IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 13, Issue 2 Ver. I (Mar. - Apr. 2017), PP 31-41
www.iosrjournals.org

Fast Fourier Transform Over Residue Ring $\mathbb{Z}_p[x]/(f(x))$

P.Anuradha Kameswari, Y.Swathi
Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.

Abstract: *A transform analogous to the Discrete Fourier transform in a residue ring $\mathbb{Z}_p[x]/(f(x))$, where $f(x)$ in $\mathbb{Z}_p[x]$ is not necessarily irreducible, is defined. The convolution property is useful in the product of large polynomials in $\mathbb{Z}_p[x]$ and in between the Discrete Fourier transform on $\mathbb{Z}_p$ is also applied.*
Key words :*Residue Ring, Fourier Transform*

I. Introduction

Fast Fourier Transform (FFT) is generalized to general rings and finite fields which is useful in construction of fast algorithm for polynomial multiplication. J.M. Pollard generalized the FFT to certain finite fields and showed how it could be used for multiplication of polynomials over these fields. For Fast Fourier transform in a finite field, consider a finite field with p^n elements denoted as F_{p^n}. Let d be a divisor of $p^n - 1$, and α be an element of order d in $F^* = F - \{0\}$, a multiplicative group of F [3][4]. Then in [1] the transform of a sequence $\{a_i\}\ 0 \le i \le d-1$ of members of F is defined to be the sequence $\{A_i\}$ where

$$A_i = \sum_{j=0}^{d-1} a_j \alpha^{ij} \qquad (1)$$

The transformed sequence A_i depends on the choice of r, which is fixed throughout. The inverse transform to (1) is given as

$$a_j = -d' . \sum_{i=0}^{d-1} A_i \alpha^{-ij} \qquad (2)$$

where d' is the integer for which

$$d'd = p^n - 1.$$

This Discrete Fourier transform is with the basic properties (1) ⇔ (2) and the convolution property. The convolution property is as follows:
For three pairs of sequences, $(\{a_i\}\ and\ \{A_i\}), (\{b_i\}\ and\ \{B_i\}), (\{c_i\}\ and\ \{C_i\})\ (0 \le i \le d-1)$ form transform pairs and that

$$C_i = A_i B_i, (0 \le i \le d-1).$$

$$\text{Then}, c_i = \sum_{\substack{j=0 \\ j+k=i(\text{mod } d)}}^{d-1} \sum_{k=0}^{d-1} a_j b_k, (0 \le i \le d-1).$$

In particular by making the sequence period with period d, above equation may be written

$$c_i = \sum_{j=0}^{d-1} a_i b_{i-j}.$$

where the subscript $i-j$ is computed modulo d [7]. Basic properties can be evaluated from the following remark.

1.1 Remark:In any field F, for any α in F^* with $O(\alpha) = d$, for any integer k

$$\sum_{i=0}^{d-1} \alpha^{ik} = \begin{cases} d, \text{if } k \equiv 0 (\text{mod } d) \\ 0, \text{otherwise} \end{cases}$$

The Fast Fourier Transform over finite fields is quite useful in the Multiplication of Polynomials over F_{p^n}, Multiplication of Integer Polynomials, Multiplication of Very Large Integers, Division of Polynomials Over F_p. A version of the transform

$$A_i = \sum_{j=0}^{d-1} a_j \alpha^{ij}$$

is in a ring which is not field, Z_m of Integer modulo a composite number m is given in [1]. Adapting these ideas, in this paper we give a version of the transform as above in the residue ring $\mathbb{Z}_p[x]/(f(x))$ for any polynomial $f(x) \in \mathbb{Z}_p[x]$, where $f(x)$ in $\mathbb{Z}_p[x]$ is not necessarily irreducible.

II. Fast Fourier Transform In The Residue Ring $\mathbb{Z}_p[x]/(f(x))$

Let $f(x)$ be a polynomial in $\mathbb{Z}_p[x]$. In this paper, we introduce a version of the transform

$$A_i(x) = \sum_{j=0}^{d-1} a_j(x)\alpha(x)^{ij}$$

is given on a particular Ring $\mathbb{Z}_p[x]/(f(x))$, where $f(x)$in $\mathbb{Z}_p[x]$ is not necessarily irreducible. In our paper Counting in $\mathbb{Z}_p[x]$ [2] it is proved that the multiplicative group $(\mathbb{Z}_p[x]/(f(x)))^*$, the group of units of $\mathbb{Z}_p[x]/(f(x))$ is of order equal to $\phi_p(f(x)) = p^{deg(f(x))} \prod_{g(x)|f(x)} (1-\frac{1}{p^{deg(g(x))}})$. Note this order divisible by $p-1$ and for a polynomial $\alpha(x) \in (\mathbb{Z}_p[x]/(f(x)))^*$ with $o(\alpha(x)) = d$ for some $d|p-1$, we have the following lemma in $\mathbb{Z}_p[x]/(f(x))$.

