

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

$$\mathbf{a}_L(\mathbf{x}) = a_0 + a_1x + a_2x^2 + \dots + a_{15}x^{15} \in R_q$$

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

$$\begin{aligned} a_r(x) &= a_{16}x^{16} + a_{17}x^{17} + a_{18}x^{18} + \dots + a_{31}x^{31} \in R_q \\ &= (a_{16}x + a_{17}x^1 + a_{18}x^2 + \dots + a_{31}x^{15})x^{16} \in R_q \\ &= \mathbf{a}_R(\mathbf{x})x^{16} \in R_q \quad \text{where } \mathbf{a}_R(\mathbf{x}) = (a_{16}x + a_{17}x^1 + \dots + a_{31}x^{15})x^{16} \end{aligned}$$

We use this method to repeatedly decompose a polynomial $a(x) \in R_q$ of degree $2n$ into two sub-polynomials each of degree d . We stop reducing when we reach factors of degree 1.

$$a(x) = a_L(x) + a_R(x)x^{16} \quad a_L(x) \in R_q, a_R(x) \in R_q, a_L(x) \text{ and } a_R(x) \text{ have degree } \leq 15.$$

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

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

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

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

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

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

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

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

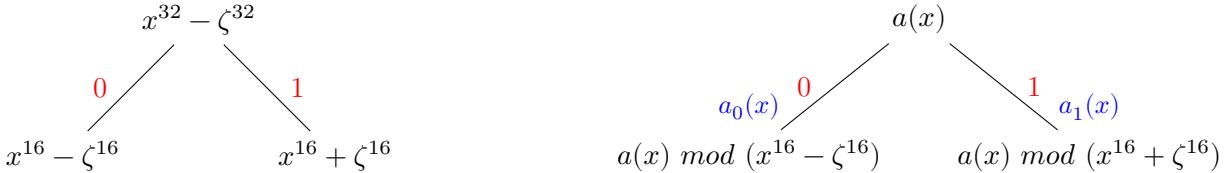


Figure 1: Step 1 of Polynomial Factoring

Figure 2: Step 1 of NTT Evaluation

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

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

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:

