Polynomial Multiplication in NTRU Prime

Comparison of Optimization Strategies on Cortex-M4

Erdem Alkim Dean Yun-Li Cheng Chi-Ming Marvin Chung Hülya Evkan Leo Wei-Lun Huang
Vincent Hwang Ching-Lin Trista Li Ruben Niederhagen Cheng-Jhih Shih Julian Wälde Bo-Yin Yang

CHES 2021 – September 17, 2021

NTRU Prime

Parameter Sets and follow up works on Cortex-M4.

Table 1: Round 2 parameter sets.

Scheme	security level	p	q	w
{ntrulpr, sntrup}653	2	653	4621	$\{252, 288\}$
{ntrulpr, sntrup}761	3	761	4591	$\{250, 286\}$
{ntrulpr, sntrup}857	4	857	5167	$\{281, 322\}$

Table 2: Additional parameter sets for round 3.

Scheme	p	q	w
{ntrulpr, sntrup}953	953	6343	$\{345, 396\}$
{ntrulpr, sntrup}1013	1013	7177	$\{392, 448\}$
{ntrulpr, sntrup}1277	1277	7879	$\{429, 492\}$

Polynomials in NTRU Prime

- Primes p, q giving a field $\mathbb{Z}_q[x]/\langle x^p - x - 1\rangle$
- Polynomials in $\mathbb{Z}_q[x]/\langle x^p - x - 1\rangle$ and $\mathbb{Z}_3[x]/\langle x^p - x - 1\rangle$
- **small**: coefficients are all in $\{\pm 1, 0\}$
- **weight *w***: exactly w non-zero coefficients
- `Short`: **small** and **weight *w***
- We focus on the case where one of the multiplicands is **small**
- If both multiplicands are **small**, we can apply Karatsuba with unsigned long multiplication, see [Li21].

Polynomial Multiplication for {ntrulpr, sntrup}761

- Good's trick:
  - Ring $\mathbb{Z}_{q'}[x]/\langle x^{1536} - 1\rangle$
  - Multi-dimensional mapping:

$$\mathbb{Z}_{q'}[x]/\langle x^{1536} - 1\rangle \cong \left(\mathbb{Z}_{q'}[z]/\langle z^3 - 1\rangle\right)[y]/\langle y^{512} - 1\rangle$$

- Mixed-radix:
  - Ring $\mathbb{Z}_{4591}[x]/\langle x^{\{1620,1530\}} - 1\rangle$
  - Small radices
  - Rader's trick for a large radix

Convolution and Its Application to NTRU Prime

Convolution

For $\boldsymbol{a}(x), \boldsymbol{b}(x) \in R[x]/\langle f(x) \rangle$.

- Convolution: $f(x) = x^N - 1$
- NTRU Prime: $R[x]/\langle x^p - x - 1 \rangle$, not convolutions
- Observe: $\deg(\boldsymbol{a}(x)\boldsymbol{b}(x)) \leq 2p - 2$
- $\boldsymbol{a}(x)\boldsymbol{b}(x) \in R[x]$ can be computed in $R[x]/\langle x^N - 1 \rangle$ with $N > 2p - 2$
- Reduce $\boldsymbol{a}(x)\boldsymbol{b}(x)$ from $R[x]$ to $R[x]/\langle x^p - x - 1 \rangle$

Good’s Trick

General Idea of Good's Trick [Goo51]

- Suppose $q_0 \perp q_1$ and map $x \mapsto yz$ for $y^{q_0} = z^{q_1} = 1$.
  We have:

$$R[x]/\langle x^{q_0 q_1} - 1\rangle \cong \left(R[z]/\langle z^{q_1} - 1\rangle\right)[y]/\langle y^{q_0} - 1\rangle \overset{q_0\text{-NTT}}{\cong} \prod_{i=0}^{q_0-1} \left(R[x]/\langle x^{q_1} - 1\rangle\right)[y]/\langle y - \psi^i\rangle$$

- $x^i \mapsto (yz)^i = y^i z^i = y^{i \bmod q_0} z^{i \bmod q_1}$
- $a_i x^i \mapsto a_{(i \bmod q_0, i \bmod q_1)} y^{i \bmod q_0} z^{i \bmod q_1}$

