Number Theoretic Transform

Jonghyun Kim

Korea University

January 28, 2026

Table of Contents

Number Theoretic Transform - Basics

Modular Exponentiation Using CRT

$\mathbb{Z}_{pq}$

$\log_2 d \approx \log_2 pq$

$$
\begin{tikzcd}[column sep=huge]
C \arrow[r, "{\begin{array}{c} 2 \cdot \log_2 pq \cdot \mathsf{Mult}_{pq} \\ \approx 16 \cdot \log_2 p \cdot \mathsf{Mult}_p \end{array}}", "{(\because \mathsf{Mult}_{pq} \approx 4\mathsf{Mult}_p,\ p \approx q)}"'] \arrow[d] & M = C^d \bmod pq \\
\begin{array}{c} (C_p = C \bmod p, \\ C_q = C \bmod q) \end{array} \arrow[r, "4 \cdot \log_2 p \cdot \mathsf{Mult}_p", "{(\because \mathsf{Mult}_p \approx \mathsf{Mult}_q)}"'] & \begin{array}{c} (M_p = C_p^{d_p} \bmod p, \\ M_q = C_q^{d_q} \bmod q) \end{array} \arrow[u, "\text{CRT}"']
\end{tikzcd}
$$

p and q are different prime numbers with $p \approx q$.

$\mathbb{Z}_p \times \mathbb{Z}_q$

$d_p = d \bmod p - 1$
$d_q = d \bmod q - 1$

Polynomial Multiplication Using NTT

$$\mathbb{Z}_q[x]/\langle f(x)\rangle$$

$$\begin{tikzcd}
a(x), b(x) \arrow[rr, "c(x) = a(x)\cdot b(x)", "\mathcal{O}(n^2)"'] \arrow[d, "\mathcal{O}(nk)"] & & c(x) \\
\begin{matrix}(a_1(x), \cdots, a_{2^k}(x)),\\ (b_1(x), \cdots, b_{2^k}(x))\end{matrix} \arrow[rr, "c_i(x) = a_i(x)\cdot b_i(x)", "\mathcal{O}(n) \text{ if } k = \log n"'] & & (c_1(x), \cdots, c_{2^k}(x)) \arrow[u, "\mathcal{O}(nk)"']
\end{tikzcd}$$

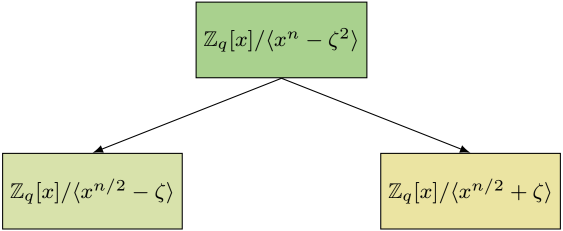
$f_i(x)$ are relatively prime and have the same degree.

$$\prod_{i=1}^{k} \mathbb{Z}_q[x]/\langle f_i(x)\rangle$$

$deg(f_i) = 1$ if $k = \log n$

Radix-2 NTT Layer

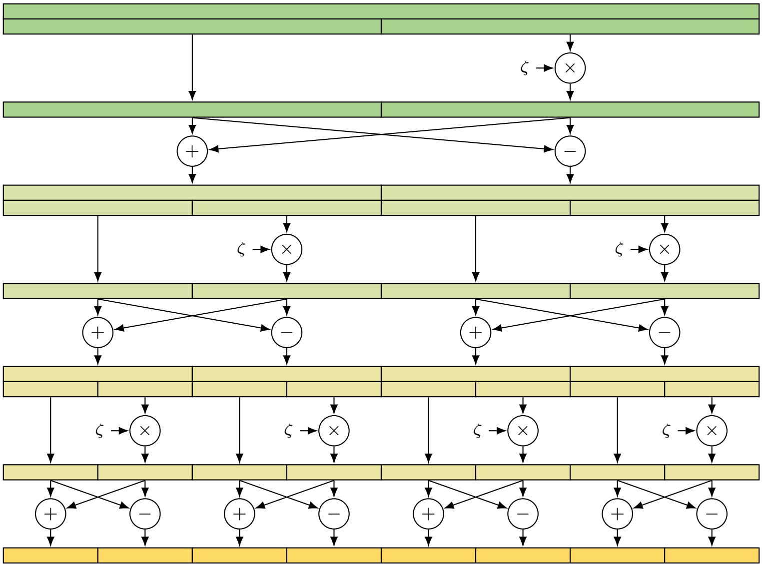
$$a(x) = a_0(x) + a_1(x)x^{n/2}$$



$$\hat{a}_0(x) = a_0(x) + a_1(x)\zeta \qquad \hat{a}_1(x) = a_0(x) - a_1(x)\zeta$$

$$2a_0(x) = \hat{a}_0(x) + \hat{a}_1(x)$$
$$2a_1(x) = (\hat{a}_0(x) - \hat{a}_1(x))\zeta^{-1}$$

