Polynomial Multiplication on $\mathbb{Z}_q[X]/(X^n+1)$

Abstract. In this document, we describe how to implement the Polynomial Multiplication on $\mathbb{Z}_q[X]/(X^n+1)$.

Keywords: Polynomial Multiplication, CRT

1 Introduction

Let q be an odd positive integer and denote by $\mathbb{Z}_q$ the integers modulo q, which will be represented in the range $[-\frac{q-1}{2}, \frac{q-1}{2}]$. Let n be a positive integer, and R and R_q be the rings $\mathbb{Z}[X]/(X^n+1)$ and $\mathbb{Z}_q[X]/(X^n+1)$, respectively.

Suppose $x, y \in R_q$, we want to calculate $z = x \times y \in R_q$.

Normal Method of Polynomial Multiplication. As a normal version of polynomial multiplication, one can simply multiply each term of x with the ones of y and it will do big number multiplication n^2 times and do big number addition n^2 times. A reduction from polynomial of degree $2n$ to polynomial of degree n need n big number additions. In total, there are n^2 big number multiplications and n^2+n big number additions.

Our Method. We will describe how to use CRT to speed up the polynomial Multiplication.

2 Preliminaries

Below we suppose q be a large prime such that $q \equiv 17 \bmod 32$ and $n = 256$, which is set/used by SALRS.

Let g be a generator of $\mathbb{Z}_q^*$, we have that $ord_q(g) = q-1$ and $g^{q-1} \equiv 1 \bmod q$, $ord_q(g^{\frac{p-1}{16}}) = 16$, and $g^{\frac{q-1}{2}} \equiv -1 \bmod q$. Let $I = \{i | 1 < i < 16, gcd(i, 16) = 1\}$. From [2, Theorem 2.3], $X^{256}+1$ factors as

$$X^{256}+1 = \prod_{i \in I}(X^{32} - g^{\frac{i(q-1)}{16}})$$

and $X^{32} - g^{\frac{i(q-1)}{16}}$ (for $i \in I$) are irreducible in $\mathbb{Z}_q[X]$.

On the other side, we have

$$
\begin{aligned}
X^{256}+1 =& \underbrace{(X^{128}+g^{\frac{q-1}{4}})}_{m_1}\underbrace{(X^{128}-g^{\frac{q-1}{4}})}_{m_2} \\
=& \underbrace{(X^{64}+g^{\frac{q-1}{4}}g^{\frac{q-1}{8}})}_{m_{11}}\underbrace{(X^{64}-g^{\frac{q-1}{4}}g^{\frac{q-1}{8}})}_{m_{12}}\underbrace{(X^{64}+g^{\frac{q-1}{8}})}_{m_{21}}\underbrace{(X^{64}-g^{\frac{q-1}{8}})}_{m_{22}} \\
=& \underbrace{(X^{32}+g^{\frac{q-1}{4}}g^{\frac{q-1}{8}}g^{\frac{q-1}{16}})}_{m_{111}}\underbrace{(X^{32}-g^{\frac{q-1}{4}}g^{\frac{q-1}{8}}g^{\frac{q-1}{16}})}_{m_{112}} \\
&\cdot\underbrace{(X^{32}+g^{\frac{q-1}{8}}g^{\frac{q-1}{16}})}_{m_{121}}\underbrace{(X^{32}-g^{\frac{q-1}{8}}g^{\frac{q-1}{16}})}_{m_{122}} \\
&\cdot\underbrace{(X^{32}+g^{\frac{q-1}{4}}g^{\frac{q-1}{16}})}_{m_{211}}\underbrace{(X^{32}-g^{\frac{q-1}{4}}g^{\frac{q-1}{16}})}_{m_{212}} \\
&\cdot\underbrace{(X^{32}+g^{\frac{q-1}{16}})}_{m_{221}}\underbrace{(X^{32}-g^{\frac{q-1}{16}})}_{m_{222}}
\end{aligned}
$$

It is easy to verify that the set $\{m_{ijk}\}_{i,j,k\in\{1,2\}}$ is just the set $\{X^{32} - g^{\frac{i(q-1)}{16}} | i \in I\}$. Thus, we have that m_1 and m_2 are relatively prime, m_{11} and m_{12} are relatively prime, m_{21} and m_{22} are relatively prime.

Consider a polynomial $y \in \mathbb{Z}_q[X]/(X^{256}+1)$.

