V4: The Number-Theoretic Transform (NTT)

Kyber and Dilithium

August 2024

Number-Theoretic Transform (NTT)

- NTT is a finite field analogue of the Discrete Fourier Transform (DFT).
- It enables one to multiply two polynomials in $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ using $O(n \log n)$ $\mathbb{Z}_q$-operations (vs. $O(n^2)$ $\mathbb{Z}_q$- operations with classical algorithms).

V4 outline

- V4a: Dilithium NTT
- V4b: Kyber NTT

V4a: Dilithium NTT

1. Multiplication in R_q
2. NTT definition
3. NTT computation
4. Example
5. Dilithium NTT

Multiplication in R_q

- Recall that $R_q = \mathbb{Z}_q[x]/(x^n + 1)$.
- Let $a(x), b(x) \in R_q$, and let $c(x) = a(x)b(x) \bmod (x^n + 1)$.
- The classical algorithm for computing $c(x)$ is:

$O(n^2)$ 1. Compute the polynomial product
$d(x) = a(x)b(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{2n-3}x^{2n-3} + d_{2n-2}x^{2n-2}$.

2. Reduce modulo $x^n + 1$:
Replace x^n by -1, x^{n+1} by $-x$, …, x^{2n-2} by $-x^{n-2}$ to get
$(d_0 + d_1x + \cdots + d_{n-1}x^{n-1}) + (-d_n - d_{n+1}x - \cdots - d_{2n-3}x^{n-3} - d_{2n-2}x^{n-2})$.

$O(n)$ 3. Add to get:
$c(x) = c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}$.

- Overall run time: $O(n^2)$.

NTT outline

- The Number-Theoretic Transform is a function $\text{NTT} : R_q \longrightarrow \mathbb{Z}_q^n$.
- The function is invertible, with inverse function $\text{NTT}^{-1} : \mathbb{Z}_q^n \longrightarrow R_q$.
  - For all $a \in R_q$, $\text{NTT}^{-1}(\text{NTT}(a)) = a$.
- To compute $c(x) = a(x)b(x) \bmod (x^n + 1)$ where $a(x), b(x) \in R_q$:

$O(n \log n)$ 1. Compute $\hat{a} = \text{NTT}(a)$ and $\hat{b} = \text{NTT}(b)$.

$O(n)$ 2. Compute $\hat{c} = \hat{a} \circ \hat{b}$ (component-wise multiplication in $\mathbb{Z}_q^n$).

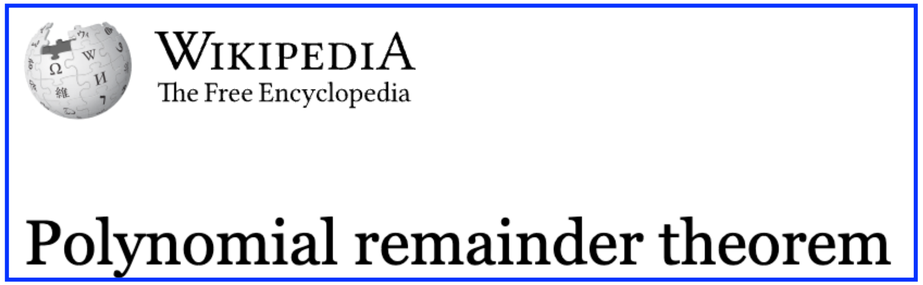
$O(n \log n)$ 3. Compute $c = \text{NTT}^{-1}(\hat{c})$.

- Overall run time: $O(n \log n)$.

NTT definition

- Let $n = 2^k$, and let q be a prime such that $q - 1$ is divisible by $2n$.
  - Dilithium: $n = 256 = 2^8$, $q = 2^{23} - 2^{13} + 1$, and $q - 1 = 2^{13}(2^{10} - 1)$.
- Let $\zeta \in \mathbb{Z}_q^*$ be an element of order $2n$; note that $\zeta^n = -1$.
  - The order of ζ is the smallest positive integer t such that $\zeta^t = 1$.
- Let $a(x) \in R_q$. Then NTT(a) $= \hat{a} = (a(\zeta), a(\zeta^3), a(\zeta^5), \ldots, a(\zeta^{2n-1})) \in \mathbb{Z}_q^n$.
- So, NTT(a) is polynomial evaluation of $a(x)$ at $\zeta, \zeta^3, \zeta^5, \ldots, \zeta^{2n-1}$.
- And, NTT^{-1} is polynomial interpolation.
- Multiplication: Let $a(x), b(x) \in R_q$, and let $c(x) = a(x)b(x) \bmod (x^n + 1)$, say $c(x) = a(x)b(x) + \ell(x)(x^n + 1)$. For odd integers i, we have $c(\zeta^i) = a(\zeta^i)b(\zeta^i) + \ell(\zeta^i)(\zeta^{ni} + 1)$ $= a(\zeta^i)b(\zeta^i)$. Thus, $\hat{c} = \hat{a} \circ \hat{b}$, where $\circ$ is component-wise multiplication in $\mathbb{Z}_q$:
$$\hat{c} = (a(\zeta)b(\zeta),\ a(\zeta^3)b(\zeta^3),\ \ldots\ , a(\zeta^{2n-1})b(\zeta^{2n-1})).$$
- Addition: $\hat{c} = \hat{a} + \hat{b}$, where $+$ is component-wise addition in $\mathbb{Z}_q$.