2.1 Lemma: In $\mathbb{Z}_p[x]/(f(x))$, if $f(x) = g_1(x)^{e_1} g_2(x)^{e_2} g_3(x)^{e_3} \dots g_r(x)^{e_r}$ where $d|(p-1)$ and $o(\alpha(x)) = d$ in $\mathbb{Z}_p[x]/(f(x))$then

$$\sum_{i=0}^{d-1} \alpha(x)^{ik} = \begin{cases} \text{d, if } k \equiv 0(\text{mod } d) \\ 0, \text{if } k \not\equiv 0(\text{mod } d) \end{cases}$$

Proof. Let $f(x) = g_1(x)^{e_1} g_2(x)^{e_2} g_3(x)^{e_3} \dots g_r(x)^{e_r}$ and $o(\alpha(x)) = d$. By a known result we have $\alpha(x)^k = \alpha(x)^0$ $if\ and\ only\ if\ k \equiv 0(\text{mod} o(\alpha(x)))$ This implies $\alpha(x)^k = 1$ for all $k \equiv 0(\text{mod} d)$, therefore we have

$$\sum_{i=0}^{d-1} \alpha(x)^{ik} = \sum_{i=0}^{d-1} 1 = d \text{ for all } k \equiv 0(\text{mod} d)$$

Now for $k \not\equiv 0 \text{mod } d$, consider

$$\left(\sum_{i=0}^{d-1} \alpha(x)^{ik}\right)(1-\alpha(x)^k) \text{ in } \mathbb{Z}_p[x]/(f(x))$$

then we have

$$\left(\sum_{i=0}^{d-1} \alpha(x)^{ik}\right)(1-\alpha(x)^k) = \alpha(x)^0 - \alpha(x)^{kd}$$
$$= 1 - \alpha(x)^{kd}$$
$$= 0.$$

$$\text{Therefore in} \mathbb{Z}_p[x]/(f(x)), \left(\sum_{i=0}^{d-1} \alpha(x)^{ik}\right)(1-\alpha(x)^k) = 0$$

Now note if we have $1-\alpha(x)^k \not\equiv 0 \text{ mod}(g_i(x))$ then by above equation

$$\sum_{i=0}^{d-1} \alpha(x)^{ik} \equiv 0 \text{ mod}(f(x))$$

, as, $1-\alpha(x)^k \not\equiv 0 \text{ mod}(g_i(x))$ implies $1-\alpha(x)^k \not\equiv 0 \text{ mod}(g_i(x)^{e_i})$ for all $g_i(x)^{e_i}$, then this implies

$1-\alpha(x)^k \not\equiv 0 \bmod(f(x))$ implies $1-\alpha(x)^k$ is in $(\mathbb{Z}_p[x]/(f(x)))^*$, further

$$\sum_{i=0}^{d-1} \alpha(x)^{ik} \not\equiv 0 \bmod(f(x))$$

also implies

$$\sum_{i=0}^{d-1} \alpha(x)^{ik}$$

is in $(\mathbb{Z}_p[x]/(f(x)))^*$ hence their product would be in $(\mathbb{Z}_p[x]/(f(x)))^*$, which implies

$$\left(\sum_{i=0}^{d-1} \alpha(x)^{ik}\right)(1-\alpha(x)^k) \not\equiv 0 \bmod(f(x))$$

which is a contradiction to above observation that in $\mathbb{Z}_p[x]/(f(x))$, $\left(\sum_{i=0}^{d-1} \alpha(x)^{ik}\right)(1-\alpha(x)^k) = 0$.
Therefore it remains to prove $1-\alpha(x)^k \not\equiv 0 \bmod(g_i(x))$.For this, note the set

$$H = \{\alpha(x)^0, \alpha(x)^1, \alpha(x)^2, \dots, \alpha(x)^{d-1}\}$$

forms a subgroup of $(\mathbb{Z}_p[x]/(f(x)))^*$ of order d and the set N given as

