**NTT**

**Finite Fields and Generators**

A finite field of size Q, represented as FQ, is a set of all positive elements from 1 to Q-1.

i.e., FQ = {1, 2, 3, …, Q-1}

The order of this field/group is Q-1.

Suppose we consider an element ‘a’ such that a ∈ FQ, then ‘a’ will be a generator of FQ if

a1modQ, a2modQ, a3modQ, …,a(Q−1)modQ generates all elements of FQ in the mod domain.

Example

For the finite field F5 = {1,2,3,4}, let us consider the element 2.

We see that 2 ∈ F5 and 21mod5 = **2**, 22mod5 = **4**, 23mod5 = **3**, 24mod5 = **1**

As the powers of 2 generate all elements of F5, 2 is a generator of the Finite Field F5.

However, if we consider the element 4, we observe 41mod5 = **4**, 42mod5 = **1**, 43mod5 = **4**, 44mod5 = **1**. Here as the powers of 4 do not generate all the elements of F5, 4 is not a generator of F5.

**Another way to check if an element ‘a’ is a generator** of the finite field FQ, if ‘a’ is a generator then **a(Q-1)/P1**, **a(Q-1)/P2**… ≠ 1modQ where P1, P2… are prime factors of Q-1.

If we take the same example F5 = {1,2,3,4}.

Here Q – 1 = 4 and P1 = 2 is the only prime factor of 4.

Take a = 2, 24/2 = 4 ≠ 1mod5. Hence 2 is a generator of F5.

Take a = 4, 44/2 = 4 = 1mod5. Hence 4 is **not** a generator of F5

**Points to Note**

* Generators always appear in pairs of inverses. For F5, 2 and 3 are inverses and since 2 is a generator, 3 is also a generator.
* The element ‘2’ is not a generator for every finite field.

For F7, Q-1 = 6 = 2 × 3. Let P1 = 2, 26/2 = 8 and 8mod7 = 1. Hence 2 here is not a generator.

* The element ‘1’ can never be a generator for any finite field.

**Linear NTT**

Linear NTT is used to transform polynomials between the coefficient form and the evaluation form.

Given an input vector X = (X(0), X(1), X(2), X(3),…., X(n-1)) choose a field size ‘Q’ such that the following conditions are satisfied

1. Q > n, where ‘n’ is the number of elements in the input vector X
2. Q must be greater than all elements in the input vector X, i.e., Q > X(0), X(1), X(2), X(3) etc.
3. Q = kn +1, where k >1, ‘n’ is again the number of elements in X
4. Q must be a prime

For this finite field FQ, ω = gkmodQ, where ‘g’ is a generator of FQ, k is obtained from condition III and ‘ω’ is called the nth primitive root of unity.

The output vector Y is given by Y = (Y(0), Y(1), Y(2), Y(3),…., Y(n-1)) where,

The inverse transform, which restores the original input vector is given by

**Points to Note**

* All computations of Y and X must be done in the mod domain.
* In the inverse transform the inverse of n should also be taken in the mod domain.

Example

Consider the polynomial

Clearly this is in the coefficient form and we need to compute its evaluation form.

In other words we need to express this polynomial in the form

Here our input vector is X = (3, 10, 2, 7, 5) and hence using conditions for Q and k, we get

Q = kn + 1, here n = 5, if k = 2, Q = 11 satisfies all our conditions.

Hence our field size is 11 and our finite field is F11.

Calculating Generators of F11

Q - 1 = 10 = 2 × 5. Let P1 = 2 and P2 = 5.

|  |  |  |
| --- | --- | --- |
| Element | Check for Generator | Is it a Generator? |
| 2 |  | YES |
| 3 |  | NO |
| 4 |  | NO |
| 5 |  | NO |
| 6 | *and* | YES |
| 7 | *and* | YES |
| 8 | *and* | YES |
| 9 |  | NO |
| 10 |  | NO |

For F11 field, generators are 2, 6, 7 and 8.

Here again we observe the fact that generators have occured in inverse pairs.

‘2’ and ‘6’ are inverses in the mod 11 domain. Similarily ‘7’ and ‘8’ are also inverses in this domain.

Let us take g = 6 (one of the generators), then ω = 62 = 36 = 3 (in the mod domain)

Computing the output vector (all final computations are again in the mod domain)

Hence the output vector comes out to be Y = (5, 7, 4, 0, 10)

Interpretation

Y(b) gives us the value of p(x) when x = ωb.

In this example, Y(0) = 5 and if we put x = ω0 = 30 = 1 (b = 0)

= 5 (in the mod domain again)

We find that p(1) = Y(0)

One equation of the evaluation form is 5 = p(1)

Similarily, Y(1) = 7 and if x = ω1 = 31 = 3 (b = 1)

= 7

Second equation is 7 = p(3)

The other equations can be directly written

Y(2) = 4, x = x = ω2 = 32 = 9 (b = 2), equation is 4 = p(9)

Y(3) = 0, x = x = ω3 = 33 = 27 = 5 (b = 3), equation is 0 = p(5)

Y(4) = 10, x = x = ω4 = 34 = 81 = 4 (b = 4), equation is 10 = p(4)

Hence we have computed all five equations of the evaluation form.