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

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

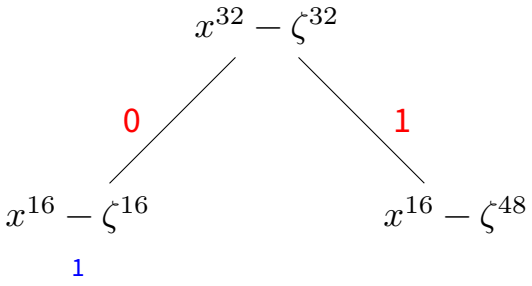
In general, whenever we see a term of the form

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

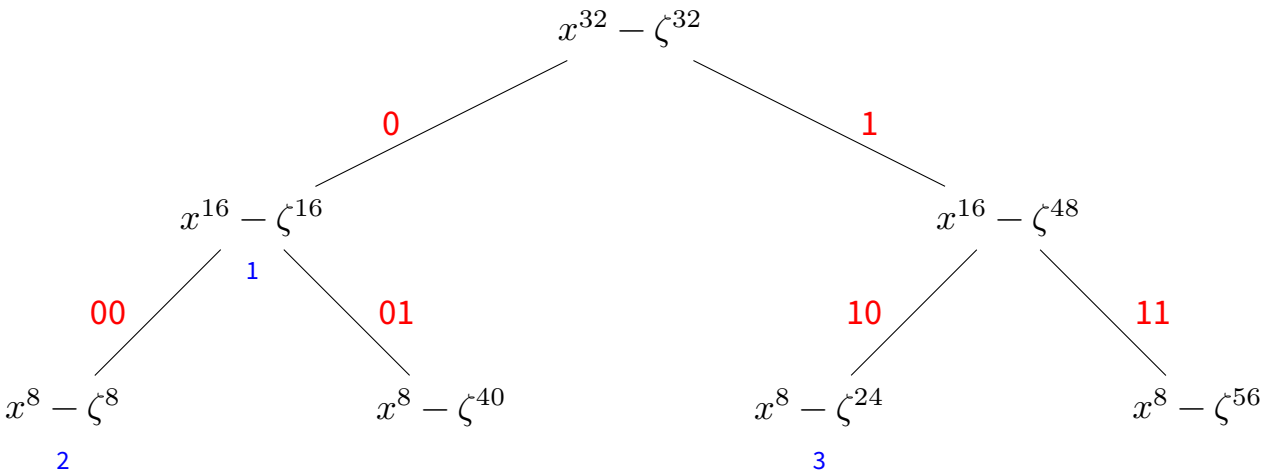
we can replace it with

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

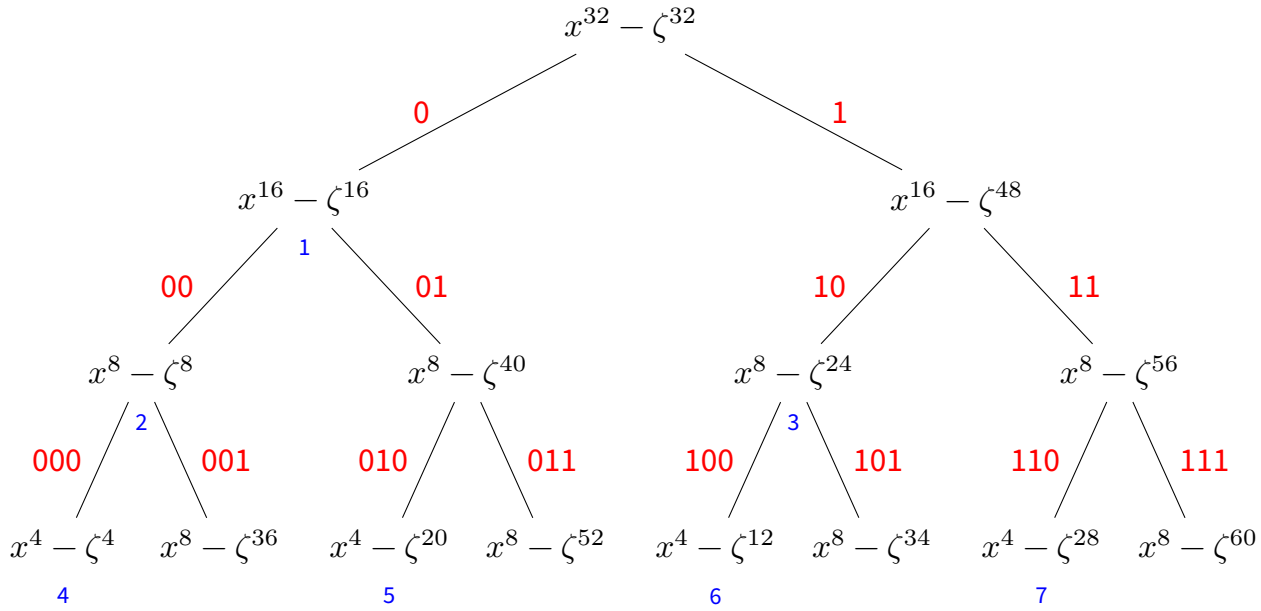
Level 1 - Factors of $x^{32}-\zeta^{32}$