NTT preliminaries



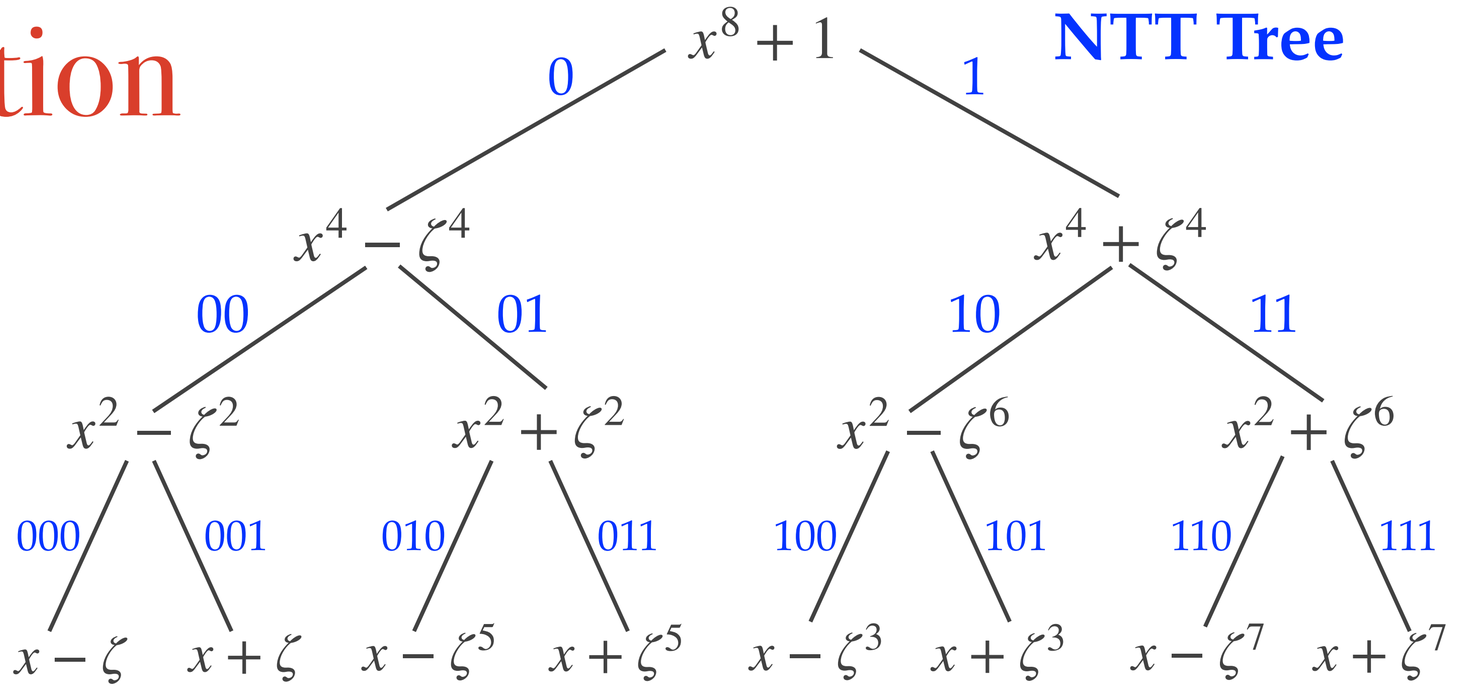
- Recall: $\text{NTT}(a) = (a(\zeta), a(\zeta^3), a(\zeta^5), \ldots, a(\zeta^{2n-1}))$.
- Note that $a(\zeta^i) = a(x) \bmod (x - \zeta^i)$.
- We'll use the following result to recursively compute $a(\zeta^i) = a(x) \bmod (x - \zeta^i)$:
  - If $f(x)$ divides $g(x)$, then $a(x) \bmod f(x) = (a(x) \bmod g(x)) \bmod f(x)$

NTT preliminaries (2)

- For concreteness, we'll take $q = 113$ and $n = 2^3 = 8$, and note that $2n = 16$ divides $q - 1 = 112 = 16 \times 7$. Then $R_q = \mathbb{Z}_{113}[x]/(x^8 + 1)$.
- $\zeta = 42$ has order 16 in $\mathbb{Z}_{113}^*$; hence $\zeta^8 = -1$ in $\mathbb{Z}_{113}^*$.
- Now,

$$\begin{aligned} x^8 + 1 &= x^8 - \zeta^8 \\ &= (x^4 - \zeta^4)(x^4 + \zeta^4) \\ &= (x^4 - \zeta^4)(x^4 - \zeta^{12}) \\ &= (x^2 - \zeta^2)(x^2 + \zeta^2)(x^2 - \zeta^6)(x^2 + \zeta^6) \\ &= (x^2 - \zeta^2)(x^2 - \zeta^{10})(x^2 - \zeta^6)(x^2 - \zeta^{14}) \\ &= (x - \zeta)(x + \zeta)(x - \zeta^5)(x + \zeta^5)(x - \zeta^3)(x + \zeta^3)(x - \zeta^7)(x + \zeta^7) \\ &= (x - \zeta)(x - \zeta^9)(x - \zeta^5)(x - \zeta^{13})(x - \zeta^3)(x - \zeta^{11})(x - \zeta^7)(x - \zeta^{15})\,. \end{aligned}$$

NTT computation



To compute NTT(a):

1. Compute
$a_0 = a \bmod (x^4 - \zeta^4)$,
$a_1 = a \bmod (x^4 + \zeta^4)$.

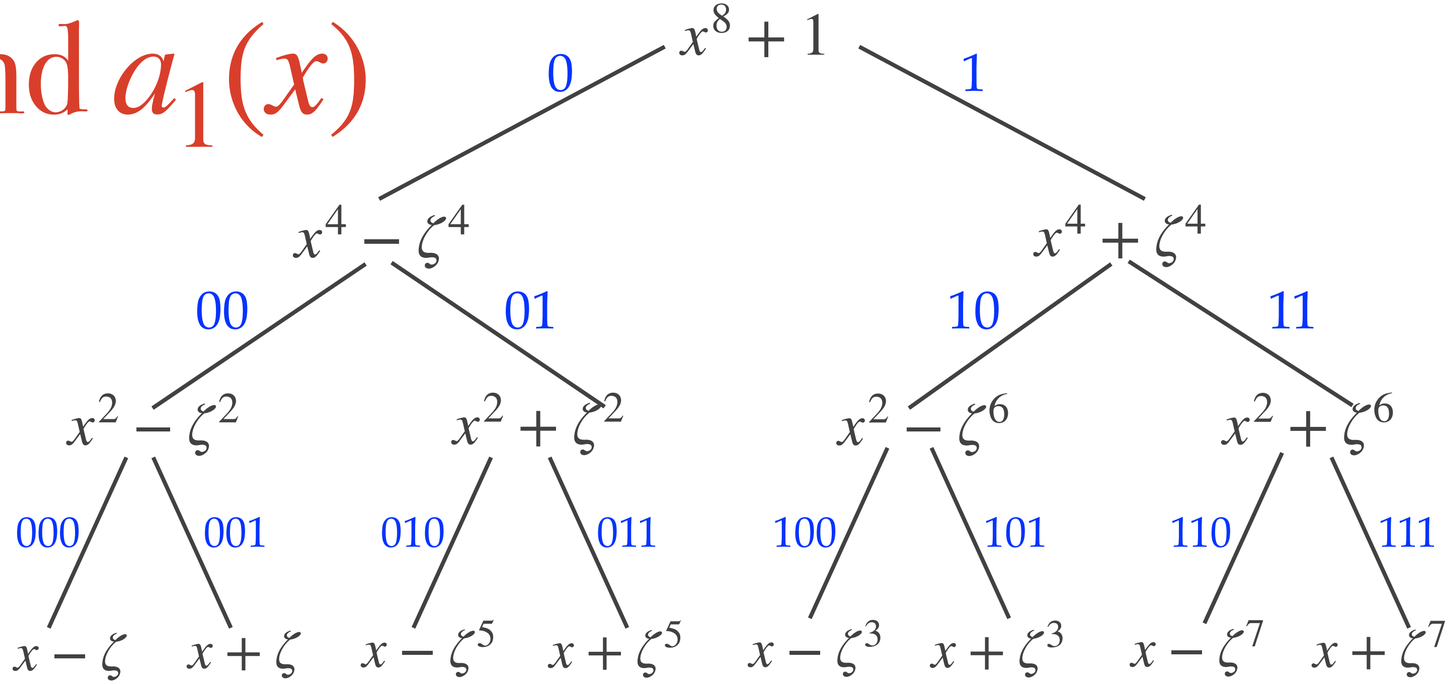
2. Compute
$a_{00} = a_0 \bmod (x^2 - \zeta^2)$,
$a_{01} = a_0 \bmod (x^2 + \zeta^2)$,
$a_{10} = a_1 \bmod (x^2 - \zeta^6)$,
$a_{11} = a_1 \bmod (x^2 + \zeta^6)$.