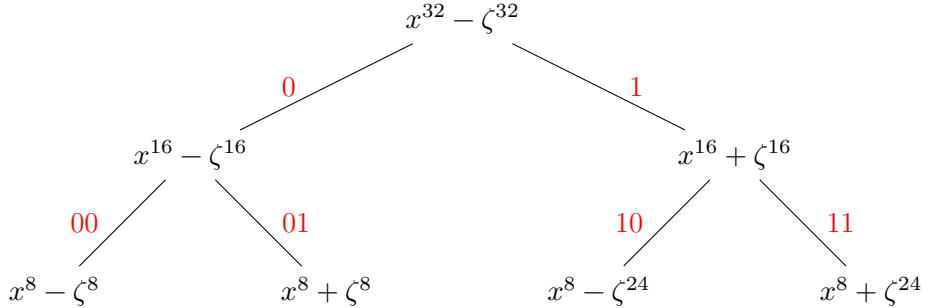


Figure 3: Step 2 of Polynomial Factoring

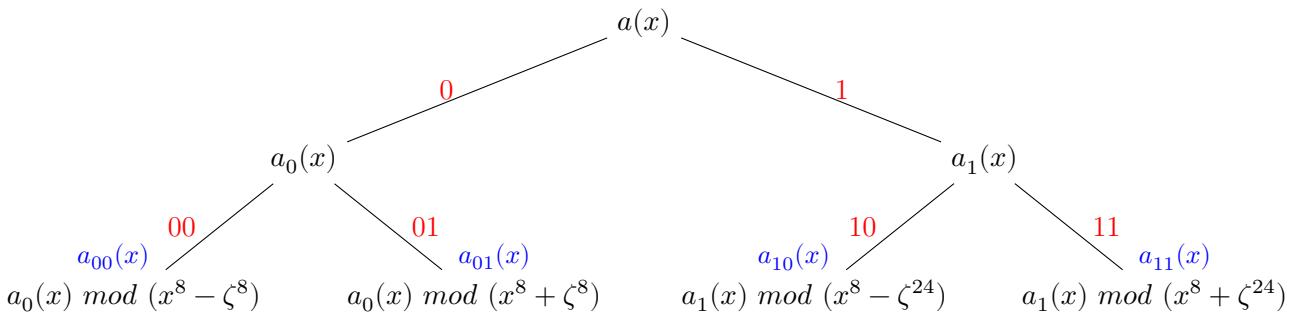


Figure 4: Step 2 of NTT Evaluation

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 $a(x)$.

