Perspectives of Convolution and NTT under Prime Power Moduli

Yimeng He[1]

Nanyang Technological University, 50 Nanyang Ave, Singapore
yimeng002@e.ntu.edu.sg

Abstract. Abstract to be done. **(To reference)**

1 Introduction

The convolution problem We are interested in the discrete circular convolution problem where the underlying modulus is a prime power. Specifically, given 2 sequences $\boldsymbol{a} = (a_0, \dots, a_{N-1})$, $\boldsymbol{b} = (b_0, \dots, b_{N-1}) \in \mathbb{Z}_{p^m}^N$ for prime power modulus p^m and length N. We aim to efficiently compute their circular convolution product mod p^m:

$$\boldsymbol{c} = \boldsymbol{a} \circledast \boldsymbol{b} \qquad \text{where } c_i = \sum_{i=0}^{N-1} a_i b_{N-i} \, \forall 0 \le i < N$$

Alternatively, we can recast the problem into one of wrapped polynomial multiplication. Let $f(x) = a_0 + a_1 x + \dots + a_{N-1} x^{N-1}$, $g(x) = b_0 + b_1 x + \dots + b_{N-1} x^{N-1} \in \mathbb{Z}_{p^m}[x]$, we want to efficiently calculate the product $h(x) = f(x)g(x) \pmod{p^m, x^N - 1}$.

There is another interpretation of the problem. We define the circulant matrix $\boldsymbol{H} \in \mathbb{Z}_{p^m}^{N \times N}$, $\boldsymbol{H}_{i,j} = a_{j-i \bmod N}$. The goal is to efficiently calculate the matrix vector product $\boldsymbol{c} = \boldsymbol{H} \cdot \boldsymbol{b} \in \mathbb{Z}_{p^m}^N$.

Classical Number Theoretic Transform (NTT) In the special(and important) case where the length $N = 2^n$ and the modulus $p = k2^n + 1$ is a prime, we can find a primitive N^{th} root of unity $\omega \in \mathbb{Z}_p^\times$. The above problem can be handled by the famous radix-2 Cooley-Tuckey algorithm under $O(N \log N)$ time [8].

Let us briefly recall the classical NTT strategy:

1. Find a multiplicative generator $g \in \mathbb{Z}_p^\times$
2. Raise to a power $\omega = g^{\frac{p-1}{N}}$ so that ω is a primitive N^{th} root of unity
3. Use Cooley-Tuckey radix 2 algorithm to compute the fourier transform $\mathsf{FFT}(\boldsymbol{a})_i = \sum a_j \omega^{ij}$, $\mathsf{FFT}(\boldsymbol{b})_i = \sum b_j \omega^{ij}$
4. Perform the elementwise product $\boldsymbol{c}' = \mathsf{FFT}(\boldsymbol{a}) \odot \mathsf{FFT}(\boldsymbol{b})$
5. Finally, use the radix-2 algorithm again to calculate the inverse fourier transform $\boldsymbol{c} = \mathsf{InvFFT}(\boldsymbol{c}')$, $\boldsymbol{c}_i = \frac{1}{N} \sum_{j=0}^{N-1} c'_j \omega^{-ij}$

The more general case Though elegant, classical NTT imposes significant restrictions on the modulus and the convolution length. Since NTT has found important applications in Cryptography, Coding Theory, Communication Theory etc. there is an ongoing research attempting to work around this limitation. The aim is to efficiently compute the circular convolution / NTT under more general modulus and length.

This paper considers this general question and focuses on prime power modulus p^m and arbitrary length. We are mostly interested in a very small prime p: the most interesting case is $p = 2$, since this is the default base in most modern computer architectures.

To the best of our knowledge, the most practical "generic" solution to the arbirary modulus, arbitrary length problem makes use of multimodular NTT, a combination of classical NTT with Residue Number System and Chinese Remainder Theorem. See for example [15] Sect 6. We refer the reader to the related work section for a brief overview of this strategy.

Our perspectives and solutions This paper approaches the convolution/NTT problem from a perspective different from the multimodular method. In that method, we must lift both arguments to *integer sequences* and solve the integer circular convolution problem. Apart from bounding the size of the final result, the initial modulus plays almost no role in the multimodular NTT algorithm.