Number-Theoretic Transforms (NTTs)

Number-theoretic Transforms (NTTs)

Let q be a prime and $N|(q-1)$. Size N NTT is the isomorphism:

$$\begin{cases} \mathbb{Z}_q[x]/\left\langle x^N - 1\right\rangle & \rightarrow \prod_{j=0}^{N-1} \mathbb{Z}_q[x]/\left\langle x - \psi_N^j \right\rangle \\ \sum_{i=0}^{N-1} a_i x^i & \mapsto (\hat{a_0}, \ldots, \hat{a_{N-1}}) \end{cases}$$

where $\hat{a}_j = \sum_{i=0}^{N-1} a_i \psi_N^{ij}$ for an Nth root of unity ψ_N.

We can implement $\boldsymbol{a}(x)\boldsymbol{b}(x)$ as $\texttt{NTT}^{-1}\left(\texttt{NTT}(\boldsymbol{a}(x))(\cdot)\texttt{NTT}(\boldsymbol{b}(x))\right)$ where $(\cdot)$ is the point-multiplication.

Efficient algorithms for NTTs are called FFTs.

Why Good's Trick?

$$
\begin{aligned}
R[x]/\langle x^{q_0 q_1} - 1\rangle &\cong \left(R[z]/\langle z^{q_1} - 1\rangle\right)[y]/\langle y^{q_0} - 1\rangle \\
&\cong \prod_{i=0}^{q_0 - 1} \left(R[z]/\langle z^{q_1} - 1\rangle\right)[y]/\langle y - \psi^i\rangle
\end{aligned}
$$

multiplication:

$$O(q_0^2 q_1^2) \Longrightarrow O(q_0 q_1^2 + q_0^2 q_1)$$

There is an example showing Good's trick is fast for $x^6 - 1$ in the appendix.

Cooley-Tukey Fast Fourier Transforms (FFTs)

General Idea of Cooley-Tukey FFT i

If $\zeta \in R$ is invertible, we have

$$R[x]/\left\langle x^N - \zeta^N \right\rangle \cong \prod_{i=0}^{N-1} R[x]/\langle x - \zeta\psi_N^i \rangle.$$

We apply this by observing roots of unity are invertible.

General Idea of Cooley-Tukey FFT ii

$\psi = \psi_{N_0 N_1}$ and pick $\psi_{N_0} = \psi^{N_1}$ and $\psi_{N_1} = \psi^{N_0}$.

$$R[x]/\left\langle x^{N_0 N_1} - 1 \right\rangle \overset{N_0\text{-}\mathtt{NTT},\zeta=1}{\cong} \prod_{i=0}^{N_0-1} R[x]/\left\langle x^{N_1} - \psi^{N_1 i} \right\rangle$$

$$\overset{N_1\text{-}\mathtt{NTT},\zeta=\psi^i}{\cong} \prod_{i=0}^{N_0-1} \prod_{j=0}^{N_1-1} R[x]/\left\langle x - \psi^{i+N_0 j} \right\rangle$$

If $N_0 = 2^{k_0}$ and $N_1 = 2^{k_1}$, FFT is very fast.

If N_0 and N_1 are not sharing a same radix, we call it mixed-radix.

$(p, q) = (761, 4591)$: 2D Good's Trick for 1536

Observe $1536 = 512 \times 3$.

$$\left(R[z]/\left\langle z^3 - 1\right\rangle\right)[y]/\left\langle y^{512} - 1\right\rangle \cong \prod_{i=0}^{511} \left(R[z]/\left\langle z^3 - 1\right\rangle\right)[y]/\left\langle y - \psi^i\right\rangle$$

For 512-`NTT` with $\mathbb{Z}_q$, we need $512 | (q - 1)$, but $512 \not| (4591 - 1)$.