1. Let $y_1 \equiv y \bmod m_1, y_2 \equiv y \bmod m_2$. Let $M_1 = m_2, M_2 = m_1$. We compute c_1, c_2 such that $c_1M_1 \equiv 1 \bmod m_1, c_2M_2 \equiv 1 \bmod m_2$, and obtain $c_1 = \frac{1}{2}g^{\frac{q-1}{4}}$, $c_2 = -\frac{1}{2}g^{\frac{q-1}{4}}$. Thus, from CRT, we have

$$
\begin{aligned}
y &= y_1M_1c_1 + y_2M_2c_2 = y_1m_2c_1 + y_2m_1c_2 \\
&= (y_1m_2 - y_2m_1)\cdot\frac{1}{2}g^{\frac{q-1}{4}} \bmod (X^{256}+1)
\end{aligned}
$$

2. Note that $y_1 \in \mathbb{Z}_q[X]/m_1$, $m_1 = m_{11}m_{12}$; $y_2 \in \mathbb{Z}_q[X]/m_2$, $m_2 = m_{21}m_{22}$.
   - Let $y_{11} \equiv y_1 \bmod m_{11}$, $y_{12} \equiv y_1 \bmod m_{12}$. Let $M_{11} = m_1/m_{11} = m_{12}$, $M_{12} = m_1/m_{12} = m_{11}$. We compute c_{11}, c_{12} such that $c_{11}M_{11} \equiv 1 \bmod m_{11}, c_{12}M_{12} \equiv 1 \bmod m_{12}$, and obtain $c_{11} = \frac{1}{2}g^{\frac{q-1}{8}}$, $c_{12} = -\frac{1}{2}g^{\frac{q-1}{8}}$. Thus, from CRT, we have

$$
\begin{aligned}
y_1 &= y_{11}M_{11}c_{11} + y_{12}M_{12}c_{12} = y_{11}m_{12}c_{11} + y_{12}m_{11}c_{12} \\
&= (y_{11}m_{12} - y_{12}m_{11})\cdot\frac{1}{2}g^{\frac{q-1}{8}} \bmod m_1.
\end{aligned}
$$

– Let $y_{21} \equiv y_2 \bmod m_{21}$, $y_{22} \equiv y_2 \bmod m_{22}$. Let $M_{21} = m_2/m_{21} = m_{22}$, $M_{22} = m_2/m_{22} = m_{21}$. We compute c_{21}, c_{22} such that $c_{21}M_{21} \equiv 1 \bmod m_{21}, c_{22}M_{22} \equiv 1 \bmod m_{22}$, and obtain $c_{21} = \frac{1}{2}g^{\frac{3(q-1)}{8}}$, $c_{22} = -\frac{1}{2}g^{\frac{3(q-1)}{8}}$. Thus, from CRT, we have

$$\begin{aligned} y_2 &= y_{21}M_{21}c_{21} + y_{22}M_{22}c_{22} = y_{21}m_{22}c_{21} + y_{22}m_{21}c_{22} \\ &= (y_{21}m_{22} - y_{22}m_{21}) \cdot \frac{1}{2}g^{\frac{3(q-1)}{8}} \bmod m_2. \end{aligned}$$

3. Note that $y_{11} \in \mathbb{Z}_q[X]/m_{11}$, $m_{11} = m_{111}m_{112}$; $y_{12} \in \mathbb{Z}_q[X]/m_{12}$, $m_{12} = m_{121}m_{122}$; $y_{21} \in \mathbb{Z}_q[X]/m_{21}$, $m_{21} = m_{211}m_{212}$; $y_{22} \in \mathbb{Z}_q[X]/m_{22}$, $m_{22} = m_{221}m_{222}$.
   – Let $y_{111} \equiv y_{11} \bmod m_{111}$, $y_{112} \equiv y_{11} \bmod m_{112}$. Let $M_{111} = m_{11}/m_{111} = m_{112}$, $M_{112} = m_{11}/m_{112} = m_{111}$. We compute c_{111}, c_{112} such that $c_{111}M_{111} \equiv 1 \bmod m_{111}, c_{112}M_{112} \equiv 1 \bmod m_{112}$, and obtain $c_{111} = \frac{1}{2}g^{\frac{q-1}{16}}$, $c_{112} = -\frac{1}{2}g^{\frac{q-1}{16}}$. Thus, from CRT, we have

$$\begin{aligned} y_{11} &= y_{111}M_{111}c_{111} + y_{112}M_{112}c_{112} = y_{111}m_{112}c_{111} + y_{112}m_{111}c_{112} \\ &= (y_{111}m_{112} - y_{112}m_{111}) \cdot \frac{1}{2}g^{\frac{q-1}{16}} \bmod m_{11}. \end{aligned}$$