Radix-2 NTT Structure (1)

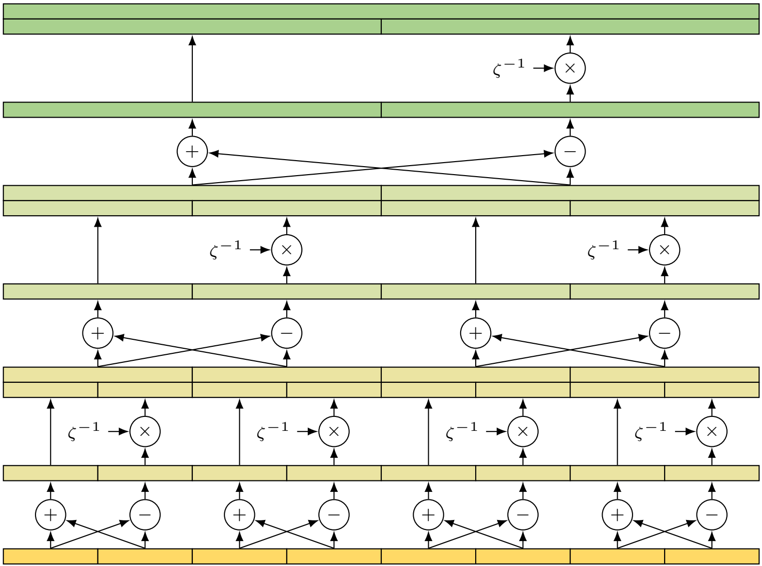


Radix-2 NTT Structure (2)

$$
k = \log n \left\{
\begin{array}{cc}
\mathbb{Z}_q[x]/\langle f(x)\rangle & deg(f) = n \\
\downarrow \mathcal{O}(n) & \\
\mathbb{Z}_q[x]/\langle f_{1,1}(x)\rangle \times \mathbb{Z}_q[x]/\langle f_{1,2}(x)\rangle & deg(f_{1,i}) = n/2 \\
\downarrow \mathcal{O}(n) & \\
\vdots & \\
\downarrow \mathcal{O}(n) & \\
\prod_{i=1}^{n/2} \mathbb{Z}_q[x]/\langle f_{k-1,i}(x)\rangle & deg(f_{k-1,i}) = 2 \\
\downarrow \mathcal{O}(n) & \\
\prod_{i=1}^{n} \mathbb{Z}_q[x]/\langle f_{k,i}(x)\rangle & deg(f_{k,i}) = 1
\end{array}\right.
$$

Total : $\mathcal{O}(nk) = \mathcal{O}(n \log n)$

Radix-2 Inverse NTT Structure



Condition for applying NTT (1)

- $\mathbb{Z}_q[x]/\langle x^n+1\rangle$, where n is a power of 2
  - $\boxed{\zeta\text{: primitive } 2n\text{-th root of unity modulo } q}$
    - $\zeta^i \not\equiv 1 \pmod{q}$ for $i \in [1, 2n-1]$
    - $\zeta^{2n} \equiv 1 \pmod{q}$
  - Fact 1: $\zeta^n + 1 \equiv 0 \pmod{q}$
    - $\zeta^{2n} - 1 \equiv (\zeta^n+1)(\zeta^n-1) \equiv 0 \pmod{q}$
    - By the definition of ζ, $\zeta^n - 1 \not\equiv 0 \pmod{q} \Rightarrow \zeta^n + 1 \equiv 0 \pmod{q}$
  - Fact 2: $\zeta^i \not\equiv \zeta^j \pmod{q}$ for $i, j \in [1, 2n]$ with $i \neq j$
    - If there exist i, j with $1 \leq i < j \leq 2n$ such that $\zeta^i \equiv \zeta^j \pmod{q}$, then $\zeta^{j-i} \equiv 1 \pmod{q}$, a contradiction since $j - i \in [1, 2n-1]$.

