Number Theoretic Transforms in ML DSA

Jan-2026

Efficient Implementation of Polynomial Arithmetic

Number Theoretic Transforms (NTTs) are integral to the ML DSA specification. The NTT representation enables efficient polynomial addition, subtraction, and multiplication. In this section, we develop all the key ideas behind NTTs in a step-by-step fashion. To illustrate these concepts, we define *Tiny DSA*, a simplified system that follows the ML-DSA structure. This development draws heavily from Prof. Alfred Menezes' excellent notes and videos.

Polynomial Reduction

Let $a(x) \in R_q$ be a polynomial of degree ≤ 31.

$$a(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{15} x^{15} + a_{16} x^{16} + ... + a_{30} x^{30} + a_{31} x^{31} \in R_q$$

We can reorganize the terms in $a(x)$ into two distinct polynomials. The first polynomial, $a_L(x)$, contains terms with degree $0 \leq d \leq 15$:

$$\mathbf{a_L(x)} = a_0 + a_1 x + a_2 x^2 + ... + a_{14} x^{14} + a_{15} x^{15} \in R_q$$

The second polynomial, $a_r(x)$ has terms with degree $16 \leq d \leq 31$:

$$\begin{array}{rcl} a_r(x) & = & a_{16} x^{16} + a_{17} x^{17} + a_{18} x^{18} + ... + a_{31} x^{31} \\ & = & (a_{16} + a_{17} x + a_{18} x^2 + ... + a_{30} x^{14} + a_{31} x^{15}) x^{16} \\ & = & \mathbf{a_R(x)} x^{16} \ \ \textit{where } \mathbf{a_R(x)} = (a_{16} + a_{17} x + ... + a_{30} x^{14} + a_{31} x^{15}) \in R_q \end{array}$$

In general, for any $a(x) \in R_q$, we can write

$$a(x) = a_L(x) + a_R(x) x^{16} \ \ \textit{where } a_L(x) \textit{ and } a_R(x) \textit{ have degree} \leq 15.$$

We use this method to decompose a polynomial $a(x) \in R_q$ of degree $2d + 1$ into two sub-polynomials each of degree d. Once the polynomial is in this form, notice that

$$\begin{array}{rcl} a(x) \bmod (x^{32} + 1) & = & (a_L(x) + a_R(x) x^{16}) \bmod (x^{32} + 1). \\ & = & a_L(x) + a_R(x) x^{16} \bmod (x^{32} - \zeta^{32}). \\ & = & a_L(x) + a_R(x) x^{16} \bmod (x^{16} - \zeta^{16})(x^{16} + \zeta^{16}). \end{array}$$

We stop reducing when we reach factors of degree 1.

Tiny DSA - Factoring the Reduction Polynomial $x^{32} + 1$

In this section we derive the irreducible factors of the reduction polynomial $x^{32} + 1$.

The first interesting fact to notice is the following equivalence under the polynomial ring R_q

$$\begin{aligned} x^{32} + 1 &= x^{32} + \boxed{\zeta^0} \\ &= x^{32} \boxed{-\zeta^{32+0}} \\ &= x^{32} - \zeta^{32} \end{aligned}$$

In general, we replace a term of the form

$$x^m + \zeta^n \in R_q \qquad m \geq 1, n \geq 0$$

by

$$x^m - \zeta^{32+n}$$

and break this down further till we reach an irreducible term of degree 1, $x \pm z^k \;\; 1 \leq k \leq 63$. In Tiny DSA, we obtain 32 irreducible terms

$$\begin{aligned} &x \pm z^k \quad k = 2i + 1,\; 0 \leq i \leq 15. \\ &\qquad \text{In other words, } k \in \{1, 3, 5, 7, 9, \ldots, 23, 25, 27, 29, 31\}. \end{aligned}$$

In ML DSA, there are 256 irreducible factors of degree 1:

$$\begin{aligned} &x \pm z^k \quad k = 2i + 1,\; 0 \leq i \leq 127. \\ &\qquad \text{In other words, } k \in \{1, 3, 5, 7, 9, \ldots, 23, 25, 27, 29, 31\}. \end{aligned}$$

Reducing Polynomial $a(x)$ by the factors of $x^{32} - \zeta^{32}$

This is the first (level 1) reduction of the given polynomial $a(x)$.