$$N = \{a(x) \in \mathbb{Z}_p[x]/(f(x)) : a(x) \equiv 1 \bmod g_i(x)\}$$

$$= \{g_i(x)\, t_i(x) + 1 : i = 1,2,3, \dots, p^{deg(f(x))-deg(g_i(x))}\}$$

is a subgroup in $(\mathbb{Z}_p[x]/(f(x)))^*$ of order $p^{deg(f(x))-deg(g_i(x))}$.Now $for\ all\ \alpha(x)^k \in H, if\ \alpha(x)^k \in N$, then we have $\alpha(x)^k \in H \cap N$. But note as $o(H) = d$, where $d|p-1$ and $o(N) = p^{deg(f(x))-deg(g_i(x))}$ we have $(d, p^{deg(f(x))-deg(g_i(x))}) = 1 \Rightarrow o(H \cap N) = 1, \Rightarrow H \cap N = \{1\}$, implies $\alpha(x)^k = 1$ giving k= 0, contradiction as we have $k \not\equiv 0 \bmod d$, hence for all $k \not\equiv 0 \bmod d$, $\alpha(x)^k \not\equiv 1\ in\ H$, implies$\alpha(x)^k \notin N$, that is $\alpha(x)^k \not\equiv 1 \bmod g_i(x)$.

In the following theorem, we introduce the Discrete Fourier Transform in the residue ring $\mathbb{Z}_p[x]/(f(x))$

$for\ f(x) = \prod_{i=1}^{r} g_i(x)^{e_i}$,

$g_i(x) \in \mathbb{Z}_p[x]/(f(x))$ is an irreducible polynomial.

2.2 Theorem: For any sequence $\{a_j(x)\}$ of polynomials in $\mathbb{Z}_p[x]/(f(x))$ there is a transform $\{A_i(x)\}$ given as

$$A_i(x) = \sum_{j=0}^{d-1} a_j(x)\alpha(x)^{ij}$$

for $\alpha(x) \in \mathbb{Z}_p[x]$ with the inverse transform given

$$a_j(x) = -d' \sum_{i=0}^{d-1} A_i(x)\alpha(x)^{-ij}$$

where $dd' = p-1$.

Proof. Given Sequence$\{a_i(x)\}$ with

$$A_i(x) = \sum_{j=0}^{d-1} a_j(x)\alpha(x)^{ij}$$

.

$$\text{We have } -d' \sum_{i=0}^{d-1} A_i(x)\alpha(x)^{-ij} = -d' \sum_{i=0}^{d-1} \left(\sum_{l=0}^{d-1} a_l(x)\alpha(x)^{li}\right)(\alpha(x)^{-ij})$$

$$= -d' \sum_{i=0}^{d-1} \sum_{l=0}^{d-1} a_l(x)\alpha(x)^{i(l-j)}$$

$$= -d'\left[\left(\sum_{\substack{l=0 \\ l\equiv j \bmod d}}^{d-1} a_l(x)\sum_{i=0}^{d-1}\alpha(x)^{i(l-j)}\right)+\left(\sum_{\substack{l=0 \\ l\not\equiv j \bmod d}}^{d-1} a_l(x)\sum_{i=0}^{d-1}\alpha(x)^{i(l-j)}\right)\right]$$

$$= -d'\left(a_j(x).d+0\right)(By\ Lemma)$$

$$= a_j(x).$$

$$\text{Therefore} a_j(x) = \sum_{i=0}^{d-1} A_i(x)\alpha(x)^{-ij}$$

$$\text{Conversely, given sequence } A_i(x)\ with\ a_i = -d'\sum_{j=0}^{d-1} A_j(x)\alpha(x)^{-ij}$$

.

We have

$$\sum_{j=0}^{d-1} a_j(x)\alpha(x)^{ij} = -d'\sum_{j=0}^{d-1}\left(\sum_{k=0}^{d-1}(A_k(x)\alpha(x)^{-kj})\alpha(x)^{ij}\right)$$

$$= -d'\sum_{k=0}^{d-1} A_k(x)\sum_{j=0}^{d-1}\alpha(x)^{j(i-k)}$$

$$= -d'\sum_{\substack{k=0 \\ i-k\equiv 0 \bmod d}}^{d-1} A_k(x)d\ (By\ Lemma)$$

$$= -d'dA_i(x)$$
$$= A_i(x).$$

$$\text{Therefore} A_i(x) = \sum_{j=0}^{d-1} a_j(x)\alpha(x)^{ij}\ .$$

2.3 Example: Let $\mathbb{Z}_{13}[x]/(x^2-4)$ denote the Residue Ring modulo (x^2-4).

Let d be the divisor of $(p-1)=(13-1)$ and $\alpha(x)=5x+6$ be a member of $\mathbb{Z}_{13}[x]/(x^2-4)$ of order $d=3$ in the multiplicative group, $(\mathbb{Z}_{13}[x]/(x^2-4))^*$ say, of nonzero elements of $\mathbb{Z}_{13}[x]/(x^2-4)$.