Condition for applying NTT (2)

- $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$, where n is a power of 2
  - $\boxed{\zeta\text{: primitive } 2n\text{-th root of unity modulo } q}$
    - $\zeta^i \not\equiv 1 \pmod{q}$ for $i \in [1, 2n-1]$
    - $\zeta^{2n} \equiv 1 \pmod{q}$
  - Fact 1: $\zeta^n + 1 \equiv 0 \pmod{q}$
  - Fact 2: $\zeta^i \not\equiv \zeta^j \pmod{q}$ for $i, j \in [1, 2n]$ with $i \neq j$
  - $$\begin{aligned} x^n + 1 &= x^n - \zeta^n \qquad \because \text{Fact 1} \\ &= (x^{n/2} - \zeta^{n/2})(x^{n/2} + \zeta^{n/2}) \\ &= (x^{n/2} - \zeta^{n/2})(x^{n/2} - \zeta^{3n/2}) \qquad \because \text{Fact 1} \\ &= (x^{n/4} - \zeta^{n/4})(x^{n/4} + \zeta^{n/4})(x^{n/4} - \zeta^{3n/4})(x^{n/4} + \zeta^{3n/4}) \\ &= (x - \zeta)(x - \zeta^3)(x - \zeta^5) \cdots (x - \zeta^{2n-1}) \end{aligned}$$

All the factors are distinct ($\because$ Fact 2) $\Rightarrow$ they are relatively prime.

Finding $2n$-th root of unity modulo q

1. Find a generator $g \in \mathbb{Z}_q^* = \{1, \cdots, q-1\}$.
   - $g^i \not\equiv 1 \pmod q$ for $i \in [1, q-2]$
   - $g^{q-1} \equiv 1 \pmod q$

$$\{1, \cdots, q-1\} = \{g^1, \cdots, g^{q-1}\}$$

2. Compute the integer $k = \frac{q-1}{2n}$, $\boxed{\text{assuming that } 2n | q-1}$.

3. Output $\zeta = g^k \bmod q$ as a primitive $2n$-th root of unity.
   - $\zeta^i \equiv (g^k)^i \not\equiv 1$ for $i \in [1, 2n-1]$ by the definition of g
   - $\zeta^{2n} \equiv (g^k)^{2n} \equiv g^{2nk} \equiv g^{q-1} \equiv 1 \pmod q$

Generator Test for $g \in \mathbb{Z}_q^* = \{1, \ldots, q-1\}$ (1)

- $\mathbb{Z}_{13}^*$
  - $g^{q-1} \equiv g^{2^2 \cdot 3} \equiv 1 \pmod 7$
    $\Rightarrow g^{\{1,2,4,6\}} \overset{?}{\not\equiv} 1 \pmod{13} \Rightarrow g^{\{4,6\}} \overset{?}{\not\equiv} 1 \pmod{13}$

i	1	2	3	4	5	6	7	8	9	10	11	12
1^i	1	1	1	1	1	1	1	1	1	1	1	1
2^i	2	4	8	3	6	12	11	9	5	10	7	1
3^i	3	9	1	3	9	1	3	9	1	3	9	1
4^i	4	3	12	9	10	1	4	3	12	9	10	1
5^i	5	12	8	1	5	12	8	1	5	12	8	1
6^i	6	10	8	9	2	12	7	3	5	4	11	1
7^i	7	10	5	9	11	12	6	3	8	4	2	1
8^i	8	12	5	1	8	12	5	1	8	12	5	1
9^i	9	3	1	9	3	1	9	3	1	9	3	1
10^i	10	9	12	3	4	1	10	9	12	3	4	1
11^i	11	4	5	3	7	12	2	9	8	10	6	1
12^i	12	1	12	1	12	1	12	1	12	1	12	1

Generator Test for $g \in \mathbb{Z}_q^* = \{1, \ldots, q-1\}$ (1)

1. Factorize $q-1$ as $q-1 = p_1^{r_1} \cdots p_\ell^{r_\ell}$
   - p_i are distinct primes.

2. For each $i \in \{1, \ldots, \ell\}$:
   - If $g^{(q-1)/p_i} \equiv 1 \pmod{q}$, then return "$g$ is not a generator."