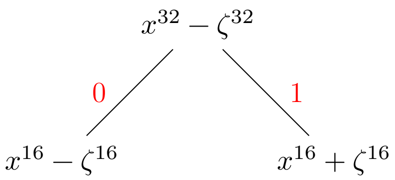


Figure 1: Step 1 of Polynomial Factoring

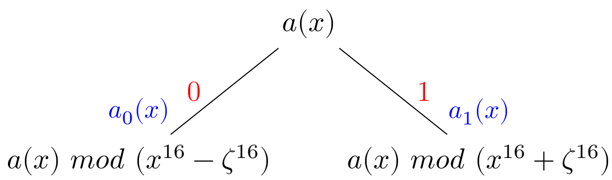


Figure 2: Step 1 of NTT Evaluation

$$\begin{aligned} a_0(x) &= a(x) \bmod (x^{16} - \zeta^{16}) \\ &= (a_L(x) + a_R(x)\, x^{16}) \bmod (x^{16} - \zeta^{16}) \\ &= a_l(x) + a_R(x)\, \zeta^{16} \qquad \textit{(polynomial remainder theorem)} \end{aligned}$$

$$\begin{aligned} a_1(x) &= a(x) \bmod (x^{16} + \zeta^{16}) \\ &= (a_L(x) + a_R(x)\, x^{16}) \bmod (x^{16} + \zeta^{16}) \\ &= (a_L(x) + a_R(x)\, x^{16}) \bmod (x^{16} - (-\zeta^{16})) \\ &= a_l(x) + a_R(x) \cdot (-\zeta^{16}) \qquad \textit{(polynomial remainder theorem)} \\ &= a_l(x) - a_R(x)\, \zeta^{16} \end{aligned}$$

Level 2 - Factors of $x^{16} - \zeta^{16}$ and $x^{16} - \zeta^{48}$

We will now factor the smaller-degree polynomials obtained in the previous step:

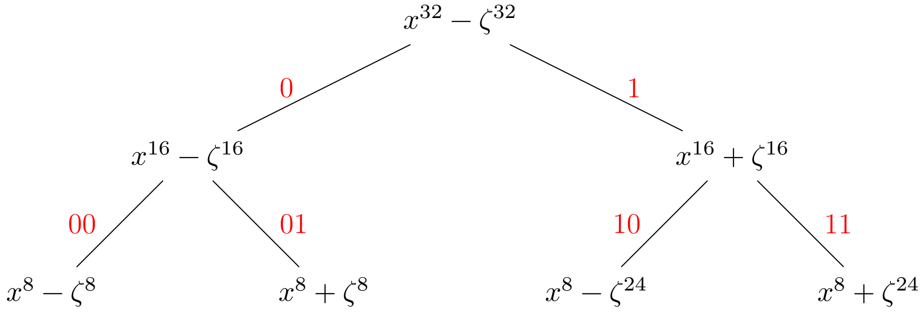


Figure 3: Step 2 of Polynomial Factoring

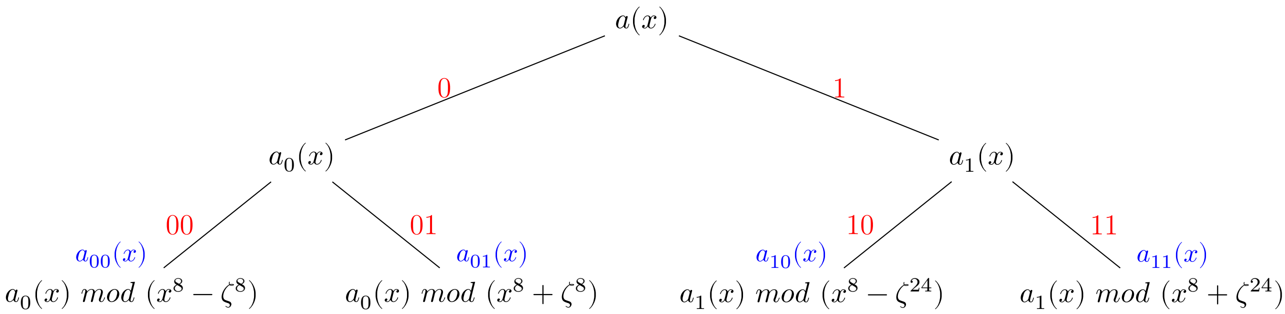


Figure 4: Step 2 of NTT Evaluation

Level 3 - Factors of $x^8 \pm \zeta^8$ and $x^8 \pm \zeta^{24}$

We use the equalities $x^8 + \zeta^8 = x^8 - \zeta^{40}$ and $x^8 + \zeta^{24} = x^8 - \zeta^{56}$ in evaluating the NTT of polynomial $a(x)$.