In contrast, we propose NTT-like strategies that closely follows the modular arithmetic. For simplicity, we focus on the prime power modulus p^m, $m \ge 1$. At a high level, our strategy is the same as the classical NTT and its numerous variants. Namely:

1. Find a “suitable” set of roots of unity
2. Pad the arguments to “suitable” lengths
3. Employ “suitable” quasi-linear time algorithms to compute the fourier transform. pointwise multiply the intermediate result and use similar quasi-linear time algorithm to compute the inverse transform

We need a number of less well-known techniques to make the strategy work in our setting. We do not claim novelty over these techniques per se, but only over their combination in order to solve the general circular convolution problem. In more detail:

- Section 3 finds and calculates a class of roots of unity compatible with both NTT application and arithmetic of the ring $\mathbb{Z}_{p^m}$. The main idea is to find these roots in the Galois ring extension $\mathsf{GR}(p^m, r)$. For each $r \geq 1$, there is a suitable root of unity of order $p^r - 1$. We will see why such a root is appropriate and provide efficient algorithms to calculate the root.
- In section 4 we briefly recall how to pad arguments so that we can transform a circular convolution problem of length N to one of a more convenient length $N' > N$.
- Efficient convolution and NTT is the main topic of **(To reference Section 3)**. We suggest 2 algorithms based on factorization characteristics of N'
  - If $N' = q^e$ is a power of a small prime q, we take inspiration from [14] and propose an $O(N \log N)$ recursion algorithm to compute the circular convolution without doing the fourier and inverse fourier transforms.
  - If $N' = N_1 N_2$ where N_1, N_2 are coprime. We employ the Good-Thomas Prime Factorization technique [11,16] and reduce the calculation of length N' fourier transform to 2 consecutive block-wise length N_1 and length N_2 fourier transforms.
  - Finally, we combine the 2 methods above to handle those N' having factorization $N' = q_1 \dots q_{n-1} q_n^e$, where $e \geq 1$ and $q_1, \dots, q_n$ are distinct small primes
- The last section contains some benchmark results of a proof-of-concept Sagemath/Python implementation of our strategy. We will also discuss the strengths and weaknesses; the time complexities; and the applications of our approach

Applications NTT has become a cornerstone in modern cryptographic applications, particularly within Post-Quantum Cryptography and Homomorphic Encryption. It plays a vital role in lattice-based cryptography schemes such as Dilithium, Falcon, and Kyber [4,10,3]. In Homomorphic Encryption schemes like BFV, BGV, and CKKS [5,6,7], NTT is also critical for such operations as modulus switching and ciphertext relinearization. However as hinted before, classical NTT imposes severe restrictions on the set of parameters, particularly the existence of suitable N^{th} or $2N^{\text{th}}$ roots of unity (for negacyclic convolution) modulo a prime q. We believe that overcoming the limitation of classical NTT will also open up the range of parameter choices in those schemes and will help us find better and more secure instantiations.

If we focus on the power of 2 modulus, where $p = 2$, our perspective might also have implications in domains such as Coding Theory and Communication. Efficient computation of (linear) circular convolutions is integral to the encoding and decoding procedures of certain codes (see for example [1,9] for cyclic and negacyclic codes). In addition, our result might also testify to the perspective that some operations on finite fields have useful analogues in finite ring settings.

2 Related Works

To be done

3 On Roots of Unity

Whether NTT or FFT, all fourier transform related algorithms require certain roots of unity. Suppose we need to compute the fourier transform of N data points, we generally need N distinct roots of unity, but the nature of these roots depends on context.

In scientific computations, data are real/complex numbers in general. The N roots of unity are usually taken to be the evenly-spaced points on the complex unit circle $0 \leq k < N : \zeta^k := \exp\left(\frac{2\pi i k}{N}\right)$.

In discrete computational problems, data are usually finite field/finite domain elements. The often repeated mantra is that the N roots of unity are generated by a *primitive* N^{th} root of unity, an element ζ in the field/domain such that $\zeta^N = 1, \forall 0 < k < N : \zeta^k \neq 1$.

In non-integral rings, for example $\mathbb{Z}_{32}, \mathbb{Z}_{24}$, primitivity alone no longer suffices

Example 1. $x^2 - 1 = 0$ has 4 solutions over $\mathbb{Z}_8$: $x = 1, 3, 5, 7 \pmod 8$, among which $3, 5, 7$ are all primitive 2^{nd} roots of unity. Are they suitable for a length-2 NTT? Let us look at the the fourier(Vandermonde) matrix of the root $\zeta = 5$.

$$\boldsymbol{V} = \begin{pmatrix} \zeta^0 \, \zeta^0 \\ \zeta^0 \, \zeta^1 \end{pmatrix} = \begin{pmatrix} 1 \, 1 \\ 1 \, 5 \end{pmatrix} \qquad \det(\boldsymbol{V}) = 5 - 1 = 4$$

$\boldsymbol{V}$ is not even inverible over $\mathbb{Z}_8$. This is also true for other primitive roots of unity.

On close inspection, the non-invertibility of $\boldsymbol{V}$ is the only obstruction. We conclude that in the context of non-integral rings, the N^{th} root of unity suitable for NTT/FFT application is one for which its corresponding fourier matrix $\boldsymbol{V}$ is invertible.