3. Return "g is a generator.

Finding prime numbers q such that $2n|q-1$ (SageMath)

```
def find_ntt_prime(n,bits):
    qs =[];
    k = 1;

    while True:
        q = 2*n*k+1;
        if q > 2^bits:
            break;
        if q in Primes():
            qs.append(q);
        k += 1;
    return qs;
```

Finding generators g of $\mathbb{Z}_q^*$ (SageMath)

```
def find_generator(q):
    Zq = IntegerModRing(q);
    gs = range(1,q);

    for x in list(factor(q-1)):
        p = x[0];
        t = [];
        for g in gs:
            if Zq(g)^((q-1)/p) != 1:
                t.append(Zq(g));
        gs = t;

    return gs;
```

Finding primitive $2n$-th root of unity modulo q (SageMath)

```
def find_w(q):

    k = Integer((q-1)/(2*n));

    ws = [g^k for g in find_generator(q)];

    return sorted(list(set(ws)));
```

Generating Precomputation Table (1)

$$\boxed{\begin{aligned}\hat{a}_0(x) &= a_0(x) + a_1(x)\zeta \\ \hat{a}_1(x) &= a_0(x) - a_1(x)\zeta \\ \\ 2a_0(x) &= \hat{a}_0(x) + \hat{a}_1(x) \\ 2a_1(x) &= (\hat{a}_0(x) - \hat{a}_1(x))\zeta^{-1}\end{aligned}}$$

$$\boxed{\zeta^n \equiv -1 \pmod{q}}$$

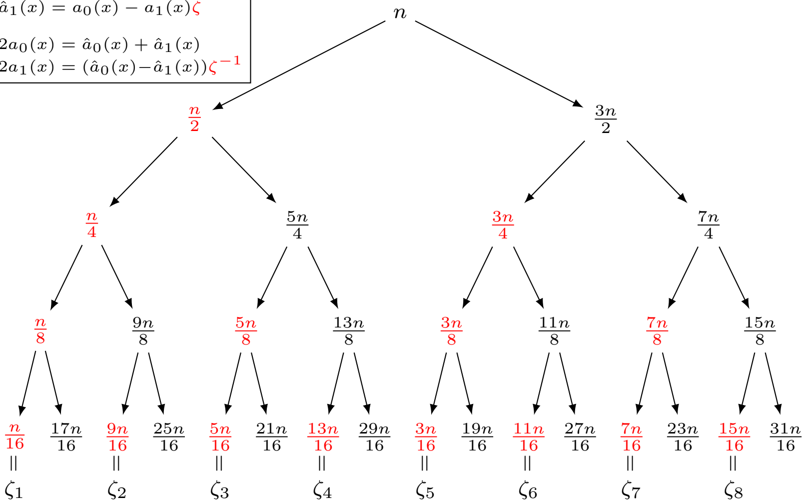
$$\begin{tikzcd}[column sep=tiny]
 & & & \mathbb{Z}_q[x]/\langle x^n+1\rangle \arrow[d, equal] & & & \\
 & & & \mathbb{Z}_q[x]/\langle x^n-\zeta^n\rangle \arrow[dll] \arrow[drr] & & & \\
 & \mathbb{Z}_q[x]/\langle x^{n/2}-\zeta^{n/2}\rangle \arrow[ddl] \arrow[ddr] & & & & \mathbb{Z}_q[x]/\langle x^{n/2}+\zeta^{n/2}\rangle \arrow[d, equal] & \\
 & & & & & \mathbb{Z}_q[x]/\langle x^{n/2}-\zeta^{3n/2}\rangle \arrow[dl] \arrow[dr] & \\
 \mathbb{Z}_q[x]/\langle x^{n/4}-\zeta^{n/4}\rangle & & \mathbb{Z}_q[x]/\langle x^{n/4}+\zeta^{n/4}\rangle \arrow[d, equal] & & \mathbb{Z}_q[x]/\langle x^{n/4}-\zeta^{3n/4}\rangle & & \mathbb{Z}_q[x]/\langle x^{n/4}+\zeta^{3n/4}\rangle \arrow[d, equal] \\
 & & \mathbb{Z}_q[x]/\langle x^{n/4}-\zeta^{5n/4}\rangle & & & & \mathbb{Z}_q[x]/\langle x^{n/4}-\zeta^{7n/4}\rangle
\end{tikzcd}$$