- Compute as in $\mathbb{Z}$, and then reduce to $\mathbb{Z}_q$
- Cortex-M4 with powerful 32-bit arithmetic: For $\mathbb{Z}_{q'}[x]/\left\langle x^{1536} - 1\right\rangle$, choose a prime $q' > q \cdot p$ with $512 | (q' - 1)$ so $R = \mathbb{Z}_{q'}$
- For 512-`NTT`, consider $512 = 2 \cdot 256$, $256 = 2 \cdot 128$, ... , $4 = 2 \cdot 2$, so eventually, we have the bit-reversal of $1, \psi^1, \dots \psi^{511}$
- Instead of $(*512^{-1})$, $\mathbb{Z}_{q'} \to \mathbb{Z}_q$, $\left\langle x^{1536} - 1\right\rangle \to \left\langle x^{761} - x - 1\right\rangle$, we compute $\left\langle x^{1536} - 1\right\rangle \to \left\langle x^{761} - x - 1\right\rangle$, $(*512^{-1})$, $\mathbb{Z}_{q'} \to \mathbb{Z}_q$.
- $\left\langle x^{1536} - 1\right\rangle \to \left\langle x^{761} - x - 1\right\rangle$ before $\mathbb{Z}_{q'} \to \mathbb{Z}_q$, choose $q' > q \cdot (2p - 1)$
- For `Short`, one can replace p with w

$(p, q) = (761, 4591)$: Mixed-radix i

- $4591 - 1 = 2 \times 3^3 \times 5 \times 17$
- $1620 = 270 \times 6 = 2 \times 3^3 \times 5 \times 6$
- $\psi = \psi_{270}$ and let $\begin{cases} \psi' = \psi^{5i_0+10i_1+30i_2+90i_3} \\ \psi'' = \psi^{i_0+2i_1+6i_2+18i_3+54i_4}, dr_{270}(.) \end{cases}$

$$\mathbb{Z}_q[x]/\langle x^{1620} - 1\rangle \overset{\text{2-NTT,3-NTT}}{\cong} \prod_{i_0=0}^{1} \prod_{i_1=0}^{2} \mathbb{Z}_q[x]/\langle x^{270} - \psi^{45i_0+90i_1}\rangle$$

$$\overset{\text{3-NTT,3-NTT}}{\cong} \prod_{i_0=0}^{1} \prod_{i_1=0}^{2} \prod_{i_2=0}^{2} \prod_{i_3=0}^{2} \mathbb{Z}_q[x]/\langle x^{30} - \psi'\rangle$$

$$\overset{\text{5-NTT}}{\cong} \prod_{i_0=0}^{1} \prod_{i_1=0}^{2} \prod_{i_2=0}^{2} \prod_{i_3=0}^{2} \prod_{i_4=0}^{4} \mathbb{Z}_q[x]/\langle x^{6} - \psi''\rangle$$

$(p, q) = (761, 4591)$: **Mixed-radix ii**

- $4591 - 1 = 17 \times 3^3 \times 10$
- $1530 = 17 \times 90 = 17 \times 9 \times 10$
- $\psi = \psi_{17\cdot 9}$ so $\psi^9 = \psi_{17}$ and $\psi^{17} = \psi_9$
- Rader's trick for 17-NTT

$$\mathbb{Z}_q[x]/\langle x^{1530} - 1\rangle \overset{17\text{-NTT}}{\cong} \prod_{i=0}^{16} \mathbb{Z}_q[x]/\langle x^{90} - \psi^{9i}\rangle$$

$$\overset{9\text{-NTT}}{\cong} \prod_{i=0}^{16}\prod_{j=0}^{8} \mathbb{Z}_q[x]/\langle x^{10} - \psi^{i+17\cdot j}\rangle$$

General Framework of Rader's Trick [Rad68]

- For a prime p, compute part of the size p NTT as a size $(p-1)$ convolution
- $\exists g \in \mathbb{Z}_p$ with $[1, \dots, p-1] \overset{i \mapsto g^i}{\cong} [1, \dots, p-1]$ as sets.
- $\forall j > 0$,

$$\begin{aligned} \hat{a}_j - a_0 &= \sum_{i=1}^{p-1} (\psi^{-1})^{-ij} a_i \\ \iff \hat{a}_{g^j} - a_0 &= \sum_{i=1}^{p-1} (\psi^{-1})^{g^{j-i}} a_{g^i} \end{aligned}$$

- Indices in blue sum to a fix $j \implies$ convolution.