3. Compute

$a_{000} = a_{00} \bmod (x - \zeta)$, $a_{001} = a_{00} \bmod (x + \zeta)$,
$a_{010} = a_{01} \bmod (x - \zeta^5)$, $a_{011} = a_{01} \bmod (x + \zeta^5)$,
$a_{100} = a_{10} \bmod (x - \zeta^3)$, $a_{101} = a_{10} \bmod (x + \zeta^3)$,
$a_{110} = a_{11} \bmod (x - \zeta^7)$, $a_{111} = a_{11} \bmod (x + \zeta^7)$.

4. Then NTT(a) = $(a_{000}, a_{100}, a_{010}, a_{110}, a_{001}, a_{101}, a_{011}, a_{111})$.

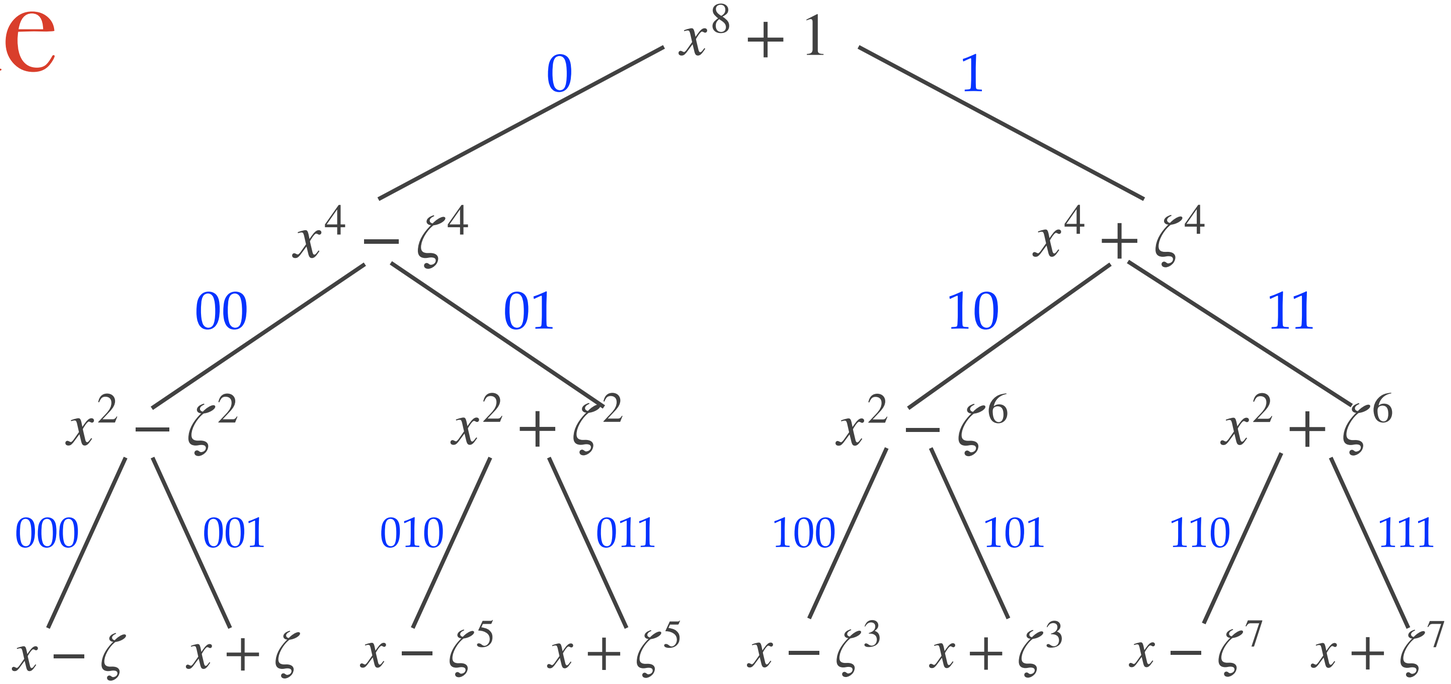
Computing $a_0(x)$ and $a_1(x)$



- Let $a(x) \in R_q$ be a polynomial of degree ≤ 7.
- Write $a(x) = a_L(x) + a_R(x)x^4$, where $a_L(x), a_R(x)$ have degree ≤ 3.
- Then $a_0(x) = a(x) \bmod (x^4 - \zeta^4) = a_L(x) + \zeta^4 a_R(x)$.
- And $a_1(x) = a(x) \bmod (x^4 + \zeta^4) = a_L(x) - \zeta^4 a_R(x)$.
- $a_{00}(x)$ and $a_{01}(x)$ are computed from $a_0(x)$ in a similar manner, as are $a_{10}(x)$ and $a_{11}(x)$ computed from $a_1(x)$.
- And so on…..