Definition 1. *(Principal root of unity, adapted from [18]) Let $\mathcal{R}$ be a commutative ring with identity. We call $\zeta \in \mathcal{R}$ a principal N^{th} root of unity if*

1. *N is invertible (equivalently, N is coprime to the ring characterstic $\mathsf{char}(\mathcal{R})$)*
2. *$\zeta^N = 1$*
3. *$\forall 1 \le k < N :\ \sum_{i=0}^{N-1} \zeta^{ik} = 0$*

The following proposition is a direct consequence of definition 1.

Proposition 1. *If ζ is a principal N^{th} root of unity, then the fourier matrix $\boldsymbol{V} := \boldsymbol{V}(1, \zeta, \ldots, \zeta^{N-1})$, $\forall 0 \le i, j < N :\ \boldsymbol{V}_{i,j} = \zeta^{ij}$ is invertible with inverse $\boldsymbol{V}^{-1} = \frac{1}{N}\boldsymbol{V}^*$, $\boldsymbol{V}^*_{i,j} = \zeta^{-ij}$.*

Let $p \neq 2$ be a prime. A well known result due to Gauß says for any $m \ge 1$, the unit group $\mathbb{Z}_{p^m}^\times \cong \mathcal{C}_{\phi(p^m)} = \mathcal{C}_{p^{m-1}(p-1)}$ is cyclic. In fact, all units in the (unique) order $(p-1)$ subgroup of $\mathbb{Z}_{p^m}^\times$ are principal.

Proposition 2. *Let $\zeta \in \mathbb{Z}_{p^m}^\times$ generates the unique subgroup of order $(p-1)$. Then ζ is a principal $(p-1)^{th}$ root of unity.*

Proof. Let $N = p - 1$. 1 and 2 in definition 1 is obvious. Note that for any $1 \le k < N$, $(\zeta^k - 1)(1 + \zeta^k + \ldots + \zeta^{k(N-1)}) = \zeta^{Nk} - 1 = 0$. Since $\zeta \bmod p$ is a primitive $(p-1)^{\text{th}}$ root of unity in $\mathbb{Z}_p$, $\zeta^k - 1 \neq 0 \pmod p$. Hence $\zeta^k - 1$ is relatively prime to p^m and is invertible over $\mathbb{Z}_{p^m}$. This proves 3 in definition 1. □

Although $\mathbb{Z}_{p^m}$ contains a principal $(p-1)^{\text{th}}$ root of unity, which is a generator of the unique cyclic subgroup of $\mathbb{Z}_{p^m}^\times$ order $(p-1)$, the problem is that in most cases of interest, the convolution length $N \gg p$ (this holds in particular when $p = 2$). To find large principal roots of unity while still preserving the modular structure forces us to look at extension rings. This is where the Galois Ring comes into our picture.

Galois Rings can be motivated, defined and represented in a number of different ways. We refer the reader to [2,12] for more backgrounds and theories. Here we would like to think of a Galois Ring $\mathsf{GR}(p^m, r)$ as degree r extension of $\mathbb{Z}_{p^m}$ in the same way that the Galois field $\mathbb{F}_{p^r}$ is a degree r extension of $\mathbb{Z}_p$.

Definition 2. *(Galois Ring [17]) The Galois Ring $\mathsf{GR}(p^m, r)$ can be represented by a quotient polynomial ring $\mathbb{Z}[x]/(p^m, f(x))$ where $f(x)$ is a degree r monic polynomial which is also irreducible* mod p.

Just like finite fields, all Galois Rings with the same modulus p^m and extension degree r are isomorphic. In some sense $\mathsf{GR}(p^m, r)$ doesn't depend on the particular choice of $f(x)$. However, some $f(x)$ are more convienient from a computational point of view.

In finite field theory, a degree r polynomial $f(x) \in \mathbb{Z}_p[x]$ is called *primitive* if $f(x)$ is monic irreducible and $x \pmod{p, f(x)}$ has order $p^r - 1$ in $\mathbb{F}_{p^r} \cong \mathbb{Z}_p[x]/(f(x))$. In other words, the equivalent class of $[x]$ is a primitive $(p^r - 1)^{\text{th}}$ root of unity.

We would like to find analogues of primitive polynomials over the ring $\mathbb{Z}_{p^m}[x]$. Indeed, using Hensel's lifting technique, we can lift a primitive polynomial $f(x) \in \mathbb{Z}_p[x]$ to $F(x) \in \mathbb{Z}_{p^m}[x]$. We will show that the lifted polynomial has desirable properties.