Rader's Trick for Size 5 NTT

- Consider $i \mapsto 2^i : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$
- $$\begin{cases} \hat{a}_2 - a_0 = (\psi^{-1})^2 a_2 + (\psi^{-1})^1 a_4 + (\psi^{-1})^3 a_3 + (\psi^{-1})^4 a_1 \\ \hat{a}_4 - a_0 = (\psi^{-1})^4 a_2 + (\psi^{-1})^2 a_4 + (\psi^{-1})^1 a_3 + (\psi^{-1})^3 a_1 \\ \hat{a}_3 - a_0 = (\psi^{-1})^3 a_2 + (\psi^{-1})^4 a_4 + (\psi^{-1})^2 a_3 + (\psi^{-1})^1 a_1 \\ \hat{a}_1 - a_0 = (\psi^{-1})^1 a_2 + (\psi^{-1})^3 a_4 + (\psi^{-1})^4 a_3 + (\psi^{-1})^2 a_1 \end{cases}$$
- convolution of $\left((\psi^{-1})^2, (\psi^{-1})^1, (\psi^{-1})^3, (\psi^{-1})^4\right)$ and (a_2, a_4, a_3, a_1)

Implementations

Basic Arithmetic

Cortex-M4F: Armv7-M with DSP and FPv4-SP extensions.

- One multiplication: `smul{b, t}{b, t}`, `smla{b, t}{b, t}`
- Two multiplications: `smu{a, s}d{, x}`, `sml{a, s}d{, x}`

Algorithm 1 32-bit Barrett

1: `smmulr` t, a, q^{-1}
2: `mls` a, t, q, a

Algorithm 2 32-bit montgomery_mul

1: `smull` c_{low}, c_{high}, a, b
2: `mul` $t, c_{low}, -q'^{-1}$
3: `smlal` c_{low}, c_{high}, t, q'

Figure 1: Inputs and outputs.

Butterfly Operations in $\mathbb{Z}_{4591}$

A typical sequence:

Algorithm 3 Radix-3 butterfly $w = \psi_3^2 || \psi_3$.

Require: a_0, $a_{1,2} = a_2 || a_1$ where ψ_3 3rd root of unity, $t_0 = \text{0x00010001}$

Ensure: reduced $a_0 = a_0 + a_1 + a_2$, $a_{1,2} = a_0 + \psi_3^2 \cdot a_1 + \psi_3 \cdot a_2 || a_0 + \psi_3 \cdot a_1 + \psi_3^2 \cdot a_2$

`smlad` $t_0, a_{1,2}, t_0, a_0$ ▷ $t_0 \leftarrow a_0 + a_1 + a_2$

`smlad` $t_1, a_{1,2}, w, a_0$ ▷ $t_1 \leftarrow a_0 + \psi_3 \cdot a_1 + \psi_3^2 \cdot a_2$

`smladx` $t_2, a_{1,2}, w, a_0$ ▷ $t_2 \leftarrow a_0 + \psi_3^2 \cdot a_1 + \psi_3 \cdot a_2$

`smmulr` t, t_0, q^{-1} ▷ reduce t_0

`mls` a_0, t, q, t_0

`smmulr` t, t_1, q^{-1} ▷ reduce t_1

`mls` t_1, t, q, t_1

`smmulr` t, t_2, q^{-1} ▷ reduce t_2

`mls` t_2, t, q, t_2

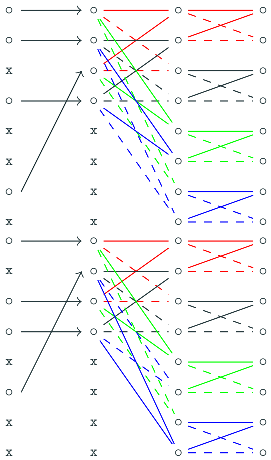
`pkhbt` $a_{1,2}, t_1, t_2, LSL\#16$ ▷ $a_{1,2} \leftarrow t_2 || t_1$