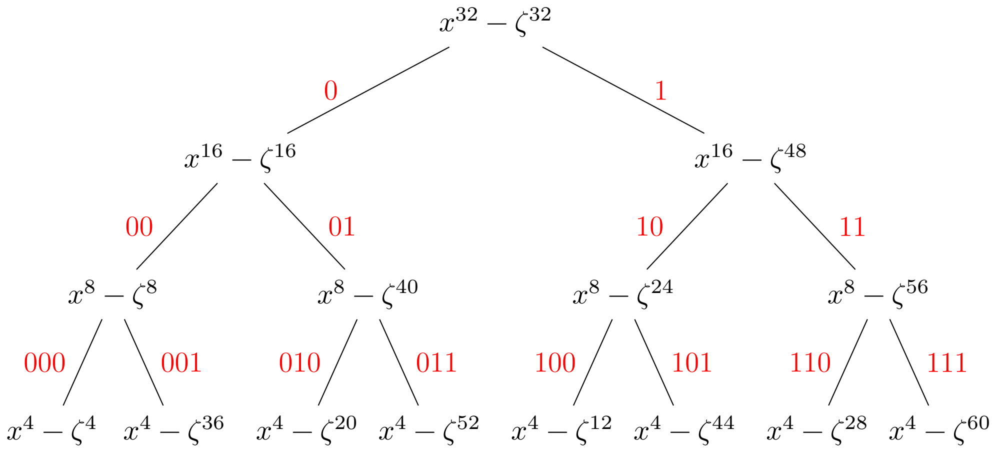


Figure 5: Step 3 of Polynomial Factoring

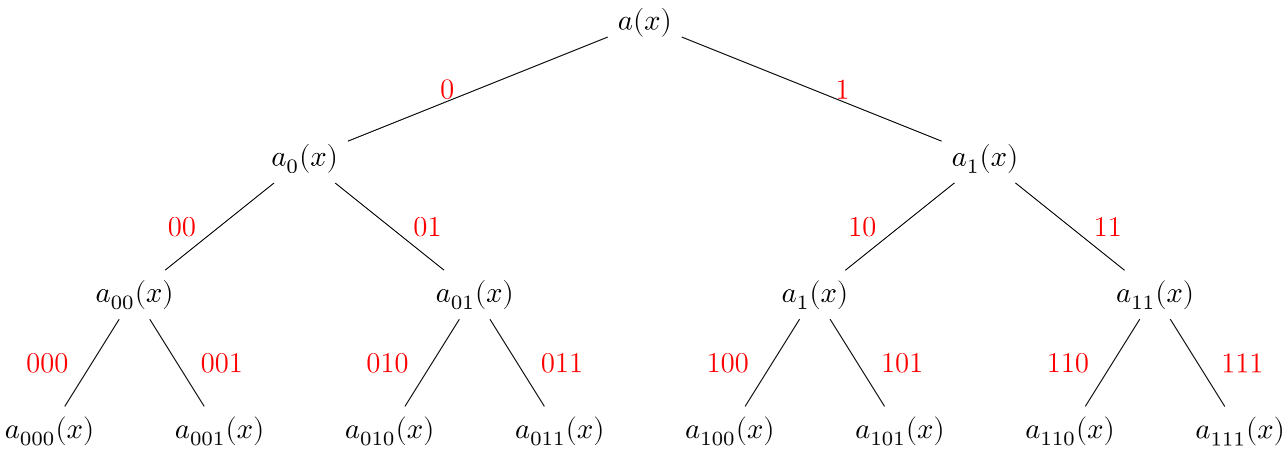
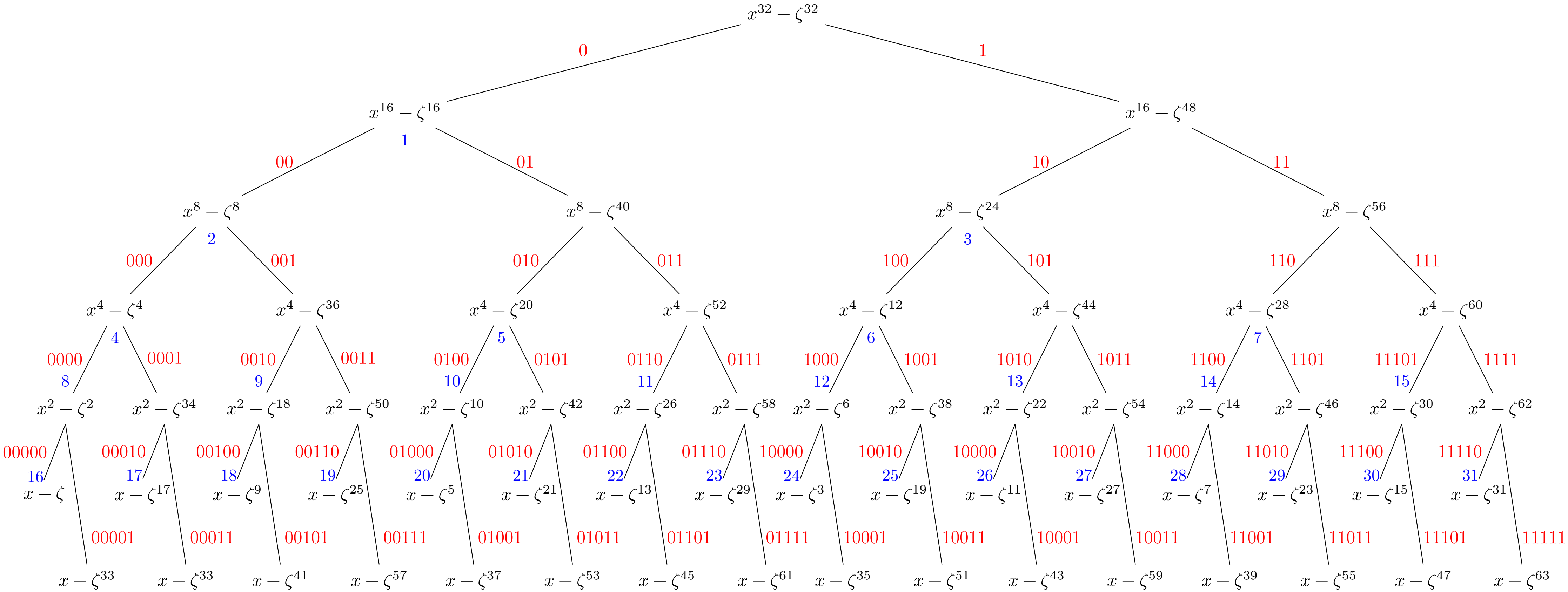