Theorem 1. *(Hensel Lifting, integral form [20]) Suppose $f(x) \equiv \alpha_0 g(x) h(x) \pmod p$, where α_0 is not divisible by p and $g(x), h(x)$ are monic polynomials that are coprime* mod p. *Then $\forall k \ge 1$ there exist polynomials $g_k(x), h_k(x) \in \mathbb{Z}[x]$ unique up to* mod p^k *such that*

1. *$g_k(x) \equiv g(x) \pmod p \qquad f_k(x) \equiv f(x) \pmod p$*
2. *$f(x) \equiv \alpha_0 g_k(x) f_k(x) \pmod{p^k}$*

Proposition 3. *Let $f(x)$ be a primitive polynomial* mod p *of degree r, there exists a monic polynomial $g(x)$ unique up to* mod p *such that*

$$x^{p^r-1}-1 \equiv f(x)g(x) \pmod p$$

Now apply theorem 1 Hensel lifting to the equation above. We can find a unique polynomial $f_m(x) \in \mathbb{Z}_{p^m}[x]$ such that $f_m(x) \equiv f(x) \pmod p$ and $f_m(x) \mid x^{p^r-1}-1$ over $\mathbb{Z}_{p^m}[x]$.

Let the Galois Ring be defined over this polynomial $\mathsf{GR}(p^m,r) \cong \mathbb{Z}[x]/(p^m, f_m(x))$. We claim that:

1. *The equivalent class $x \pmod{p^m, f_m(x)}$ has order p^r-1 over $\mathsf{GR}(p^m,r)^\times$. Moreover,*
2. *The equivalent class $x \pmod{p^m, f_m(x)}$ is a principal $(p^r-1)^{th}$ root of unity over $\mathsf{GR}(p^m,r)$. Hence*
3. *For any $N \mid p^r-1$, the equivalent class $x^{\frac{p^r-1}{N}} \pmod{p^m, f_m(x)}$ is a principal N^{th} root of unity.*

Proof. 1. Since $f_m(x) \mid x^{p^r-1}-1$ over $\mathbb{Z}_{p^m}[x]$, $x^{p^r-1} \equiv 1 \pmod{p^m, f_m(x)}$. Suppose there exists a $0<k<p^r-1$ such that $x^k \equiv 1 \pmod{p^m, f_m(x)}$. Since $f_m(x) \equiv f(x) \pmod p$, we can reduce mod p and obtain $x^k \equiv 1 \pmod{p, f(x)}$, contradiction to the fact that $f(x)$ is a primitive polynomial mod p.

2. The only nontrivial part to verify is condition 3 in definition 1. Let $N = p^r-1$ and fix $0<k<N$. It is easy to see that $(x^k-1)(\sum_{i=0}^{N-1} x^{ik}) = x^{kN}-1 \equiv 0 \pmod{p^m, f_m(x)}$. We claim that $x^k-1 \pmod{p^m, f_m(x)}$ has a multiplicative inverse over $\mathbb{Z}_{p^m}[x]$. If the claim is true, we can multiply the inverse and obtain $\sum x^{ik} \equiv 0 \pmod{p^m, f_m(x)}$. The equivalent class $[x]$ is therefore a principal $(p^r-1)^{\text{th}}$ root of unity.

Claim: $\exists h(x): (x^k-1)h(x) \equiv 1 \pmod{p^m, f_m(x)}$
proof of Claim. Since $0<k<N$, $x^k-1 \pmod{p, f(x)}$ is nonzero and has a multiplicative inverse $h_1(x)$, i.e., $(x^k-1)h_1(x) \equiv 1 \pmod{p, f_m(x)}$ (recall that $\mathbb{Z}[x]/(p,f(x)) = \mathbb{Z}[x]/(p, f_m(x))$ is a field). We are going to lift the inverse mod p to one mod p^m. To do so it is most convenient to employ a technique known as Newton-Raphson division [19]

Newton-Rhaphson division: Let $l>0$. Suppose $\exists h_l(x)$ s.t. $(x^k-1)h_l(x) \equiv 1 \pmod{p^l, f_m(x)}$. Define

$$h_{l+1}(x) = 2h_l(x) - (x^k-1)h_l(x)^2$$

Then $(x^k-1)h_{l+1}(x) \equiv 1 \pmod{p^{l+1}, f_m(x)}$
proof of lifting. Write $(x^k-1)h_l(x) = 1 = p^l M_l(x) + f_m(x)N_l(x)$ for some polynomials $M_l(x), N_l(x)$. Then

$$\begin{aligned}
&(x^k-1)^2 h_l(x)^2 = 1 + 2p^l M_l(x) + p^{l+1}(p^{l-1}M_l(x)^2) + f_m(x)\big(f_m(x)N_l(x)^2\\
&+2N_l(x)(1+p^l M_l(x))\big)\\
&2(x^k-1)h_l(x) = 2 + 2p^l M_l(x) + f_m(x)N_l(x)\\
\implies &(x^k-1)h_{l+1}(x) = 1 + p^{l+1}M_{l+1}(x) + f_m(x)N_{l+1}(x)
\end{aligned}$$

for some polynomials $M_{l+1}(x), N_{l+1}(x)$. Therefore we can use Newton-Rhaphson division to lift the inverse up to mod p^m. This shows that x^k-1 and the claim is proven.

