from $\omega_4 = \omega_8^2$.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- Proceeding from the previous example, we now try to decompose the ring $\mathbb{Z}_p[x]/(x^8 - 1)$.
- We assume that the modulus number p will make the existence of 8-th primitive root ω_8, that is, $\omega_8^8 = 1$ and $\omega_8^4 = -1$. Existence of ω_4 follows from $\omega_4 = \omega_8^2$.
- We have

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

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- Proceeding from the previous example, we now try to decompose the ring $\mathbb{Z}_p[x]/(x^8 - 1)$.
- We assume that the modulus number p will make the existence of 8-th primitive root ω_8, that is, $\omega_8^8 = 1$ and $\omega_8^4 = -1$. Existence of ω_4 follows from $\omega_4 = \omega_8^2$.
- We have

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

- Hence, we have the decomposition:

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

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^n - 1)$

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

.

- The decomposition can be further written as:

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

.

- The decomposition can be further written as:

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

.

- The decomposition can be further written as:

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

.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The decomposition can be further written as:

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

- It can then be sofisticatedly written as:

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

The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ will be discussed in the next slide.

Decomposition of $\mathbb{Z}_p[x]/(x^n-1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8-1)$

- The decomposition can be further written as:

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

- It can then be sofisticatedly written as:

$$\mathbb{Z}_p[x]/(x^8-1) \cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x-\omega_2^{\mathrm{brv}_1(k)})$$

The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ will be discussed in the next slide.

- The decomposition can be further written as:

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

- It can then be sofisticatedly written as:

$$
\mathbb{Z}_p[x]/(x^8-1) \cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x-\omega_2^{\mathrm{brv}_1(k)}) \cong \prod_{k=0}^{3} \mathbb{Z}_p[x]/(x-\omega_4^{\mathrm{brv}_2(k)})
$$

The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ will be discussed in the next slide.

Decomposition of $\mathbb{Z}_p[x]/(x^n-1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8-1)$

- The decomposition can be further written as:

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

- It can then be sofisticatedly written as:

$$\mathbb{Z}_p[x]/(x^8-1) \cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x-\omega_2^{\mathrm{brv}_1(k)}) \cong \prod_{k=0}^{3} \mathbb{Z}_p[x]/(x-\omega_4^{\mathrm{brv}_2(k)}) \cong \prod_{k=0}^{7} \mathbb{Z}_p[x]/(x-\omega_8^{\mathrm{brv}_3(k)}).$$

The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ will be discussed in the next slide.

- The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ are referred to as bit-reversal permutation.

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^n - 1)$

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^8 - 1)$

- The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ are referred to as bit-reversal permutation.
- $\mathrm{brv}_j(k)$ is defined as:

$$\mathrm{brv}_j(k) = \sum_{i=0}^{j-1} b_i 2^{j-1-i},$$

where b_i is the i-th bit of the binary representation of k.

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^n - 1)$

DECOMPOSITION OF $\mathbb{Z}_p[x]/(x^8 - 1)$

- The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ are referred to as bit-reversal permutation.
- $\mathrm{brv}_j(k)$ is defined as:

$$\mathrm{brv}_j(k) = \sum_{i=0}^{j-1} b_i 2^{j-1-i},$$

  where b_i is the i-th bit of the binary representation of k.
- If you think that the above formula is too complicated, it is equivalent to:
  1. Write the number k in binary representation.
  2. Pad the binary representation with zeros to make it j-bit long.
  3. Reverse the bitstring.
  4. Convert the reversed bitstring to decimal.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