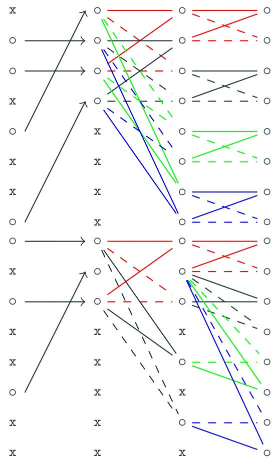
Three Layers of Radix-2 32-bit CT Butterflies

Algorithm 4 Cooley-Tukey NTT with three layers, no mul. if $\omega = \pm 1$.

vmov r1 $= \omega'_0$	▷ butterflies (r4 ↔ r8), (r5 ↔ r9), (r6 ↔ r10), (r7 ↔ r11) below
montgomery_mul r8, r1	▷ r8 $= \omega_0 a_4$
montgomery_mul r9, r1	▷ r9 $= \omega_0 a_5$
montgomery_mul r10, r1	▷ r10 $= \omega_0 a_6$
montgomery_mul r11, r1	▷ r11 $= \omega_0 a_7$
add r4, r8	▷ r4 $= a_0 + \omega_0 a_4$
add r5, r9	▷ r5 $= a_1 + \omega_0 a_5$
add r6, r10	▷ r6 $= a_2 + \omega_0 a_6$
add r7, r11	▷ r7 $= a_3 + \omega_0 a_7$
sub r8, r4, r8, lsl #1	▷ r8 $= a_0 - \omega_0 a_4$
sub r9, r5, r9, lsl #1	▷ r9 $= a_1 - \omega_0 a_5$
sub r10, r6, r10, lsl #1	▷ r10 $= a_2 - \omega_0 a_6$
sub r11, r7, r11, lsl #1	▷ r11 $= a_3 - \omega_0 a_7$
vmov r1 $= \omega'_1, \omega'_2$	▷ butterflies (r4 ↔ r6), (r5 ↔ r7), (r8 ↔ r10), (r9 ↔ r11)
vmov r1 $= \omega'_3, \omega'_4, \omega'_5, \omega'_6$	▷ butterflies (r4 ↔ r5), (r6 ↔ r7), (r8 ↔ r9), (r10 ↔ r11)

Butterflies for Good's Trick with Zeros





Results

Results: Big by Small Polynomial Multiplication

Toom–Cook	Good's	Rader's	Small radices
223 871	159 176	152 177	185 010

(p, q)	Ring for NTT	Approach	Cycles
(653, 4621)	$\mathbb{Z}_{4621}[x]/\langle x^{1320} - 1\rangle$	Rader's	120 137
(761, 4591)	$\mathbb{Z}_{4591}[x]/\langle x^{1530} - 1\rangle$	Rader's	152 177
(857, 5167)	$\mathbb{Z}_{q'}[x]/\langle x^{1728} - 1\rangle$	2D Good's	183 430
(953, 6343)	$\mathbb{Z}_{q'}[x]/\langle x^{1920} - 1\rangle$	3D Good's	185 790
(1013, 7177)	$\mathbb{Z}_{q'}[x]/\langle x^{2048} - 1\rangle$	2048-NTT	225 484
(1277, 7879)	$\mathbb{Z}_{q'}[x]/\langle x^{2560} - 1\rangle$	2D Good's	284 015

Results: Cycles of Full Schemes

	Toom-Cook	Good's	Rader's	small radices
	ntrulpr761 Speed (cycles)			
G	823655	735168	727298	760 947
E	1309214	1110628	1093927	1153 722
D	1491900	1214546	1187447	1 284 253
	sntrup761 Speed (cycles)			
G	10901785	10787337	10773799	1 0808 526
E	789442	701612	689996	726 930
D	742182	586244	563885	637 286

Results of Follow up Works (Merged into pqm4)

Streamlined NTRU Prime			
(p, q)	**K**	**E**	**D**
(653, 4621)	6 714 568	631 853	486 707
(761, 4591)	7 951 328	683 652	538 141
(857, 5167)	10 264 255	853 302	689 920
(953, 6343)	12 761 557	943 350	744 434
(1013, 7177)	13 955 859	1 031 757	838 171
(1277, 7879)	22 989 117	1 326 335	1 071 964