Then we can define the transform of a sequence $\{a_i(x)\}\big(0\le i\le(d-1)\big)\ x+2, x+3, x+4$ of members of $\mathbb{Z}_{13}[x]/(x^2-4)$ to be the sequence $\{A_i(x)\}$ where

$$A_i(x) = \sum_{j=0}^{d-1} a_j(x)(\alpha(x))^{ij}$$

.

Now calculate $A_i(x)'s$:

$$A_0(x) = \sum_{j=0}^{2} a_j(x)(\alpha(x))^{0j}$$

$$= a_0(x)+a_1(x)+a_2(x)$$
$$= x+2+x+3+x+4$$

$$\text{Therefore} A_0(x) = 3x+9.$$

$$A_1(x) = \sum_{j=0}^{2} a_j(x)(\alpha(x))^{1j}$$
$$= a_0(x) + a_1(x)\alpha(x) + a_2(x)(\alpha(x))^2$$
$$= x + 2 + (x+3)(5x+6) + (x+4)(5x+6)^2$$
$$= x + 2 + 5x^2 + 6x + 15x + 18 + (x+4)(25x^2 + 60x + 36)$$
$$= x + 2 + 5x^2 + 6x + 15x + 18 + (x+4)(12x^2 + 8x + 10)$$
$$= 12x^3 + 61x^2 + 64\text{x} + 60$$

Therefore $A_1(x) = 8x + 5$.

$$A_2(x) = \sum_{j=0}^{2} a_j(x)(\alpha(x))^{2j}$$
$$= a_0(x) + a_1(x)(\alpha(x))^2 + a_2(x)(\alpha(x))^4$$
$$= x + 2 + (x+3)(5x+6)^2 + (x+4)(5x+6)^4$$
$$= x + 2 + (x+3)(12x^2 + 8x + 10) + (x+4)(5x+6)$$
$$= x + 2 + 12x^3 + 8x^2 + 10x + 36x^2 + 24x + 30 + 24x + 5x^2 + 26x + 24$$
$$= 12x^3 + 10x^2 + 9x + 4$$

Therefore $A_2(x) = 5x + 5$.

We get $A_0(x) = 3x + 9, A_1(x) = 8x + 5, A_2(x) = 5x + 5$.

Now we find inverse transform to

$$A_i(x) = \sum_{j=0}^{d-1} a_j(x)(\alpha(x))^{ij}, \text{is}$$

$$a_j(x) = -d' \sum_{i=0}^{d-1} A_i(x)(\alpha(x))^{-ij}$$

where d' is the integer for which $d'd = p - 1$.

Now calculate $a_j(x)'s$:

$$a_j(x) = -d' \sum_{i=0}^{d-1} A_i(x)(\alpha(x))^{-ij}$$
$$a_0(x) = d'[A_0(x) + A_1(x) + A_2(x)]$$
$$= 9[3x + 9 + 8x + 5 + 5x + 5]$$
$$= 9[16x + 19]$$
$$= x + 2.$$
Therefore $a_0(x) = x + 2$.

$$a_1(x) = -d' \sum_{i=0}^{d-1} A_i(x)(\alpha(x))^{-i1}$$
$$= d'[A_0(x) + A_1(x)\alpha(x)^{-1} + A_2(x)\alpha(x)^{-2}]$$
$$= 9[3x + 9 + (8x+5)(5x+6)^{-1} + (5x+5)(5x+6)^{-2}]$$
$$= 9[3x + 9 + (8x+5)(12x^2 + 8x + 10) + (5x+5)(5x+6)]$$
$$= 9[3x + 9 + (5x^3 + 12x^2 + 2x + 8x^2 + x + 11) + 12x^2 + 3x + 4]$$
$$= 9[5x^3 + 6^2 + 9x + 11]$$
$$= 45x^3 + 54x^2 + 81x + 99$$

$= 6x^3 + 2x^2 + 3x + 8$
$= x + 3.$

Therefore$a_1(x) = x + 3.$

$$a_2(x) = -d' \sum_{i=0}^{d-1} A_i(x)(\alpha(x))^{-i2}$$

$= d'[A_0(x) + A_1(x)\alpha(x)^{-2} + A_2(x)\alpha(x)^{-4}]$
$= 9[3x + 9 + (8x + 9)(5x + 6) + (5x + 5)(12x^2 + 8x + 10)]$
$= 9[3x + 9 + 40x^2 + 48x + 25x + 30 + 60x^3 + 40x^2 + 30x + 60x^2 + 40x + 50]$
$= 9[60x^3 + 140x^2 + 166x + 89]$
$= 540x^3 + 1260x^2 + 1494x + 801$
$= 7x^3 + 12x^2 + 12x + 8$
$= x + 4.$