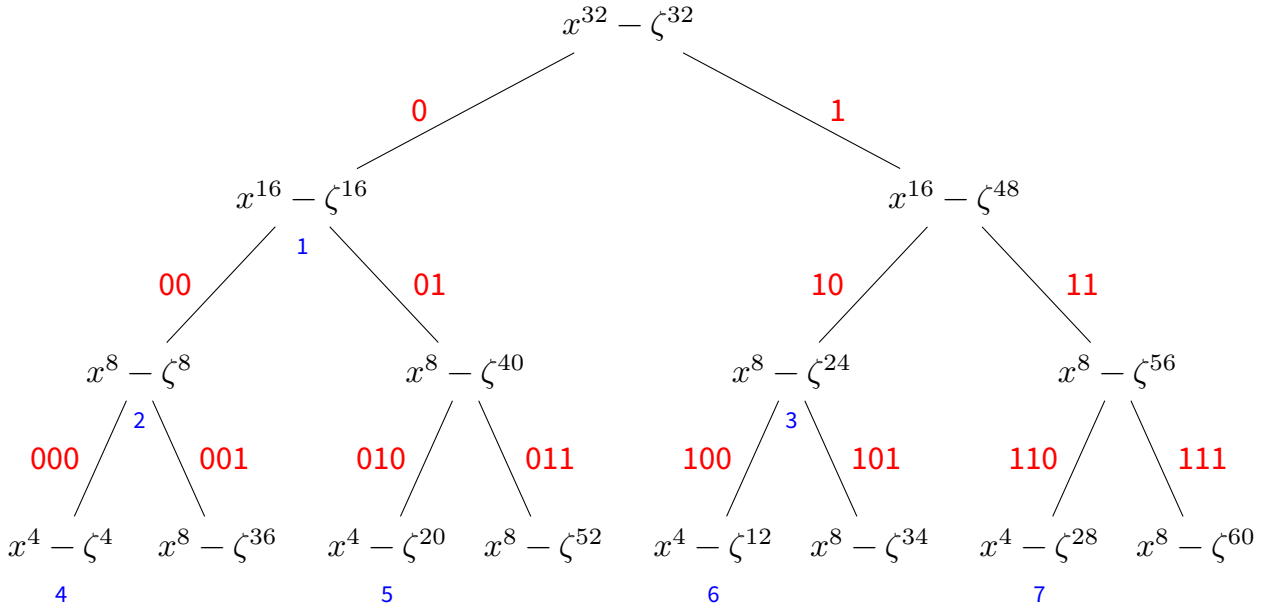
Level 2 - Factors of $x^{16}-\zeta^{16}$ and $x^{16}-\zeta^{48}$



Level 3 - Factors of $x^8 - \zeta^8$, $x^8 - \zeta^{40}$, $x^8 - \zeta^{24}$ and $x^8 - \zeta^{56}$



Level 4


$x^{32} - \zeta^{32}$
0
1
$x^{16} - \zeta^{16}$
1
$x^{16} - \zeta^{48}$
00
01
10
11
$x^8 - \zeta^8$
$x^8 - \zeta^{40}$
$x^8 - \zeta^{24}$
$x^8 - \zeta^{56}$
2
3
000
001
010
011
100
101
110
111
$x^4 - \zeta^4$
$x^8 - \zeta^{36}$
$x^4 - \zeta^{20}$
$x^8 - \zeta^{52}$
$x^4 - \zeta^{12}$
$x^8 - \zeta^{34}$
$x^4 - \zeta^{28}$
$x^8 - \zeta^{60}$
4
5
6
7

Tiny DSA and Number Theoretic Transforms

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.