Figure 6: Step 3 of NTT Evaluation

Level 4


$x^{32} - \zeta^{32}$
0
1
$x^{16} - \zeta^{16}$
1
$x^{16} - \zeta^{48}$
00
01
10
11
$x^8 - \zeta^8$
2
$x^8 - \zeta^{40}$
$x^8 - \zeta^{24}$
3
$x^8 - \zeta^{56}$
000
001
010
011
100
101
110
111
$x^4 - \zeta^4$
4
$x^4 - \zeta^{36}$
$x^4 - \zeta^{20}$
5
$x^4 - \zeta^{52}$
$x^4 - \zeta^{12}$
6
$x^4 - \zeta^{44}$
$x^4 - \zeta^{28}$
7
$x^4 - \zeta^{60}$
0000
8
0001
0010
9
0011
0100
10
0101
0110
11
0111
1000
12
1001
1010
13
1011
1100
14
1101
11101
15
1111
$x^2 - \zeta^2$
$x^2 - \zeta^{34}$
$x^2 - \zeta^{18}$
$x^2 - \zeta^{50}$
$x^2 - \zeta^{10}$
$x^2 - \zeta^{42}$
$x^2 - \zeta^{26}$
$x^2 - \zeta^{58}$
$x^2 - \zeta^6$
$x^2 - \zeta^{38}$
$x^2 - \zeta^{22}$
$x^2 - \zeta^{54}$
$x^2 - \zeta^{14}$
$x^2 - \zeta^{46}$
$x^2 - \zeta^{30}$
$x^2 - \zeta^{62}$
00000
16
00010
17
00100
18
00110
19
01000
20
01010
21
01100
22
01110
23
10000
24
10010
25
10000
26
10010
27
11000
28
11010
29
11100
30
11110
31
$x - \zeta$
$x - \zeta^{17}$
$x - \zeta^9$
$x - \zeta^{25}$
$x - \zeta^5$
$x - \zeta^{21}$
$x - \zeta^{13}$
$x - \zeta^{29}$
$x - \zeta^3$
$x - \zeta^{19}$
$x - \zeta^{11}$
$x - \zeta^{27}$
$x - \zeta^7$
$x - \zeta^{23}$
$x - \zeta^{15}$
$x - \zeta^{31}$
00001
00011
00101
00111
01001
01011
01101
01111
10001
10011
10001
10011
11001
11011
11101
11111
$x - \zeta^{33}$
$x - \zeta^{33}$
$x - \zeta^{41}$
$x - \zeta^{57}$
$x - \zeta^{37}$
$x - \zeta^{53}$
$x - \zeta^{45}$
$x - \zeta^{61}$
$x - \zeta^{35}$
$x - \zeta^{51}$
$x - \zeta^{43}$
$x - \zeta^{59}$
$x - \zeta^{39}$
$x - \zeta^{55}$
$x - \zeta^{47}$
$x - \zeta^{63}$

Tiny DSA and Number Theoretic Transforms

Tiny DSA uses the following constants, symbols, and mathematical expressions:

	q	The prime number $q = 2^{10} - 2^8 + 1 = 769$.
	$\mathbb{N}$	The set of natural numbers.
	$\mathbb{Z}$	The ring of integers.
	$\mathbb{Z}_q$	The ring of integers modulo q whose set of elements is $\{0, 1, \ldots, q-1\}$.
	$\mathbb{Z}_q^n$	The set of n-tuples over Z_q.
	T_q	The ring $\Pi_{j=0}^{32} \mathbb{Z}_q$.
R	$Z[X]/(X^{32}+1)$	The ring of single-variable polynomials over $\mathbb{Z}$ modulo $X^{32}+1$. The coefficients of polynomials in R belong to the ring $\mathbb{Z}$. The highest-degree term is at most x^{31}.
R_q	$Z_q[X]/(X^{32}+1)$	The ring of single-variable polynomials over $\mathbb{Z}_q$ modulo $X^{32}+1$. The coefficients of polynomials in R_q belong to the ring $\mathbb{Z}_q$. The highest-degree term is at most x^{31}.
	$(X^{32}+1)$	The *reduction polynomial*.
$\omega,\ z$	ζ	The **primitive 64$^{\text{th}}$ root** of unity in $\mathbb{Z}_q$. $\zeta^{64} \equiv 1 \bmod q$. $\zeta^k \not\equiv 1 \bmod q \ for\ all\ k < 64$. $\zeta = 12$ in Tiny DSA.
	$[a, b]$	For two integers $a \le b$, $[a, b]$ denotes the set of integers $\{a, a+1, \ldots, b\}$.