- The notation $\mathrm{brv}_1(k)$, $\mathrm{brv}_2(k)$, and $\mathrm{brv}_3(k)$ are referred to as bit-reversal permutation.
- $\mathrm{brv}_j(k)$ is defined as:

$$\mathrm{brv}_j(k) = \sum_{i=0}^{j-1} b_i 2^{j-1-i},$$

  where b_i is the i-th bit of the binary representation of k.
- If you think that the above formula is too complicated, it is equivalent to:
  1. Write the number k in binary representation.
  2. Pad the binary representation with zeros to make it j-bit long.
  3. Reverse the bitstring.
  4. Convert the reversed bitstring to decimal.
- You can check this

$$\prod_{k=0}^{7} \mathbb{Z}_p[x]/(x - \omega_8^{\mathrm{brv}_3(k)})$$

  equals to

$$(\mathbb{Z}_p[x]/(x - \omega_8^0)) \times (\mathbb{Z}_p[x]/(x - \omega_8^4)) \times (\mathbb{Z}_p[x]/(x - \omega_8^2)) \times (\mathbb{Z}_p[x]/(x - \omega_8^6))$$
$$\times (\mathbb{Z}_p[x]/(x - \omega_8)) \times (\mathbb{Z}_p[x]/(x - \omega_8^5)) \times (\mathbb{Z}_p[x]/(x - \omega_8^3)) \times (\mathbb{Z}_p[x]/(x - \omega_8^7))$$

- Now we can finally state the decomposition formula of $\mathbb{Z}_p[x]/(x^n - 1)$:

$$
\begin{aligned}
\mathbb{Z}_p[x]/(x^n - 1) &\cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x^{\frac{n}{2}} - \omega_2^{\mathrm{brv}_1(k)}) \cong \prod_{k=0}^{3} \mathbb{Z}_p[x]/(x^{\frac{n}{4}} - \omega_4^{\mathrm{brv}_2(k)}) \\
&\cong \prod_{k=0}^{7} \mathbb{Z}_p[x]/(x^{\frac{n}{8}} - \omega_8^{\mathrm{brv}_3(k)}) \\
&\vdots \\
&\cong \prod_{k=0}^{n-1} \mathbb{Z}_p[x]/(x - \omega_n^{\mathrm{brv}_{\log_2 n}(k)}).
\end{aligned}
$$

We will say that this is a $\log_2 n$-level decomposition.

- Now we can finally state the decomposition formula of $\mathbb{Z}_p[x]/(x^n - 1)$:

$$\begin{aligned}\mathbb{Z}_p[x]/(x^n - 1) &\cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x^{\frac{n}{2}} - \omega_2^{\mathrm{brv}_1(k)}) \cong \prod_{k=0}^{3} \mathbb{Z}_p[x]/(x^{\frac{n}{4}} - \omega_4^{\mathrm{brv}_2(k)}) \\ &\cong \prod_{k=0}^{7} \mathbb{Z}_p[x]/(x^{\frac{n}{8}} - \omega_8^{\mathrm{brv}_3(k)}) \\ &\vdots \\ &\cong \prod_{k=0}^{n-1} \mathbb{Z}_p[x]/(x - \omega_n^{\mathrm{brv}_{\log_2 n}(k)}).\end{aligned}$$

  We will say that this is a $\log_2 n$-level decomposition.
- An important observation is that: In order to make the decomposition until the $\log_2 n$-level, we need to have the existence of n-th primitive root. If, say, the current coefficient ring only has 4-th primitive root, then we can only decompose until the 2-level:

$$\mathbb{Z}_p[x]/(x^n - 1) \cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x^{\frac{n}{2}} - \omega_2^{\mathrm{brv}_1(k)}).$$

- An important observation is that: In order to make the decomposition until the $\log_2 n$-level, we need to have the existence of n-th primitive root. If, say, the current coefficient ring only has 4-th primitive root, then we can only decompose until the 2-level:

$$\mathbb{Z}_p[x]/(x^n - 1) \cong \prod_{k=0}^{1} \mathbb{Z}_p[x]/(x^{\frac{n}{2}} - \omega_2^{\mathrm{brv}_1(k)}).$$

This is the so-called incomplete NTT. Though not fully decoposed, it is still beneficial (sometimes better) to our purpose. Again, the performance should be measured by the cycle-count.