3. is a straightforward consequence of 2. □

3.1 On Efficient Lifting

We need o address an uncomfortable algorithmic issue before we proceed to the next section. Traditionally, Hensel Lifting is usually accomplished by starting with a coprime factoization $f(x) = g(x)h(x) \pmod p$ and use inexpensive polynomial GCD operations to lift to the factorization $f(x) = f_m(x)g_m(x) \pmod{p^m}$. Our trouble is that both $x^{p^r-1}-1$ and $x^{p^r-1}-1/f(x)$ are too big even for moderately large r (We tried to key in $x^{2^{32}-1}-1$ into the Sagemath/Python but the system complains and refuses to digest it) .

Fortunately, there is a way to only lift the primitive polynomial $f(x)$ without knowing or caring about its coprime factor. The method we use comes from [13], but it may already be described and used in other contexts.

Proposition 4. *(Adapted from [13] Theorem 1) Let $k>0$ and suppose a monic polynomial $f_k(x) \in \mathbb{Z}[x]$ satisfies:*

- *$f_k(x)$* mod *p^k is irreducible over $\mathbb{Z}_{p^k}[x]$*
- *$\exists M$ coprime to p such that $f_k(x) \mid x^M-1$ over $\mathbb{Z}_{p^k}[x]$*

We let $f_{k+1}(x)$ be a monic polynomial whose roots are the p^{th} power of the roots of $f_k(x)$ over an algebraically closed field. f_{k+1} satisfies the following properties:

1. *$f_{k+1}(x) \in \mathbb{Z}[x]$ is integral*
2. *$f_{k+1}(x) \equiv f_k(x) \pmod{p^k}$, hence $f_{k+1}(x)$ is irreducible over $\mathbb{Z}_{p^{k+1}}[x]$*
3. *$f_{k+1}(x) \mid x^M - 1$ over $\mathbb{Z}_{p^{k+1}}[x]$*

In otherwords, the Hensel Lifting of $f_k(x) \bmod p^k$ is exactly $f_{k+1}(x) \bmod p^{k+1}$

Proof. For the proof we are going to use some p-adic theory. Let $\mathcal{Z}_p$ be the ring of p-adic integers and $\mathcal{Q}_p$ the field of p-adic rationals. Since M is coprime to p the polynomial $x^M - 1$ has M distinct roots of unity over an extension field of $\mathcal{Q}_p$.

By Hensel Lifting Lemma theorem 1, there exists $f_{k+1}(x), g(x) \in \mathbb{Z}[x]$ such that $f_{k+1}(x) \mid x^M - 1$ over $\mathbb{Z}_{p^{k+1}}[x]$ and $f_{k+1}(x) \equiv f_k(x) + p^k g(x) \pmod{p^{k+1}}$. Therefore item 1 and 2 of proposition 4 are immediate, and it remains to show item 3.

Moreover, if α_k is a root of $f_k(x)$ over $\mathbb{Z}_{p^k}$, namely $f_k(\alpha_k) \equiv 0 \pmod{p^k}$. There would exist a root $\alpha_{k+1} = \alpha_k + p^k\delta$, where δ lies in an extension field of $\mathcal{Q}_p$, of $f_{k+1}(x)$ over $\mathbb{Z}_{p^{k+1}}$. In other words, $f_{k+1}(\alpha_{k+1}) \equiv 0 \pmod{p^{k+1}}$.

Since $f_k(x) \mid x^M - 1$ over $\mathbb{Z}_{p^k}[x]$, there exists an ϵ in an extension field of $\mathcal{Q}_p$ such that $\alpha_k^M = 1 + p^k\epsilon$. Because

$$\begin{aligned} \alpha_{k+1}^p &= (\alpha_k + p^k\delta)^p = \alpha_k^p + O(p^{k+1}) \equiv \alpha_k^p \pmod{p^{k+1}} \\ \alpha_{k+1}^{pM} &= (\alpha_k + p^k\delta)^{pM} = \alpha_k^{pM} + O(p^{k+1}) = (1 + p^k\epsilon)^p + O(p^{k+1}) = 1 + O(p^{k+1}) \equiv 1 \pmod{p^{k+1}} \end{aligned}$$

Hence the p^{th} power of distinct roots α_k of $f_k(x)$ over $\mathbb{Z}_{p^k}$ are all distinct roots of $x^M - 1$ over $\mathbb{Z}_{p^{k+1}}$. In addition, $\alpha_{k+1}^p \equiv \alpha_k^p \equiv \alpha_k \pmod{p}$, and we must therefore have $f_k(\alpha_k^p) \equiv 0 \pmod{p^k}$.