Examples of Polynomial Rings

Polynomial ring $Z[x]$ is the set of all polynomials with coefficients in Z = {-∞, ..., -1, 0, 1, ..., ∞}.
Polynomial ring $Z_q[x]$ is the set of all polynomials with coefficients in Z_q = {0, 1, ..., $q-1$}.
Example 1 - Polynomial $a(x) \in \mathbb{Z}[x]$.

$$a(x) = -12 + 20367x - 2081x^{56} + 10x^{1023}$$

■

Example 2 - Polynomial $b(x) \in \mathbb{Z}_q[x]$.
The coefficients of $a(x)$ from *Example 1* are mapped to $\mathbb{Z}_q$ in polynomial $b(x)$ below.
Keep in mind, Tiny DSA defines $q = 769$.

$$
\begin{aligned}
a(x) &= -12 + 20367x - 2081x^{56} + 10x^{1023} \\
b(x) &= (-12 \bmod 769) \\
&\quad + (20367 \bmod 769)x \\
&\quad + (-(2081 \bmod 769) \bmod 769)x^{56} \\
&\quad + 10x^{1023} \\
&= (769 - 12) + 373x + (769 - 543)x^{56} + 10x^{1023} \\
&= 757 + 373x + 226x^{56} + 10x^{1023}
\end{aligned}
$$

■

Examples of Polynomials in Tiny DSA

If polynomial $a(x) \in R[x]$, its coefficients are in the ring $\mathbb{Z}$ and its highest-degree term is at most x^{31}.
If polynomial $a(x) \in R_q[x]$, its coefficients are in the ring $\mathbb{Z}_q$ and its highest-degree term is at most x^{31}.
Example 1 - Polynomial $a(x) \in R_q[x]$.
In the polynomial $a(x) = 7 + 23x^{31}$, first term is the lowest-degree term, and the second, the highest-degree term.

■
Example 2 - Polynomial $a(x) \in R_q$.
Consider the polynomial $a(x) = 63 + 159x + 48x^2 + 746x^{28} + x^{30}$. Its coefficients are in $\mathbb{Z}_\mathfrak{q}$, and the highest-degree term is x^{30}. Therefore, $a(x) \in R_q$.

■
Example 3 - Polynomial $a(x) \in R$ and $a(x) \notin R_q$.
Consider the polynomial $a(x) = 2163 - 169x + 1048x^2 - 1746x^{28} + 2x^{30} \in R$. Note $a(x) \notin R_q$ because ***not all coefficients*** are in Z_q. The coefficients of all terms except the last one are in $\mathbb{Z}$.

■
Example 4 - Transform $a(x) \in R$ to $b(x) \in R_q$.
For a number $z \in \mathbb{Z}$, z mod q maps it to $\mathbb{Z}_q$. Therefore, given a polynomial $a(x) \in R$, transforming its coefficients *mod 769* transforms the polynomial to R_q.

$$
\begin{aligned}
a(x) &= 2163 - 169x + 1048x^2 - 1746x^{28} + 2x^{30} && \in R \\
b(x) &= (2163 \; mod \; 769) \\
&\quad + (-169 \; mod \; 769)x \\
&\quad + (1048 \; mod \; 769)x^2 \\
&\quad + ((-(1746 \; mod \; 769) \; mod \; 769))x^{28} \\
&\quad + (2 \; mod \; 769)x^{30} \\
&= 625 + 600x + 279x^2 + 561x^{28} + 2x^{30} && \in R_q
\end{aligned}
$$

■

Primitive Roots of Unity

Let $n = 2^k$, and let q be a prime such that $q - 1$ is divisible by $2n$.

$$
\begin{aligned}
n &= 32 && = 2^5 \\
2n &= 64 && = 2^6 \\
q &= 2^{10} - 2^8 + 1 && = 769 \\
q - 1 &= 2^8(2^2 - 1) && = 768 \\
(q-1)/2n &= 2^8(2^2-1)/2^6 && = 12
\end{aligned}
$$