NTRU LPrime			
(p, q)	**K**	**E**	**D**
(653, 4621)	677 981	1 157 987	1 233 059
(761, 4591)	726 507	1 312 278	1 393 675
(857, 5167)	921 143	1 547 852	1 668 045
(953, 6343)	1 007 380	1 677 959	1 795 115
(1013, 7177)	1 102 228	1 842 328	1 991 243
(1277, 7879)	1 420 658	2 341 222	2 530 410

Polynomial Multiplication in NTRU Prime

- Compute as in $\mathbb{Z}$
  - Choose an $N = 2^k \times 3^{\{0,1,2,3\}} \times 5^{\{0,1\}} \geq 2p-1$ for fast computation
  - Good's trick if $3|N$ or $5|N$
  - Choose q' with $N|(q'-1)$ for 32-bit arithmetic on Cortex-M4
    - $\mathbb{Z}_{q'} \to \mathbb{Z}_q$ before $\left\langle x^N - 1 \right\rangle \to \langle x^p - x - 1 \rangle$, then $q' > qp$
    - $\mathbb{Z}_{q'} \to \mathbb{Z}_q$ after $\left\langle x^N - 1 \right\rangle \to \langle x^p - x - 1 \rangle$, then $q' > q(2p-1)$
    - `Short` $\Longrightarrow$ replace p with w
- Compute as in $\mathbb{Z}_q$
  - For a divisor d of $q-1$, we can compute size d NTT
  - Find an $N \geq 2p-1$ with $d|N$ and small $\frac{N}{d}$
  - Small radices: fast
  - Large radices: Rader's trick
  - Butterflies with DSP extension: `smul{b, t}{b, t}`, `smla{b, t}{b, t}`, `smu{a, s}d{, x}`, `sml{a, s}d{, x}`

Thank you for your attention

Reference

- Irving J. Good.
  Random motion on a finite abelian group.
  Proceedings of the Cambridge Philosophical Society, 47:756–762, 1951.
  MR 13,363e.
- Ching-Lin Trista Li.
  Implementation of polynomial modular inversion in lattice-based cryptograpgy on arm.
  Master's thesis, National Taiwan University, 2021.
- Charles M. Rader.
  Discrete fourier transforms when the number of data samples is prime.
  Proceedings of the IEEE, 56(6):1107–1108, 1968.

Convolution in $R[x]/\langle x^6 - 1\rangle$

For $\boldsymbol{a}(x) = \sum_{i=0}^{5} a_i x^i$, $\boldsymbol{b}(x) = \sum_{i=0}^{5} b_i x^i \in R[x]/\langle x^6 - 1\rangle$,

$$\boldsymbol{a}(x)\boldsymbol{b}(x) = \sum_{i=0}^{5} \sum_{i_a + i_b \equiv i} a_{i_a} b_{i_b} x^i \in R[x]/\langle x^6 - 1\rangle$$

- # multiplications: $6 \cdot 6 = 36$
- # additions: $6 \cdot 5 = 30$

Can we do better? Yes, with Good's trick.

Permutation

- $i \mapsto (i \bmod 2, i \bmod 3)$
- $$\begin{cases} (a_0, \ldots, a_5) \mapsto \begin{pmatrix} a_0 & a_4 & a_2 \\ a_3 & a_1 & a_5 \end{pmatrix} =: A \\ (b_0, \ldots, b_5) \mapsto \begin{pmatrix} b_0 & b_4 & b_2 \\ b_3 & b_1 & b_5 \end{pmatrix} =: B \end{cases}$$

Add-sub the Rows

$$\left\{\begin{array}{l}\begin{pmatrix} a_0 & a_4 & a_2 \\ a_3 & a_1 & a_5 \end{pmatrix} \mapsto \begin{pmatrix} a_0 + a_3 & a_4 + a_1 & a_2 + a_5 \\ a_0 - a_3 & a_4 - a_1 & a_2 - a_5 \end{pmatrix} \\ \begin{pmatrix} b_0 & b_4 & b_2 \\ b_3 & b_1 & b_5 \end{pmatrix} \mapsto \begin{pmatrix} b_0 + b_3 & b_4 + b_1 & b_2 + b_5 \\ b_0 - b_3 & b_4 - b_1 & b_2 - b_5 \end{pmatrix}\end{array}\right.$$