Generating Precomputation Table (2)

$$\hat{a}_0(x) = a_0(x) + a_1(x)\zeta$$
$$\hat{a}_1(x) = a_0(x) - a_1(x)\zeta$$

$$2a_0(x) = \hat{a}_0(x) + \hat{a}_1(x)$$
$$2a_1(x) = (\hat{a}_0(x) - \hat{a}_1(x))\zeta^{-1}$$

$$\zeta^n \equiv -1 \pmod{q}$$



$$\zeta_i \zeta_{9-i} \equiv \zeta^n \equiv -1 \pmod{q} \quad \Rightarrow \quad \zeta_i^{-1} \equiv -\zeta_{9-i} \pmod{q}$$

Generating Precomputation Table (3) (SageMath)

```
level = Integer(log(n,2));

zetas = [];

tree = zero_matrix(ZZ,level+1,1 << level);
tree[0,0] = n;

for l in range(level):
    for i in range(1 << l):
        tree[l+1,2*i  ] = tree[l  ,  i] / 2;
        tree[l+1,2*i+1] = tree[l+1,2*i] + n;

        zetas.append(Zq(w)^tree[l+1,2*i]);
```

Signed Montgomery Reduction

- Signed Montgomery Reduction [3]
  - For $0 < q < \frac{\beta}{2}$:

$$\hat{a} = \mathsf{Mont}(a) \equiv a\beta^{-1} \pmod{q}$$

    - Constraints on a: $-\frac{\beta}{2}q \leq a < \frac{\beta}{2}q$
    - Range of $\hat{a}$: $-q < \hat{a} < q$

- Montgomery Reduction for Multiplication
  - Transform to Montgomery Form
    - $\hat{a} = \mathsf{Mont}(a \cdot (\beta^2 \bmod q)) \equiv a\beta \pmod{q}$
    - $\hat{b} = \mathsf{Mont}(b \cdot (\beta^2 \bmod q)) \equiv b\beta \pmod{q}$
  - Montgomery Multiplication
    - $\hat{a}\hat{b} \equiv ab\beta^2 \pmod{q}$
    - $\mathsf{Mont}(\hat{a}\hat{b}) \equiv \mathsf{Mont}(ab\beta^2) \equiv ab\beta \pmod{q}$

NTT Using Montgomery Reduction

$$a(x) = a_0(x) + a_1(x)x^{n/2}$$

$$\begin{tikzcd}
 & \boxed{\mathbb{Z}_q[x]/\langle x^n - \zeta^2 \rangle} \arrow[dl] \arrow[dr] & \\
\boxed{\mathbb{Z}_q[x]/\langle x^{n/2} - \zeta \rangle} & & \boxed{\mathbb{Z}_q[x]/\langle x^{n/2} + \zeta \rangle}
\end{tikzcd}$$

$$\hat{a}_0(x) = a_0(x) + a_1(x)\zeta \qquad \hat{a}_1(x) = a_0(x) - a_1(x)\zeta$$

$$\mathsf{Mont}(a_1(x) \times \underbrace{\zeta\beta \bmod q}_{\text{pre-computation}})) = a_1(x)\zeta \bmod q$$

Number Theoretic Transform - Advanced

Variants of NTT (1)

- Incomplete NTT
  - $\mathbb{Z}_q[x]/\langle x^n + 1\rangle \approx \prod_{i=1}^{n/2} \mathbb{Z}_q[x]/\langle x^2 - \zeta_i\rangle$
    - $n = 2^m$ for some $m \in \mathbb{N}$
    - ζ: primitive $(2n/2)$-th root of unity modulo q
    - q: prime number with $q = (2n/2) \cdot k + 1$ for some $k \in \mathbb{N}$
    - Supports a larger set of modulus q for the NTT

- Example
  - Complete NTT in CRYSTAL-KYBER (Round 1)
    - $n = 256$, $q = 7681$
  - Incomplete NTT in CRYSTAL-KYBER (Round 2 & 3)
    - $n = 256$, $q = 3329$

Variants of NTT (2)

- Radix-2 NTT Layer for Cyclotomic Trinomial [2]
  - $\mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1\rangle \approx \prod_{i=1}^{2} \mathbb{Z}_q[x]/\langle x^{n/2} - \zeta_i\rangle$
    - $n = 2^a 3^b$ for some $a, b \in \mathbb{N}$