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 $reduction\ polynomial$.
$\omega,\ z,\ zeta$	ζ	The $\mathbf{primitive\ 64^{th}\ root}$ 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 $a \leq b$, $[a, b]$ 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 $\mathbb{Z}_q$, 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, $\zeta = 12$, $\zeta^{2n} \equiv 1$ mod q, and $\zeta^n \equiv -1$ mod q.

```python
# 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 $\zeta, \zeta^3, \zeta^5, ..., \zeta^{2n-1}$.

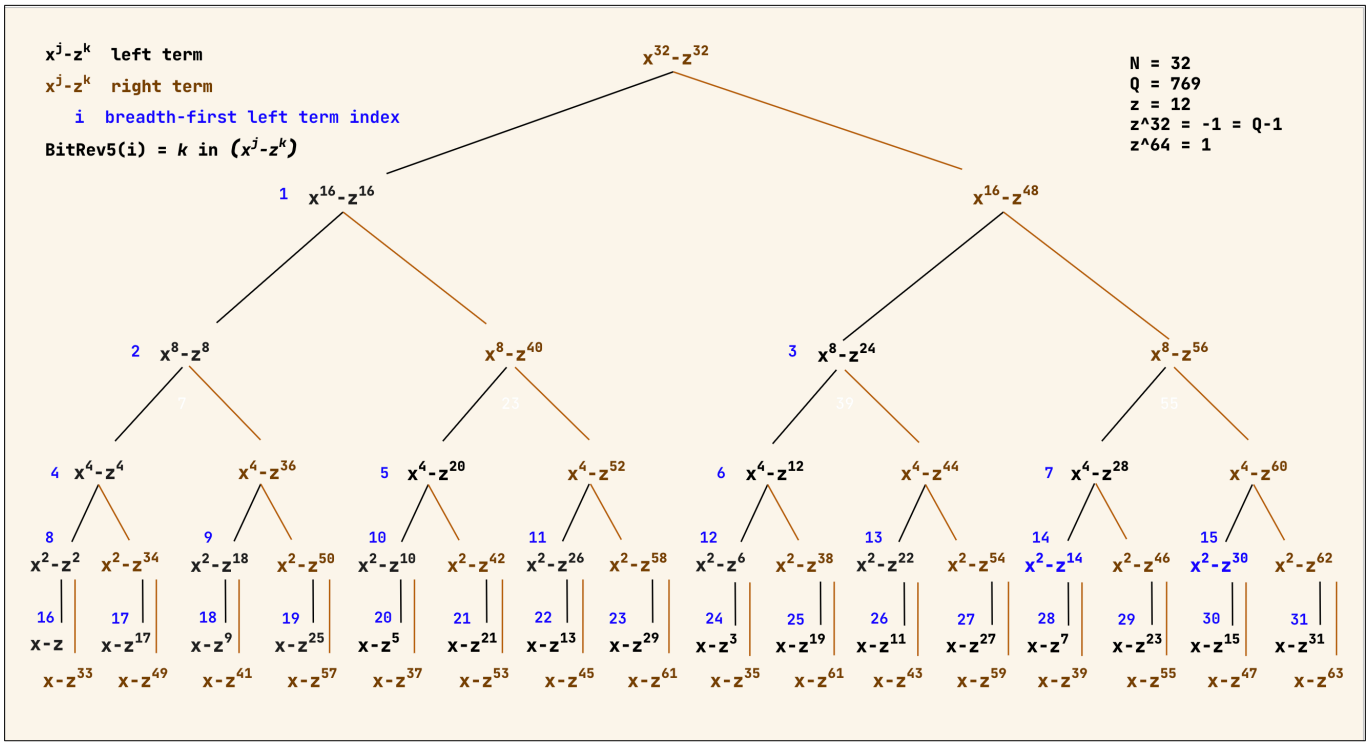


Figure 1: The Irreducible Factors of $X^{32} + 1$

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