Identities Involving Zeta

Jan-2026

A Few Identities involving ζ in Tiny DSA

Tiny DSA defines the following values:

n 32
q The prime number $q = 2^{10} - 2^8 + 1 = 769$.
$\mathbb{Z}_q$ The ring of integers modulo q whose set of elements is $\{0, 1, \ldots, q-1\}$.
ζ The *primitive* 64^{th} *root of unity* in $\mathbb{Z}_q$.
$\zeta = 12$
$\zeta^{32} \equiv -1 \bmod q$
$\zeta^{64} \equiv 1 \bmod q$
$\zeta^k \not\equiv 1 \bmod q \quad \textit{for all } k < 64.$

We start with the two importatnt equalitites:

$$\begin{array}{lllll} \zeta^{2n} & = & \zeta^{64} & = & 1 \\ \zeta^{n} & = & \zeta^{32} & = & -1 \end{array}$$

From these we can derive another useful equality. Recall that in Tiny DSA, $n = 32$:

$$\begin{array}{lll} \zeta^n / \zeta^{2n} & = & -1/1 \\ \zeta^{n-2n} & = & -1 \\ \zeta^{-n} & = & -1 \\ & = & \zeta^n \end{array}$$

In summary,

$$\zeta^n = \zeta^{-n} = -1$$

We can now use this result to find another equality: $\zeta^{-m} = -\zeta^{n-m}$

$$\begin{array}{ll} \zeta^{-m} & \\ & = \zeta^0 \ \zeta^{-m} \\ & = \zeta^n \ \zeta^{-n} \ \zeta^{-m} \\ & = \zeta^n \ \zeta^{-m} \ \zeta^{-n} \\ & = \zeta^{n-m} \ \ \zeta^{-n} \\ & = -\zeta^{n-m} \qquad\qquad \because \zeta^{-n} = -1 \end{array}$$

The result $\zeta^{-m} = -\zeta^{32-m}$ comes handy while evaluating NTT^{-1} function.

Simple Python Code to Verify the Equalities

```
# python3
n = 32
q = 769
z = 12
assert pow(z, 2*n, q) == 1
assert pow(z, n, q) == q-1
# 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)])
##
# check the main result of this section
for m in range(0, 32):
    assert pow(z, -m, q) == q-pow(z, 32-m, q)
```

Application in ML DSA

Recall that the definition of Tiny DSA closely mimics the structure of ML DSA. Therefore, the main equalities shown in the previous section are also applicable to ML DSA.

The values of n, q, and ζ, however, are different in ML DSA:

n	256
q	The prime number $q = 2^{23} - 2^{10} + 1 = 8380417$.
ζ	The *primitive* 512^{th} *root of unity* in $\mathbb{Z}_q$. $\zeta = 1753$ $\zeta^{256} \equiv -1 \bmod q$ $\zeta^{512} \equiv 1 \bmod q$ $\zeta^k \not\equiv 1 \bmod q$ *for all* $k < 512$.

Exercise

Modify the identifiers in the Python code shown above to match the definition of ML DSA. Run the code and verify that all assertions hold.

■