NTT running time

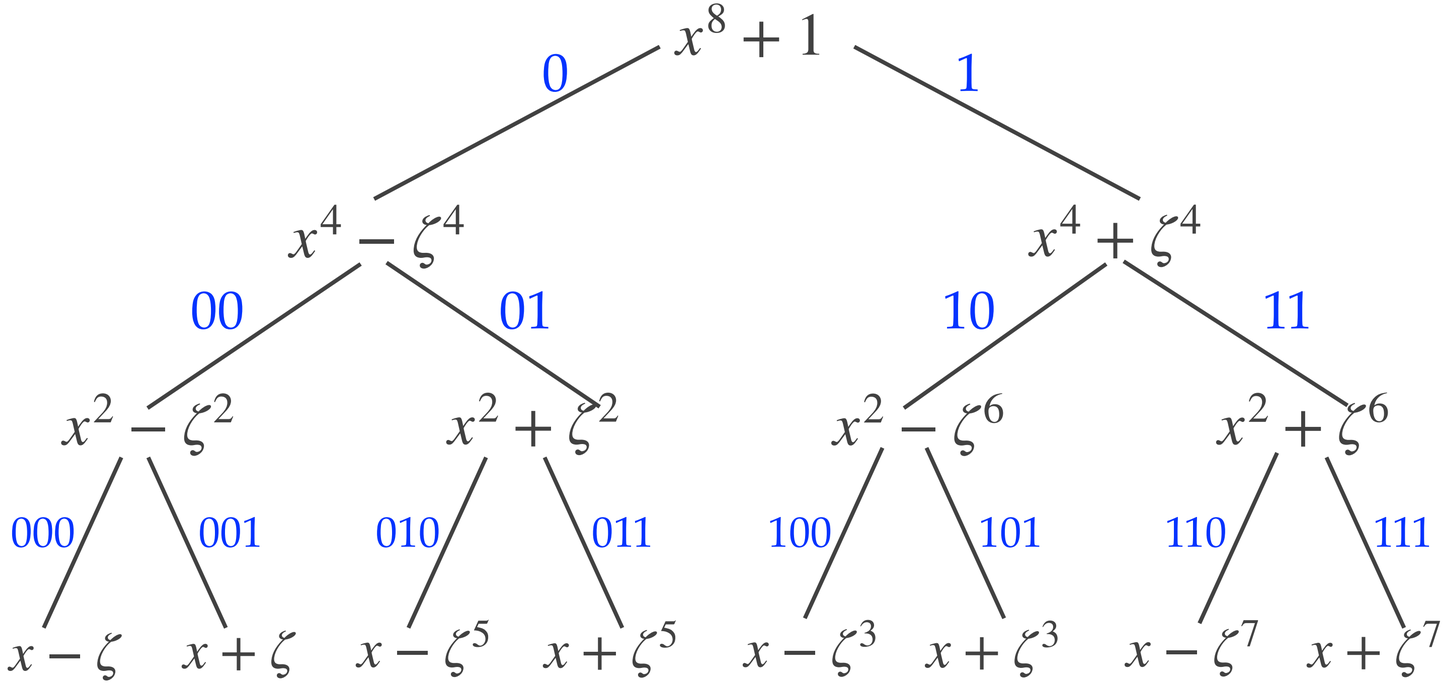
- Suppose $n = 2^k$.
- Let $T(n)$ denote the time to compute NTT(a).
- Then $T(n) = 2T(n/2) + n$.
- Thus, $T(n) = O(n \log n)$.



Compute $a_0(x) = a(x) \bmod (x^4 - \zeta^4) = a_L(x) + \zeta^4 a_R(x)$

Compute $a_1(x) = a(x) \bmod (x^4 + \zeta^4) = a_L(x) - \zeta^4 a_R(x)$

Computing NTT^{-1}



- We'll show how to compute $a(x)$ from $a_0(x)$ and $a_1(x)$.
- Recall that $a_0(x) = a_L(x) + \zeta^4 a_R(x)$ and $a_1(x) = a_L(x) - \zeta^4 a_R(x)$.
- Hence, $a_L(x) = (a_0(x) + a_1(x))/2$ and $a_R(x) = (a_0(x) - a_1(x))/(2\zeta^4)$.
- Then $a(x) = a_L(x) + x^4 a_R(x)$.

- $a_0(x)$ can be compute from $a_{00}(x)$ and $a_{01}(x)$ in a similar manner, as can $a_1(x)$ from $a_{10}(x)$ and $a_{11}(x)$
- This establishes that NTT is an invertible function.
- NTT^{-1} can also be computed in time $O(n \log n)$.

NTT example (1)

- Consider $q = 113$, $n = 2^3 = 8$ (so $R_q = \mathbb{Z}_{113}[x]/(x^8 + 1)$), and $\zeta = 42$.
- Let $a(x) = 99 + 52x + 7x^3 + 29x^5 + 33x^6 + 100x^7 \in R_q$, and
  $b(x) = 6 + 45x^2 + 12x^3 + 14x^4 + 78x^5 + 65x^6 + 112x^7 \in R_q$.
- We wish to compute $c(x) = a(x)b(x) \bmod (x^8 + 1)$.
- Let's first compute $\hat{a} = \text{NTT}(a)$.
  - We have $a_L(X) = 99 + 52x + 7x^3$ and $a_R(x) = 29x + 33x^2 + 100x^3$.
  - So, $a_0(x) = a_L(x) + \zeta^4 a_R(x) = 99 + 35x + 43x^2 + 38x^3$ and
    $a_1(x) = a_L(x) - \zeta^4 a_R(x) = 99 + 69x + 70x^2 + 89x^3$.

NTT example (2)

- Furthermore, $a_{00}(x) = 15 + 58x$, $a_{01}(x) = 70 + 12x$, $a_{10}(x) = 3 + 89x$, and $a_{11}(x) = 82 + 49x$.
- And $a_{000} = 78$, $a_{001} = 65$, $a_{010} = 59$, $a_{011} = 81$, $a_{100} = 59$, $a_{101} = 60$, $a_{110} = 62$, $a_{111} = 102$.
- Thus, $\text{NTT}(a) = (78, 59, 59, 62, 65, 60, 81, 102)$.

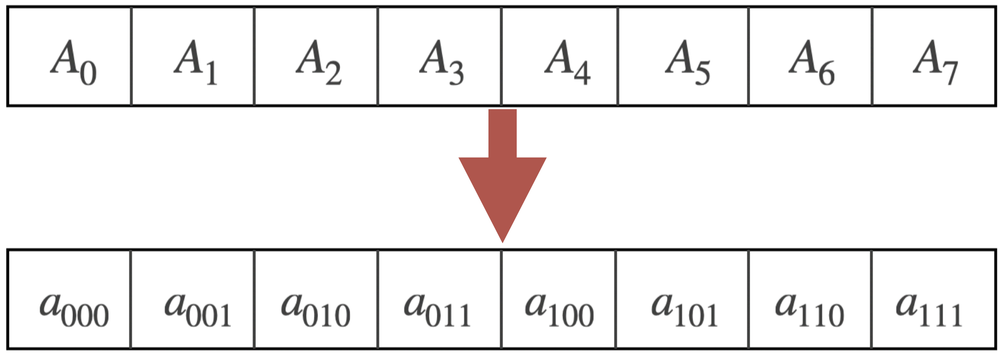
- Similarly, $\text{NTT}(b) = (76, 20, 18, 29, 92, 105, 0, 47)$.
- Then $\hat{c} = \text{NTT}(c) = \text{NTT}(a) \circ \text{NTT}(b) = (52, 50, 45, 103, 104, 85, 0, 48)$.
- Finally, $c(x) = \text{NTT}^{-1}(\hat{c}) = 75 + 92x + 86x^2 + 84x^3 + 4x^4 + 99x^5 + 25x^6 + 86x^7$.