3×3 Convolutions

$$\left(\begin{pmatrix} a_0 + a_3 & a_4 + a_1 & a_2 + a_5 \\ a_0 - a_3 & a_4 - a_1 & a_2 - a_5 \end{pmatrix}, \begin{pmatrix} b_0 + b_3 & b_4 + b_1 & b_2 + b_5 \\ b_0 - b_3 & b_4 - b_1 & b_2 - b_5 \end{pmatrix}\right)$$

$$\mapsto \begin{pmatrix} c_0 & c_4 & c_2 \\ c_3 & c_1 & c_5 \end{pmatrix} =: C$$

$$\text{where} \begin{cases} c_0 & = \sum_{i_a + i_b \equiv 0} a_{i_a} b_{i_b} + \sum_{i_a + i_b \equiv 3} a_{i_a} b_{i_b} \\ c_3 & = \sum_{i_a + i_b \equiv 0} a_{i_a} b_{i_b} - \sum_{i_a + i_b \equiv 3} a_{i_a} b_{i_b} \\ c_4 & = \sum_{i_a + i_b \equiv 4} a_{i_a} b_{i_b} + \sum_{i_a + i_b \equiv 1} a_{i_a} b_{i_b} \\ c_1 & = \sum_{i_a + i_b \equiv 4} a_{i_a} b_{i_b} - \sum_{i_a + i_b \equiv 1} a_{i_a} b_{i_b} \\ c_2 & = \sum_{i_a + i_b \equiv 2} a_{i_a} b_{i_b} + \sum_{i_a + i_b \equiv 5} a_{i_a} b_{i_b} \\ c_5 & = \sum_{i_a + i_b \equiv 2} a_{i_a} b_{i_b} - \sum_{i_a + i_b \equiv 5} a_{i_a} b_{i_b} \end{cases}$$

Add-sub the Rows

$$\begin{pmatrix} c_0 & c_4 & c_2 \\ c_3 & c_1 & c_5 \end{pmatrix} \mapsto \begin{pmatrix} c_0 + c_3 & c_4 + c_1 & c_2 + c_5 \\ c_0 - c_3 & c_4 - c_1 & c_2 - c_5 \end{pmatrix}$$

$$= 2 \begin{pmatrix} \sum_{i_a+i_b\equiv 0} a_{i_a} b_{i_b} & \sum_{i_a+i_b\equiv 4} a_{i_a} b_{i_b} & \sum_{i_a+i_b\equiv 2} a_{i_a} b_{i_b} \\ \sum_{i_a+i_b\equiv 3} a_{i_a} b_{i_b} & \sum_{i_a+i_b\equiv 1} a_{i_a} b_{i_b} & \sum_{i_a+i_b\equiv 5} a_{i_a} b_{i_b} \end{pmatrix}$$

Permutation

$(i \bmod 2, i \bmod 3) \mapsto i$

$$2\begin{pmatrix} \sum_{i_a+i_b\equiv 0} a_{i_a}b_{i_b} & \sum_{i_a+i_b\equiv 4} a_{i_a}b_{i_b} & \sum_{i_a+i_b\equiv 2} a_{i_a}b_{i_b} \\ \sum_{i_a+i_b\equiv 3} a_{i_a}b_{i_b} & \sum_{i_a+i_b\equiv 1} a_{i_a}b_{i_b} & \sum_{i_a+i_b\equiv 5} a_{i_a}b_{i_b} \end{pmatrix}$$

$$\mapsto 2\left(\sum_{i_a+i_b\equiv i} a_{i_a}b_{i_b}\right)_{0\le i<6}$$

$$= 2\sum_{i=0}^{5}\sum_{i_a+i_b\equiv i} a_{i_a}b_{i_b}x^i$$

How Many Additions and Multiplications?