Therefore$a_2(x) = x + 4.$

III. Application of The Transform

3.1 Theorem(**Convolution Property**):If the three pairs of sequences,

$\{a_i(x)\}$ and $\{A_i(x)\})$, $(\{b_i(x)\}$ and$\{B_i(x)\}),(\{c_i(x)\}$ and $\{C_i(x)\})$ for $0 \le i \le d-1$ form transform pairs and that

$$C_i(x) = A_i(x)B_i(x), (0 \le i \le d-1).$$

$$\text{Then, } c_i(x) = \sum_{\substack{j=0 \\ j+k=i(\text{mod } d)}}^{d-1} \sum_{k=0}^{d-1} a_j(x)b_k(x), (0 \le i \le d-1).$$

Proof. Given Sequence $\{c_i(x)\}$ with

$$C_i(x) = \sum_{j=0}^{d-1} c_j(x)\alpha(x)^{ij}$$

Suppose for the given transform pairs we have $C_i(x) = A_i(x)B_i(x)$.
Then as $\{c_i(x)\}, \{C_i(x)\} 0 \le i \le d-1$ form a transform pair we have

$$C_i(x) = \sum_{j=0}^{d-1} c_j(x)\alpha(x)^{ij}$$

$$\text{with inverse transform} c_j(x) = -d' \sum_{i=0}^{d-1} C_i(x)\alpha(x)^{-ij}$$

$$c_i(x) = -d' \sum_{j=0}^{d-1} C_j(x)\alpha(x)^{-ij} = -d' \sum_{j=0}^{d-1} A_j(x)B_j(x)\alpha(x)^{-ij}$$

$$= -d' \sum_{j=0}^{d-1} \left(\sum_{k=0}^{d-1} a_k(x)\alpha(x)^{jk} \right) \left(\sum_{s=0}^{d-1} b_s(x)\alpha(x)^{js} \right) \alpha(x)^{-ij}$$

$$= -d' \sum_{k=0}^{d-1} \sum_{s=0}^{d-1} a_k(x)b_s(x) - d' \sum_{j=0}^{d-1} \alpha(x)^{j(k+s-i)}$$

$$= -d' \sum_{\substack{k=0 \\ k+s=i \bmod d}}^{d-1} \sum_{j=0}^{d-1} a_k(x) b_s(x) d \text{ (By } Lemma)$$

$$= \sum_{\substack{k=0 \\ k+s=i \bmod d}}^{d-1} \sum_{s=0}^{d-1} a_k(x) b_s(x)$$

$$\text{Therefore } c_i(x) = \sum_{k=0}^{d-1} a_k(x) b_{i-k}(x)$$

3.2The Multiplication of very Large Polynomials:

In the following we demonstrate the convolution property in the multiplication of large polynomials.
Suppose $g(x)$, $h(x)$ be large polynomials.
Let $r(x)$ be the polynomial with $deg(r(x)) < deg(f(x))$, $(r(x), f(x)) = 1$ and $o(r(x)) = d$
Suppose the polynomials are expressed to the base $r(x)$,

$$g(x) = \sum_{i=0}^{m_1} a_i(x)(r(x))^i,$$

$$h(x) = \sum_{i=0}^{m_2} b_i(x)(r(x))^i$$

where$(0 \le a_i(x) \le r(x), 0 \le b_i(x) \le r(x))$.

Then by the Convolution property, their product is

$$s(x) = \sum_{i=0}^{m_1+m_2} c_i(x)(r(x))^i,$$

where the $(c_i(x))$, defined as

$$c_k(x) = \sum_{0 \le i \le m_1; 0 \le j \le m_2; i+j=k} a_i(x) b_j(x),$$
$$(0 \le k \le (m_1 + m_2)),$$

do not necessarily satisfy $0 \le c_i(x) \le r(x)$.