Dilithium NTT

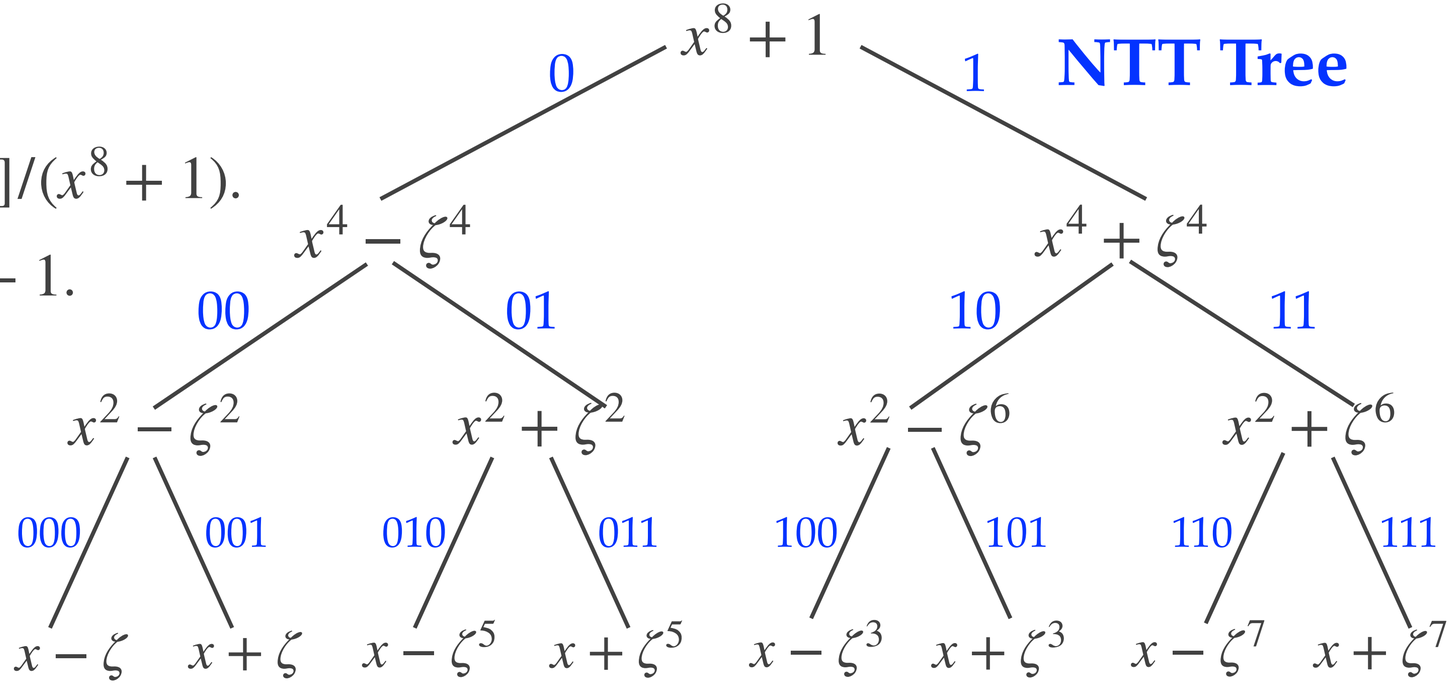
- Used in DL-DSA-44, DL-DSA-65 and DL-DSA-87.
- $q = 2^{23} - 2^{13} + 1$, $n = 2^8 = 256$, $\zeta = 1753$ has order $2n = 512$ in $\mathbb{Z}_q^*$.
- To avoid the permutation after the last step, the Dilithium NTT is defined slightly differently.
- Bit reversal: For integer $v \in [0,255]$, let $\text{brv}(v)$ denote the 8-bit integer obtained by reversing the 8-bit binary representation of v.
  - Example: $\text{brv}(143) = \text{brv}((10001111)_2) = (11110001)_2 = 241$.
- Definition: Let $a \in R_q$ and let $\zeta_i = \zeta^{\text{brv}(128+i)} \bmod q$ for $0 \le i \le 127$. Then $\text{NTT}(a) = (a(\zeta_0), a(-\zeta_0), a(\zeta_1), a(-\zeta_1), \ \ldots, a(\zeta_{127}), a(-\zeta_{127})) \in \mathbb{Z}_q^{256}$.
- Note: $\text{NTT}(a) = (a(\zeta), a(\zeta^{257}), a(\zeta^{129}), a(\zeta^{385}), a(\zeta^{65}), a(\zeta^{321}), \ \ldots \ , a(\zeta^{255}), a(\zeta^{511}))$.
- This facilitates the computation of NTT and NTT^{-1} "in place".

In-place computation of the Dilithium NTT

- Consider $q = 113,\ n = 8,\ R_q = \mathbb{Z}_{113}[x]/(x^8 + 1)$.
- $\zeta = 42$ has order 16 in $\mathbb{Z}_{113}^*$, and $\zeta^8 = -1$.
- Let $A = A_0 + A_1 x + \cdots + A_7 x^7 \in R_q$.
- We want to compute NTT(A).



- Then NTT(A) $= (a_{000}, a_{001}, a_{010}, a_{011}, a_{100}, a_{101}, a_{110}, a_{111})$.



i	brv(4+i)
0	1
1	5
2	3
3	7

Using NTT in Dilithium key generation

- Recall: $q = 2^{23} - 2^{12} + 1$ and $n = 256$.
- Recall key generation:
  $A_R \in R_q^{k \times \ell}$ is obtained using ExpandA(ρ), $s_1 \in_R S_\eta^\ell$, $s_2 \in_R S_\eta^k$, $t = As_1 + s_2$.
- NTT can be extended to R_q^ℓ, R_q^k, and $R_q^{k \times \ell}$ (by applying NTT to each polynomial).
- To avoid many applications of NTT and NTT^{-1} when computing As_1, A is generated in NTT form and used in key generation as follows:
  1. Compute $\hat{A} = \text{ExpandA}(\rho)$.
     (Each entry in $\hat{A}$ is selected uniformly at random from $\mathbb{Z}_q^{256}$.)
  2. Select $s_1 \in_R S_\eta^\ell$ and $s_2 \in_R S_\eta^k$, and compute $\hat{s}_1 = \text{NTT}(s_1)$.
  3. Compute $\hat{b} = \hat{A} \circ \hat{s}_1$ and $b = \text{NTT}^{-1}(\hat{b})$.
  4. Compute $t = b + s_2$.
- NTT and NTT^{-1} are also used in *signature generation* and *signature verification*.

Using NTT in Dilithium signature generation

- The dominant computation in signature generation is the computation of $w = Ay$, where $A \in R_q^{k \times \ell}$ and $y \in \tilde{S}_{\gamma_1}^{\ell}$.
- Let's consider the ML-DSA-87 parameters, with $(k, \ell) = (8,7)$.
- Without NTT: Computing Ay requires $k\ell$ polynomial mults, each requiring n^2 $\mathbb{Z}_q$-mults (where $n = 256$), for a total of $\approx 2^{22}$ $\mathbb{Z}_q$-mults.
- With NTT: Recall that public key $\hat{A}$ is generated in NTT form.
  So, to compute $w = Ay$, one first computes $\hat{y} = \text{NTT}(y)$, then $\hat{w} = \hat{A}\hat{y}$, and finally $w = \text{NTT}^{-1}(\hat{w})$. The NTT and NTT^{-1}operations each require $\ell \times n \log n$ $\mathbb{Z}_q$-mults, and computing $\hat{A}\hat{y}$ requires $k\ell n$ $\mathbb{Z}_q$-mults, for a total of $\approx 2^{15}$ $\mathbb{Z}_q$ mults, *a factor-128 speed-up*.