The roots of f_{k+1} over $\mathbb{Z}_{p^{k+1}}$ are, up to mod p^{k+1} the p^{th} power of all the roots of $f_k(x)$ over $\mathbb{Z}_{p^k}$. Therefore item 3 is proven. □

Similar to GCD operations, we can in fact calculate the lifting using operations over the ground ring $\mathbb{Z}$. This can be done with polynomial resultants.

Definition 3. *(Univariate Resultant [21]) Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $g(x) = b_0 + b_1x + \ldots + b_mx^m$ where $a_n, b_m \neq 0$. The resultant of f, g is the determinant of the $(m+n) \times (m+n)$ Silvester matrix:*

$$\mathsf{Res}(f,g) := \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{pmatrix}$$

In particular, if $(\alpha_i)_{i=1}^n$, $(\beta_j)_{j=1}^m$ are the roots of f, g in some extension field. Then

$$\mathsf{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j)$$

Proposition 5. *Let $d > 0$, $f(x) \in \mathbb{Z}[x]$ be a degree n monic polynomial, $g(x) = \mathsf{Res}_y(x - y^d, f(y))$ the resultant of $x - y^d, f(y)$ considered as polynomials in y with coefficients in $\mathbb{Z}[x]$. Then $g(x) \in \mathbb{Z}[x]$ with leading coefficient ± 1. Moreover, the roots of $g(x)$ are exactly the d^{th} power of all the roots of $f(x)$ over an algebraically closed field.*

Proof. Let $\mathcal{K}$ be an algebraically closed field containing $\mathbb{Q}(x)$. Let $\beta_0, \ldots, \beta_{n-1} \in \mathcal{K}$ be the roots of $f(y)$ and $\zeta \in \mathcal{K}$ a primitive d^{th} root of unity. We have

$$x - y^d = \prod_{i=0}^{d-1} (x^{\frac{1}{d}} - \zeta^i y), \qquad f(y) = \prod_{i=0}^{n-1} (y - \beta_i)$$

Therefore the product over root property in definition 3 asserts that

$$\begin{aligned}
&\mathsf{Res}_y(x - y^d, f(y)) = (-1)^n \prod_{i=0}^{d-1} f(\zeta^{d-i} x^{\frac{1}{d}}) = (-1)^n \prod_{i=0}^{d-1} \prod_{j=0}^{n-1} (\zeta^{d-i} x^{\frac{1}{d}} - \beta_j) \\
&= (-1)^n \prod_{j=0}^{n-1} \left(\prod_{i=0}^{d-1} \zeta^{d-i} \right) \prod_{i=0}^{d-1} (x^{\frac{1}{d}} - \zeta^i \beta_j) = (-1)^n \zeta^{\frac{d(d-1)n}{2}} \prod_{j=0}^{n-1} (x - \beta_j^d) \\
&= \pm \prod_{j=0}^{n-1} (x - \beta_j^d)
\end{aligned}$$

Therefore, up to sign, $g(x)$ is the monic polynomial whose roots are exactly the d^{th} power of the roots of $f(x)$. $g(x) \in \mathbb{Z}[x]$ since the coefficients of $x - y^n, f(y)$ all belong to $\mathbb{Z}[x]$ □

We can combine propositions 4 and 5 to construct an efficient algorithm to lift primitive polynomials.

Algorithm 1 Hensel Lift Primitive Polynomial

```
Input: Monic degree $r$ primitive polynomial $f(x) \in \mathbb{Z}_p[x]$ and exponent $m$
Output: The Hensel Lifted monic polynomial $f_m(x) \in \mathbb{Z}_{p^m}[x]$
1: Let $f_1(x) = f(x)$ and regard $f_1(x) \in \mathbb{Z}[x]$
2: for $k \leftarrow 2$ to $m$ do
3:     Calculate $g(x) = \mathsf{Res}_y(x - y^p, f_{k-1}(y))$ and normalize $g(x)$ to be monic
4:     Let $f_k(x) = g(x) \bmod p^k$
5: end for
6: Return $f_m(x)$
```

Remark 1. Alternatively, we may simply calculate $g(x) = \mathsf{Res}_y(x - y^{p^m}, f(y))$ and directly obtain $f_m(x) = g(x) \bmod p^m$. The difference is mainly that of efficiency.