- Radix-3 NTT Layer [1]
  - $\mathbb{Z}_q[x]/\langle x^n - \zeta^3\rangle \approx \prod_{i=1}^{3} \mathbb{Z}_q[x]/\langle x^{n/3} - \zeta_i\rangle$
    - $n = 2^a 3^b$ for some $a, b \in \mathbb{N}$

Table: Combinations of NTT layers in NTRU+

n	q	Radix-2 for CT	Radix-3	Radix-2	d	ζ	$\ell = 3n/d$
576	3457	1	2	3	4	81	432
768	3457	1	1	5	4	22	576
864	3457	1	2	4	3	9	864
1152	3457	1	2	4	4	9	864

ζ : primitive ℓ-th root of unity modulo q

Radix-2 NTT Layer for Cyclotomic Trinomial (1)

- $R_q = \mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1\rangle$
  - ψ : primitive 6-th root of unity modulo q
    - $\psi^i \not\equiv 1 \pmod q$ for $i \in [1, 5]$
    - $\psi^6 \equiv 1 \pmod q$
  - Fact 1: $\psi^2 - \psi + 1 \equiv 0 \pmod q$
    - $\psi^6 - 1 \equiv (\psi^3 - 1)(\psi + 1)(\psi^2 - \psi + 1) \equiv 0 \pmod q$
    - By the definition of ψ, $\psi^2 - \psi + 1 \equiv 0 \pmod q$
    - Fact 1-1: $\psi^3 + 1 \equiv (\psi + 1)(\psi^2 - \psi + 1) \equiv 0 \pmod q$
  - Fact 2: $x^2 - x + 1 = (x - \psi)(x - \psi^5)$
    - $(x - \psi)(x - \psi^5) \equiv x^2 - (\psi + \psi^5) + \psi^6 \pmod q$
    - Fact 2-1: $\psi + \psi^5 \equiv \psi - \psi^2 \equiv 1 \pmod q$
    - $\psi^6 \equiv 1 \pmod q$
  - $x^n - x^{n/2} + 1 = (x^{n/2} - \psi)(x^{n/2} - \psi^5)$ ($\because$ Fact 2)

Radix-2 NTT Layer for Cyclotomic Trinomials (2)

$$a(x) = a_0(x) + a_1(x)x^{n/2}$$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1\rangle \arrow[dl] \arrow[dr] & \\
\mathbb{Z}_q[x]/\langle x^{n/2} - \psi\rangle & & \mathbb{Z}_q[x]/\langle x^{n/2} - \psi^5\rangle
\end{tikzcd}$$

$$\hat{a}_0(x) = a_0(x) + a_1(x)\psi$$

$$\begin{aligned}
\hat{a}_1(x) &= a_0(x) + a_1(x)\psi^5 \\
&= a_0(x) + a_1(x)(1 - \psi) \quad (\because \text{Fact 2-1}) \\
&= a_0(x) + a_1(x) - a_1(x)\psi
\end{aligned}$$

$$\begin{aligned}
2a_0(x) &= \hat{a}_0(x) + \hat{a}_1(x) - a_1(x) \\
a_1(x) &= (\hat{a}_0(x) - \hat{a}_1(x))(\zeta - \zeta^5)^{-1}
\end{aligned}$$

Radix-3 NTT Layer (1)

- $R_q = \mathbb{Z}_q[x]/\langle x^n - \zeta^3 \rangle$
  - ω : primitive 3-th root of unity modulo q
    - $\omega^i \not\equiv 1 \pmod q$ for $i \in [1, 2]$
    - $\omega^3 \equiv 1 \pmod q$
  - Fact 1: $\omega^2 + \omega + 1 \equiv 0 \pmod q$
    - $\omega^3 - 1 \equiv (\omega - 1)(\omega^2 + \omega + 1) \equiv 0 \pmod q$
    - By the definition of ω, $\omega^2 + \omega + 1 \equiv 0 \pmod q$
  - Fact 2: $x^3 - \zeta^3 = (x - \alpha)(x - \beta)(x - \gamma)$
    - $\alpha = \zeta$, $\beta = \zeta\omega$, $\gamma = \zeta\omega^2$
    - $(x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\gamma\alpha)x - \alpha\beta\gamma$
    - $\alpha + \beta + \gamma \equiv \zeta(1 + \omega + \omega^2) \equiv 0 \pmod q$ ($\because$ Fact 1)
    - $\alpha\beta + \beta\gamma + \gamma\alpha \equiv \zeta(\omega + \omega^3 + \omega^2)$
      $\equiv \zeta(1 + \omega + \omega^2) \equiv 0 \pmod q$ ($\because$ Fact 1)
    - $\alpha\beta\gamma \equiv \zeta^3\omega^3 \equiv \zeta^3 \pmod q$