V4b: Kyber NTT

1. Mathematical preliminaries
2. NTT definition
3. NTT computation
4. Example
5. Kyber NTT

NTT outline

- The Number-Theoretic Transform is a function $\text{NTT} : R_q \longrightarrow T_q$.
- The function is invertible, with inverse function $\text{NTT}^{-1} : T_q \longrightarrow R_q$.
  - For all $a \in R_q$, $\text{NTT}^{-1}(\text{NTT}(a)) = a$.
- To compute $c(x) = a(x)b(x) \bmod (x^n + 1)$ where $a(x), b(x) \in R_q$:
  1. Compute $\hat{a} = \text{NTT}(a)$ and $\hat{b} = \text{NTT}(b)$.
  2. Compute $\hat{c} = \hat{a} \circ \hat{b}$ (component-wise multiplication in Q_i).
  3. Compute $c = \text{NTT}^{-1}(\hat{c})$.
- Overall run time: $O(n \log n)$.

Mathematical preliminaries

- Let $n = 2^k$, and let q be a prime such that $q - 1$ is divisible by n and $q - 1$ isn't divisible by $2n$.
  - Kyber: $n = 256 = 2^8$, $q = 3329$, and $q - 1 = 2^8 \times 13$.
- Let $\zeta \in \mathbb{Z}_q^*$ be an element of order n; note that $\zeta^{n/2} = -1$.
  - The order of ζ is the smallest positive integer t such that $\zeta^t = 1$.
- Claim: For odd integers $i \in [1, n-1]$, the polynomial $x^2 - \zeta^i$ is irreducible over $\mathbb{Z}_q$.
  Proof: If the polynomial $x^2 - \zeta^i$ were reducible over $\mathbb{Z}_q$, then it would have a root $c \in \mathbb{Z}_q$. Hence, $c^2 - \zeta^i = 0$, so $c^2 = \zeta^i$. Now, $(c^2)^n = (\zeta^i)^n = (\zeta^n)^i = 1$, so the order of c divides $2n$. However, $c^n = (c^2)^{n/2} = (\zeta^i)^{n/2} = (\zeta^{n/2})^i = (-1)^i = -1$ so the order of c doesn't divide n. Hence c has order $2n$, which is impossible since $2n$ doesn't divide $q - 1$. $\square$

NTT definition

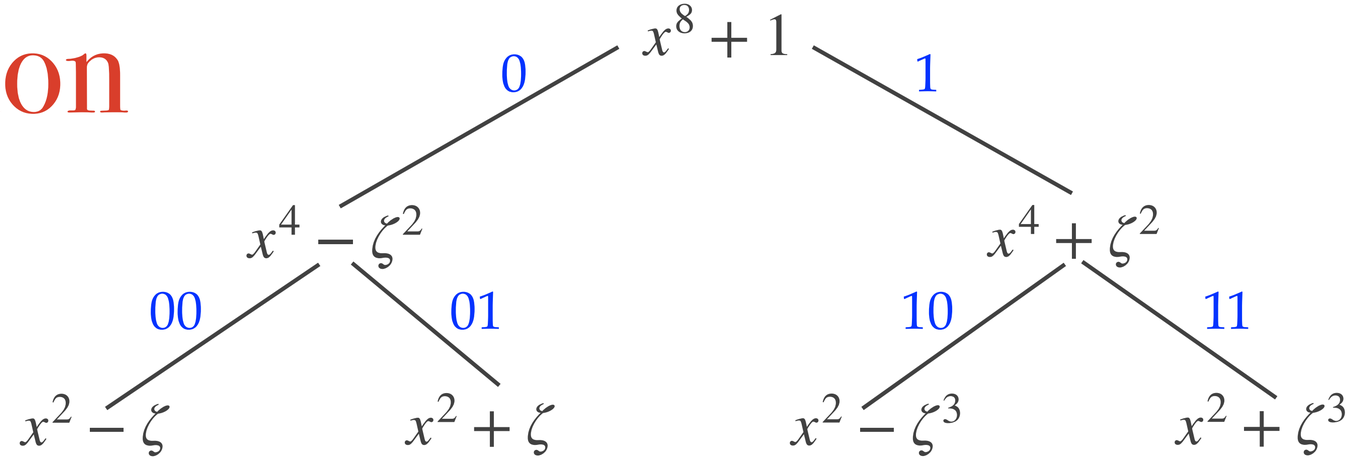
- Let $n = 2^k$, and let q be a prime such that $q - 1$ is divisible by n and $q - 1$ isn't divisible by $2n$. Let $\zeta \in \mathbb{Z}_q^*$ be an element of order n.
- For odd $i \in [1, n-1]$, define $Q_i = \mathbb{Z}_q[x]/(x^2 - \zeta^i)$.
  - Q_i is the *quadratic ring* of polynomials of degree ≤ 1 in $\mathbb{Z}_q[x]$, with multiplication performed modulo $x^2 - \zeta^i$. A polynomial $c_0 + c_1 x$ in Q_i is represented by its coefficients $(c_0, c_1) \in \mathbb{Z}_q^2$.
- Let $T_q = Q_1 \times Q_3 \times \cdots \times Q_{n-1}$. The Number-Theoretic Transform is the function NTT : $R_q \longrightarrow T_q$ defined by $\text{NTT}(a) = (a \bmod (x^2 - \zeta),\ a \bmod (x^2 - \zeta^3),\ \ldots,\ a \bmod (x^2 - \zeta^{n-1}))$.
  We'll write $\hat{a} = \text{NTT}(a)$.
- Fact: NTT is a ring isomorphism and, in particular, is invertible.
- Addition: If $a(x), b(x) \in R_q$ and $c(x) = a(x) + b(x)$, then $\hat{c} = \hat{a} + \hat{b}$ where $+$ is component-wise addition in Q_i.
- Multiplication: If $a(x), b(x) \in R_q$ and $c(x) = a(x)b(x) \bmod (x^n + 1)$, say $c(x) = a(x)b(x) + \ell(x)(x^n + 1)$, then $c(x) \bmod (x^2 - \zeta^i) = a(x)b(x) \bmod (x^2 - \zeta^i)$ since $(\zeta^i)^{n/2} = (\zeta^{n/2})^i = (-1)^i = -1$.
  Thus, $\hat{c} = \hat{a} \circ \hat{b}$, where $\circ$ is component-wise multiplication in Q_i.