In algorithm 1 we calculate $m - 1$ determinants whose matrices are of dimension $p + r - 1$ whereas here we calculate 1 determinant whose matrix is of dimension $p^m + r - 1$

Remark 2. When $p = 2$, we may use the following simplified procedure inside the for loop of algorithm 1:

- 3(b). Calculate $G(x) = f_{k-1}(x) f_{k-1}(-x)$. Replace x^2 by x to obtain $g(x) = G(\sqrt{x})$. Normalize $g(x)$ to be monic.
- 4(b). Let $f_k(x) = g(x) \bmod 2^k$

Example 2. Let $p = 2$, $f(x) = x^5 + x^2 + 1$ is a monic primitive polynomial over $\mathbb{Z}_2[x]$. According to algorithm 1 and the previous remark

$$\begin{aligned}
f_1(x) f_1(-x) &= -x^{10} + x^4 + 2x^2 + 1 \\
f_2(x) &= x^5 + 3x^2 + 2x + 3 \\
f_2(x) f_2(-x) &= -x^{10} - 4x^6 + 9x^4 + 14x^2 + 9 \\
f_3(x) &= x^5 + 4x^3 + 7x^2 + 2x + 7 \\
f_3(x) f_3(-x) &= -x^{10} - 8x^8 - 20x^6 + 33x^4 + 94x^2 + 49 \\
f_4(x) &= x^5 + 8x^4 + 4x^3 + 15x^2 + 2x + 15
\end{aligned}$$

We can verify that the class $[x]$ is a principal $2^5 - 1 = 31^{\text{th}}$ root of unity in the Galois Ring $\mathsf{GR}(2^4, 5) \cong \mathbb{Z}[x]/(16, f_4(x))$

Example 3. Let $p = 3$, $f(x) = x^5+2x+1$ is a monic primitive polynomial over $\mathbb{Z}_3[x]$. According to algorithm 1

$$\begin{aligned}
\mathsf{Res}_y(x - y^3, f(y)) &= -x^5 + 6x^2 - 8x - 1 \\
f_2(x) &= x^5 + 3x^2 + 8x + 1 \\
\mathsf{Res}_y(x - y^3, f_2(y)) &= -x^5 - 9x^4 - 27x^3 - 3x^2 - 440x - 1 \\
f_3(x) &= x^5 + 9x^4 + 3x^2 + 8x + 1 \\
\mathsf{Res}_y(x - y^3, f_2(y)) &= -x^5 - 738x^4 - 1944x^3 - 1650x^2 - 440x - 1 \\
f_4(x) &= x^5 + 9x^4 + 30x^2 + 35x + 1
\end{aligned}$$

We can easily verify that the equivalent class $[x]$ is a principal $3^5 - 1 = 242^{\text{th}}$ root of unity in the Galois Ring $\mathsf{GR}(3^4, 5) \cong \mathbb{Z}[x]/(81, f_4(x))$

4 Padding to Better Lengths

NTT/FFT related algorithms usually work best, or only work, over special lengths. Given arbitrary length argument, we usually need to 0-pad them to longer sequences to apply these algorithms. In this paper we will adopt the following simple padding strategy.

Proposition 6. *Let $\boldsymbol{u} = (u_0, \ldots, u_{N-1}), \boldsymbol{v} = (v_0, \ldots, v_{N-1})$ be 2 sequences of length N. For any $M \geq 2N - 1$, we can reduce the length N circular convolution problem to the length M circular convolution problem using the following padding strategy:*

- *Let $\Delta_1 = M - 2N + 1$ and let $\boldsymbol{u}' = \boldsymbol{u} \parallel \mathbf{0}^{\Delta_1} \parallel (u_1, \ldots, u_{N-1})$*
- *Let $\Delta_2 = M - N$ and let $\boldsymbol{v}' = \boldsymbol{v} \parallel \mathbf{0}^{\Delta_2}$*
- *Calculate the length M circular convolution $\boldsymbol{w}' = \boldsymbol{u}' \circledast \boldsymbol{v}'$ and retain only the first N result $\boldsymbol{w} = ({w'}_0, \ldots, {w'}_{N-1})$*

Proof. For any $0 \leq i < N$:

$$\begin{aligned}
w'_i &= \sum_{j=0}^{M-1} u'_j v'_{i-j} = \sum_{j=0}^{M-1} v'_j u'_{i-j} = \sum_{j=0}^{N-1} b_j a'_{i-j} \\
&= \sum_{j=0}^{i} v_j u_{i-j} + \sum_{j=i+1}^{N-1} v_j u_{M-(j-i)} = \sum_{j=0}^{i} v_j u_{i-j} + \sum_{j=i+1}^{N-1} v_j u_{N-(j-i)} \\
&= \sum_{j=0}^{N-1} v_j u_{i-j} = w_i
\end{aligned}$$