Let $\zeta \in \mathbb{Z}_q$ be an element of order $2n$. The order of of ζ is the smallest positive integer t such that $\zeta^t = 1$.
In Tiny DSA, $\zeta = 12$, $\zeta^{2n} \equiv 1 \bmod q$, and $\zeta^n \equiv -1 \bmod q$.

```
# python3
n = 32
q = 769
z = 12
assert pow(z, 2*n, q) == 1
assert pow(z, n, q) == q-1
# following two expressions evaluate to the same value.
assert pow(-1, 1, q) == q-1
assert -1 % q == q-1
# this follows directly from the above expressions.
assert -1 % q == pow(-1, 1, q)
# for all k < 64, z^k != 1 mod q.
# in other words, there is no k in [1, 63] such that z^k = 1 mod q
assert not any([pow(z, k, q)==1 for k in range(1, 2*n)])
```

NTT Definition

Let $a(x) \in R_q$.
Define NTT(a) $= \hat{a} =$ (a(ζ), a(ζ^3), a(ζ^5), ..., a(ζ^{2n-1})) $\in Z_q^n$. NTT(a) is a ***polynomial evaluation*** of $a(x)$ at ζ, ζ^3, ζ^5, ..., ζ^{2n-1}.

References

V4: The Number-Theoretic Transform (NTT). © Alfred Menezes. August 2024. https://cryptography101.ca/wp-content/uploads/2024/12/V4-slides-Kyber-and-Dilithium.pdf

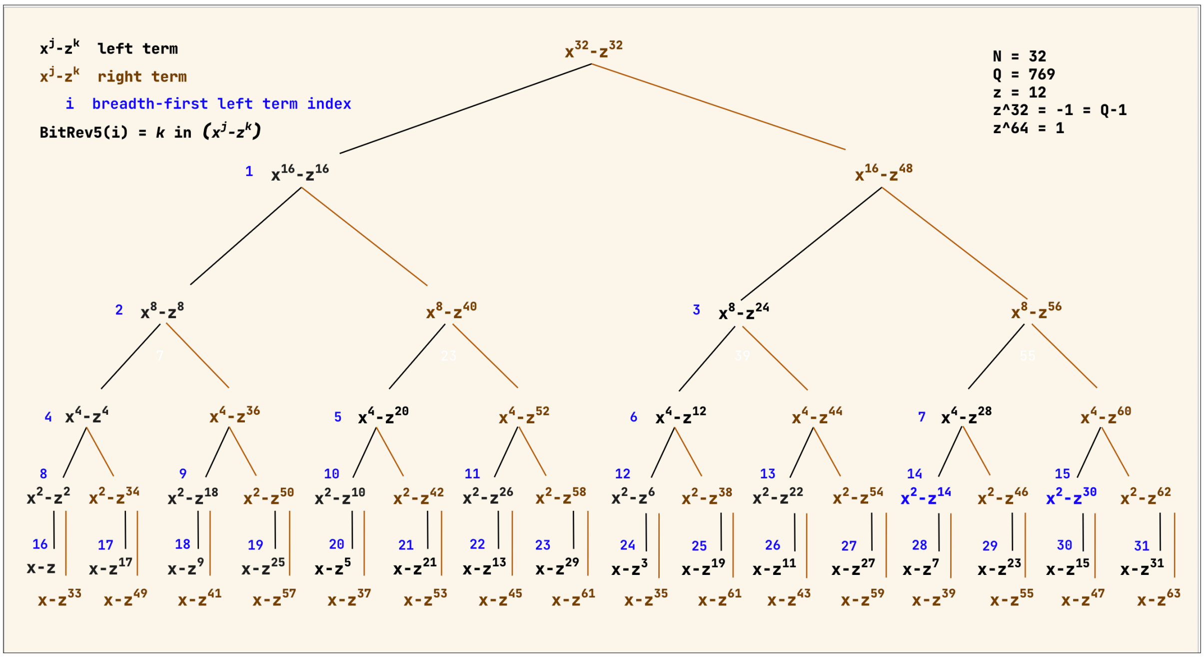


Figure 7: The Irreducible Factors of $X^{32} + 1$