NTT preliminaries

- For concreteness, let's take $q = 137$ and $n = 2^3 = 8$, and note that $n = 8$ divides $q - 1 = 136 = 8 \times 17$, and $2n = 16$ doesn't. Then $R_q = \mathbb{Z}_{137}[x]/(x^8 + 1)$.
- $\zeta = 10$ has order 8 in $\mathbb{Z}^*_{137}$, so $\zeta^4 = -1$ in $\mathbb{Z}^*_{137}$.
- NTT : $R_q \longrightarrow T_q$, where $T_q = Q_1 \times Q_3 \times Q_5 \times Q_7$ and $Q_i = \mathbb{Z}_q[x]/(x^2 - \zeta^i)$.
- We have,

$$\begin{aligned} x^8 + 1 &= x^8 - \zeta^4 \\ &= (x^4 - \zeta^2)(x^4 + \zeta^2) \\ &= (x^4 - \zeta^2)(x^4 - \zeta^6) \\ &= (x^2 - \zeta)(x^2 + \zeta)(x^2 - \zeta^3)(x^2 + \zeta^3) \\ &= (x^2 - \zeta)(x^2 - \zeta^5)(x^2 - \zeta^3)(x^2 - \zeta^7)\,. \end{aligned}$$

NTT computation



To compute NTT(a):

1. Compute $a_0 = a \bmod (x^4 - \zeta^2)$ and $a_1 = a \bmod (x^4 + \zeta^2)$.

2. Compute $a_{00} = a_0 \bmod (x^2 - \zeta)$, $a_{01} = a_0 \bmod (x^2 + \zeta)$,
   $a_{10} = a_1 \bmod (x^2 - \zeta^3)$ and $a_{11} = a_1 \bmod (x^2 + \zeta^3)$.

3. Then NTT(a) $= (a_{00}, a_{10}, a_{01}, a_{11})$.

Addition and multiplication in Q_i

- Recall: $T_q = Q_1 \times Q_3 \times \cdots \times Q_{n-1}$, where $Q_i = \mathbb{Z}_q[x]/(x^2 - \zeta^i)$.
- Addition and multiplication in T_q is component-wise (in the Q_i).
- Addition in Q_i:

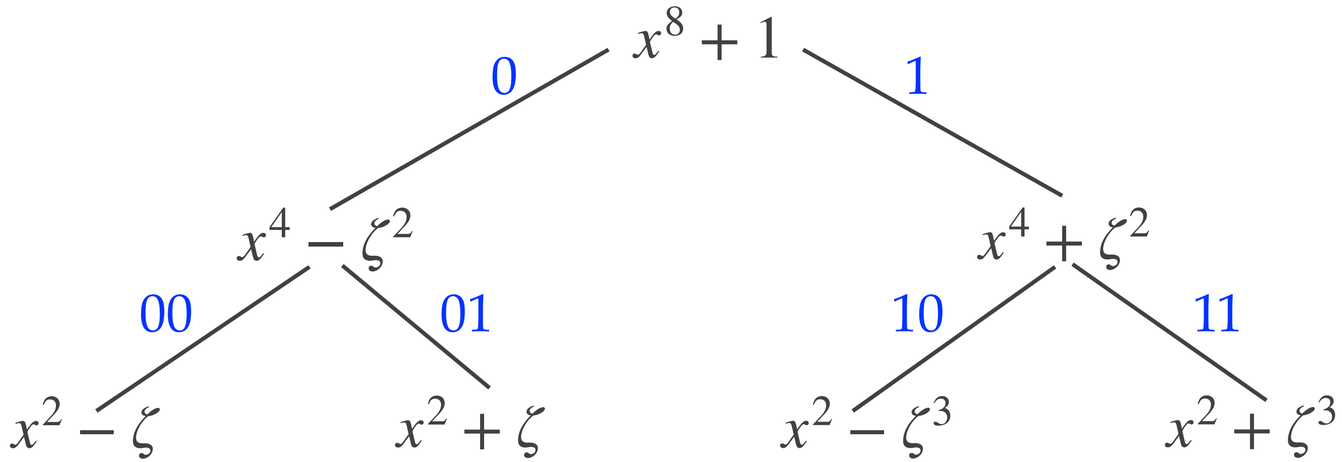
$$(a_0 + a_1 x) + (b_0 + b_1 x) = (a_0 + b_0) + (a_1 + b_1)x.$$

- Multiplication in Q_i:

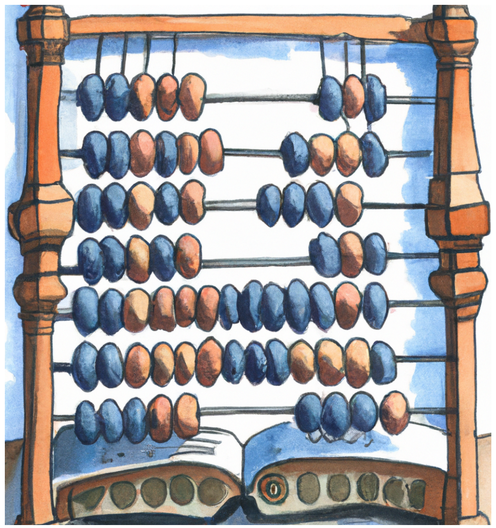
$$\begin{aligned}(a_0 + a_1 x) \cdot (b_0 + b_1 x) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2 \\ &= (a_0 b_0 + a_1 b_1 \zeta^i) + (a_0 b_1 + a_1 b_0)x\,.\end{aligned}$$

NTT running time

- Suppose $n = 2^k$.
- Let $T(n)$ denote the time to compute NTT(a).
- Then $T(n) = 2T(n/2) + n$, whence $T(n) = O(n \log n)$.
- NTT^{-1} can also be computed in time $O(n \log n)$.



NTT example (1)



- Consider $q = 137$ and $n = 2^3 = 8$ (so $R_q = \mathbb{Z}_{137}[x]/(x^8 + 1)$).
- Note that $q - 1 = 2^3 \times 17$, so n divides $q - 1$ but $2n$ doesn't.
- Set $\zeta = 10$, an element of order 8 in $\mathbb{Z}^*_{137}$.
- Let $a(x) = 99 + 52x + 7x^3 + 29x^5 + 33x^6 + 100x^7 \in R_q$ and
  $b(x) = 6 + 45x^2 + 12x^3 + 14x^4 + 78x^5 + 65x^6 + 112x^7 \in R_q$.
- We wish to compute $c(x) = a(x)b(x) \bmod (x^8 + 1)$.