   – Let $y_{121} \equiv y_{12} \bmod m_{121}$, $y_{122} \equiv y_{12} \bmod m_{122}$. Let $M_{121} = m_{12}/m_{121} = m_{122}$, $M_{122} = m_{12}/m_{122} = m_{121}$. We compute c_{121}, c_{122} such that $c_{121}M_{121} \equiv 1 \bmod m_{121}, c_{122}M_{122} \equiv 1 \bmod m_{122}$, and obtain $c_{121} = \frac{1}{2}g^{\frac{5(q-1)}{16}}$, $c_{122} = -\frac{1}{2}g^{\frac{5(q-1)}{16}}$. Thus, from CRT, we have

$$\begin{aligned} y_{12} &= y_{121}M_{121}c_{121} + y_{122}M_{122}c_{122} = y_{121}m_{122}c_{121} + y_{122}m_{121}c_{122} \\ &= (y_{121}m_{122} - y_{122}m_{121}) \cdot \frac{1}{2}g^{\frac{5(q-1)}{16}} \bmod m_{12}. \end{aligned}$$

   – Let $y_{211} \equiv y_{21} \bmod m_{211}$, $y_{212} \equiv y_{21} \bmod m_{212}$. Let $M_{211} = m_{21}/m_{211} = m_{212}$, $M_{212} = m_{21}/m_{212} = m_{211}$. We compute c_{211}, c_{212} such that $c_{211}M_{211} \equiv 1 \bmod m_{211}, c_{212}M_{212} \equiv 1 \bmod m_{212}$, and obtain $c_{211} = \frac{1}{2}g^{\frac{3(q-1)}{16}}$, $c_{212} = -\frac{1}{2}g^{\frac{3(q-1)}{16}}$. Thus, from CRT, we have

$$\begin{aligned} y_{21} &= y_{211}M_{211}c_{211} + y_{212}M_{212}c_{212} = y_{211}m_{212}c_{211} + y_{212}m_{211}c_{212} \\ &= (y_{211}m_{212} - y_{212}m_{211}) \cdot \frac{1}{2}g^{\frac{3(q-1)}{16}} \bmod m_{21}. \end{aligned}$$

   – Let $y_{221} \equiv y_{22} \bmod m_{221}$, $y_{222} \equiv y_{22} \bmod m_{222}$. Let $M_{221} = m_{22}/m_{221} = m_{222}$, $M_{222} = m_{22}/m_{222} = m_{221}$. We compute c_{221}, c_{222} such that $c_{221}M_{221} \equiv 1 \bmod$

$m_{221}, c_{222}M_{222} \equiv 1 \bmod m_{222}$, and obtain $c_{221} = \frac{1}{2}g^{\frac{7(q-1)}{16}}$, $c_{222} = -\frac{1}{2}g^{\frac{7(q-1)}{16}}$. Thus, from CRT, we have

$$\begin{aligned} y_{22} &= y_{221}M_{221}c_{221} + y_{222}M_{222}c_{222} = y_{221}m_{222}c_{221} + y_{222}m_{221}c_{222} \\ &= (y_{221}m_{222} - y_{222}m_{221}) \cdot \frac{1}{2}g^{\frac{7(q-1)}{16}} \bmod m_{22}. \end{aligned}$$

Note that $y_{111} \equiv y_{11} \bmod m_{111}$ implies $y_{111} = y_{11} - k_{111}m_{111}$ for some $k_{111} \in \mathbb{Z}_q[X]$, $y_{11} \equiv y_1 \bmod m_{11}$ implies $y_{11} = y_1 - k_{11}m_{11}$ for some $k_{11} \in \mathbb{Z}_q[X]$, and $y_1 \equiv y \bmod m_1$ implies $y_1 = y - k_1m_1$ for some $k_1 \in \mathbb{Z}_q[X]$. Thus, we have $y_{111} = y - k_1m_1 - k_{11}m_{11} - k_{111}m_{111}$, and this implies $y_{111} \equiv y \bmod m_{111}$. Similarly, we have