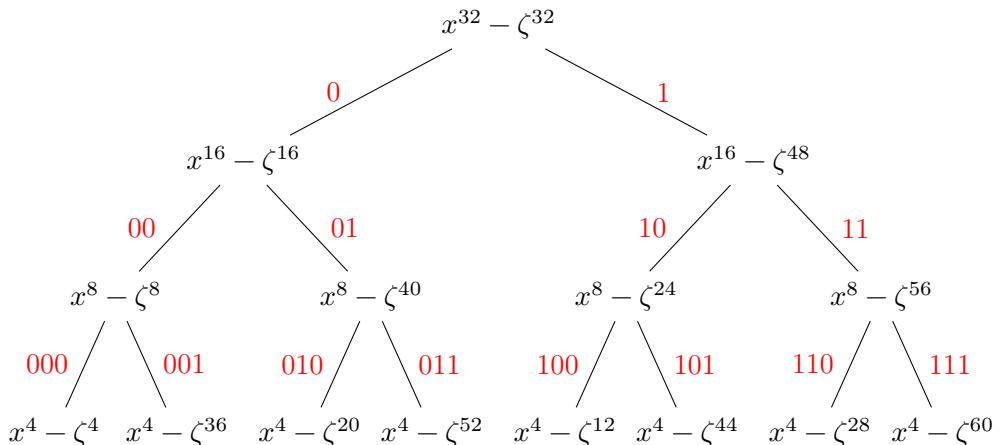


Figure 5: Step 3 of Polynomial Factoring

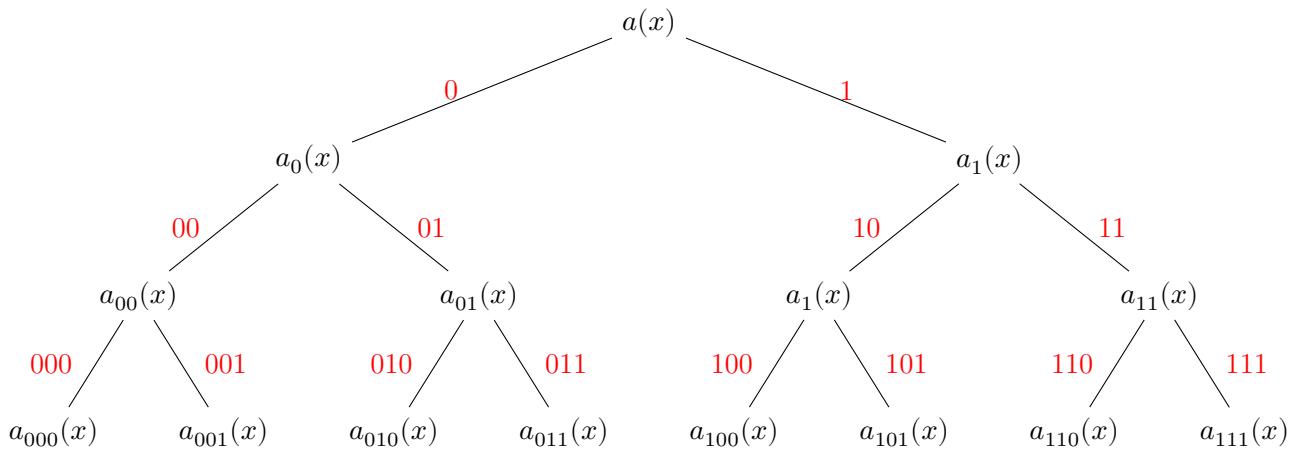
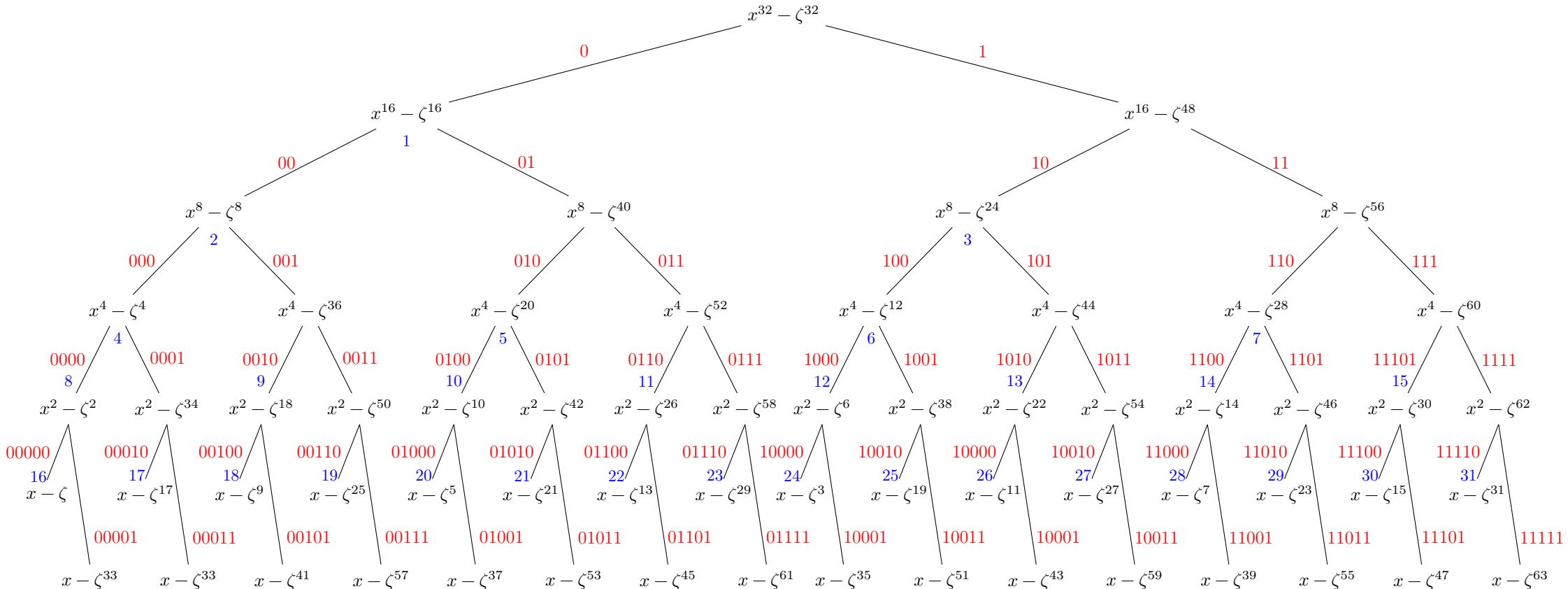


Figure 6: Step 3 of NTT Evaluation

Level 4



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 $\{0, 1, \dots, q-1\}$.	
\mathbb{Z}_q^n	The set of n -tuples over \mathbb{Z}_q .	
T_q	The ring $\prod_{j=0}^{32} \mathbb{Z}_q$.	
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 <i>reduction polynomial</i> .	
ω, z	ζ	The primitive 64th root of unity in \mathbb{Z}_q . $\zeta^{64} \equiv 1 \pmod{q}$. $\zeta^k \not\equiv 1 \pmod{q}$ for all $k < 64$. $\zeta = 12$ in Tiny DSA.
$[a, b]$	For two integers $a \leq b$, $[a, b]$ denotes the set of integers $\{a, a+1, \dots, b\}$.	