3.2.1 Example: Let $g(x) = x^6 + 10x^5 + 4x^4 + 6x^3 + 5x^2 + 3x + 2, h(x) = x^5 + 11x^4 + 8x^3 + 2x^2 + 4x + 5 \in \mathbb{Z}_{13}[x]/(x^8 + 12x^7 + 5x^6 + 5x^5 + 10x^4 + x^3 + 11x^2 + 3x + 7)$ Let $d = 12$ be a divisor of $p - 1 = 13 - 1$ and Choose a base $r(x) = x^2 + 3x + 4 \ni (r(x))^{12} = 1$ *in* $\mathbb{Z}_{13}[x]/(x^8 + 12x^7 + 5x^6 + 5x^5 + 10x^4 + x^3 + 11x^2 + 3x + 7)$

Suppose the polynomials $g(x), h(x)$ are expressed to the base $r(x)$ as

$$g(x) = \sum_{i=0}^{m_1} a_i(x)(r(x))^i, \left(0 \le \ a_i(x) \le r(x)\right)$$
$$= (6x + 8)(x^2 + 3x + 4)^0 + (6x + 10)(x^2 + 3x + 4)^1 + (x + 11)(x^2 + 3x + 4)^2 + (1)(x^2 + \ 3x + 4)^3$$

and

$$h(x) = \sum_{i=0}^{m_2} b_i(x)(r(x))^i, 0 \le \ b_i(x) \le r(x)$$

$$= (7x+2)(x^2+3x+4)^0 + (10)(x^2+3x+4)^1 + (x+5)(x^2+3x+4)^2$$

$$\text{Their product is } s(x) = \sum_{i=0}^{m_1+m_2} c_i(x)(r(x))^i$$

where do not necessarily satisfy $0 \le c_i(x) \le r(x)$.

Now we first obtained $(c_i(x))'s$, using $\left(a_i(x)\right)' s$ and$(b_i(x))'s$

$$c_i(x) = \sum_{j=0}^{d-1} a_j(x) b_{i-j}(x)$$

$$\text{Then} c_0(x) = \sum_{j=0}^{d-1} a_j(x) b_{0-j}(x)$$

$$\begin{aligned}
&= a_0(x)b_0(x) + a_1(x) + b_{0-1}(x) + a_2(x)b_{0-2}(x) + a_3(x)b_{0-3} + a_4(x)b_{0-4}(x) + \cdots \\
&\quad + \quad a_{11}(x)b_{0-11}(x) \\
&= a_0(x)b_0(x) + a_1(x)b_{11}(x) + a_2(x)b_10(x) + a_3(x)b_9(x) \\
&+a_4(x)b_8(x) + \cdots + a_{11}(x)b_1(x)(k = i + j \text{mod} d) \\
&= a_0(x)b_0(x) + 0 + 0 + 0 + 0 + \cdots + 0 \\
&= (6x+8)(7x+2) \\
&= 42x^2 + 68x + 16 \\
&= 3x^2 + 3x + 3 \text{ in } \mathbb{Z}_{13}[x] \\
c_0(x) &= 3x^2 + 3x + 3
\end{aligned}$$

$$c_1(x) = \sum_{j=0}^{d-1} a_j(x) b_{1-j}(x)$$

$$\begin{aligned}
&= a_0(x)b_{1-0}(x) + a_1(x) + b_{1-1}(x) + a_2(x)b_{1-2}(x) + a_3(x)b_{1-3} + a_4(x)b_{1-4}(x) + \cdots \\
&\quad + \quad a_{11}(x)b_{1-11}(x) \\
&= a_0(x)b_1(x) + a_1(x)b_0(x) + a_2(x)b_{11}(x) + a_3(x)b_{10}(x) \\
&+a_4(x)b_9(x) + \cdots + a_{11}(x)b_2(x)(k = i + j \bmod d) \\
&= a_0(x)b_1(x) + a_1(x)b_0(x) + 0 + 0 + 0 + \cdots + 0 \\
&= (6x+8)(10) + (6x+10)(7x+2) \\
&= 42x^2 + 142x + 100 \\
&= 3x^2 + 12x + 9 \text{ in } \mathbb{Z}_{13}[x] \\
c_1(x) &= 3x^2 + 3x + 3
\end{aligned}$$

$$c_2(x) = \sum_{j=0}^{d-1} a_j(x) b_{2-j}(x)$$

$$\begin{aligned}
&= a_0(x)b_{2-0}(x) + a_1(x) + b_{2-1}(x) + a_2(x)b_{2-2}(x) + a_3(x)b_{2-3} + a_4(x)b_{2-4}(x) + \cdots + \\
&\quad a_{11}(x)b_{2-11}(x) \\
&= a_0(x)b_2(x) + a_1(x)b_1(x) + a_2(x)b_0(x) + a_3(x)b_{11}(x) \\
&+a_4(x)b_{10(x)} + \cdots + a_{11}(x)b_3(x)(k = i + j \bmod d) \\
&= a_0(x)\mathrm{b}_2(x) + a_1(x)b_1(x) + a_2(x)b_0(x) + 0 + 0 + \cdots + 0 \\
&= (6x+8)(x+5) + (6x+10)(10) + (x+11)(7x+2) \\
&= 13x^2 + 177x + 162 \\
&= 8x + 6 \text{ in } \mathbb{Z}_{13}[x] \\
c_2(x) &= 8x + 6
\end{aligned}$$