Radix-3 NTT Layer (2)

$\mathbb{Z}_q[x]/\langle x^n - \alpha^3 \rangle$ $\quad a(x) = a_0(x) + a_1(x)x^{n/3} + a_2(x)x^{2n/3}$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \alpha \rangle$ $\quad \hat{a}_0(x) = a_0(x) + a_1(x)\alpha + a_2(x)\alpha^2$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \beta \rangle$

$$
\begin{aligned}
\hat{a}_1(x) &= a_0(x) + a_1(x)\beta + a_2(x)\beta^2 \\
&= a_0(x) - a_2(x)\alpha^2 + \omega(a_1(x)\alpha - a_2(x)\alpha^2)
\end{aligned}
$$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \gamma \rangle$

$$
\begin{aligned}
\hat{a}_2(x) &= a_0(x) + a_1(x)\gamma + a_2(x)\gamma^2 \\
&= a_0(x) - a_1(x)\alpha - \omega(a_1(x)\alpha - a_2(x)\alpha^2)
\end{aligned}
$$

Radix-3 NTT layer (3)

- NTT

$$\begin{pmatrix} \hat{a}_0(x) \\ \hat{a}_1(x) \\ \hat{a}_2(x) \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

- Inverse NTT

$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ \alpha^{-2} & \beta^{-2} & \gamma^{-2} \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix} = 3 \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

  - $\alpha^2 + \beta^2 + \gamma^2 \equiv (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) \equiv 0 \pmod q$
  - $\alpha^{-1} + \beta^{-1} + \gamma^{-1} \equiv (\alpha\beta\gamma)^{-1}(\alpha\beta + \beta\gamma + \gamma\alpha) \equiv 0 \pmod q$
  - $\alpha^{-2} + \beta^{-2} + \gamma^{-2}$
    $\equiv (\alpha^{-1} + \beta^{-1} + \gamma^{-1})^2 - 2(\alpha^{-1}\beta^{-1} + \beta^{-1}\gamma^{-1} + \gamma^{-1}\alpha^{-1})$
    $\equiv (\alpha^{-1} + \beta^{-1} + \gamma^{-1})^2 - 2\alpha^{-1}\beta^{-1}\gamma^{-1}(\alpha + \beta + \gamma) \equiv 0 \pmod q$

Radix-3 Inverse NTT Layer (1)

$\mathbb{Z}_q[x]/\langle x^n - \alpha^3 \rangle$ $\quad a(x) = a_0(x) + a_1(x)x^{n/3} + a_2(x)x^{2n/3}$

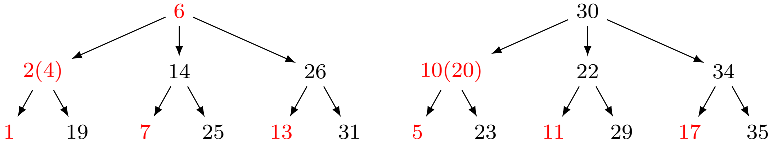
$\mathbb{Z}_q[x]/\langle x^{n/3} - \alpha \rangle$ $\quad 3a_0(x) = \hat{a}_0(x) + \hat{a}_1(x) + \hat{a}_2(x)$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \beta \rangle$
$$\begin{aligned} 3a_1(x) &= \hat{a}_0(x)\alpha^{-1} + \hat{a}_1(x)\beta^{-1} + \hat{a}_2(x)\gamma^{-1} \\ &= \alpha^{-1}(\hat{a}_0(x) - \hat{a}_1(x) - \omega(\hat{a}_1(x) - \hat{a}_2(x))) \end{aligned}$$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \gamma \rangle$
$$\begin{aligned} 3a_2(x) &= \hat{a}_0(x)\alpha^{-2} + \hat{a}_1(x)\beta^{-2} + \hat{a}_2(x)\gamma^{-2} \\ &= \alpha^{-2}(\hat{a}_0(x) - \hat{a}_2(x) + \omega(\hat{a}_1(x) - \hat{a}_2(x))) \end{aligned}$$