Decomposition of $\mathbb{Z}_p[x]/(x^n - 1)$

Decomposition of $\mathbb{Z}_p[x]/(x^8 - 1)$

asd

- 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 the algorithm of such projection.

THE IMPLEMENTATION OF ALGORITHMS

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

- Usually, the *array* structure is used to represent a polynomial. If the input polynomial is $a(x) = a_0 + a_1x + \cdots + a_7x^7$, then the initial array representation 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

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

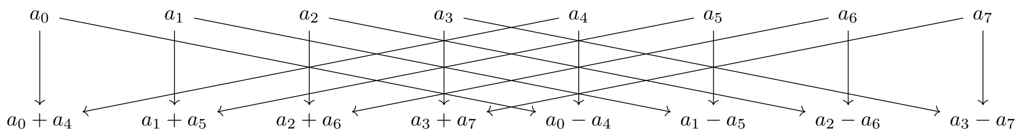
- In our array representation, the projection is simply the addition and subtraction of the corresponding elements:

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

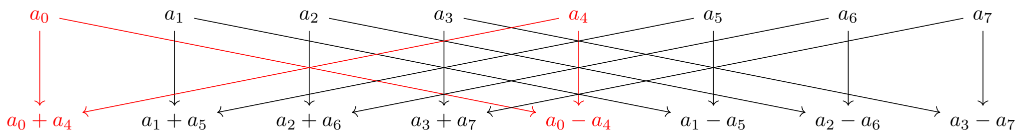
- In our array representation, the projection is simply the addition and subtraction of the corresponding elements:

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

- The pattern is not obvious, lets make a graph:



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



The Implementation of Algorithms

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

- 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 $a_0 + a_1 x + a_2 x^2 + a_3 x^3$ and $a_4 + a_5 x + a_6 x^2 + a_7 x^3$ 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:

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

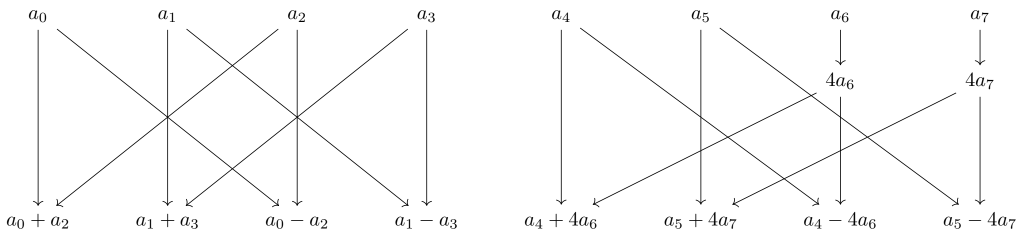
The Implementation of Algorithms

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

- 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:



The Implementation of Algorithms

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

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

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

- 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:

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

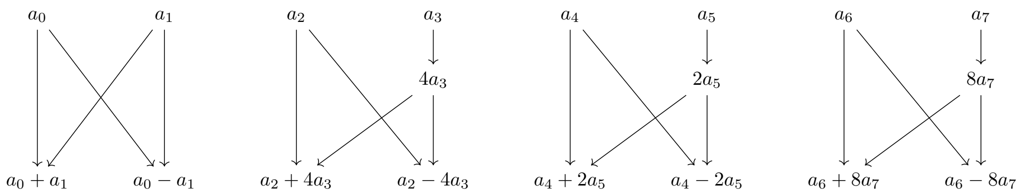
The Implementation of Algorithms

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

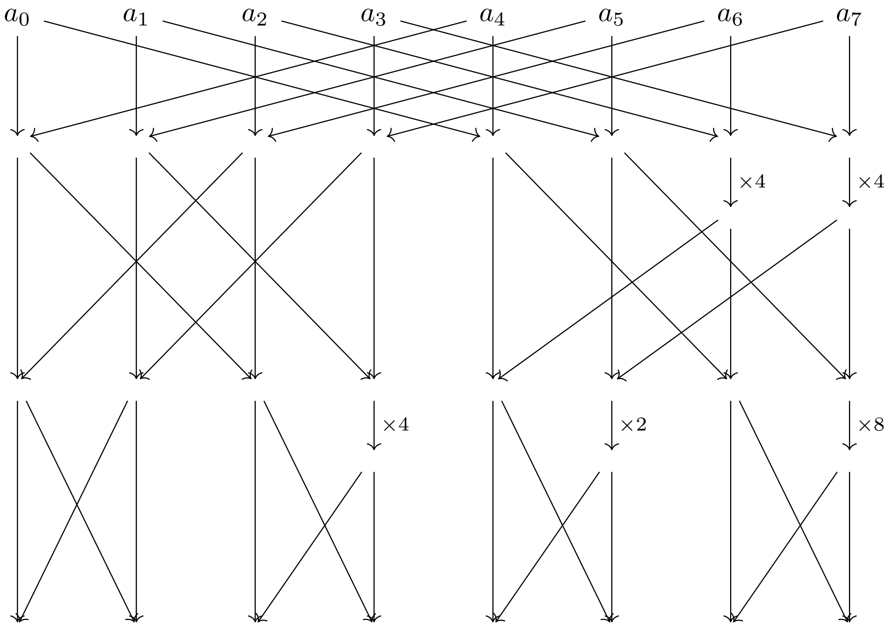
- In our array representation, the projection is to perform:

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

  The pattern is not obvious, lets make a graph:



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



The Implementation of Algorithms

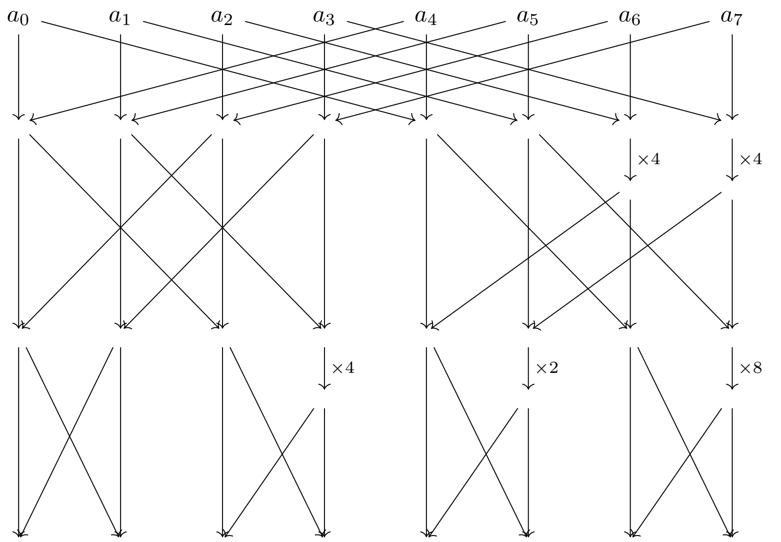
Example of $\mathbb{Z}_{17}[x]/(x^8 - 1)$

- Ok! After the projection, the point-wise multiplication is simple.
- The remark I want to make here is that, during the whole process, the multiplication is performed modulo 17. Such modulus multiplication (mod-mul for short) is a time-consuming operation.
- To deal with this, mathematicians invented various *reduction algorithms*, e.g., Barrett reduction, Montgomery reduction, Plantard reduction etc.
- The choice of reduction algorithm depends on many factors, including the machine architecture, the parallelization, etc.
- There is a review in the following paper:

The Implementation of Algorithms

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

- Finally, we have to rebuild the polynomial from the output of the last layer.
- Note that the rebuiding is the inverse of the projection, so we can rebuild the polynomial according to the graph, but you should look it conversely:



References I