$$c_3(x) = \sum_{j=0}^{d-1} a_j(x) b_{3-j}(x)$$

$= a_0(x)b_{3-0}(x) + a_1(x) + b_{3-1}(x) + a_2(x)b_{3-2}(x) + a_3(x)b_{3-3} + a_4(x)b_{3-4}(x) + \cdots + a_{11}(x)b_{1-11}(x)$
$= a_0(x)b_3(x) + a_1(x)b_2(x) + a_2(x)b_1(x) + a_3(x)b_0(x)$
$+a_4(x)b_{11}(x) + \cdots + a_{11}(x)b_4(x)(k = i + j \bmod d)$
$= 0 + a_1(x)b_2(x) + a_2(x)b_1(x) + a_3(x)b_0(x) + 0 + 0 \ldots + 0$
$= (6x + 10)(x + 5) + (x + 5)(10) + (1)(7x + 2)$
$= 6x^2 + 57x + 162$
$= 6x^2 + 5x + 6 \text{ in } \mathbb{Z}_{13}[x]$
$c_3(x) = 6x^2 + 5x + 6$

$$c_4(x) = \sum_{j=0}^{d-1} a_j(x) b_{4-j}(x)$$

$= a_0(x)b_{4-0}(x) + a_1(x) + b_{4-1}(x) + a_2(x)b_{4-2}(x) + a_3(x)b_{4-3} + a_4(x)b_{4-4}(x) + \cdots + a_{11}(x)b_{4-11}(x)$
$= a_0(x)b_4(x) + a_1(x)b_3(x) + a_2(x)b_2(x) + a_3(x)b_1(\mathrm{x})$
$+a_4(x)b_0(x) + a_5(x)b_{11}(x) \ldots + a_{11}(x)b_5(x)(k = i + j \bmod d)$
$= 0 + 0 + a_2(x)b_2(x) + a_3(x)b_1(x) + 0 + 0 + 0 \ldots + 0$
$= (x + 11)(x + 5) + (1)(10)$
$= x^2 + 16x + 65$
$= x^2 + 3x \text{ in } \mathbb{Z}_{13}[x]$
$c_4(x) = x^2 + 3x$

$$c_5(x) = \sum_{j=0}^{d-1} a_j(x) b_{5-j}(x)$$

$= a_0(x)b_{5-0}(x) + a_1(x) + b_{5-1}(x) + a_2(x)b_{5-2}(x) + a_3(x)b_{5-3}$
$+a_4(x)b_{5-4}(x) + a_5(x)b_{5-5}(x) + a_6(x)b_{5-6} + \cdots + a_{11}(x)b_{5-11}(x)$
$= a_0(x)b_5(x) + a_1(x)b_4(x) + a_2(x)b_3(x) + a_3(x)b_2(x)$
$+a_4(x)b_1(x) + a_5(x)b_0(x) + a_6(x)b_{11}(x) \ldots + a_{11}(x)b_6(x)(k = i + j \bmod d)$
$= 0 + 0 + 0 + a_3(x)b_2(x) + +0 + 0 \ldots + 0$
$= (1)(x + 5)$
$= x + 5 \text{ in } \mathbb{Z}_{13}[x]$
$c_5(x) = x + 5$

$$c_6(x) = \sum_{j=0}^{d-1} a_j(x) b_{6-j}(x)$$

$= a_0(x)b_{6-0}(x) + a_1(x) + b_{6-1}(x) + a_2(x)b_{6-2}(x) + a_3(x)b_{6-3}$
$+a_4(x)b_{6-4}(x) + a_5(x)b_{6-5}(x) + a_6(x)b_{6-6} + a_7(x)b_{6-7} + \cdots + a_{11}(x)b_{6-11}(x)$
$= a_0(x)b_6(x) + a_1(x)b_5(x) + a_2(x)b_4(x) + a_3(x)b_3(x)$
$+a_4(x)b_2(x) + a_5(x)b_1(x) + a_6(x)b_0(x) + a_7(x)b_{11} \ldots + a_{11}(x)b_7(x)(k = i + j \bmod d)$
$= 0 + 0 + 0 \ldots + 0$
$= 0 \text{ in } \mathbb{Z}_{13}[x]$
$c_6(x) = 0$