NTT example (2)

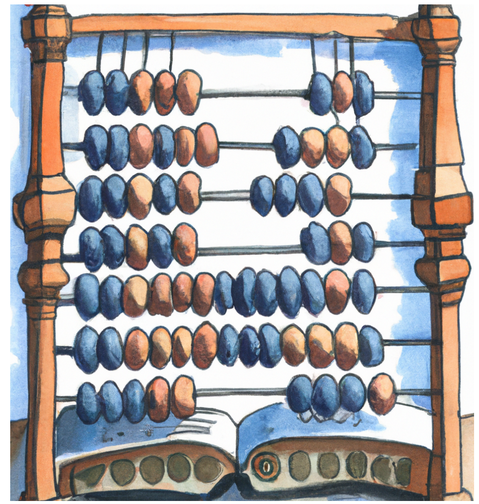
- Let's first compute $\hat{a} = \text{NTT}(a)$. $(a(x) = 99 + 52x + 7x^3 + 29x^5 + 33x^6 + 100x^7)$
- Write $a(x) = a_L(x) + a_R(x)x^4$.
- We have $a_L(x) = 99 + 52x + 7x^3$ and $a_R(x) = 29x + 33x^2 + 100x^3$.
- So, $a_0(x) = a(x) \bmod (x^4 - \zeta^2)$

$$= a_L(x) + \zeta^2 a_R(x) = 99 + 75x + 12x^2 + 6x^3 .$$

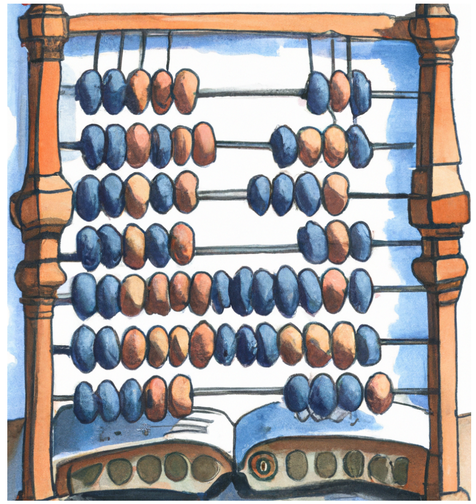
- And $a_1(x) = a(x) \bmod (x^4 + \zeta^2)$

$$= a_L(x) - \zeta^2 a_R(x) = 99 + 29x + 125x^2 + 8x^3 .$$

- Furthermore, $a_{00}(x) = 82 + 135x$, $a_{01}(x) = 116 + 15x$, $a_{10}(x) = 18 + 83x$, and $a_{11}(x) = 43 + 112x$.
- Thus, $\hat{a} = \text{NTT}(a) = (82 + 135x, 18 + 83x, 116 + 15x, 43 + 112x)$.



NTT example (3)



- $\text{NTT}(a) = (82 + 135x, 18 + 83x, 116 + 15x, 43 + 112x)$
- Similarly, $\hat{b} = \text{NTT}(b) = (45x, 5 + 114x, 72 + 74x, 84 + 41x)$.

- Then $\hat{c} = \text{NTT}(c) = \text{NTT}(a) \circ \text{NTT}(b)$
  $= (59 + 128x, 48 + x, 129 + 74x, 16 + 74x)$.
  - For example, the product of the first components of $\hat{a}$ and $\hat{b}$ is $(82 + 135x) \times 45x$. This product is in $Q_1 = \mathbb{Z}_{137}[x]/(x^2 - 10)$.
  - The product is $(82 \times 45)x + (135 \times 45)x^2 = 128x + 47x^2 = 59 + 128x$.

- Finally, $c(x) = \text{NTT}^{-1}(\hat{c})$
  $= 63 + 35x + 21x^2 + 40x^3 + 51x^4 + 113x^5 + 121x^6 + 31x^7$.

Kyber NTT

- Used in ML-KEM-512, ML-KEM-768 and ML-KEM-1024.
- $q = 3329$, $n = 2^8 = 256$, $\zeta = 17$ has order $n = 256$ in $\mathbb{Z}_q^*$.
- Bit reversal: For integer $v \in [0,127]$, let BitRev(v) denote the 7-bit integer obtained by reversing the 7-bit binary representation of v.
  - Example: $\text{BitRev}(103) = \text{BitRev}((1100111)_2) = (1110011)_2 = 115$.
- Definition: Let $a \in R_q$ and let $\zeta_i = \zeta^{2\text{BitRev}(i)+1} \bmod q$ for $0 \le i \le 127$.
  Let $Q_i = \mathbb{Z}_q[x]/(x^2 - \zeta_i)$, and $T_q = Q_0 \times Q_1 \times Q_2 \times \cdots \times Q_{127}$.
  Then NTT : $R_q \longrightarrow T_q$ is defined by
  $\text{NTT}(a) = (a \bmod (x^2 - \zeta_0), a \bmod (x^2 - \zeta_1), \ldots, a \bmod (x^2 - \zeta_{127}))$.

Computing the Kyber NTT

- The Kyber NTT and NTT^{-1} can be computed "in place" in a length-256 array whose entries are integers modulo 3329.

Algorithm 9 NTT(f)

Computes the NTT representation $\hat{f}$ of the given polynomial $f \in R_q$.

Input: array $f \in \mathbb{Z}_q^{256}$. ▷ the coefficients of the input polynomial

Output: array $\hat{f} \in \mathbb{Z}_q^{256}$. ▷ the coefficients of the NTT of the input polynomial

1: $\hat{f} \leftarrow f$ ▷ will compute in place on a copy of input array
2: $i \leftarrow 1$
3: **for** ($len \leftarrow 128$; $len \geq 2$; $len \leftarrow len/2$)
4: **for** ($start \leftarrow 0$; $start < 256$; $start \leftarrow start + 2 \cdot len$)
5: $zeta \leftarrow \zeta^{\text{BitRev}_7(i)} \bmod q$
6: $i \leftarrow i + 1$
7: **for** ($j \leftarrow start$; $j < start + len$; j++)
8: $t \leftarrow zeta \cdot \hat{f}[j + len]$ ▷ steps 8-10 done modulo q
9: $\hat{f}[j + len] \leftarrow \hat{f}[j] - t$
10: $\hat{f}[j] \leftarrow \hat{f}[j] + t$
11: **end for**
12: **end for**
13: **end for**
14: **return** $\hat{f}$

Using NTT in Kyber key generation

- Recall: $q = 3329$ and $n = 256$.
- Recall key generation:
  $A \in R_q^{k \times \ell}$ is obtained using Expand(ρ), $s \in_{CBD} S_{\eta_1}^k$, $e \in_{CBD} S_{\eta_2}^k$, $t = As + e$.
- NTT can be extended to R_q^k, and $R_q^{k \times \ell}$ (by applying NTT to each polynomial).
- To avoid many applications of NTT and NTT^{-1} when computing As, A is generated in NTT form and used in key generation as follows:
  1. Compute $\hat{A} = \text{ExpandA}(\rho)$.
     (Each entry in $\hat{A}$ is selected uniformly at random from T_q.)
  2. Select $s \in_{CBD} S_{\eta_1}^k$ and $e \in_{CBD} S_{\eta_2}^k$, and compute $\hat{s} = \text{NTT}(s)$ and $\hat{e} = \text{NTT}(e)$.
  3. Compute $\hat{t} = \hat{A} \circ \hat{s} + \hat{e}$.
  4. Alice's public key is $(\hat{A}, \hat{t})$; her private key is $\hat{s}$.
- NTT and NTT^{-1} are also used in *encryption* and *decryption*.