Example

- $\mathbb{Z}_q[x]/\langle x^{24} - x^{12} + 1\rangle \approx \prod_{i=1}^{12} \mathbb{Z}_q[x]/\langle x^2 - \zeta_i\rangle$
  - ζ: primitive 36-th root of unity modulo q.
    - $\zeta^{18} \equiv -1 \pmod q$, $\psi \equiv \zeta^6 \pmod q$, $\omega \equiv \zeta^{12} \pmod q$
  - $$\begin{aligned} x^{24} - x^{12} + 1 &= (x^{12} - \zeta^6)(x^{12} - \zeta^{30}) \\ &= (x^4 - \zeta^2)(x^4 - \zeta^{14})(x^4 - \zeta^{26})(x^4 - \zeta^{10})(x^4 - \zeta^{22})(x^4 - \zeta^{34}) \\ &= (x^2 - \zeta)(x^2 - \zeta^{19})(x^2 - \zeta^{7})(x^2 - \zeta^{25})(x^2 - \zeta^{13})(x^2 - \zeta^{31}) \\ &\quad\ (x^2 - \zeta^{5})(x^2 - \zeta^{23})(x^2 - \zeta^{11})(x^2 - \zeta^{29})(x^2 - \zeta^{17})(x^2 - \zeta^{35}) \end{aligned}$$



$$\zeta^2\zeta^{10} \equiv \zeta^{12} \equiv \omega \pmod q \quad \Rightarrow \quad \omega\zeta^{-2} \equiv \zeta^{10} \pmod q$$
$$\zeta^4\zeta^{20} \equiv \zeta^{24} \equiv \omega^2 \pmod q \quad \Rightarrow \quad \omega^2\zeta^{-4} \equiv \zeta^{20} \pmod q$$

$$\zeta^1\zeta^{17} \equiv \zeta^{18} \equiv -1 \pmod q \quad \Rightarrow \quad \zeta^{-1} \equiv -\zeta^{17} \pmod q$$

Radix-3 Inverse NTT Layer (2)

$\mathbb{Z}_q[x]/\langle x^n - \alpha^3 \rangle$ $\quad a(x) = a_0(x) + a_1(x)x^{n/3} + a_2(x)x^{2n/3}$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \alpha \rangle$ $\quad 3a_0(x) = \hat{a}_0(x) + \hat{a}_1(x) + \hat{a}_2(x)$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \beta \rangle$

$$\begin{aligned} 3a_1(x) &= \hat{a}_0(x)\alpha^{-1} + \hat{a}_1(x)\beta^{-1} + \hat{a}_2(x)\gamma^{-1} \\ &= \omega\alpha^{-1}(\hat{a}_2(x) - \hat{a}_0(x) - \omega(\hat{a}_1(x) - \hat{a}_0(x))) \end{aligned}$$

$\mathbb{Z}_q[x]/\langle x^{n/3} - \gamma \rangle$

$$\begin{aligned} 3a_2(x) &= \hat{a}_0(x)\alpha^{-2} + \hat{a}_1(x)\beta^{-2} + \hat{a}_2(x)\gamma^{-2} \\ &= \omega^2\alpha^{-2}(\hat{a}_2(x) - \hat{a}_1(x) + \omega(\hat{a}_1(x) - \hat{a}_0(x))) \end{aligned}$$

Helpful Scripts related with NTT

https://github.com/ntruplus/ntt_for_ntruplus/

Thank You for Your Attention!

Any Questions?

(I know this is shared online, so questions might be difficult.)

Contact: yoswuk@korea.ac.kr

References

Chenar Abdulla Hassan and Oğuz Yayla.
Radix-3 NTT-based polynomial multiplication for lattice-based cryptography.
Cryptology ePrint Archive, Report 2022/726, 2022.

Vadim Lyubashevsky and Gregor Seiler.
NTTRU: Truly fast NTRU using NTT.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3):180–201, 2019.

Gregor Seiler.
Faster AVX2 optimized NTT multiplication for ring-LWE lattice cryptography.
Cryptology ePrint Archive, Report 2018/039, 2018.