Similarly we get

$$c_7(x) = \sum_{j=0}^{d-1} a_j(x) b_{7-j}(x) = 0$$

$$c_8(x) = \sum_{j=0}^{d-1} a_j(x) b_{8-j}(x) = 0$$

$$c_9(x) = \sum_{j=0}^{d-1} a_j(x) b_{9-j}(x) = 0$$

$$c_{10}(x) = \sum_{j=0}^{d-1} a_j(x) b_{10-j}(x) = 0$$

$$c_{11}(x) = \sum_{j=0}^{d-1} a_j(x) b_{11-j}(x) = 0$$

Therefore the product $g(x).h(x)$ is

$$\begin{aligned} g(x)h(x) &= c_0(x)(r(x))^0 + c_1(x)(r(x))^1 + c_2(x)(r(x))^2 + c_3(x)(r(x))^3 + c_4(x)(r(x))^4 \\ &\quad + c_5(x)(r(x))^5 + c_6(x)(r(x))^6 + c_7(x)(r(x))^7 + \cdots + c_{11}(x)(r(x))^{11} \\ &= (3x^2 + 3x + 3) + (3x^2 + 12x + 9)(x^2 + 3x + 4) + (8x + 6)(x^2 + 3x + 4)^2 \\ &\quad + (6x^2 + 5x + 6)(x^2 + 3x + 4)^3 + (x^2 + 3x)(x^2 + 3x + 4)^4 + (x + 5)(x^2 + \\ &\quad 3x + 4)^5 \\ &= x^{11} + 21x^{10} + 200x^9 + 1172x^8 + 4716x^7 + 13718x^6 + 29481x^5 + 46926x^4 \\ &\quad + 54399x^3 + 43994x^2 + 22526x + 5639 \\ &= x^{11} + 8x^{10} + 5x^9 + 2x^8 + 10x^7 + 3x^6 + 10x^5 + 9x^4 + 7x^3 + 2x^2 + 10x + 10 \\ &= 6488x^7 + 2597x^6 + 2318x^5 + 5592x^4 + 43x^3 + 6035x^2 + 1351x + 3 \\ &= x^7 + 10x^6 + 4x^5 + 2x^4 + 4x^3 + 3x^2 + 12x + 10 \\ &\quad \text{in } \mathbb{Z}_{13}[x]/(x^8 + 12x^7 + 5x^6 + 5x^5 + 10x^4 + x^3 + 11x^2 + 3x + 7). \end{aligned}$$

Note this equals the usual polynomial product of $g(x)$ and $h(x)$.

$$g(x)h(x) = \sum_{k=0}^{d-1} c_k(x)x^k, \text{where}$$

$$c_k(x) = \sum_{i=0}^{k} a_i(x) b_{k-i}(x)$$

IV. Conclusion

The idea of Pollard to multiply polynomials over finite fields in less than $\mathcal{O}(n^2)$multiplications by using the Fast Fourier transform to Discrete Fourier transform, is adapted to the multiplications of large degree polynomials. These polynomials are identified aselements in the residue ring in $\mathbb{Z}_p[x]/(f(x))$and by the convolution property, the product is evaluated by using the transform on $\mathbb{Z}_p[x]/(f(x))$with a suitable element$\alpha(x)$in$(\mathbb{Z}_p[x]/(f(x)))^*$ of order$d$ such that $d|p-1$.

References

Journal Papers:

[1]. J.M.Pollard, *The Fast Fourier Transform in a Finite Field*,Mathematics of Computation,25,1971,365-374.

[2]. P.Anuradha Kameswari and Swathi, *Counting in* $\mathbb{Z}_p[x]$, International Research Jurnoal of Mathematics, Engineering and IT, volume3,issue9,2016,63-70.

Books:

[3]. P.B.Battacharya, S.K.Jain and S.R.Nagpaul, *BASIC ABSTRACT ALGEBRA* (Cambridge:Cambridge University Press,1995).

[4]. I.T.Adamson, *Introduction to Field Theory*, Oliver & Boyd, London,(New York:Interscience,1964).MR 33 # 7325.

[5]. Tom M. Apostol, *Introduction to Analytic Number Theory* (New York:Springer-Verlag,1989).

[6]. Neil Koblitz, A Course in NumberTheory and Cryptography (New York:Springer-Verlag,1994).

Thesis:

[7]. L.Maurits (1105909), *Public key Cryptography Using Discrete Logarithms in Finite Fields:* Algorithms, Efficient Implementation and Attacks, THE UNIVERSITY OF ADELAIDE, Australia.

[8]. V.Prasad, An analogue to Euler's function for RSA Like Tradoor System with Matrices, Polynomials and Gaussian Integers.M.Phill dissertation, Department of Mathematics, Andhra University 2014.