$$y_{ijk} \equiv y \bmod m_{ijk} \ \forall i, j, k \in \{1, 2\}.$$

3 Our Implementation of Polynomial Multiplication on $\mathbb{Z}_q[X]/(X^{256} + 1)$

3.1 Step 1

We pre-split $X^{256}+1$ into 8 small polynomials as introduces above. To compute $z = x \times y$ where $x, y, z \in R_q$, we split the two polynomials x and y into 8 small polynomials **step by step**, respectively. This means each time we split one polynomial into two polynomials by doing the module. We choose to do the splitting **step by step** instead of directly in one step because it is more efficient than the method introduced in [2, Part 3.2]. Doing the splitting **step by step** requires $3n$ times of big number multiplications and $6n$ times of big number additions. While doing the splitting in one step according to [2, Part 3.2] requires about $16n$ times of big number multiplications and $16n$ times of big number additions. Finally we have 16 polynomial, $x_i, y_i \in \mathbb{Z}_q[X]/(X^{32} + g_i)$ for $i = 1, 2, ..., 8$.

3.2 Step 2

For each $x_i, y_i \in \mathbb{Z}_q[X]/(X^{32}+g_i)$ $(i = 1, \ldots, 8)$, we compute $z_i = x_i \times y_i \in \mathbb{Z}_q[X]/(X^{32}+g_i)$ by using the Karatsuba multiplication algorithm [1]. In particular, let two polynomials $F, G \in \mathbb{Z}_q[X]/(X^{32} + g_i)$, and $F = F_0 + X^{16}F_1$, $G = G_0 + X^{16}G_1$, we compute $F \times G = (1 - X^{16})(F_0G_0 - X^{16}F_1G_1) + X^{16}(F_0 + F_1)(G_0 + G_1) \bmod X^{32} + g_i$.

3.3 Step 3

Now we have 8 small polynomials $z_i \in \mathbb{Z}_q[X]/(X^{32}+g_i)$ $(i = 1, \ldots, 8)$. We apply Chinese Remainder Theorem step by step , which aims to make source code more clear and make it easier to expand or reduce the scale of the splitting, to obtain the result polynomial as introduced in preliminaries above.

4 Time Complexity

There are two partially splitting operations in Step 1, where two polynomials of degree 256 are turned into sixteen polynomials of degree 32. It requires $((n/2) + (n/4) \times 2 + (n/8) \times 4) \times 2 = 3n$ times of big number multiplications and $((n/2) \times 2 + (n/4) \times 4 + (n/8) \times 8) \times 2 = 6n$ times of big number additions.

In Step 2, the computational complexity is equal to $8 \times 3 = 24$ times of polynomial multiplications of degree $n/16$, so it requires $24 \times (n/16)^2 = 3n^2/32$ times of big number multiplications and $8 \times 3 \times (n/16)^2 + 8 \times 3 \times (n/16) = 3n^2/32 + 3n/32$ times of big number additions.

There are $n/8 \times 8 + n/4 \times 4 + n/2 \times 2 = 3n$ times of big number multiplications and $n/8 \times 4 + n/4 \times 2 + n/2 = 3n/2$ times of big number additions in Step 3.

In total, there are $3n2/32 + 6n$ times of big number multiplications and $3n2/32 + 243n/32$ times of big number additions. Our method is better than normal version of polynomial multiplication when n is 256.

5 Concrete Parameters

$q = 34360786961$ and $g = -16915236577$.

For better efficiency, we hardcode the values of $g^{\frac{i(q-1)}{16}}$ where $i = 1, 2, 3, ..., 15, 16$ in our implementation. Specifically, these values are -16915236577, -8376412603, -3354919284, 11667088462, -12474372669, -3077095668, 14301820476, -1, 16915236577, 8376412603, 3354919284, -11667088462, 12474372669, 3077095668, -14301820476 and 1.

References

1. Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: Ntru prime: Reducing attack surface at low cost. In: Adams, C., Camenisch, J. (eds.) Selected Areas in Cryptography – SAC 2017. pp. 235–260. Springer International Publishing, Cham (2018)

2. Lyubashevsky, V., Seiler, G.: Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I. Lecture Notes in Computer Science, vol. 10820, pp. 204–224. Springer (2018), https://doi.org/10.1007/978-3-319-78381-9_8