	#(ADD)	#(MUL)
Permutation	0	0
Add-sub the rows (A and B)	12	0
3×3 convolutions	12	18
Add-sub the rows (C)	6	0
Permutation	0	0
Total (including division by 2)	30	$18 + 6$

If 2 is invertible in R, we multiply each coefficient with 2^{-1}. The total number of multiplications is therefore 24.

$(p, q) = (653, 4621)$: 1320 Mixed-radix

- $\psi = \psi_{132}$
- Rader's trick for 11-NTT

$$
\begin{aligned}
R[x]/\langle x^{1320} - 1 \rangle &\overset{\texttt{11-NTT}}{\cong} \prod_{i=0}^{10} R[x]/\langle x^{120} - \psi^{12i} \rangle \\
&\overset{\texttt{12-NTT}}{\cong} \prod_{i=0}^{10} \prod_{j=0}^{11} R[x]/\langle x^{10} - \psi^{i+11j} \rangle
\end{aligned}
$$

$(p, q) = (857, 5167)$: 2D Good's Trick for $1728 = 64 \times 27$

- $y^{64} = z^{27} = 1$

$$
\begin{aligned}
R[x]/\langle x^{1728} - 1\rangle &\overset{x \mapsto yz}{\cong} \left(R[z]/\langle z^{27} - 1\rangle\right)[y]/\langle y^{64} - 1\rangle \\
&\overset{64\text{-}\mathtt{NTT}}{\cong} \prod_{i=0}^{63} \left(R[z]/\langle z^{27} - 1\rangle\right)[y]/\langle y - \psi_{64}^{i}\rangle \\
&\overset{9\text{-}\mathtt{NTT}}{\cong} \prod_{i=0}^{63}\prod_{j=0}^{8} \left(R[z]/\left\langle z^{3} - \psi_{9}^{j}\right\rangle\right)[y]/\langle y - \psi_{64}^{i}\rangle
\end{aligned}
$$

$(p, q) = (953, 6343)$: 3D Good's Trick for $1920 = 3 \times 128 \times 5$

- $z_0^3 = z_1^{128} = z_2^5 = 1$
- $\mathcal{R}_1 = R[z_2]/\langle z_2^5 - 1 \rangle$
- $\mathcal{R}_0 = \mathcal{R}_1[z_1]/\langle z_1^{128} - 1 \rangle$

$$
\begin{aligned}
R[x]/\langle x^{1920} - 1 \rangle & \overset{x \mapsto z_0 z_1 z_2}{\cong} \mathcal{R}_0[z_0]/\langle z_0^3 - 1 \rangle \\
& \overset{3\text{-NTT}}{\cong} \prod_{i=0}^{2} \left(\mathcal{R}_1[z_1]/\langle z_1^{128} - 1 \rangle \right) [z_0]/\langle z_0 - \psi_3^i \rangle \\
& \overset{128\text{-NTT}}{\cong} \prod_{i=0}^{2} \left(\prod_{j=0}^{127} \mathcal{R}_1[z_1]/\left\langle z_1 - \psi_{128}^j \right\rangle \right) [z_0]/\langle z_0 - \psi_3^i \rangle
\end{aligned}
$$

$(p, q) = (1013, 7177)$: 2048 NTT

- $\psi = \psi_{512}$

$$R[x]/\langle x^{2048} - 1 \rangle \overset{\texttt{512-NTT}}{\cong} \prod_{i=0}^{511} R[x]/\langle x^4 - \psi^i \rangle$$

$(p, q) = (1277, 7879)$: 2D Good's Trick for $2560 = 512 \times 5$

- $y^{512} = z^5 = 1$
- $\psi = \psi_{512}$

$$
\begin{aligned}
R[x]/\langle x^{2560} - 1 \rangle &\overset{x \mapsto yz}{\cong} \left(R[z]/\langle z^5 - 1 \rangle \right) [y]/\langle y^{512} - 1 \rangle \\
&\overset{\texttt{512-NTT}}{\cong} \prod_{i=0}^{511} \left(R[z]/\langle z^5 - 1 \rangle \right) [y]/\langle y - \psi^i \rangle
\end{aligned}
$$