□

Example 4. Suppose $N = 3$ and $\boldsymbol{u} = (1, 2, 3)$, $\boldsymbol{v} = (-1, 0, 1)$. To calculate their circular convolution it is convenient to pad the inputs to length $M = 8 > 2N - 1$. According to proposition 6

$$\boldsymbol{u}' = (1, 2, 3, 0, 0, 0, 2, 3), \qquad \boldsymbol{v}' = (-1, 0, 1, 0, 0, 0, 0, 0)$$

We then calculate the circular convolution of $\boldsymbol{u}', \boldsymbol{v}'$, or equivalently calculate

$$\begin{bmatrix}
1 & 3 & 2 & 0 & 0 & 0 & 3 & 2 \\
2 & 1 & 3 & 2 & 0 & 0 & 0 & 3 \\
3 & 2 & 1 & 3 & 2 & 0 & 0 & 0 \\
0 & 3 & 2 & 1 & 3 & 2 & 0 & 0 \\
0 & 0 & 3 & 2 & 1 & 3 & 2 & 0 \\
0 & 0 & 0 & 3 & 2 & 1 & 3 & 2 \\
2 & 0 & 0 & 0 & 3 & 2 & 1 & 3 \\
3 & 2 & 0 & 0 & 0 & 3 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
-1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0
\end{bmatrix}$$

And only retain the first 3 components

References

1. Berlekamp, E.R.: Negacyclic codes for the lee metric. In: Bose, R.C., Dowling, T.A. (eds.) Combinatorial Mathematics and Its Applications, pp. 298–316. No. 4 in UNC Monograph Series in Probability and Statistics, University of North Carolina Press, Chapel Hill, NC (1969)
2. Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
3. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: Crystals - kyber: A cca-secure module-lattice-based kem. In: Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 353–367. IEEE (2018). https://doi.org/10.1109/EuroSP.2018.00032, https://doi.org/10.1109/EuroSP.2018.00032
4. Bos, L., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G.: Crystals–dilithium: Digital signatures from module lattices. IACR Cryptol. ePrint Arch. **2017**, 633 (2017), https://eprint.iacr.org/2017/633
5. Brakerski, Z.: Leveled fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS). pp. 309–325. ACM (2012). https://doi.org/10.1145/2090236.2090262, https://doi.org/10.1145/2090236.2090262
6. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) lwe. In: Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS). pp. 97–106. IEEE (2011). https://doi.org/10.1109/FOCS.2011.12, https://doi.org/10.1109/FOCS.2011.12
7. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic encryption for arithmetic of approximate numbers. In: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). pp. 409–437. Springer (2017). https://doi.org/10.1007/978-3-319-70694-8_15, https://doi.org/10.1007/978-3-319-70694-8_15
8. Cooley, J.W., Lewis, P.A., Welch, P.D.: Historical notes on the fast fourier transform. Proceedings of the IEEE **55**(10), 1675–1677 (1967)
9. Dougherty, S.T., Şahinkaya, S.: On cyclic and negacyclic codes with one-dimensional hulls and their applications. Advances in Mathematics of Communications **16**(4), 765–780 (2022). https://doi.org/10.3934/amc.2022096, https://doi.org/10.3934/amc.2022096
10. Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon: Fast-fourier lattice-based compact signatures over ntru. In: Proceedings of the 2018 International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). pp. 123–151. Springer (2018). https://doi.org/10.1007/978-3-030-03329-3_5, https://doi.org/10.1007/978-3-030-03329-3_5
11. Good, I.J.: The interaction algorithm and practical fourier analysis. Journal of the Royal Statistical Society Series B: Statistical Methodology **20**(2), 361–372 (1958)
12. McDonald, B.R.: Finite rings with identity. Marcel Dekker (1974)
13. McGuire, G.: An approach to hensel's lemma. Irish Math Soc. Bulletin **47**, 15–21 (2001)
14. Rosowski, A.: On fast computation of a circulant matrix-vector product. arXiv preprint arXiv:2103.02605 (2021)
15. Shoup, V.: A new polynomial factorization algorithm and its implementation. Journal of Symbolic Computation **20**(4), 363–397 (1995)
16. Thomas, L.H.: Using a computer to solve problems in physics. Applications of digital computers pp. 44–45 (1963)
17. Wikipedia contributors: Galois ring — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Galois_ring&oldid=1181997128 (2023), [Online; accessed 29-April-2025]
18. Wikipedia contributors: Principal root of unity — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Principal_root_of_unity&oldid=1223603190 (2024), [Online; accessed 29-April-2025]
19. Wikipedia contributors: Division algorithm — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Division_algorithm&oldid=1283459286 (2025), [Online; accessed 29-April-2025]
20. Wikipedia contributors: Hensel's lemma — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Hensel%27s_lemma&oldid=1275481796 (2025), [Online; accessed 29-April-2025]
21. Wikipedia contributors: Resultant — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Resultant&oldid=1280437221 (2025), [Online; accessed 30-April-2025]