Examples of Polynomial Rings

Polynomial ring $Z[x]$ is the set of all polynomials with coefficients in $Z = \{-\infty, \dots, -1, 0, 1, \dots, \infty\}$.

Polynomial ring $Z_q[x]$ is the set of all polynomials with coefficients in $Z_q = \{0, 1, \dots, q-1\}$.

Example 1 - Polynomial $a(x) \in Z[x]$.

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

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}_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 \mathbb{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 $z \in \mathbb{Z}$, $z \bmod q$ 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 .

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

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 ζ is the smallest positive integer t such that $\zeta^t = 1$.

In Tiny DSA, $\zeta = 12$, $\zeta^{2n} \equiv 1 \pmod{q}$, and $\zeta^n \equiv -1 \pmod{q}$.

```

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

```

NTT Definition

Let $a(x) \in R_q$.

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

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>

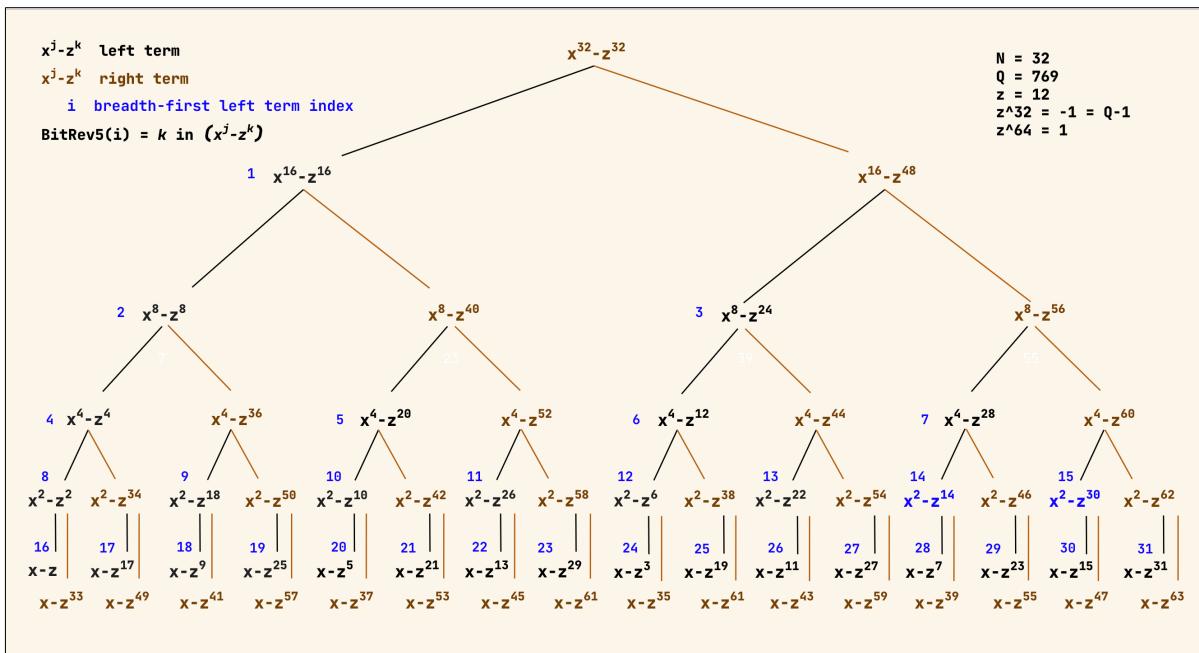


Figure 7: The Irreducible Factors of $X^{32} + 1$